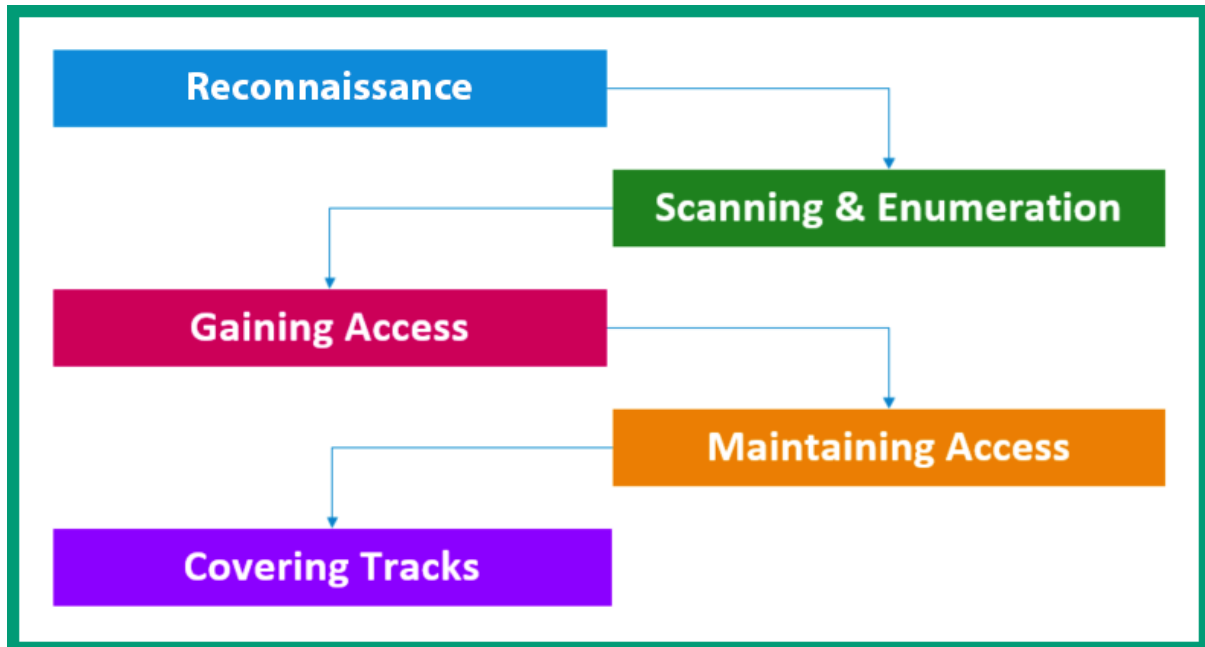


## Chapter 1: Fundamentals of Reconnaissance



<b>Anna Hansch</b> [Profile Picture]@linkedin.com 99%	Senior Customer Success Manager	Save as lead	1 source ^
<a href="http://wbv.de/openaccess/schlagwortverzeichnis/specialsearch/z/shop/detail/name/_/0...">http://wbv.de/openaccess/schlagwortverzeichnis/specialsearch/z/shop/detail/name/_/0...</a> May 02, 2022			
<b>Adam Debus</b> [Profile Picture]@linkedin.com 99%	Reliability Engineer	Save as lead	1 source ^
<a href="http://atc.usenix.org/conference/srecon22americas/presentation/debus">http://atc.usenix.org/conference/srecon22americas/presentation/debus</a> Feb 27, 2022			
<b>Kimberly Miller</b> [Profile Picture]@linkedin.com 99%		Save as lead	1 source ^
<a href="http://grimoiredujeu.com/linkedin-on-the-job-picture-2021">http://grimoiredujeu.com/linkedin-on-the-job-picture-2021</a> Feb 03, 2022			



Base Score

9.4  
(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)

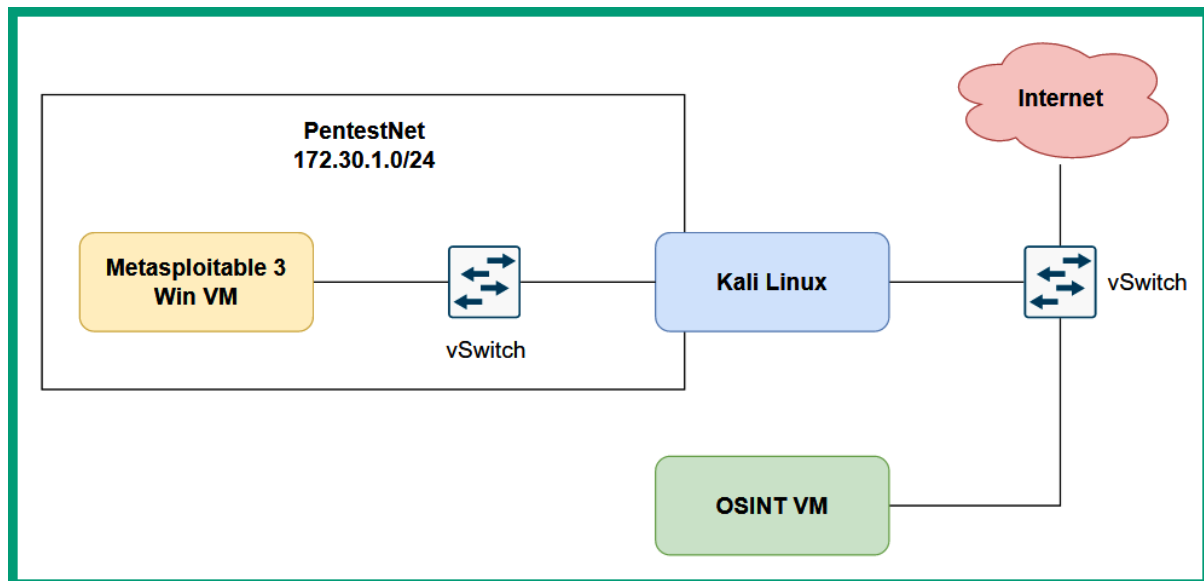
None (N)Low (L)High (H)

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

172.30.1.26				
8	7	17	4	72
CRITICAL	HIGH	MEDIUM	LOW	INFO
Vulnerabilities				Total: 108
SEVERITY	CVSS V3.0	PLUGIN	NAME	
CRITICAL	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	10.0	51988	Bind Shell Backdoor Detection	
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure	
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection	
CRITICAL	10.0	61708	VNC Server 'password' Password	
CRITICAL	10.0	10203	rexecd Service Detection	
HIGH	7.8	136808	ISC BIND Denial of Service	
HIGH	7.5	10205	rlogin Service Detection	



## Chapter 2: Setting Up a Reconnaissance Lab



The image shows a screenshot of the VirtualBox website. On the left is a navigation menu with links: [About](#), [Screenshots](#), [Downloads](#), [Documentation](#) (with sub-links for [End-user docs](#) and [Technical docs](#)), [Contribute](#), and [Community](#). The main heading is "VirtualBox" in large blue letters, followed by "Welcome to VirtualBox.org!". Below this is a paragraph of text describing VirtualBox as a powerful x86 and AMD64/Intel64 virtualization product. Another paragraph mentions the supported guest operating systems. At the bottom right, a blue button with white text "Download VirtualBox 7.0" is highlighted with a red border and a red arrow pointing to it from the left.



## VirtualBox binaries

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

If you're looking for the latest VirtualBox 6.1 packages, see [VirtualBox 6.1 builds](#).

### VirtualBox 7.0.4 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [Developer preview for macOS / Arm64 \(M1/M2\) hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

The binaries are released under the terms of the GPL version 3.

### VirtualBox 7.0.4 Oracle VM VirtualBox Extension Pack

- [All supported platforms](#)



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

```
Command Prompt
Microsoft Windows [Version 10.0.22621.1105]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox

C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=PentestNet --server-ip=172.30.1.1
--lower-ip=172.30.1.20 --upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable
```




**KALI**

☰

# Choose **your** Platform

LIGHT ☒ DARK




## Installer Images

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

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

💡 Recommended




## Virtual Machines

- ✓ Snapshots 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



## Prebuilt Virtual Machines


64-bit 32-bit



### VMware

2.6G torrent docs sum


💡 Recommended



### VirtualBox

2.6G torrent docs sum

💡 Recommended

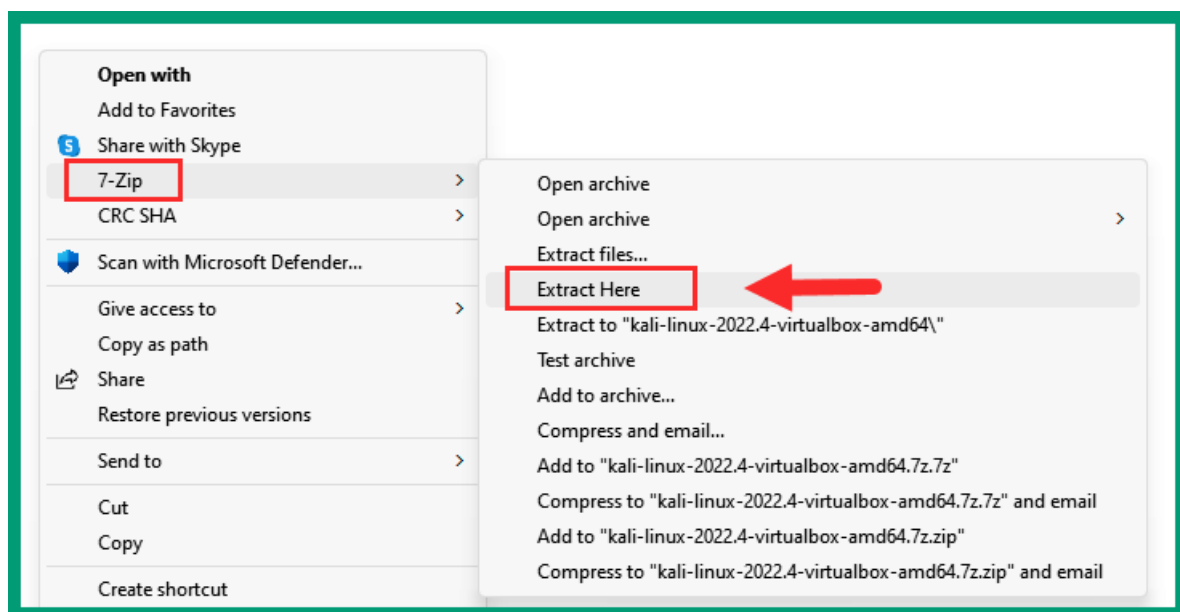
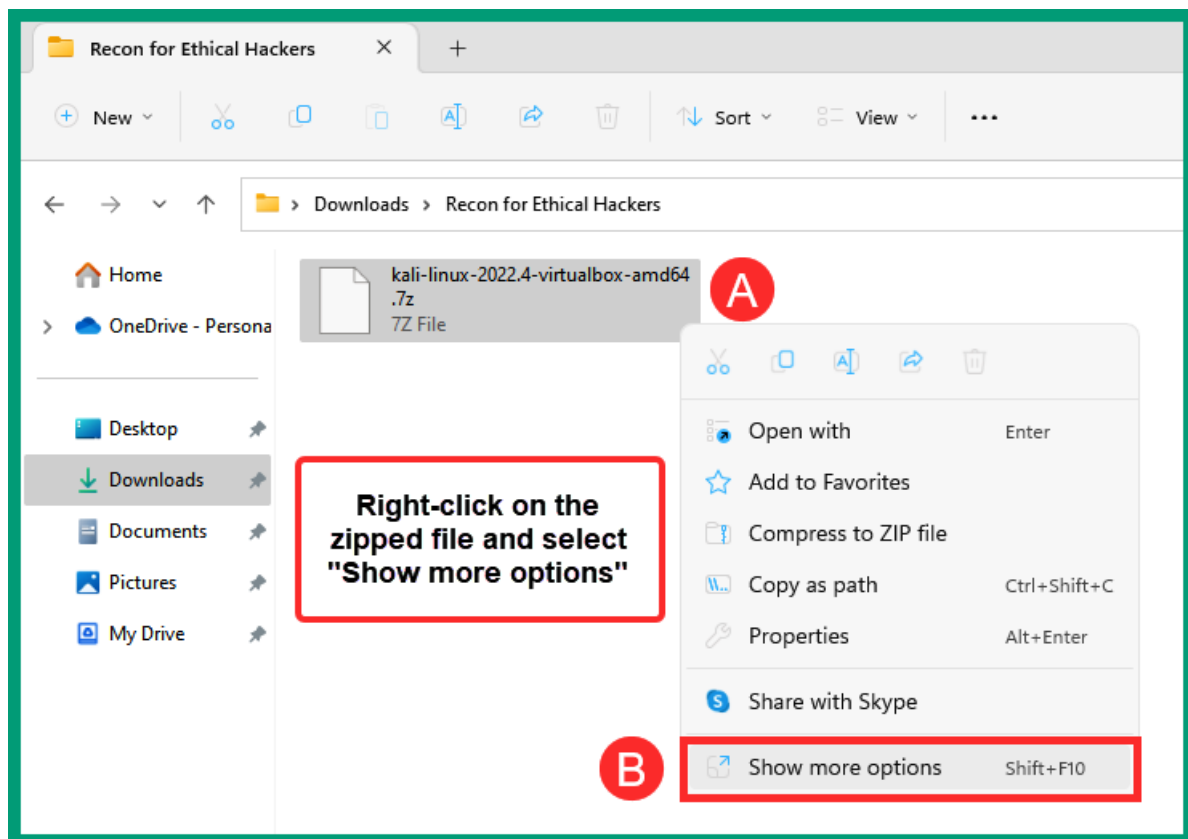


### QEMU

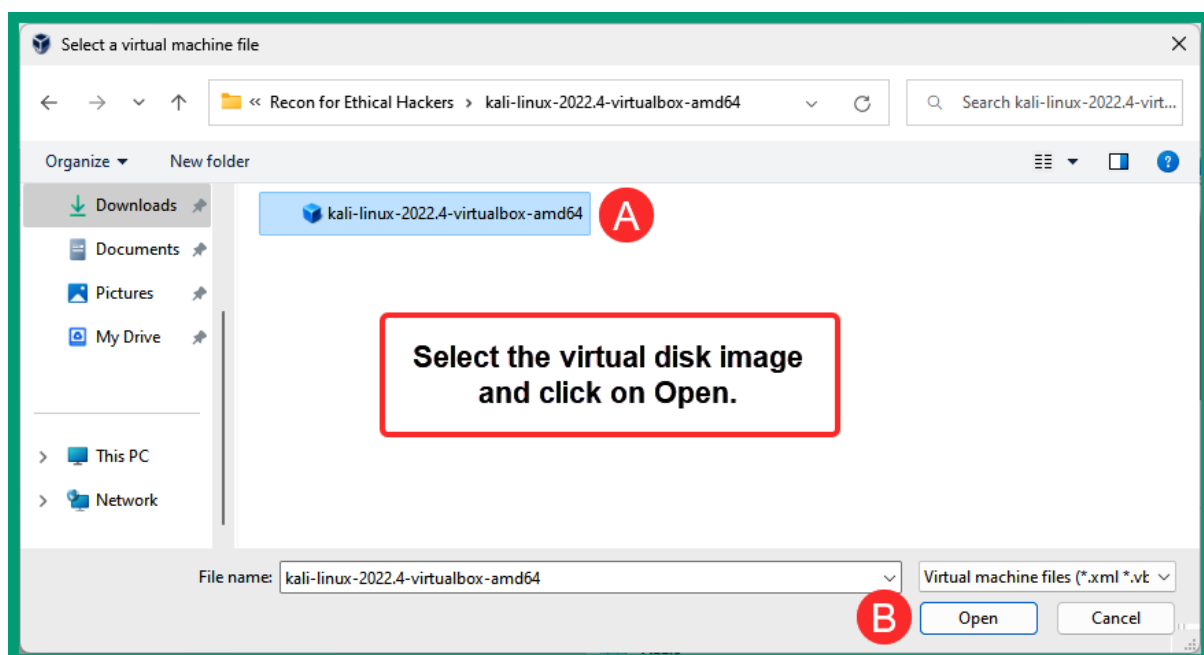
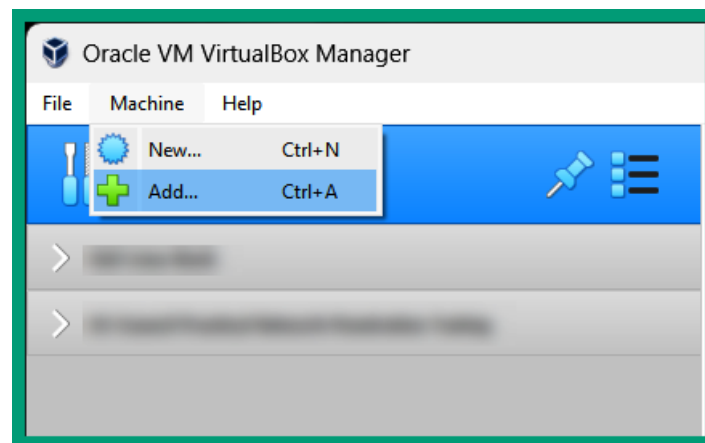
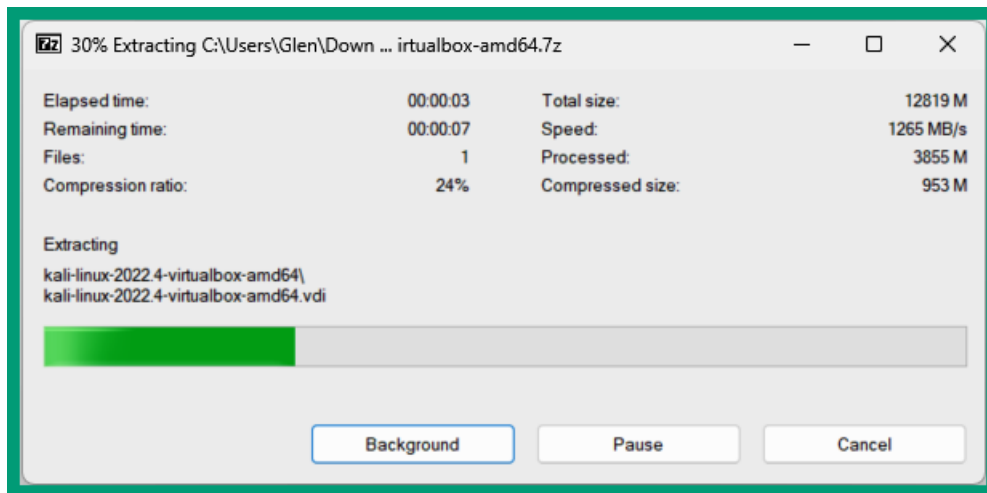
2.6G torrent docs sum

💡 Recommended

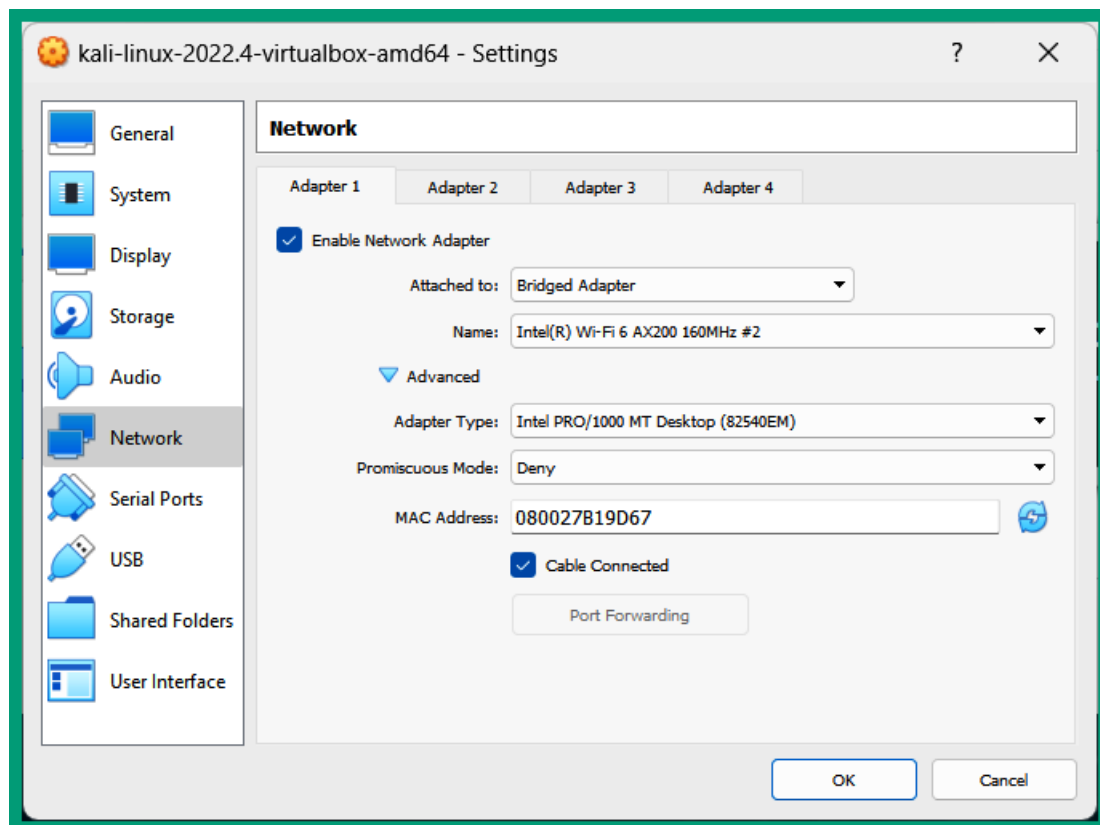
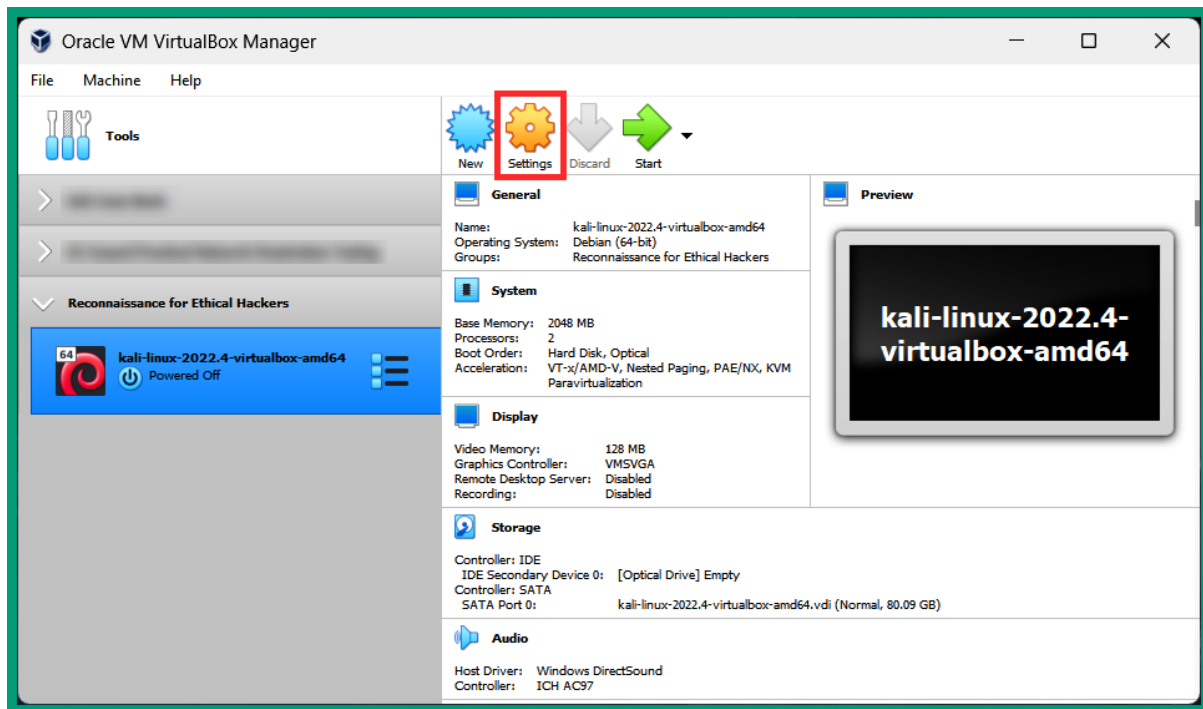




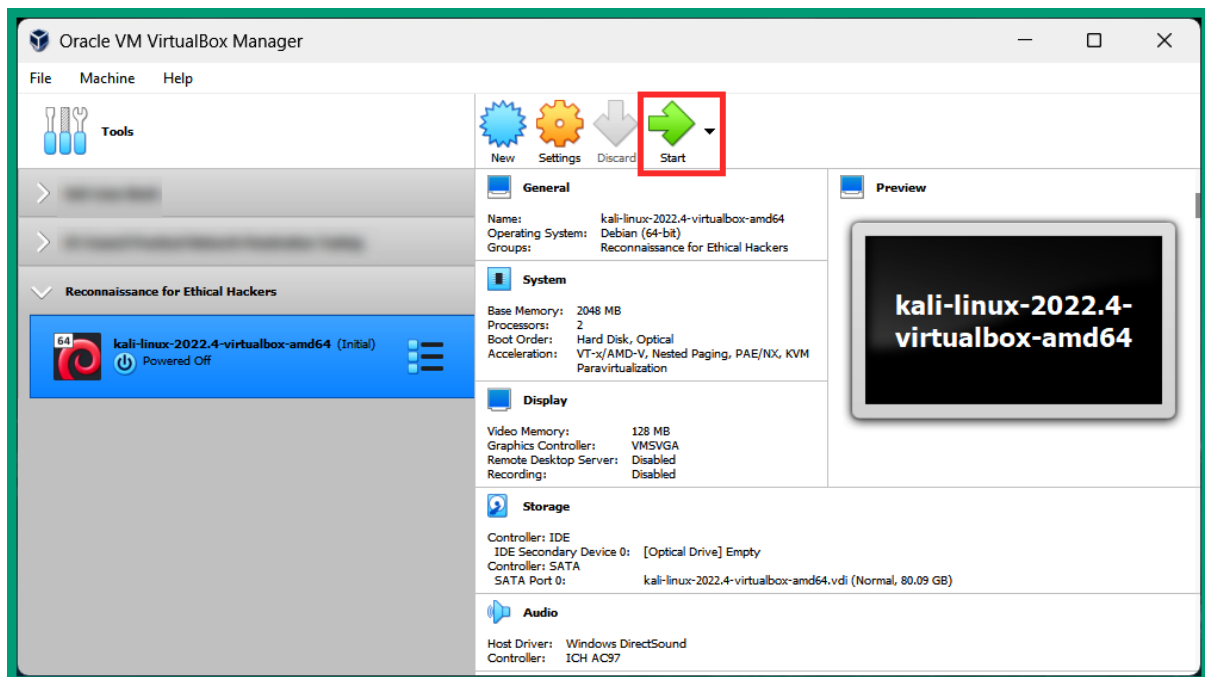
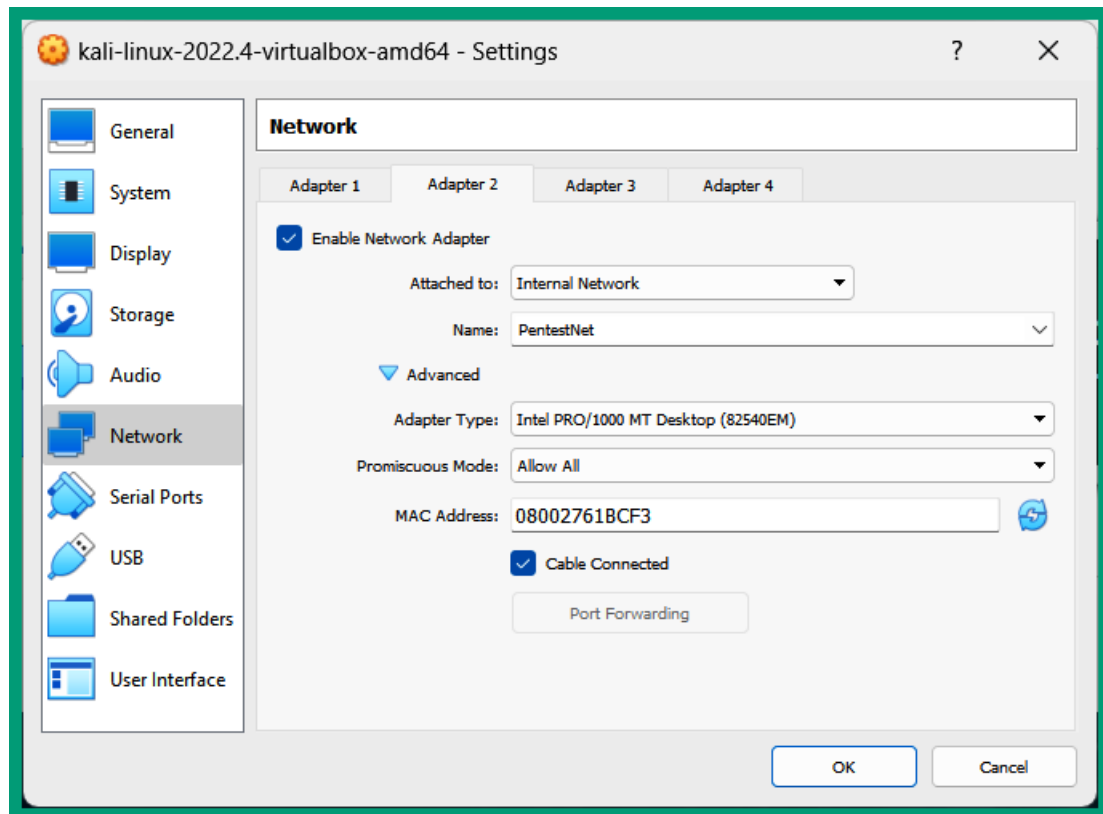




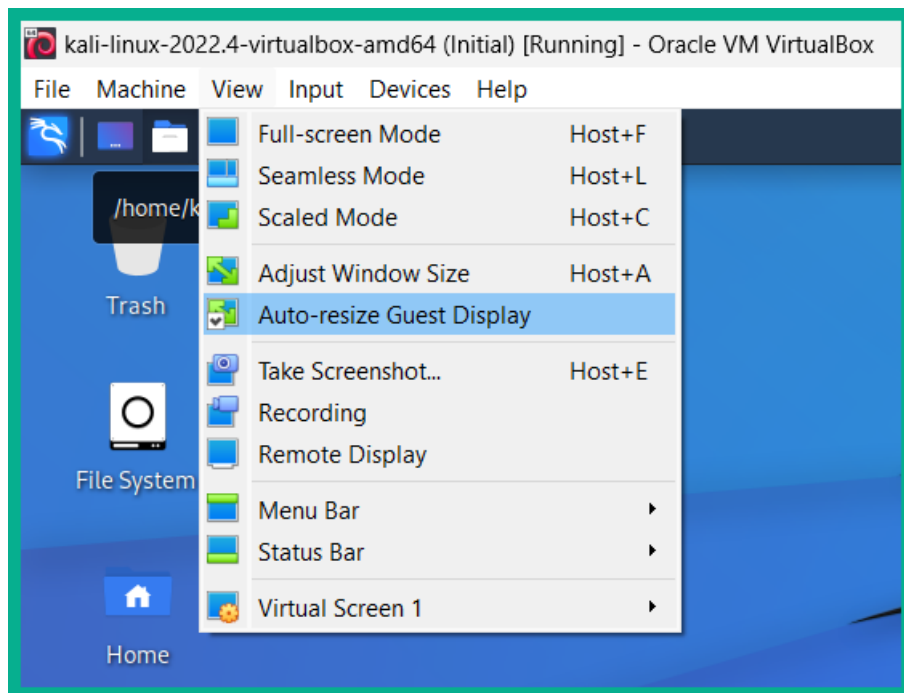
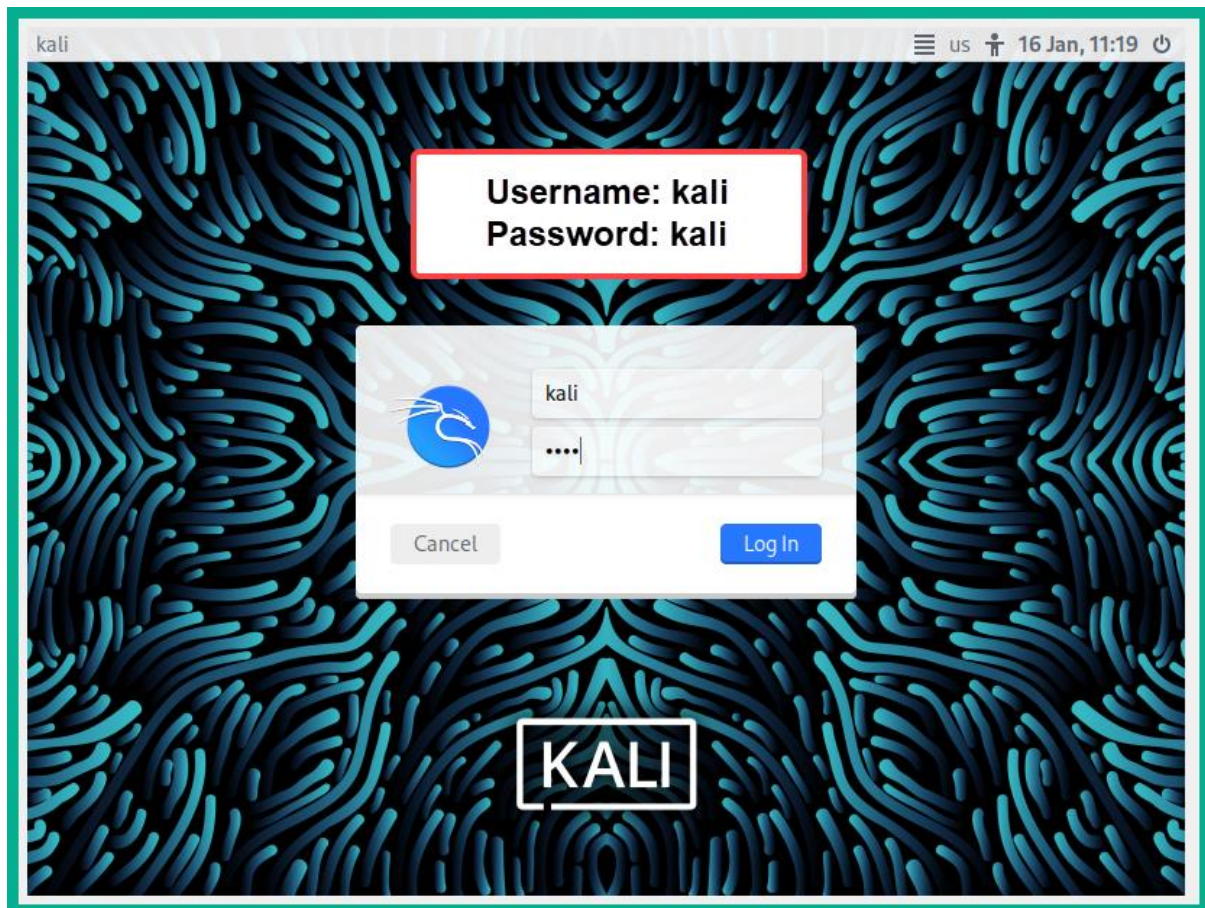




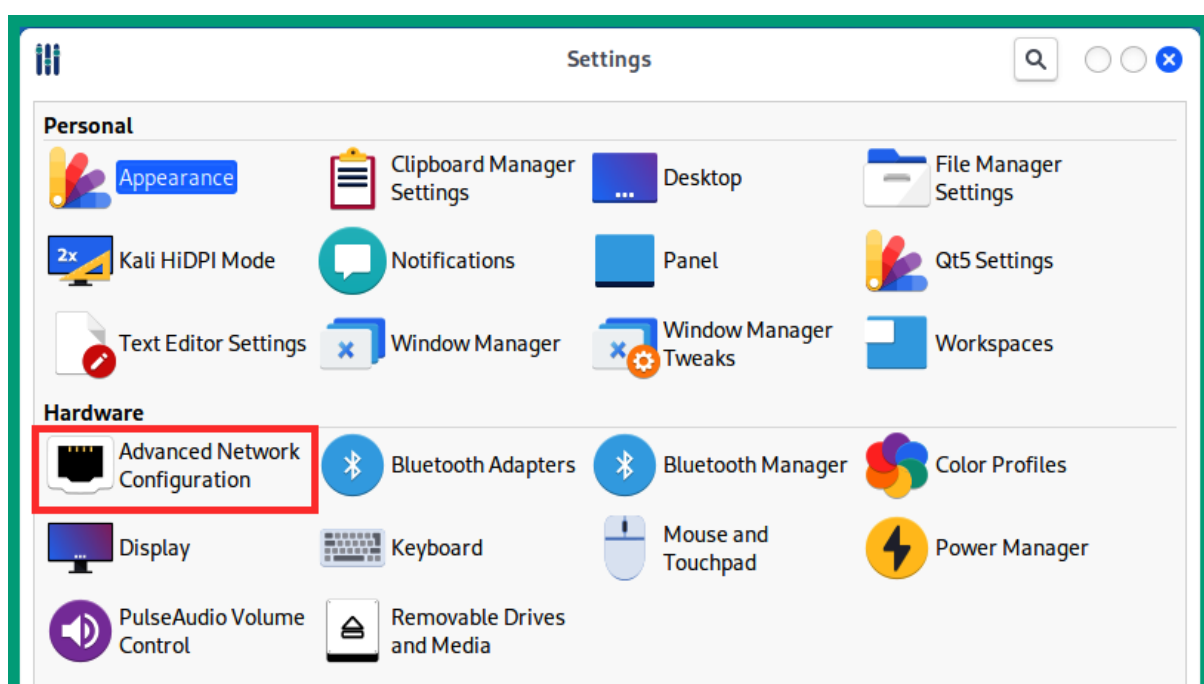
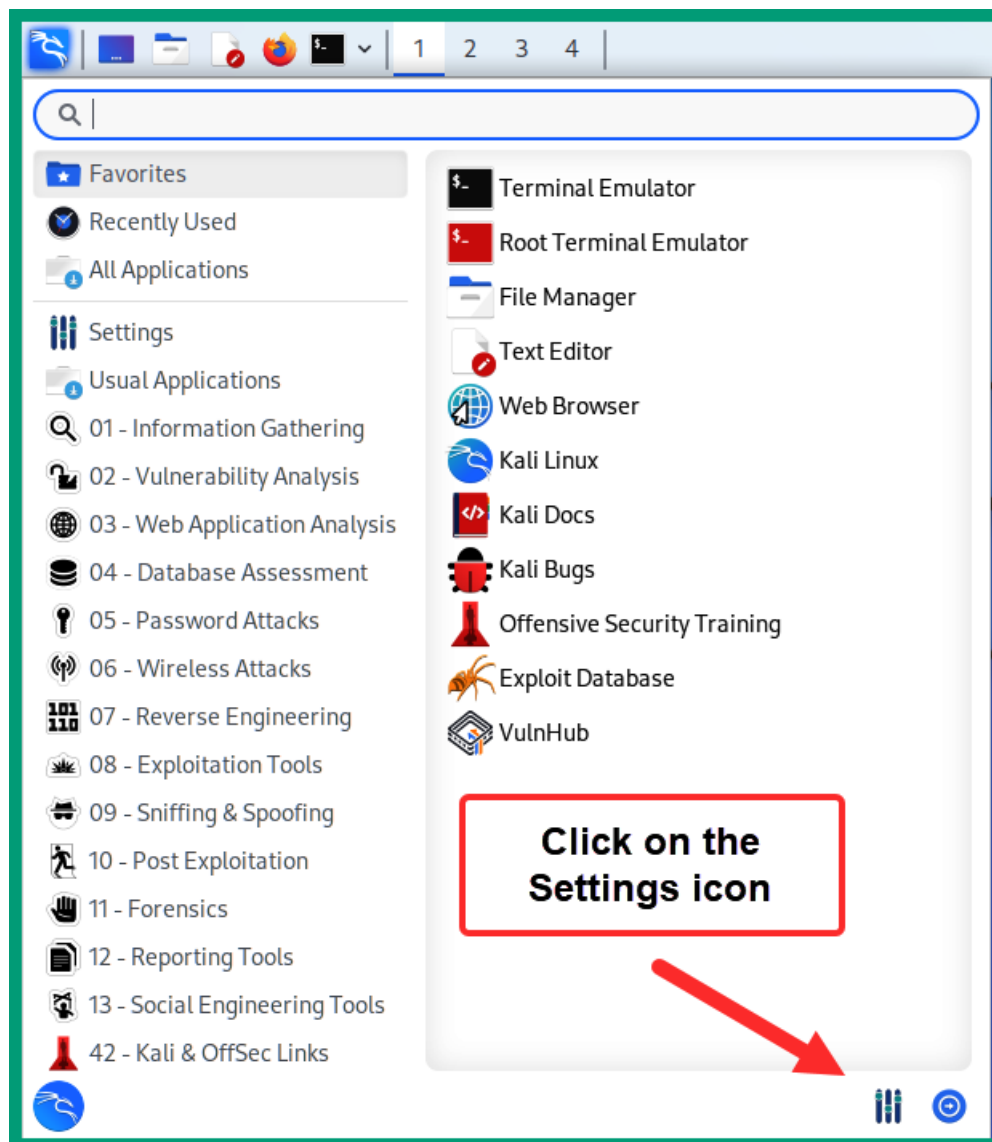




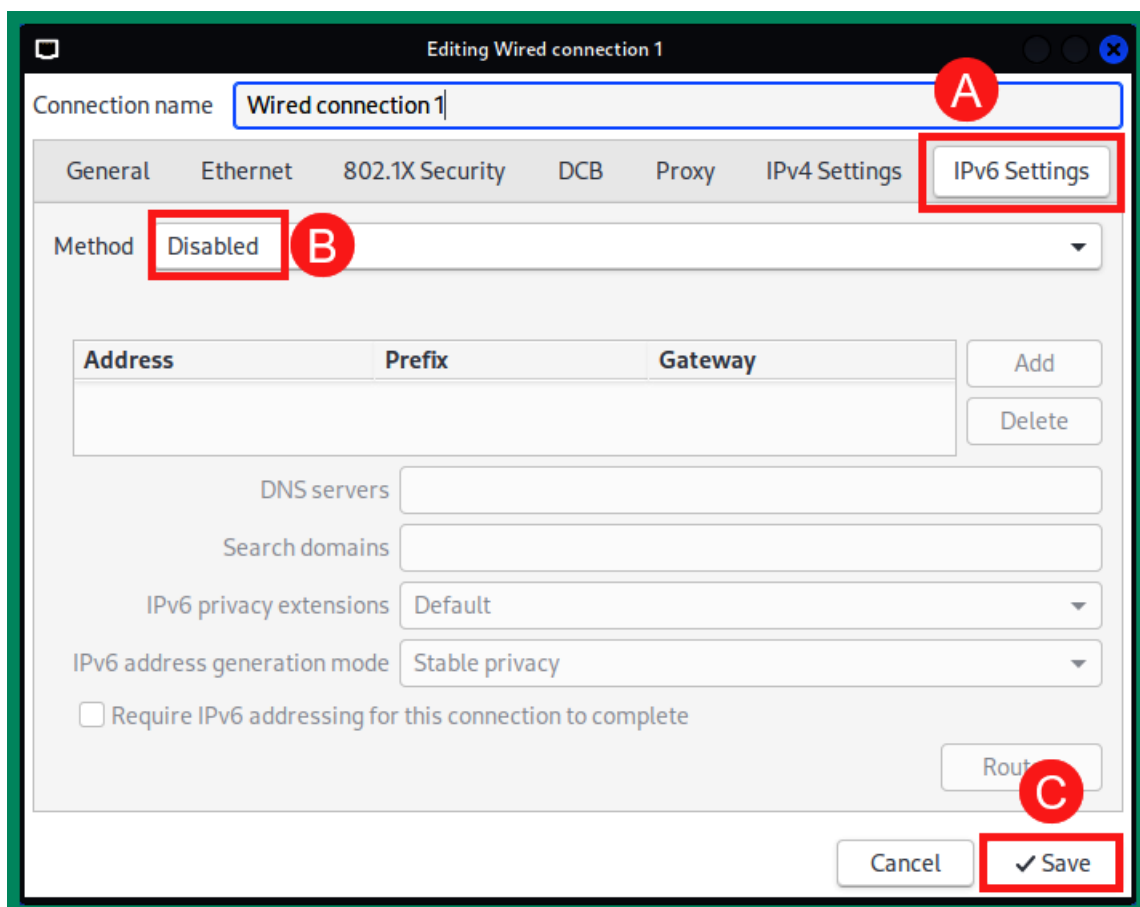
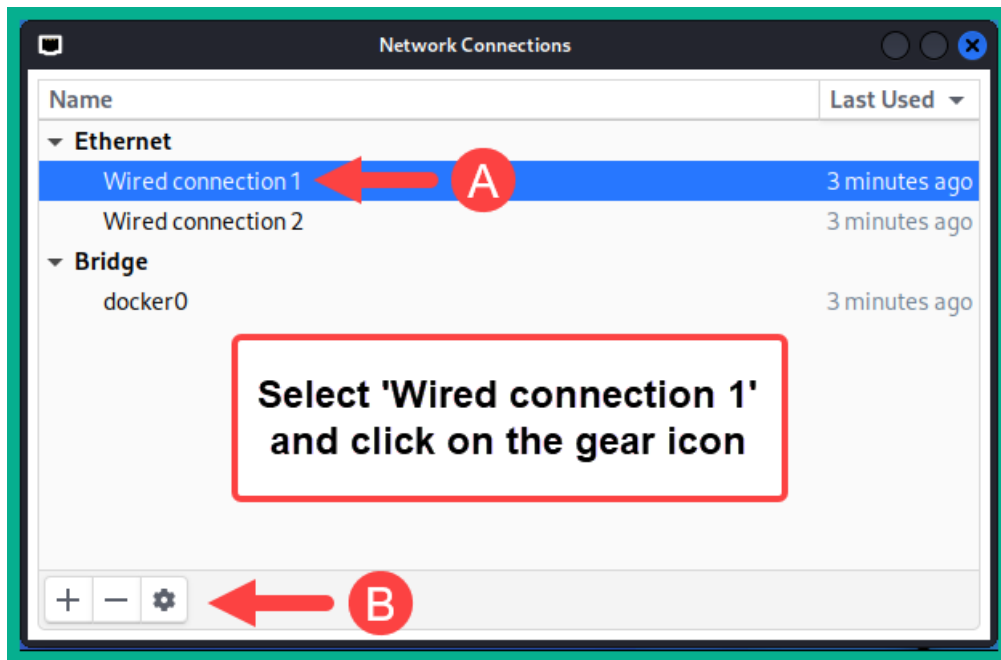




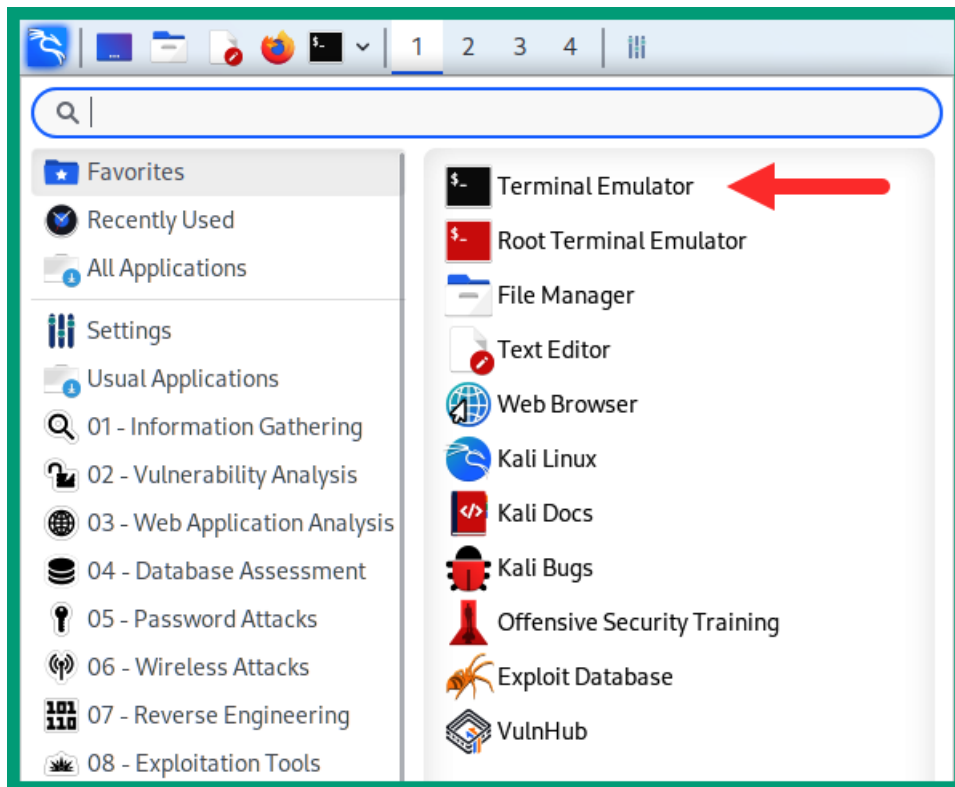












```
File Actions Edit View Help
kali@kali:~$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

```
File Actions Edit View Help
kali@kali:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
   inet 172.16.17.35/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86378sec preferred_lft 86378sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:61:bc:f3 brd ff:ff:ff:ff:ff:ff
   inet 172.30.1.42/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 579sec preferred_lft 579sec
```




```
File Actions Edit View Help

kali@kali:~$ ping www.google.com -c 4
PING forcesafesearch.google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=111 time=50.9 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=111 time=50.5 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=111 time=50.7 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=4 ttl=111 time=50.5 ms

— forcesafesearch.google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 50.463/50.654/50.922/0.183 ms
```

```
File Actions Edit View Help

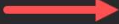
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [173 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [238 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [905 kB]
Fetched 64.8 MB in 10s (6,743 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1009 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

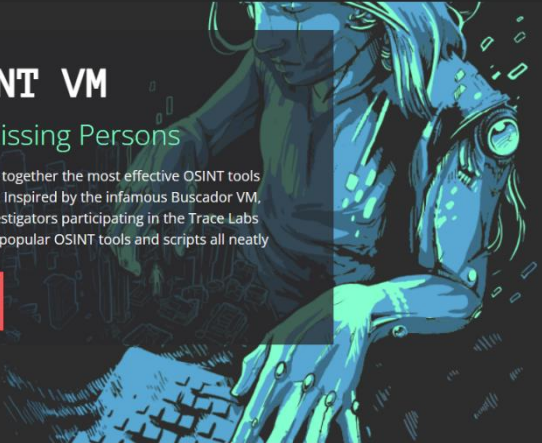
About ▾Initiatives ▾Supporters ▾Blog ▾ShopGet Involved

# Trace Labs OSINT VM

## Crowdsourced OSINT to Find Missing Persons

The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

[Download OVA](#)





## Downloads

To get started, download the OVA version of choice below and run it in your choice of VM software (ie. VMware Workstation, Virtualbox etc.). The default credentials to log in to the TL OSINT VM are **osint:osint**

VM Release	Size	Install Guide	SHA256 Hash
<a href="#">TL OSINT VM 2022.1 OVA (NA/EU Mirror)</a>	4.7 GB	<a href="#">Install Guide v2.1</a>	62c4a5e6bd8edf1d723f5d031c24163e6c90fcec73bd9228074942868ff7d8fb
<a href="#">TL OSINT VM 2022.1 AMD64 ISO (NA/EU Mirror)</a>	3.8 GB	<a href="#">Install Guide v2.1</a>	442852a5a8ffb4a3756347ac27f616ad7128457b41135d7e75623ce0450bd867
<a href="#">TL OSINT VM 2022.1 MAC M1 ISO</a>	3.5 GB	<a href="#">Install Guide v2.1</a>	32ea9357db1c741ed0d0957f1650d423ed3ebd2e981d41270a2746054fbe2af3

Oracle VM VirtualBox Manager

File Machine Help

Tools **A**

Preferences Import **B** Export New Add

### Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit [www.virtualbox.org](http://www.virtualbox.org) for more information and latest news.

Please choose a virtual appliance file to import

Downloads > Recon for Ethical Hackers

Organize New folder

Home OneDrive - Personal

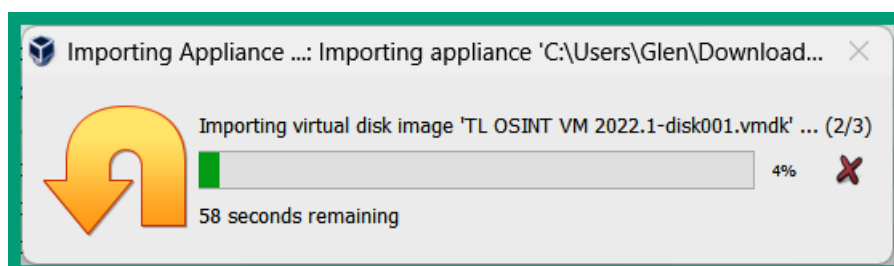
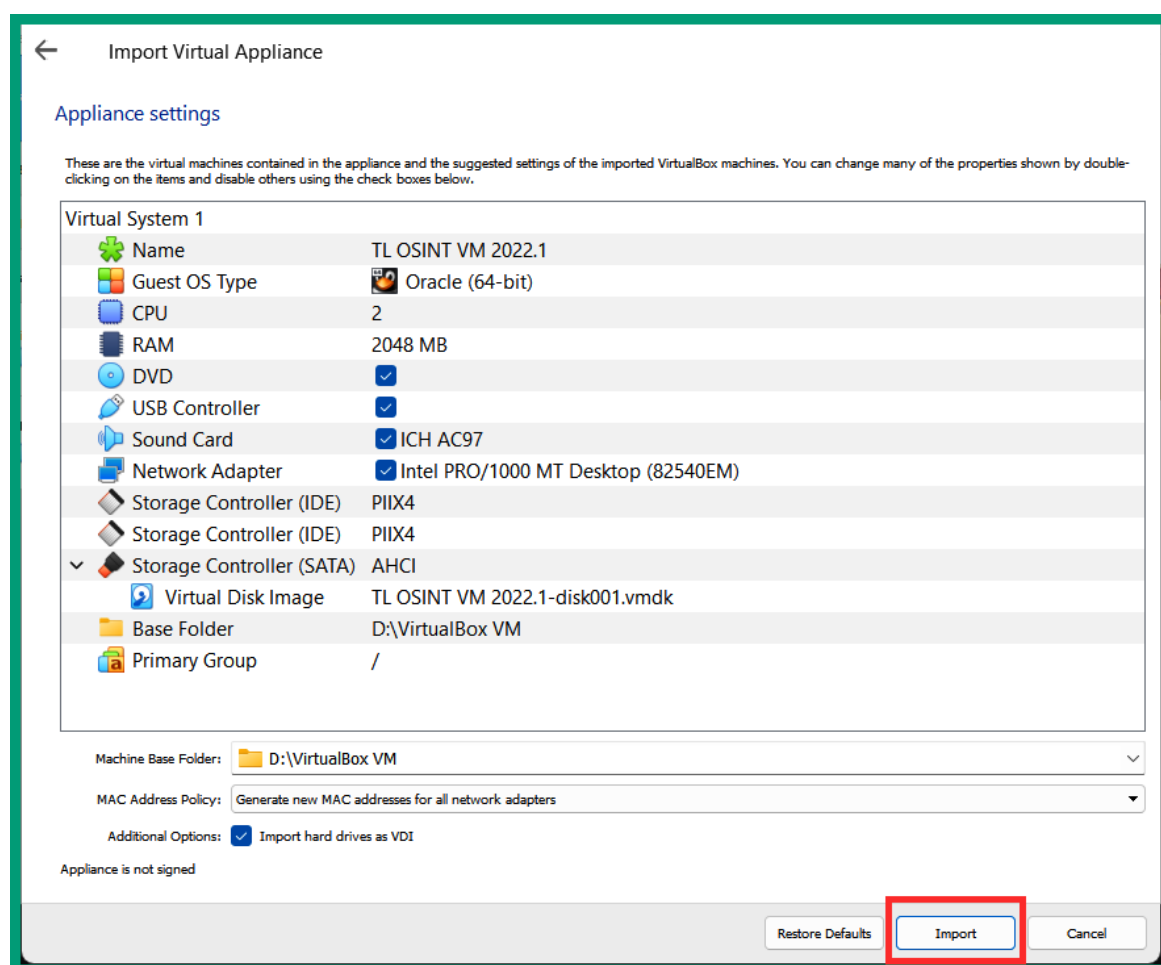
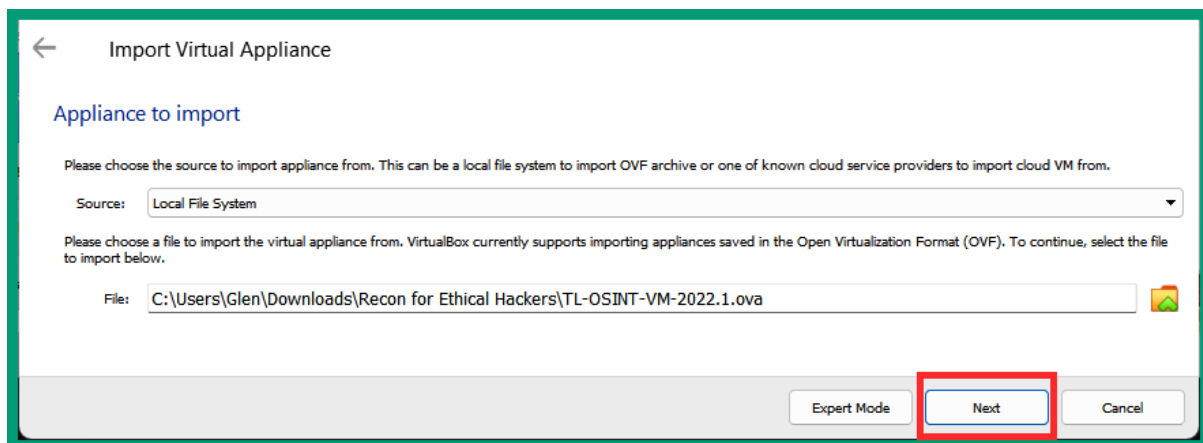
Desktop Downloads Documents Pictures My Drive

TL-OSINT-VM-2022.1 Open Virtualization Format Archive 4.74 GB **A**

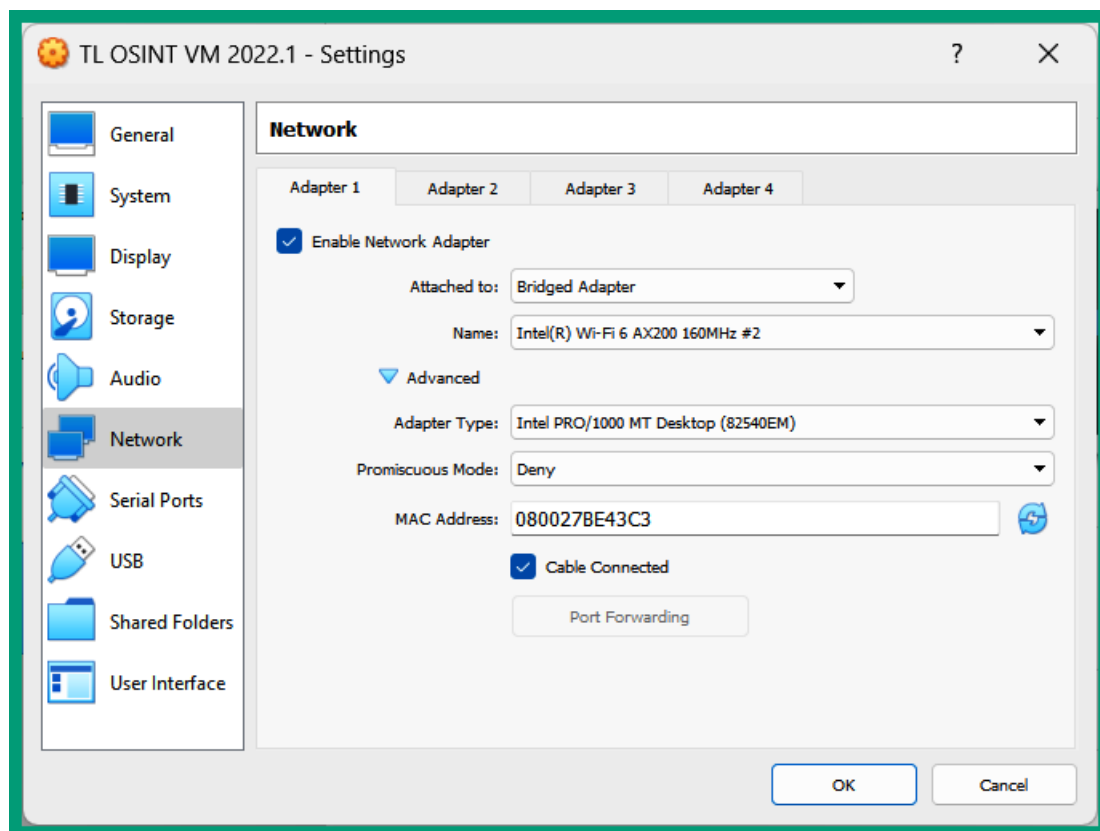
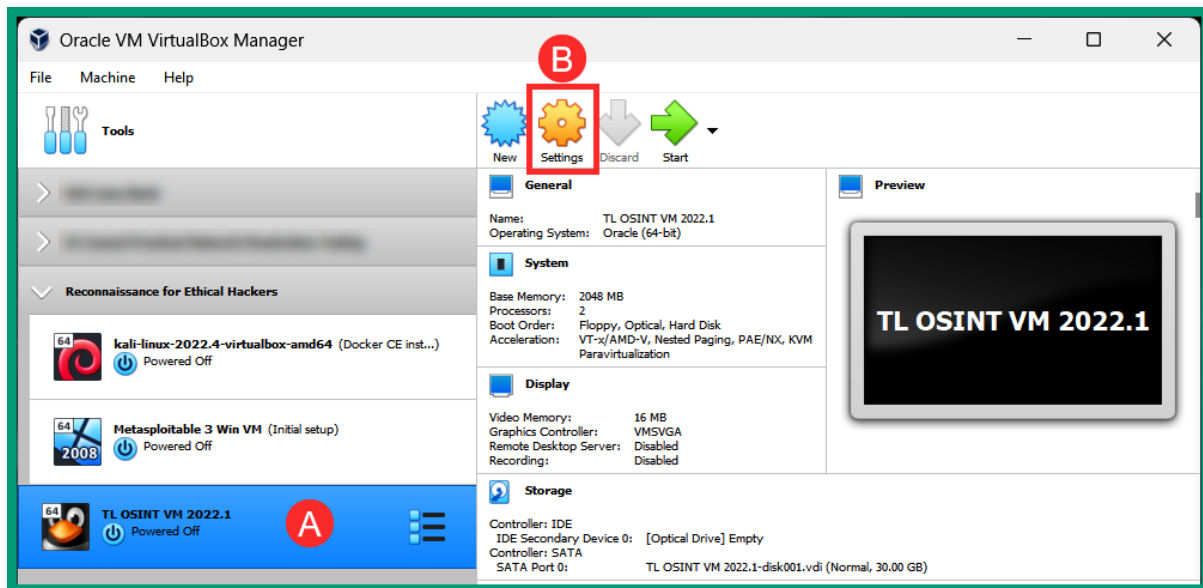
**Select the OVA file and click on Open**

File name: TL-OSINT-VM-2022.1 **B** Open Virtualization Format (\*.ova) Open Cancel

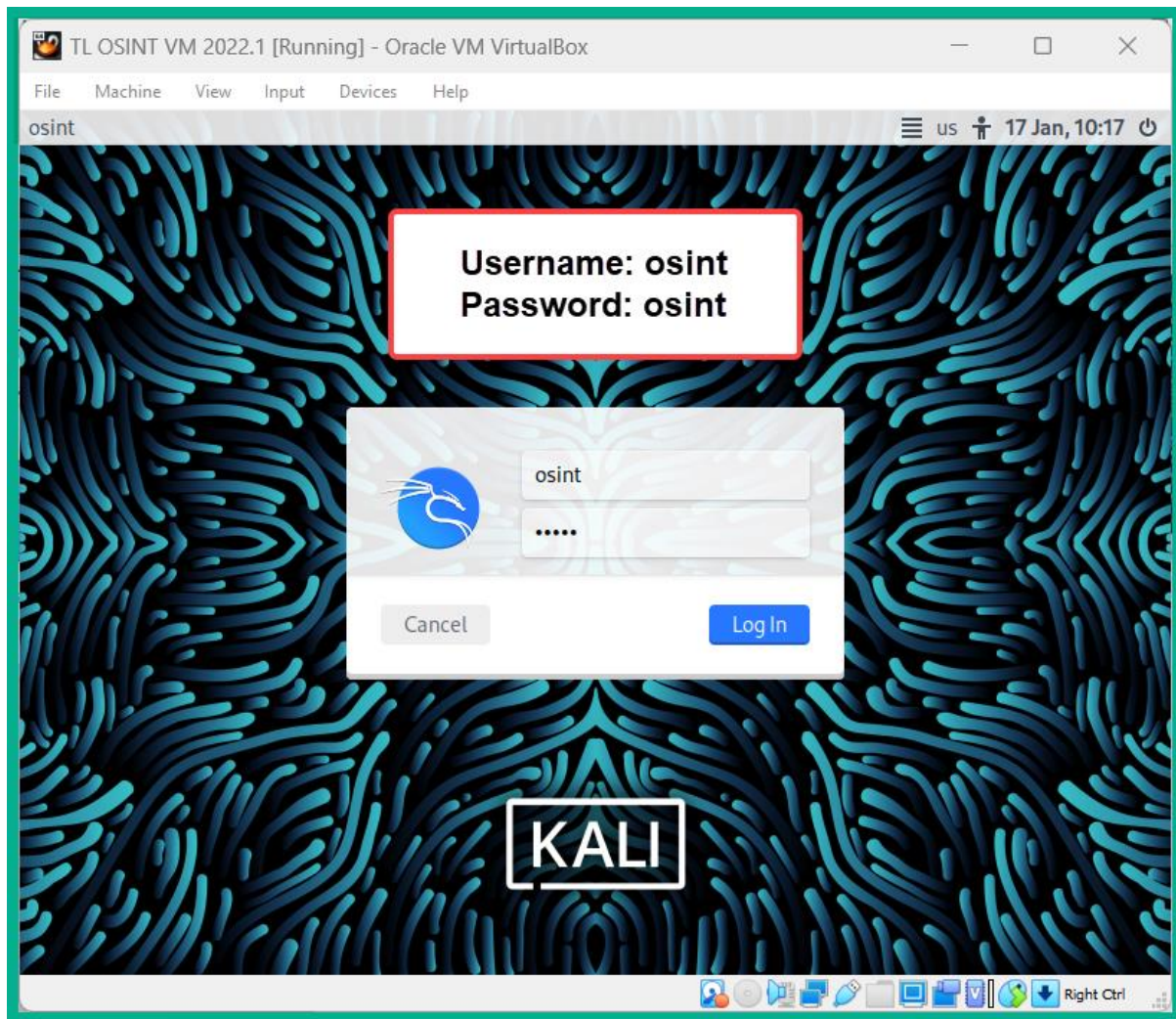












```
File Actions Edit View Help
osint@osint:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:be:43:c3 brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.44/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
        valid_lft 86311sec preferred_lft 86311sec

osint@osint:~$ ping www.google.com -c 4
PING forcesafesearch.google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=111 time=51.3 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=111 time=50.6 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=111 time=51.4 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=4 ttl=111 time=51.4 ms

— forcesafesearch.google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3602ms
rtt min/avg/max/mdev = 50.610/51.170/51.401/0.326 ms
```



```
File Actions Edit View Help

kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [173 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [238 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [905 kB]
Fetched 64.8 MB in 10s (6,622 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1009 packages can be upgraded. Run 'apt list --upgradable' to see them.

kali@kali:~$
```

```
File Actions Edit View Help

kali@kali:~$ printf '%s\n' "deb https://download.docker.com/linux/debian
bullseye stable" |
sudo tee /etc/apt/sources.list.d/docker-ce.list
deb https://download.docker.com/linux/debian bullseye stable

kali@kali:~$
```

```
File Actions Edit View Help

kali@kali:~$ curl -fsSL https://download.docker.com/linux/debian/gpg |
sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/docker-ce-archive-keyring.
gpg
kali@kali:~$ █
```

```
File Actions Edit View Help

kali@kali:~$ sudo apt update
Get:2 https://download.docker.com/linux/debian bullseye InRelease [43.3 k
B]
Get:3 https://download.docker.com/linux/debian bullseye/stable amd64 Pack
ages [16.6 kB]
Get:4 https://download.docker.com/linux/debian bullseye/stable amd64 Cont
ents (deb) [1,322 B]
Hit:1 http://kali.download/kali kali-rolling InRelease
Fetched 61.3 kB in 1s (66.4 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1009 packages can be upgraded. Run 'apt list --upgradable' to see them.
```



```
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
```

```
File Actions Edit View Help
kali@kali:~$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
fc251a6e7981: Pull complete
fda4ba87f6fb: Pull complete
a1f1879bb7de: Pull complete
a02cc7e9cd7d: Pull complete
67d517446f04: Pull complete
33382744245c: Pull complete
Digest: sha256:094ffc78021d744b048b80a92a2c7a4ccec70da1f35b99bc00701edf96
c698b8
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

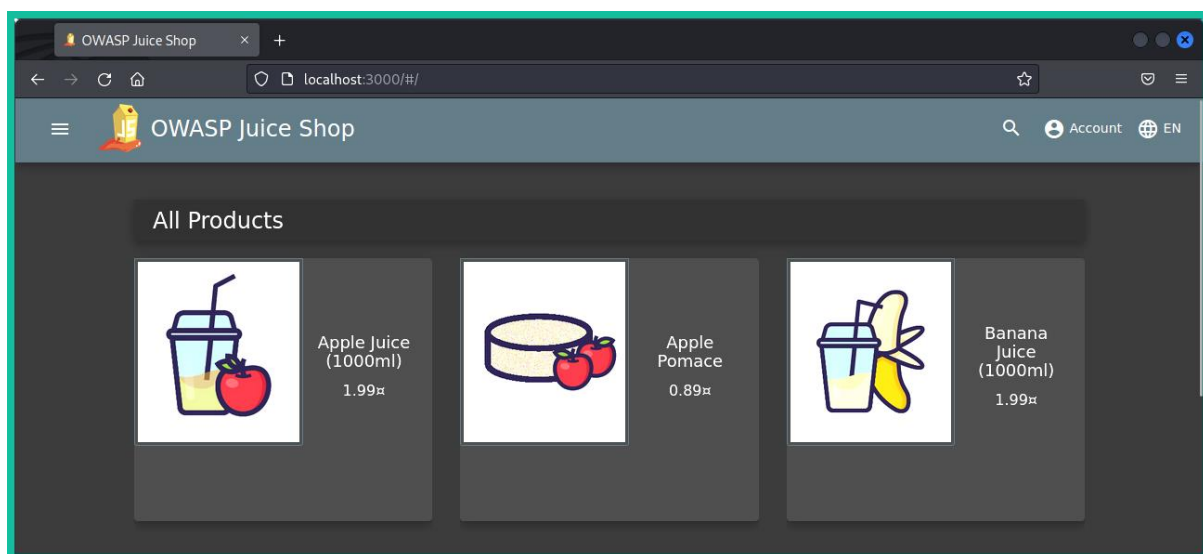
kali@kali:~$
```

The download may take a few minutes to complete



```
File Actions Edit View Help

kali@kali:~$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v18.12.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```







# Install Vagrant

Install or update to v2.3.3 of Vagrant to get started.

## Operating System A

macOS

**Windows**

Linux

B

**2.3.3**



## Binary download for Windows

AMD64

Version: 2.3.3

C

**Download**

I686

Version: 2.3.3

Download

```
C:\Users\Glen> vagrant plugin install vagrant-reload
==> vagrant: A new version of Vagrant is available: 2.3.4 (installed version: 2.3.3)!
==> vagrant: To upgrade visit: https://www.vagrantup.com/downloads.html
```

```
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Installed the plugin 'vagrant-reload (0.0.1)'!
```

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

```
C:\Users\Glen>
```

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

- 1) virtualbox
- 2) vmware
- 3) vmware\_desktop

**Choose 1 and hit Enter**

```
Enter your choice: 1
```



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

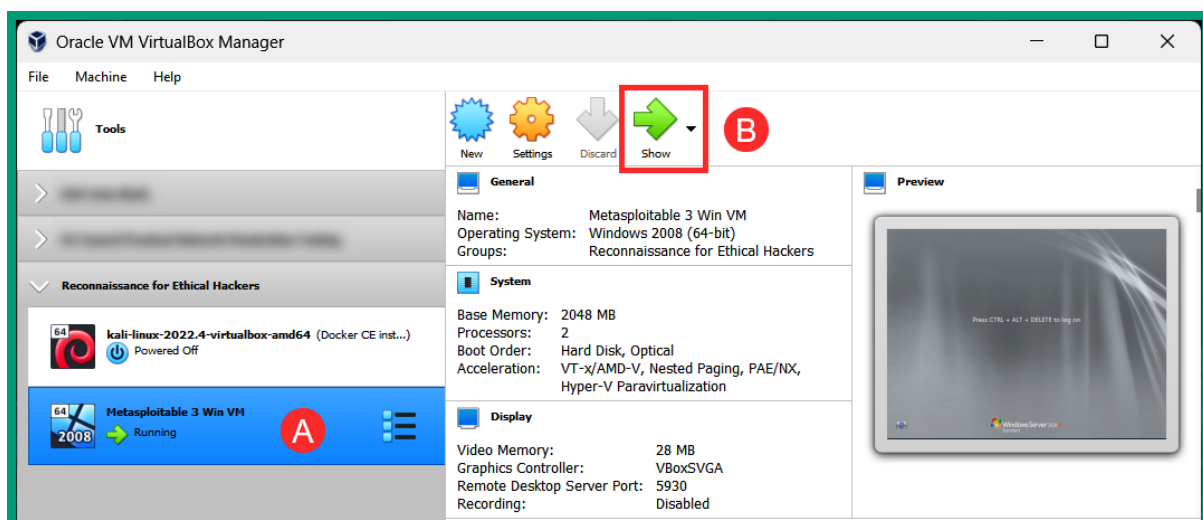
1) virtualbox
2) vmware
3) vmware_desktop

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

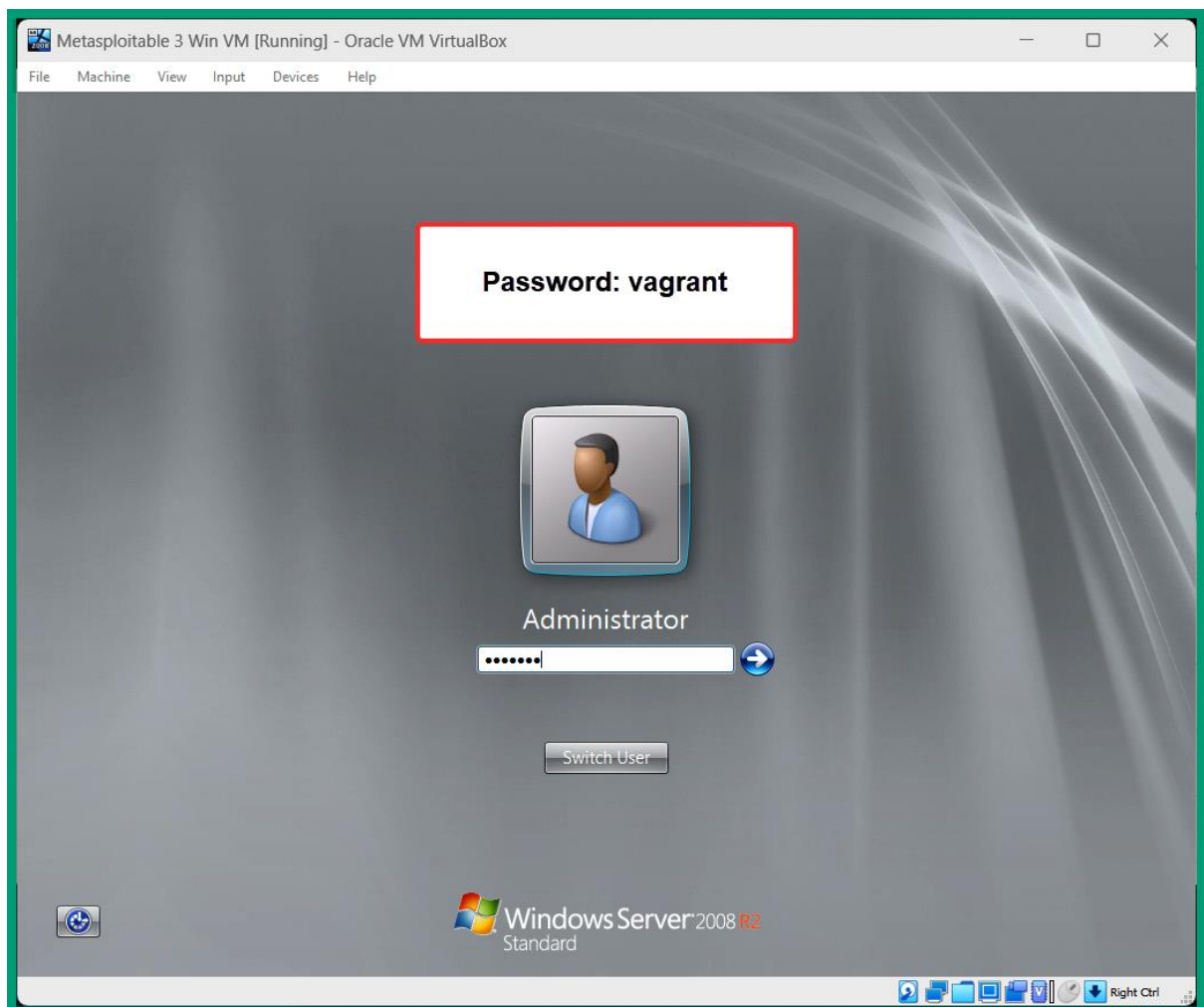
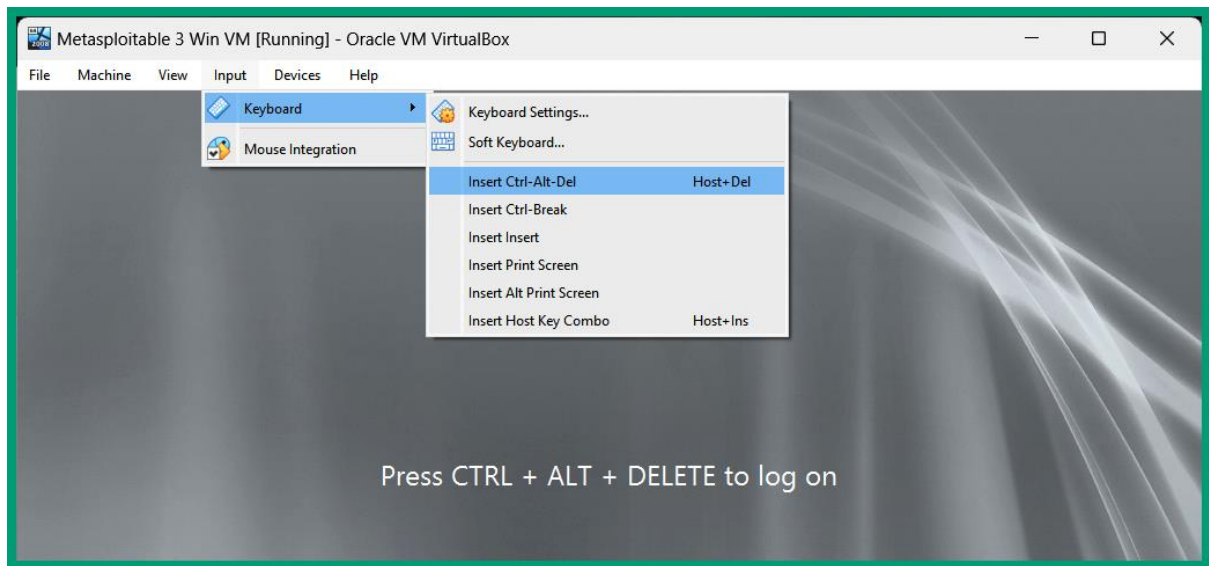
C:\Users\Glen>
```

The download process  
usually takes a few minutes

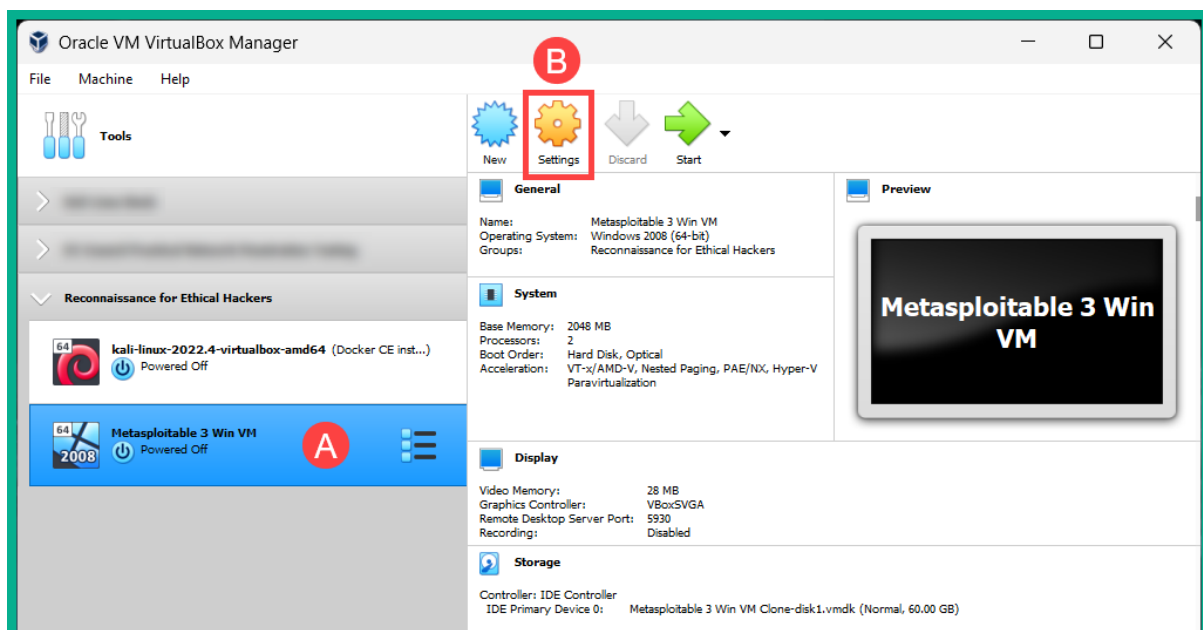
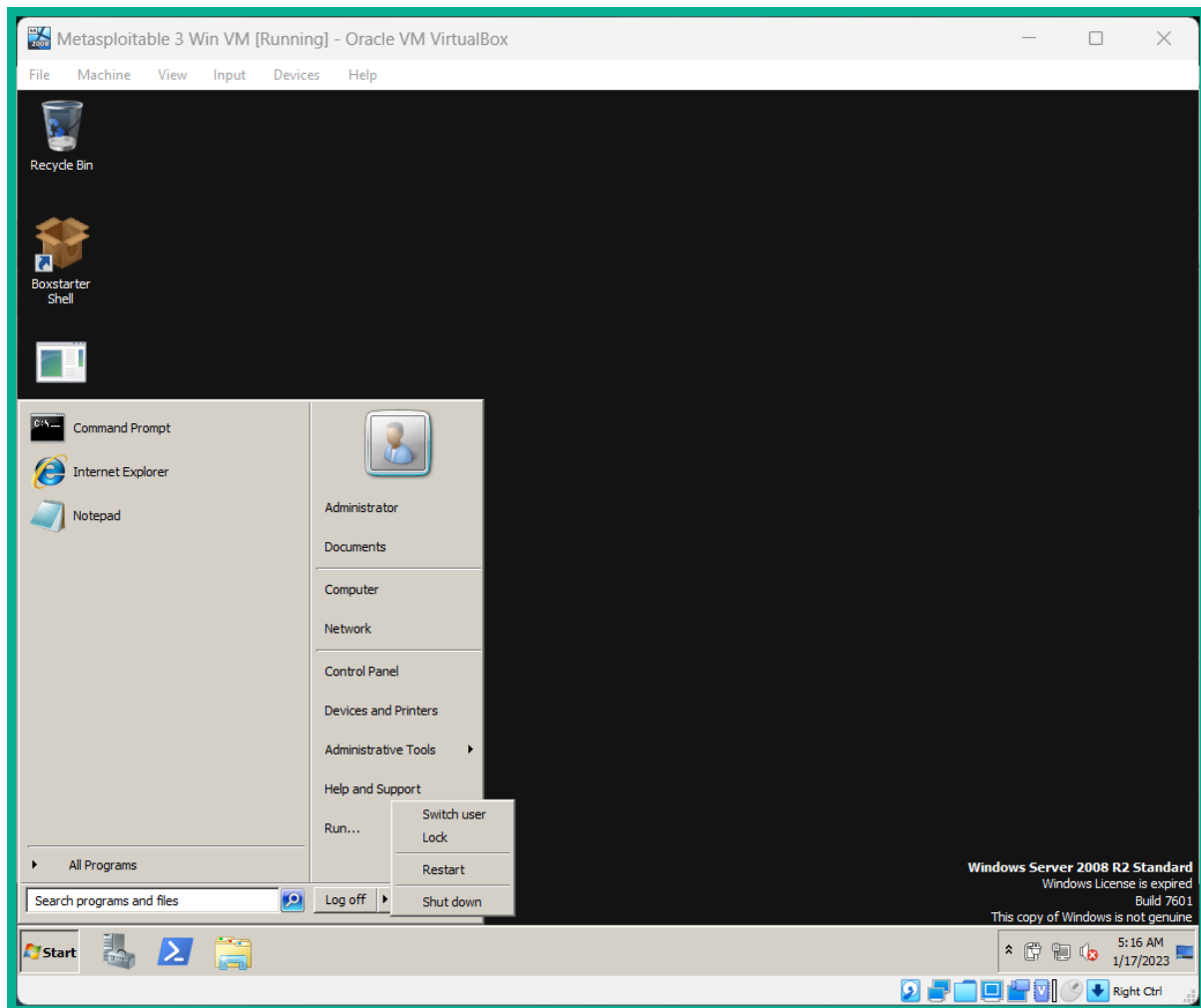
```
C:\Users\Glen\> vagrant up
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Checking if box 'metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> default: Clearing any previously set forwarded ports...
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
      default: Adapter 1: nat
==> default: Forwarding ports...
      default: 3389 (guest) => 3389 (host) (adapter 1)
      default: 22 (guest) => 2222 (host) (adapter 1)
      default: 5985 (guest) => 55985 (host) (adapter 1)
      default: 5986 (guest) => 55986 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
==> default: Booting VM...
==> default: Waiting for machine to boot. This may take a few minutes...
      default: WinRM address: 127.0.0.1:55985
      default: WinRM username: vagrant
      default: WinRM execution_time_limit: PT2H
      default: WinRM transport: negotiate
==> default: Machine booted and ready!
[default] GuestAdditions versions on your host (6.1.40) and guest (6.0.8) do not match.
Copy iso file C:\Program Files\Oracle\VirtualBox\VBBoxGuestAdditions.iso into the box $env:TEMP\VBBoxGuestAdditions.iso
The term 'Mount-DiskImage' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Mount-DiskImage -ImagePath $env:TEMP\VBBoxGuestAdditions.iso
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Mount-DiskImage:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```



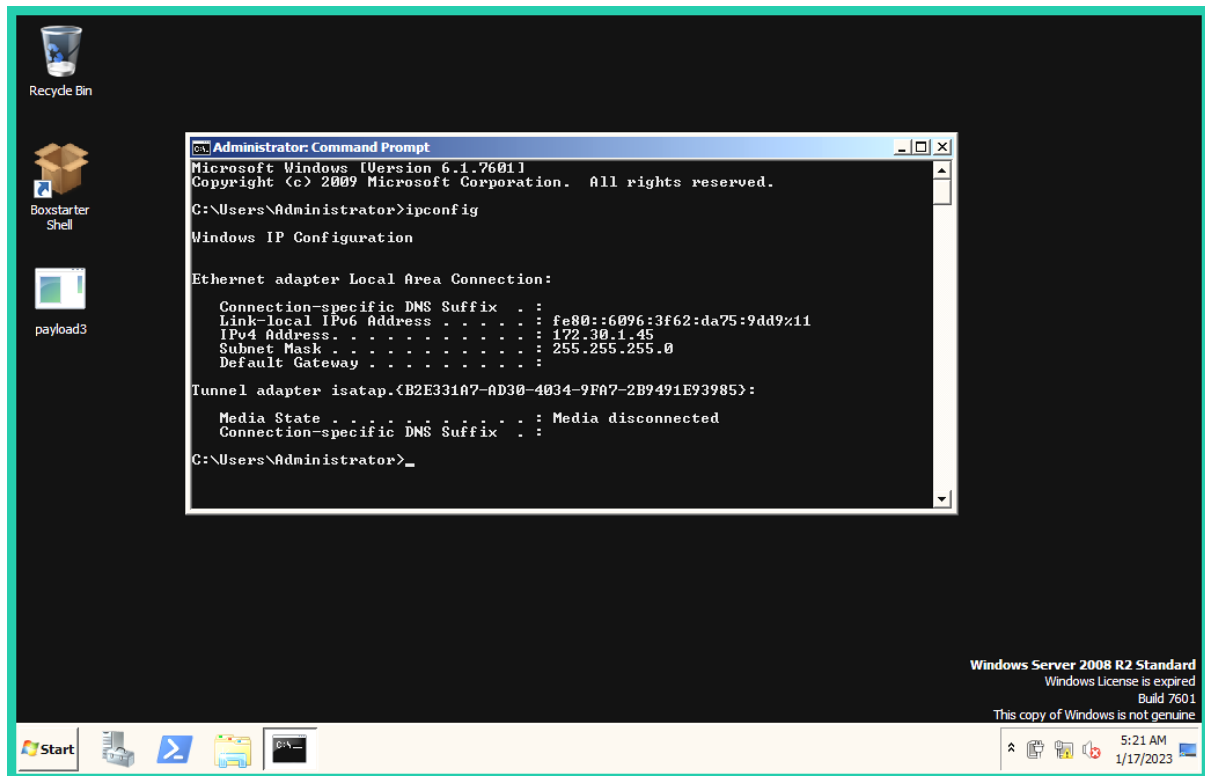
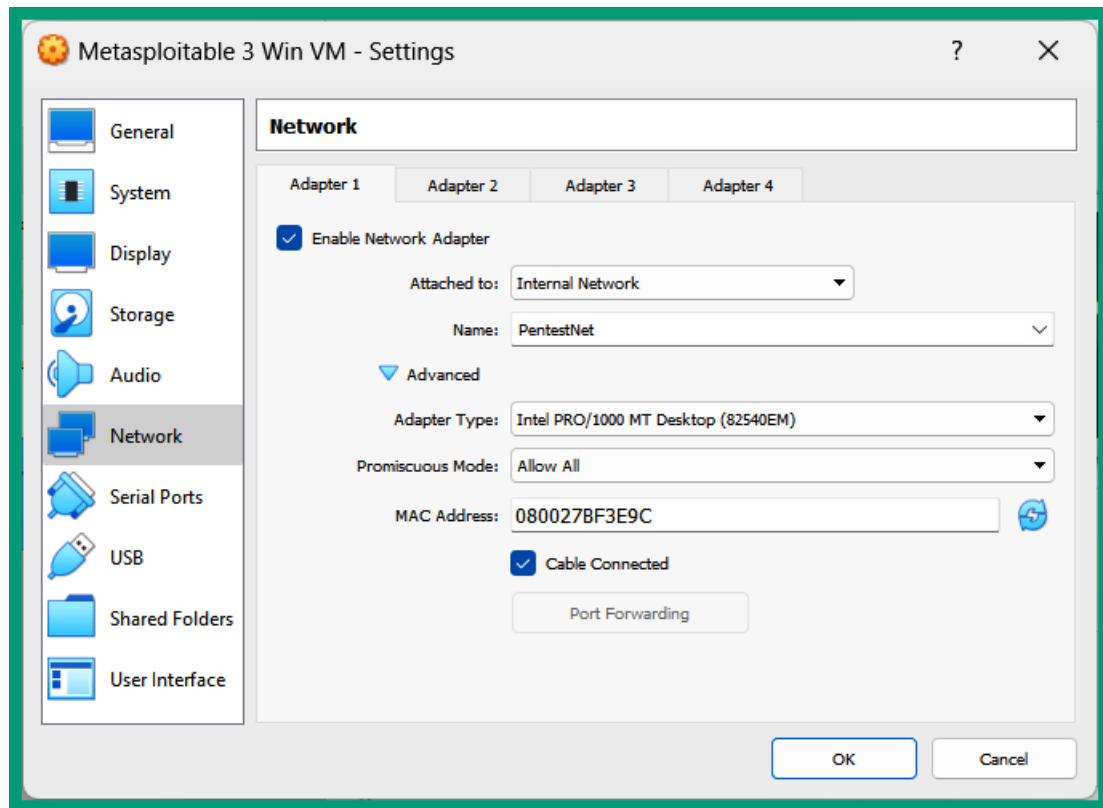






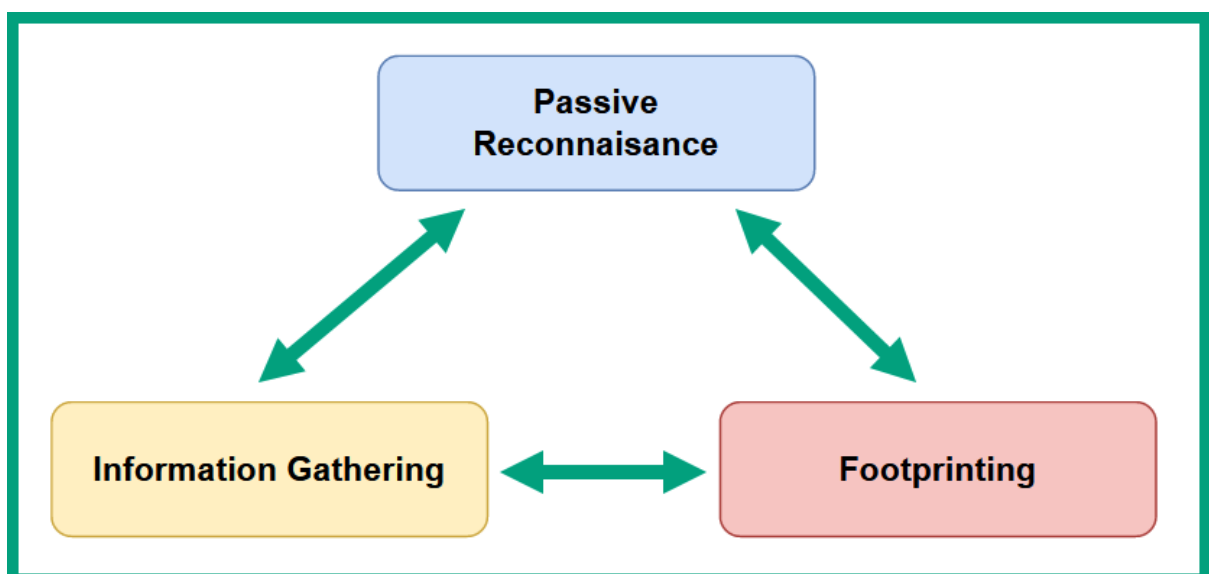
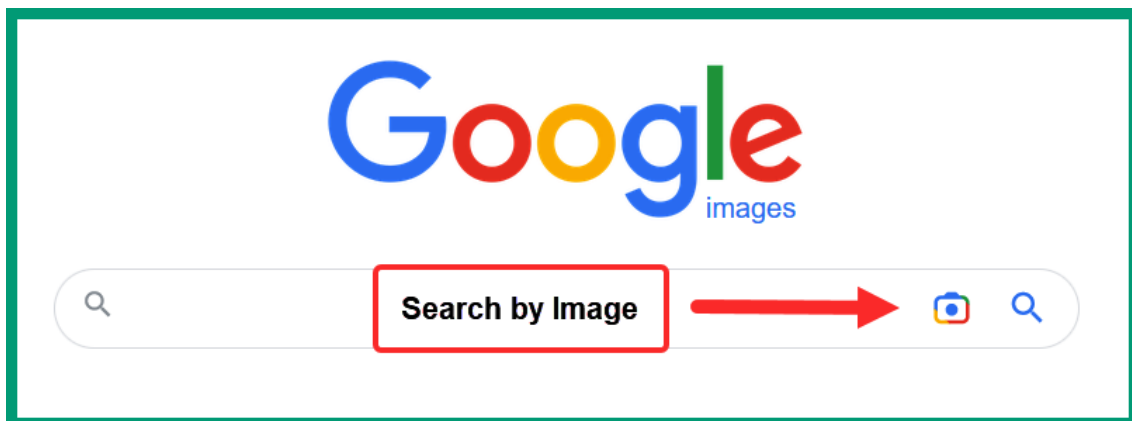
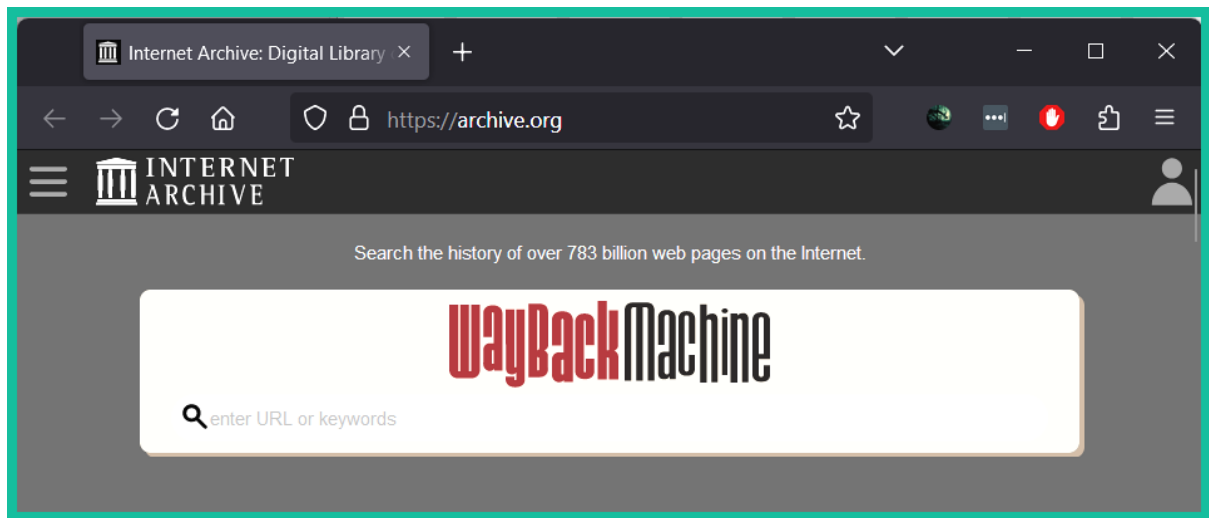




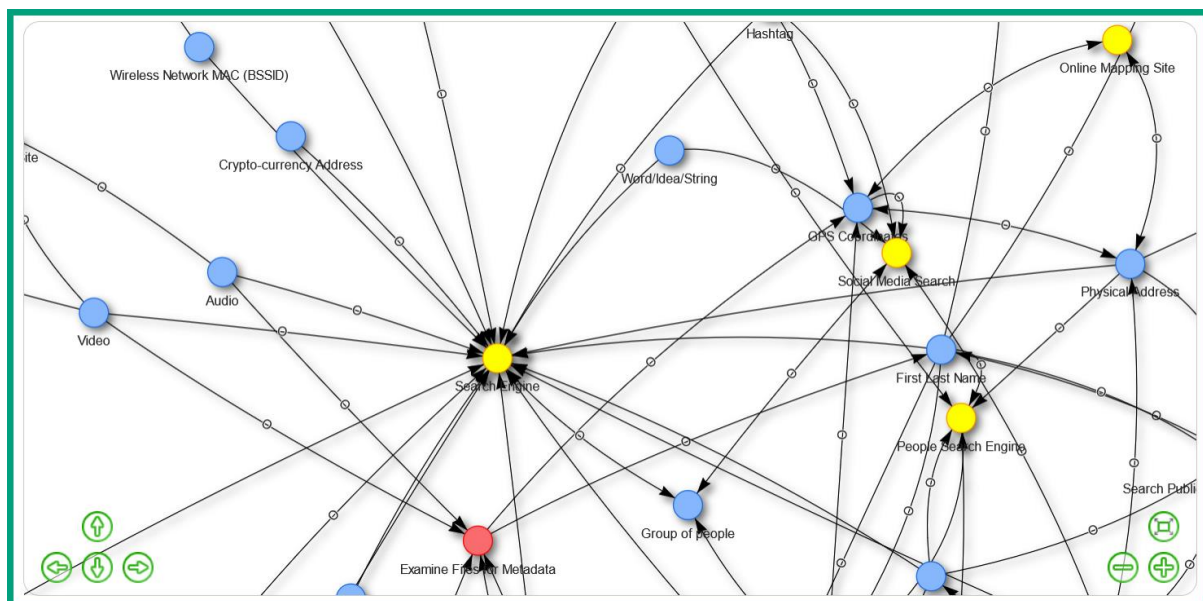
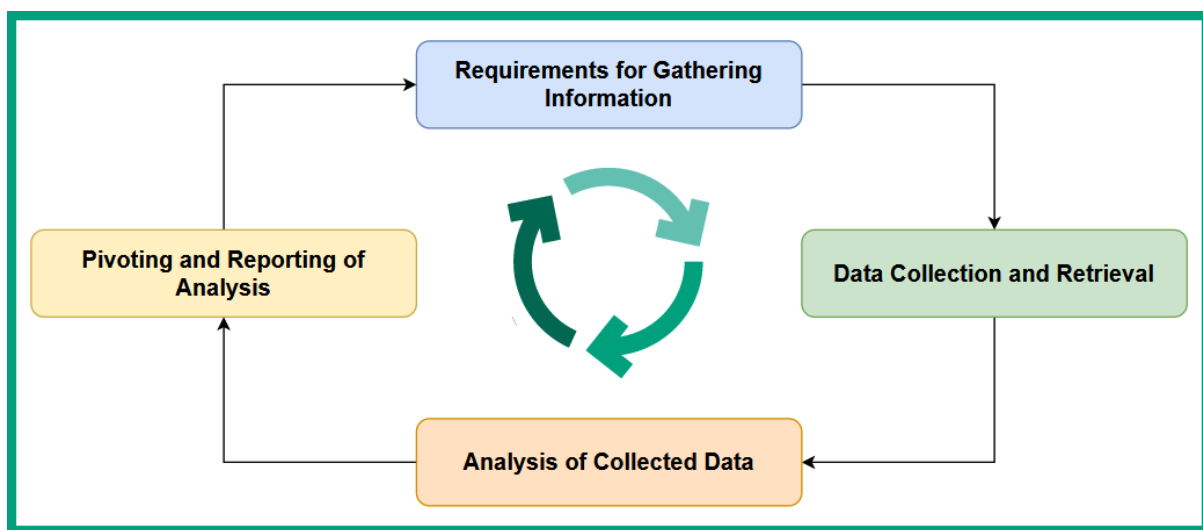
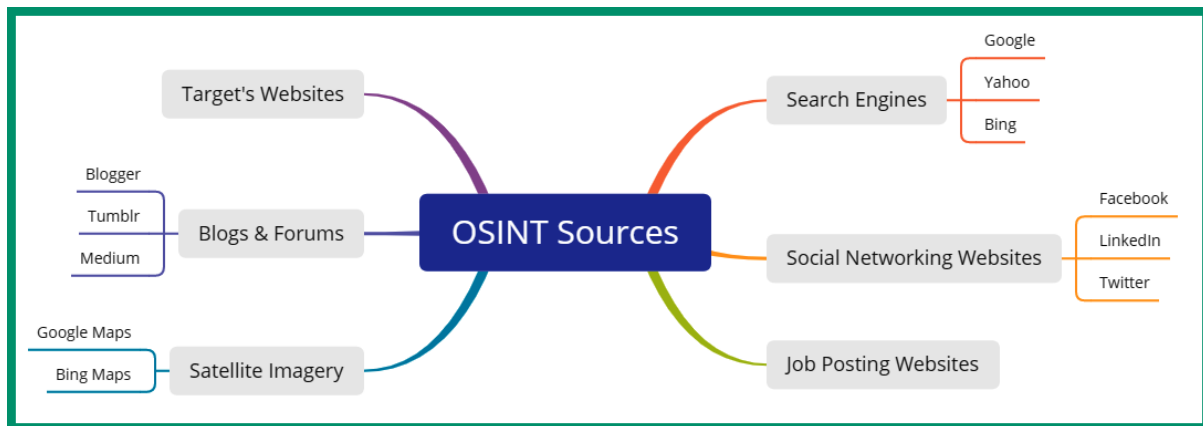




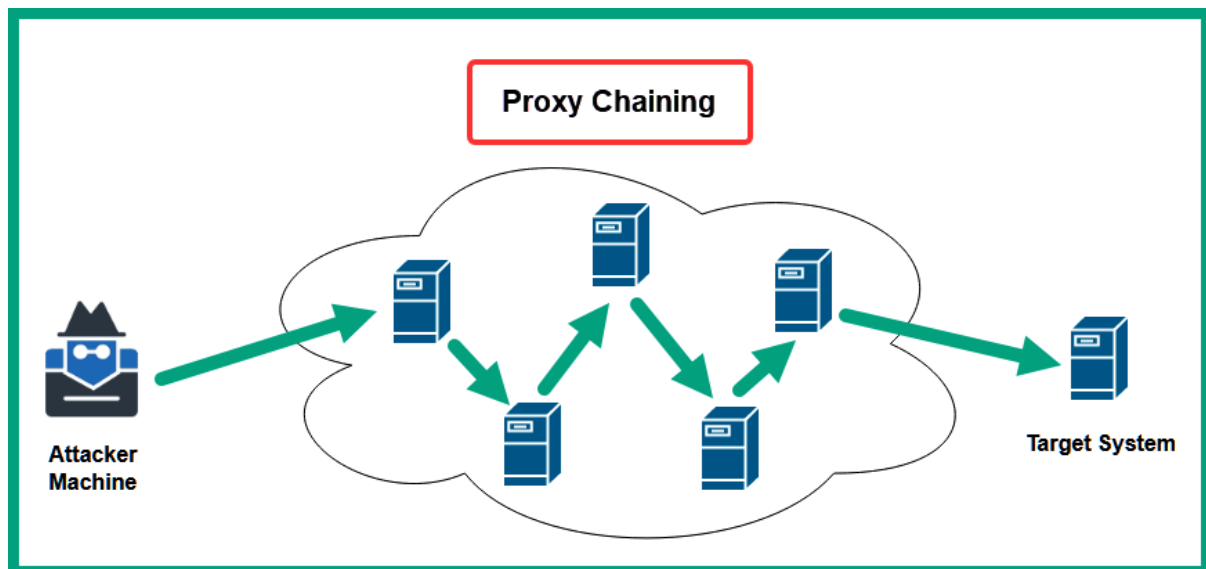
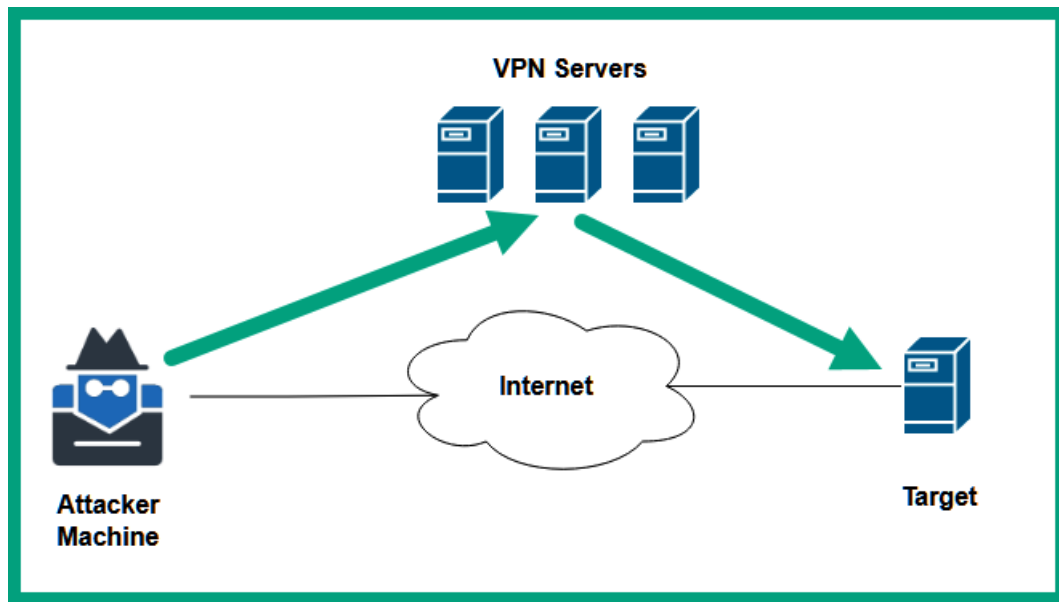
## Chapter 3: Understanding Passive Reconnaissance











```
kali@kali:~$ locate proxychain
/etc/proxychains4.conf
/etc/alternatives/proxychains
/etc/alternatives/proxychains.1.gz
/usr/bin/proxychains
/usr/bin/proxychains4
/usr/bin/proxychains4-daemon
/usr/lib/x86_64-linux-gnu/libproxychains.so.4
/usr/share/applications/kali-proxychains.desktop
```



```
# proxychains.conf  VER 4.x
#
# HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.

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


```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4          127.0.0.1 9050
socks5 104.236.45.251 31226
socks5 174.138.33.62 59166
```



```

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 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 104.236.45.251:31226 [proxychains] DLL init: proxychains-ng 4.16
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
... timeout
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... contile.services.mozilla.com:443 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... www.google.com:443 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... push.services.mozilla.com:443 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... ocsdpki.goog:80 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... ocsdpki.goog:80 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... www.gstatic.com:443 ... OK
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... adservice.google.com:443 ... OK
[proxychains] Dynamic chain ... 174.138.33.62:59166 ... googleads.g.doubleclick.net:443 ... OK

```



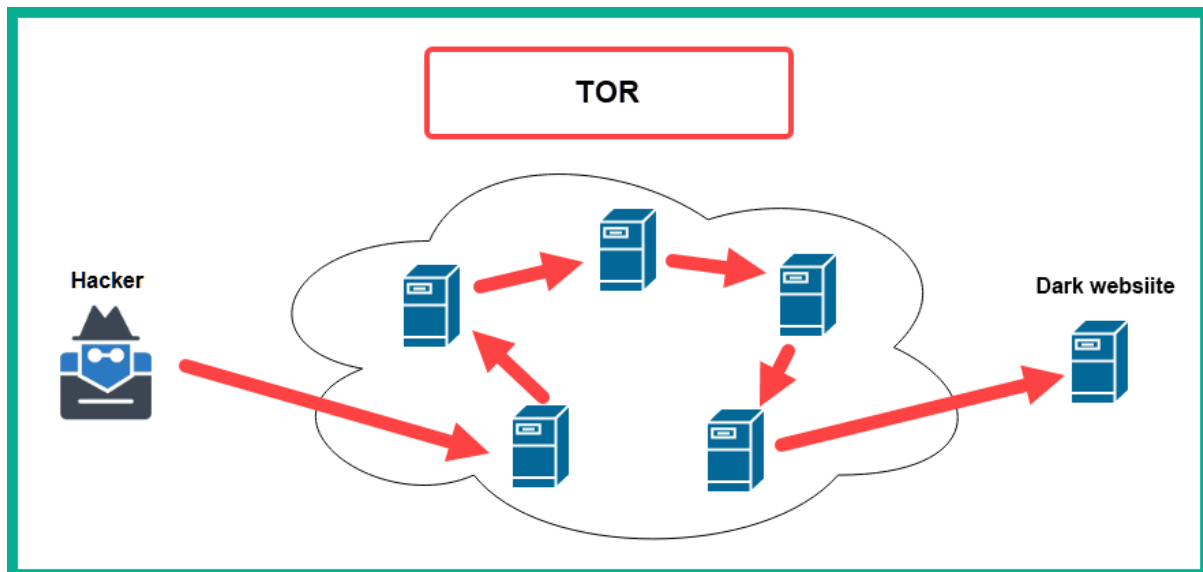
The screenshot shows the homepage of WhatIsMyIPAddress.com. The browser address bar displays the URL <https://whatismyipaddress.com>. The website header includes the logo, a search bar with the placeholder text "Enter Keywords or IP Address...", and a "Search" button. Below the header is a navigation menu with four tabs: "MY IP", "IP LOOKUP", "HIDE MY IP", and "VPNS". The "MY IP" tab is currently selected.

The main content area displays the user's IP information:

- My IP Address is:**
  - IPv4: **174.138.33.62**
  - IPv6: **Not detected**
- My IP Information:**
  - ISP: DigitalOcean LLC
  - City: North Bergen
  - Region: New Jersey
  - Country: United States

A red-bordered box highlights the text: **Exit-node IP address and geo-location is exposed**.



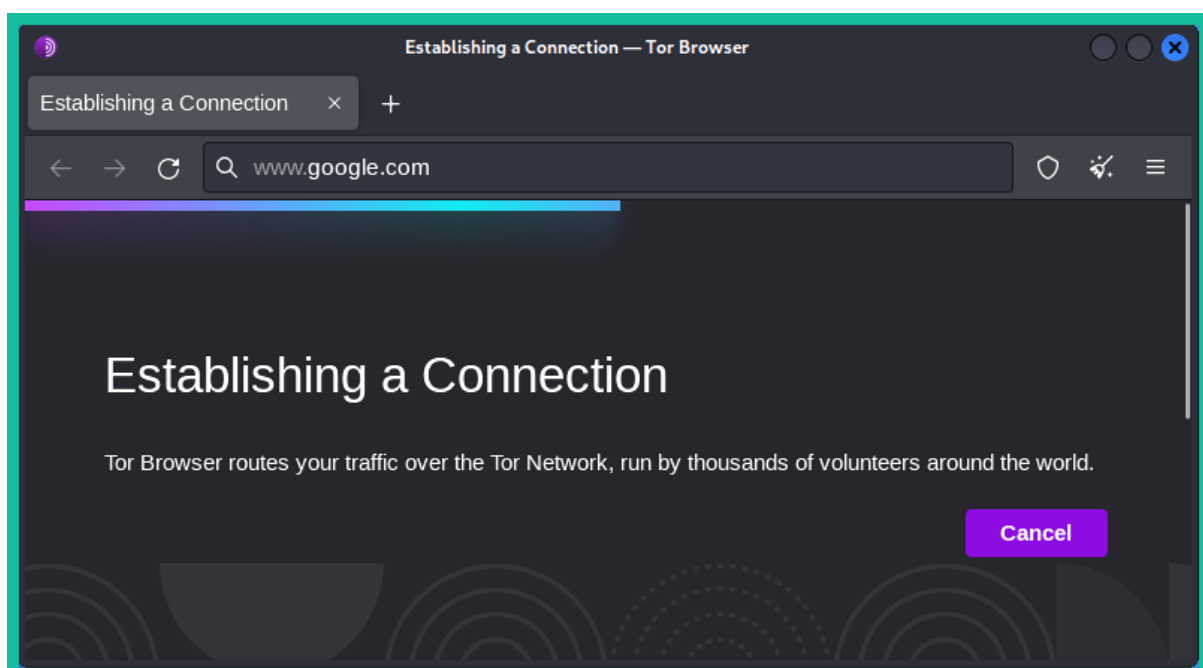
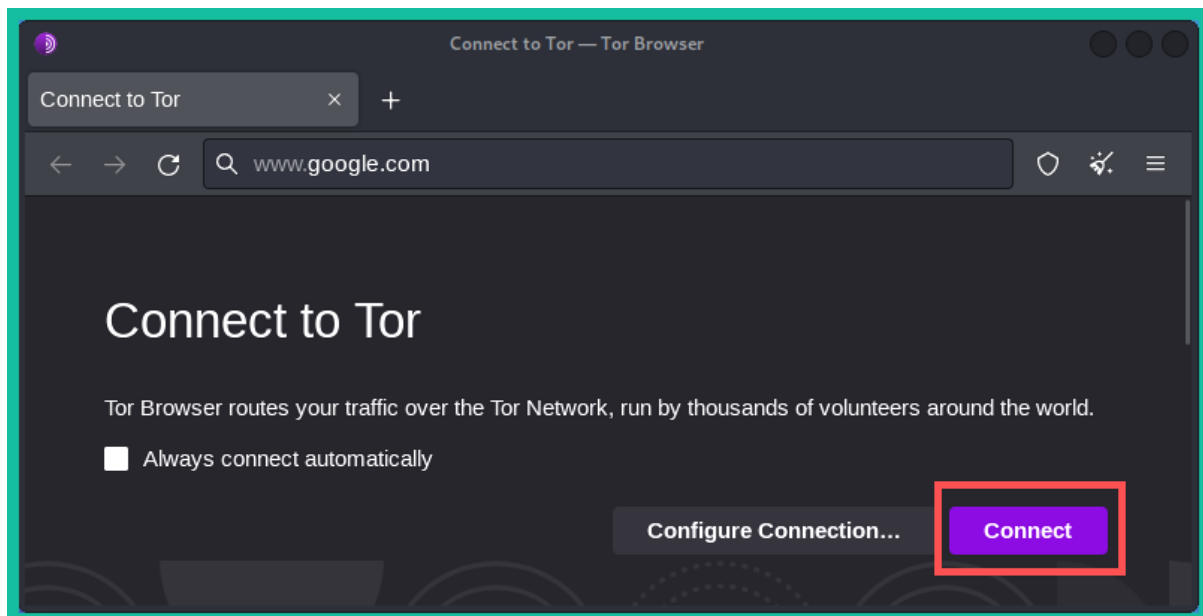


```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:2 https://download.docker.com/linux/debian bullseye InRelease [43.3 kB]
Get:3 https://download.docker.com/linux/debian bullseye/stable amd64 Packages [17.2 kB]
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [19.2 MB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.0 MB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [164 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Packages [237 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [922 kB]
Fetched 64.7 MB in 10s (6,419 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1179 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
kali@kali:~$ sudo apt install -y tor torbrowser-launcher
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster apparmor-utils nylx obfs4proxy
The following NEW packages will be installed:
  tor tor-geoipdb torbrowser-launcher torsocks
0 upgraded, 4 newly installed, 0 to remove and 1179 not upgraded.
Need to get 3,626 kB of archives.
After this operation, 17.4 MB of additional disk space will be used.
```



```
kali@kali:~$ torbrowser-launcher
Tor Browser Launcher
By Micah Lee, licensed under MIT
version 0.3.6
https://github.com/micahflee/torbrowser-launcher
Creating GnuPG homedir /home/kali/.local/share/torbrowser/gnupg_homedir
Downloading Tor Browser for the first time.
Downloading https://aus1.torproject.org/torbrowser/update_3/release/Linux_x86_64-gcc3/x/ALL
Latest version: 12.0.2
Downloading https://dist.torproject.org/torbrowser/12.0.2/tor-browser-linux64-12.0.2_ALL.tar.xz.asc
Downloading https://dist.torproject.org/torbrowser/12.0.2/tor-browser-linux64-12.0.2_ALL.tar.xz
Verifying Signature
Downloading latest Tor Browser signing key ...
Key imported successfully
```





What Is My IP Address - See Your Public Address - IPv4 & IPv6 — Tor Browser

whatismyipaddress.com - x What Is My IP Address - See x +

https://whatismyipaddress.com

WhatIs MyIPAddress .com Enter Keywords or IP Address... Search ABOUT PRESS BLOG CONTACT

MY IP IP LOOKUP HIDE MY IP VPNs ▼ TOOLS ▼ LEARN ▼

My IP Address is:

IPv6: ? **2a0b:f4c2::14**

IPv4: ? **185.220.101.14**

My IP Information:

ISP: Zwiebelfreunde E.V.  
City: Citrus Park  
Region: Florida  
Country: United States

The exit-node IP address is revealed from the TOR network, while the real source IP address is concealed.

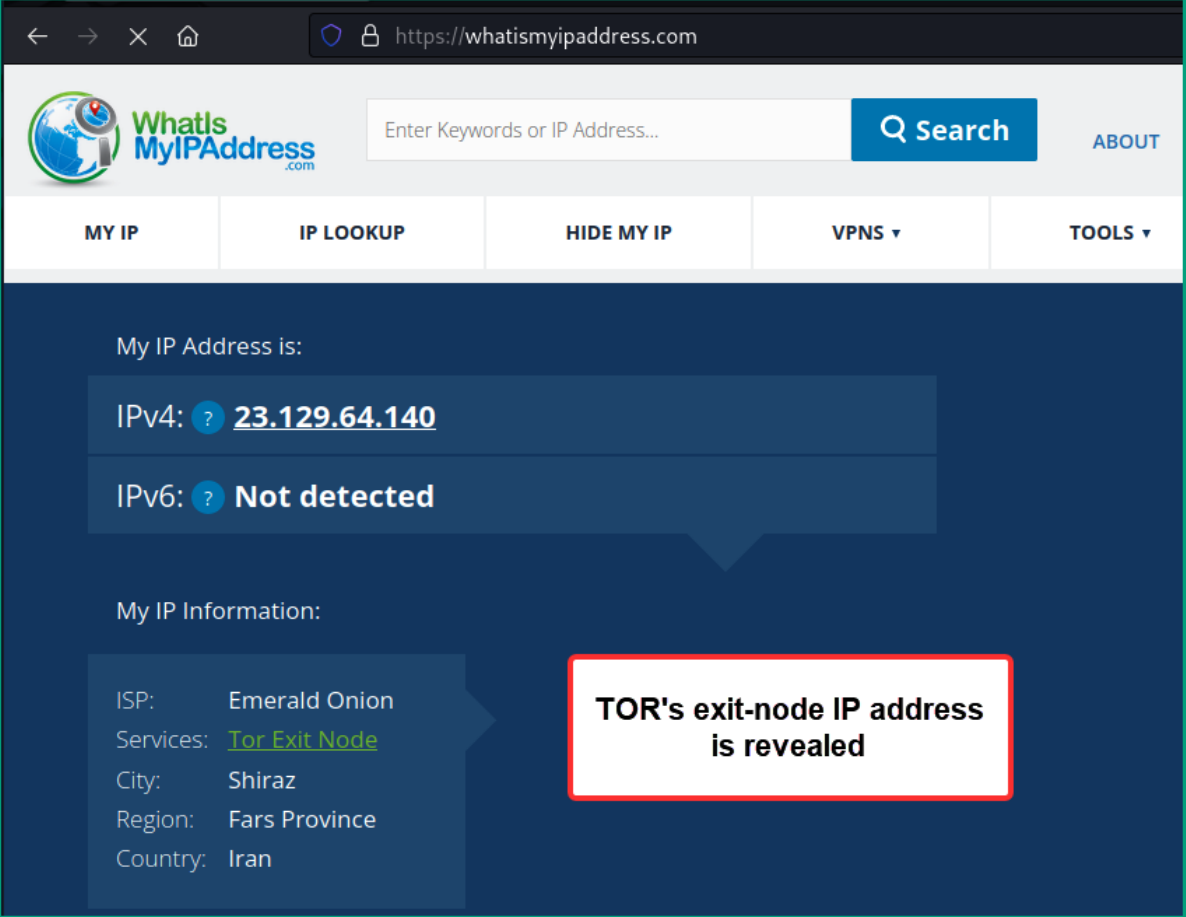
Privacy

```
#  
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks4 127.0.0.1 9050  
#socks5 104.236.45.251 31226  
#socks5 174.138.33.62 59166
```

```
kali@kali:~$ proxychains4 curl ifconfig.co  
[proxychains] config file found: /etc/proxychains4.conf  
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4  
[proxychains] DLL init: proxychains-ng 4.16  
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... ifconfig.co:80 ... OK  
192.42.116.223 ←
```



```
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 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
```



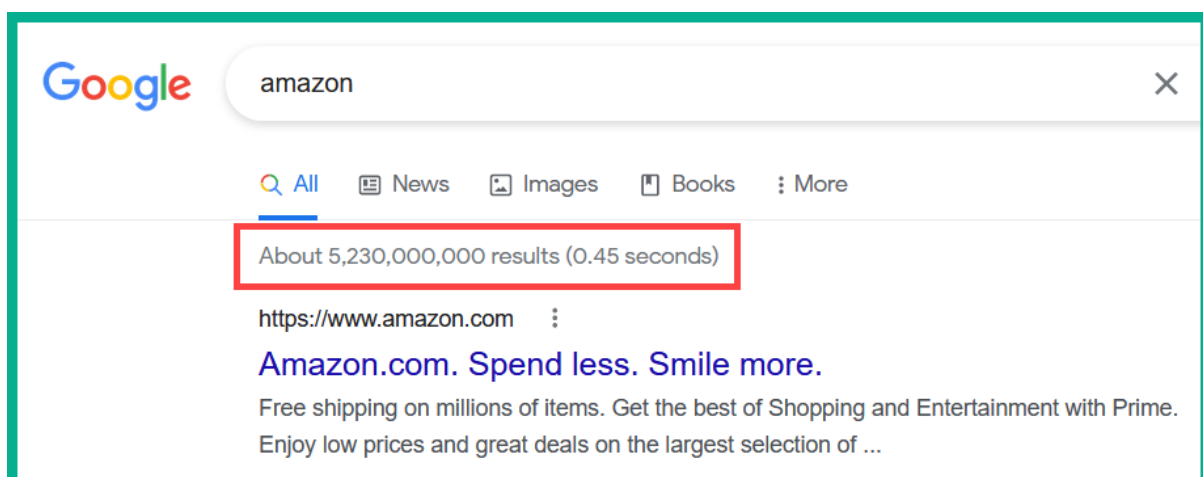
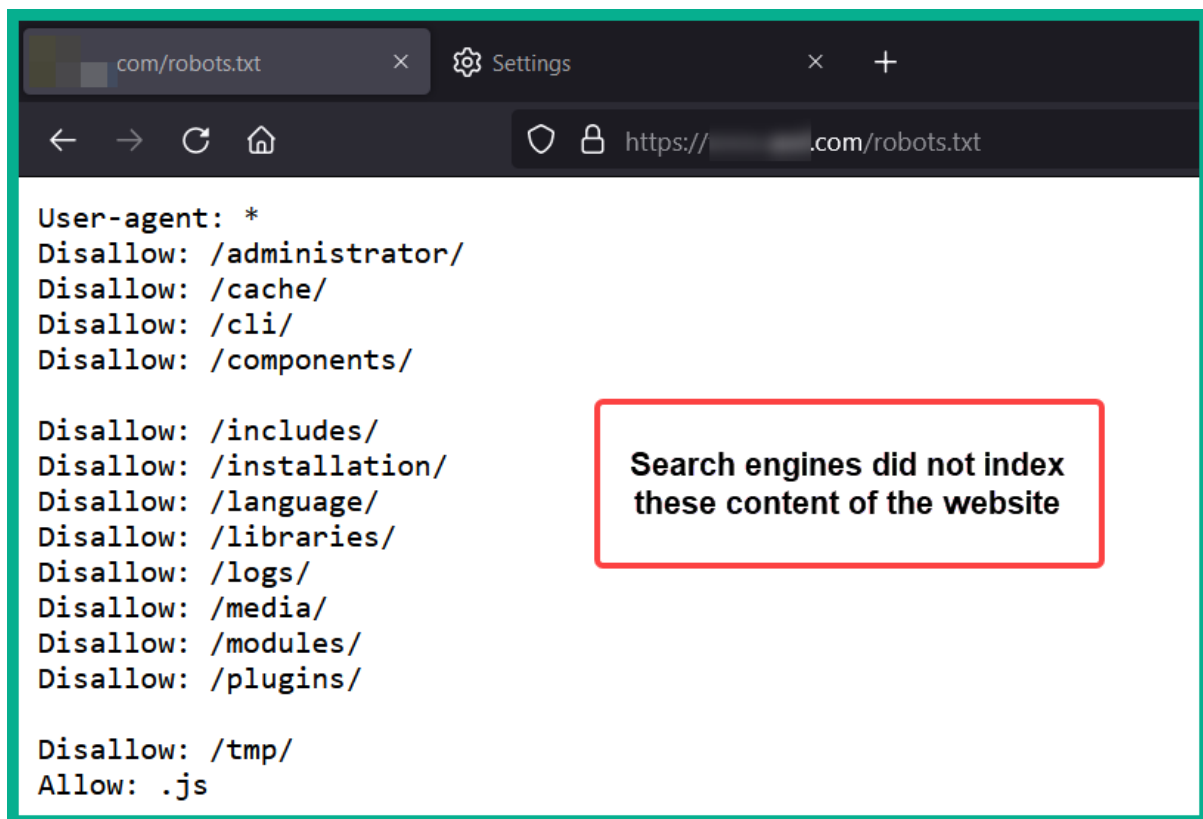
The screenshot shows the homepage of WhatIsMyIPAddress.com. The browser address bar displays <https://whatismyipaddress.com>. The page features a search bar with the text "Enter Keywords or IP Address..." and a "Search" button. Below the search bar is a navigation menu with links: MY IP, IP LOOKUP, HIDE MY IP, VPNS, and TOOLS. The main content area displays "My IP Address is:" followed by "IPv4: 23.129.64.140" and "IPv6: Not detected". Under "My IP Information:", the following details are listed: ISP: Emerald Onion, Services: [Tor Exit Node](#), City: Shiraz, Region: Fars Province, and Country: Iran. A red-bordered box highlights the text "TOR's exit-node IP address is revealed" next to the IP information.

```
kali@kali:~$ sudo systemctl stop tor
kali@kali:~$ sudo systemctl status tor
o tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; preset: disabled)
   Active: inactive (dead)

Jan 26 12:36:16 kali systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
Jan 26 12:36:16 kali systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance-master).
Jan 26 12:43:15 kali systemd[1]: tor.service: Deactivated successfully.
Jan 26 12:43:15 kali systemd[1]: Stopped Anonymizing overlay network for TCP (multi-instance-master).
```



## Chapter 4: Domain and DNS Intelligence





Google

site:microsoft.com

× | 🔊 📷 🔍

🔍 All 📖 Books 🖼 Images 📰 News ⋮ More Tools

About 176,000,000 results (0.29 seconds)

<https://careers.microsoft.com> ⋮  
**Careers at Microsoft | Microsoft jobs**  
Experienced professionals Want to make a difference? So do we. Step in to explore the wealth of career opportunities and take your career to the next level.

<https://partner.microsoft.com> ⋮  
**Welcome to the Microsoft Cloud Partner Program**  
Drive customer purchasing as you sell through the Microsoft commercial marketplace, build partner-to-partner sales channels, and use sales tools and resources.

<https://visualstudio.microsoft.com> > d... · [Translate this page](#) ⋮  
**Downloads - Visual Studio - Microsoft**  
27 Sept 2022 — Global · Visual Studio currently does not run on Android or iOS. · Visual Studio for Mac currently does not run on Android or iOS. · Visual Studio ...

<https://www.microsoft.com> > es-sv · [Translate this page](#) ⋮  
**Microsoft: página principal**  
Iconos del conjunto de aplicaciones de Microsoft 365, como Teams, Word, Outlook,. Microsoft 365. Todo lo que necesitas para lograr más en menos tiempo.

Google

printnightmare site:microsoft.com

× | 🔊 📷 🔍

🔍 All 📰 News 📺 Videos 🖼 Images ⋮ More Tools

About 6,270 results (0.36 seconds)

<https://msrc.microsoft.com> > update-guide > vulnerability ⋮  
**CVE-2021-34527 - MSRC Portal - Microsoft**  
No information is available for this page.  
[Learn why](#)




<https://learn.microsoft.com> > en-us > answers > questions ⋮  
**Patch to Fix PrintNightmare Vulnerability - Microsoft Q&A**  
28 Apr 2022 — Microsoft's **PrintNightmare** update is causing a lot of problems with network printers mapped on a print server ...  
[1 answer](#) · 0 votes: Hi there, The patch CVE-2021-34481 for the Windows Print Spooler Remo...







<https://msrc-blog.microsoft.com> > 2021/07/08 > clarifie... ⋮  
**Clarified Guidance for CVE-2021-34527 Windows Print ...**  
8 Jul 2021 — ... and is effective against the known printer spooling exploits and other public reports collectively being referred to as **PrintNightmare**.



Google

customer AND login site:microsoft.com

× |   

 All  Images  Videos  News  Books  More Tools

About 228,000 results (0.28 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.

Google

"login" site:microsoft.com

× |   

 All  Images  Books  News  Videos  More Tools

About 1,180,000 results (0.35 seconds)

<https://careers.microsoft.com/login>

### Login - Microsoft Careers

[Sign in](#) · [Personal](#) · [Employee](#) · [Follow Microsoft Careers](#) · [What's new](#) · [Microsoft Store](#) · [Education](#) · [Enterprise](#) · [Developer](#).

<https://www.microsoft.com/business/security-101>

### What Is Login Security? - Microsoft

**Login** security ensures that only genuine, authorized users can access online accounts, keeping bad actors out. Hacking into the billions of user accounts ...

<https://cmt3.research.microsoft.com>




### Conference Management Toolkit - Login

**Login** failed: [Click here to verify your email](#). Email \*. Password \*. [Log In](#). [Forgot your password?](#)  
[New to CMT? Register ...](#)




Google

site:microsoft.com filetype:txt


× |   

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

About 2 results (0.60 seconds)

<https://www.microsoft.com/robots> 

**Microsoft's robots.txt**




[https://learn.microsoft.com/en-us/java/api/com.a...](https://learn.microsoft.com/en-us/java/api/com.azure.eventhubs(EventHubDataFormatClass)) 

**EventHubDataFormat Class - Microsoft Learn**

Defines values for EventHubDataFormat. Field Summary. Modifier and Type, Field and Description. static final EventHubDataFormat, APACHEAVRO. Static value ...


Google

site:microsoft.com intitle:login

× |   


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

About 55,900 results (0.61 seconds)

<https://careers.microsoft.com/login> 

**Login - Microsoft Careers**

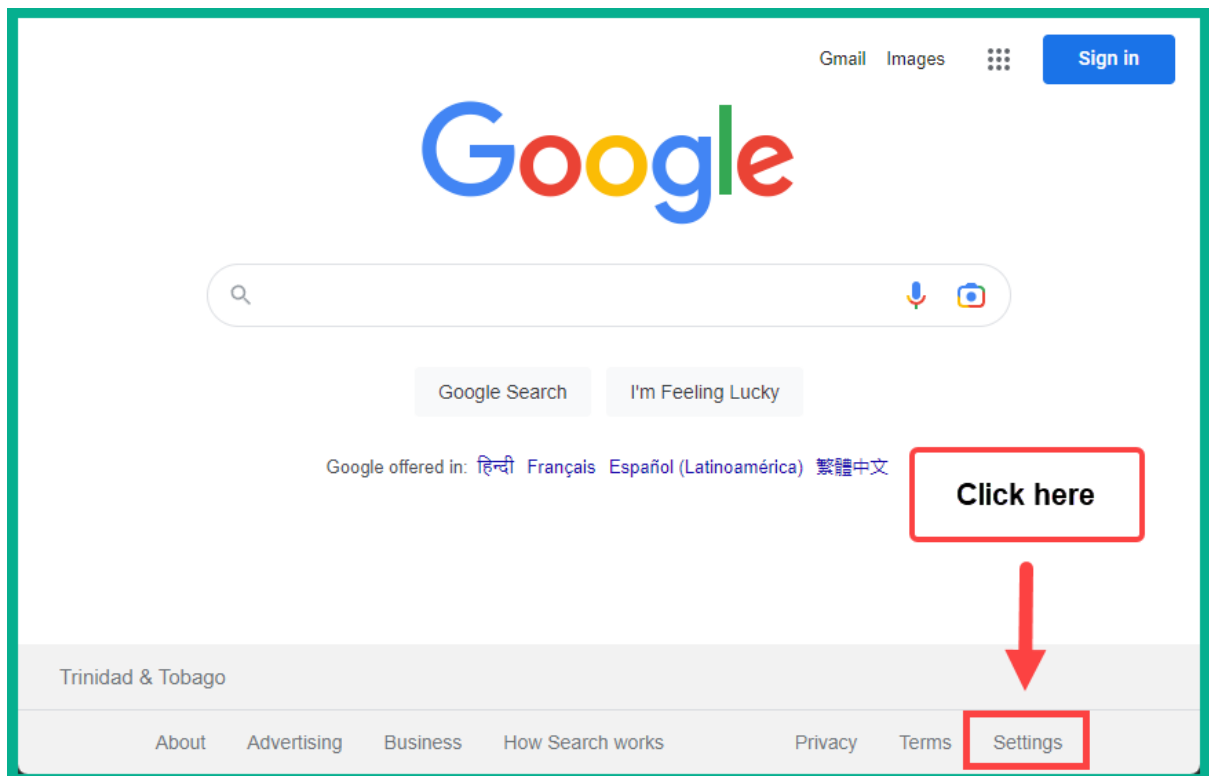
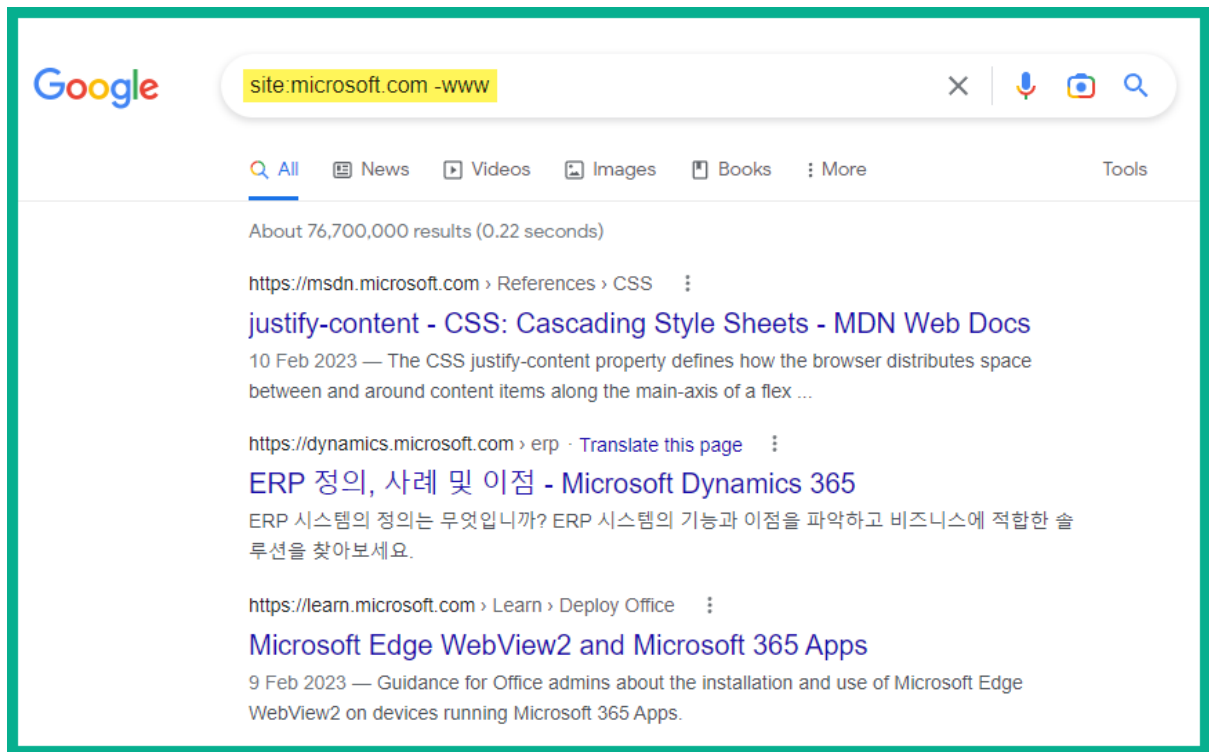
Current employee sign in here. Microsoft logo Internal. Microsoft employee sign in. LinkedIn logo Internal. LinkedIn employee sign in.

<https://cmt3.research.microsoft.com> 

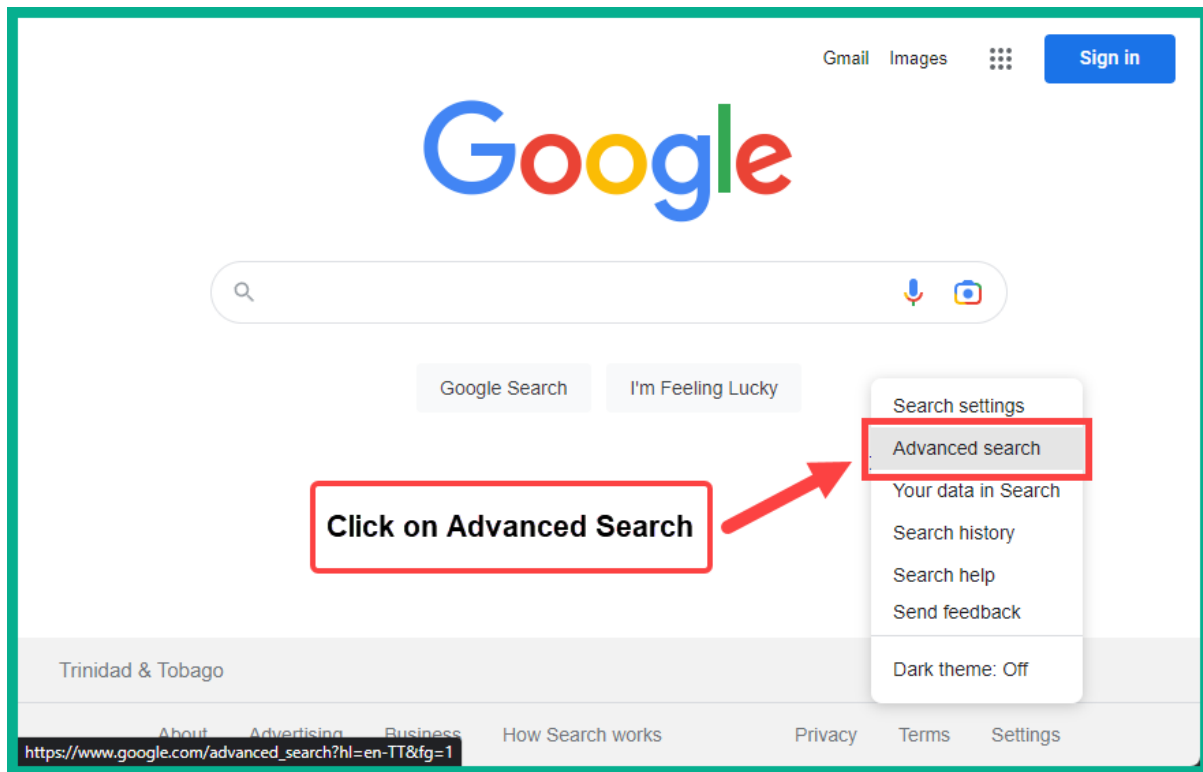
**Conference Management Toolkit - Login**

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









### Advanced Search

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:	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:	Find pages in the language that you select.
region:	Find pages published in a particular region.
last update:	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:	Search for terms in the whole page, page title or web address, or links to the page you're looking for.
file type:	Find pages in the format that you prefer.
usage rights:	Find pages that you are free to use yourself.

[Advanced Search](#)







EXPLOIT  
DATABASE



# Google Hacking Database

Filters

Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2023-02-15	intext:"index of" "backup/*.*sql"	Files Containing Juicy Info	Ahmad Kataranje
2023-02-15	# Google Dork: intitle:"index of" "admin" "cgi-bin"	Files Containing Juicy Info	Umandon Ardaw
2023-02-15	intitle:index of "wc.db"	Files Containing Juicy Info	Pradeep A
2023-02-15	site:*/AdminLogin.aspx	Pages Containing Login Portals	Reza Abasi
2023-02-15	intitle:phaser inurl:/frameprop.htm	Various Online Devices	Bilal KUŞ
2023-02-13	inurl:assysnetmob	Pages Containing Login Portals	Zayed AlJaberi
2023-02-13	intitle:"index of" "login.sh"	Pages Containing Login Portals	Anoop Kumar
2023-02-13	intitle:"index of" "/secrets/"	Files Containing Juicy Info	Bappe Sarker
2023-02-09	intitle:BioTime AND intext:ZKTeco Security LLC	Files Containing Juicy Info	Robot Shell
2023-02-09	inurl: wp-content/plugin/404-redirection-manager	Files Containing Juicy Info	Rutvik Jaini
2023-02-09	inurl: wp-content/plugin/8-degree-notification-bar	Files Containing Juicy Info	Rutvik Jaini
2023-02-07	intext:"index of" ".git"	Files Containing Juicy Info	Praharsh Kumar Singh
2023-02-07	intext:"index of" "phpinfo"	Files Containing Juicy Info	Praharsh Kumar Singh
2023-02-07	intext:"index of" "phpMyAdmin"	Files Containing Juicy Info	Praharsh Kumar Singh
2023-02-07	intext:"index of" "xmlrpc.php"	Files Containing Juicy Info	Praharsh Kumar Singh

Showing 1 to 15 of 7,567 entries

FIRST

PREVIOUS

1

2

3

4

5

...

505

NEXT

LAST

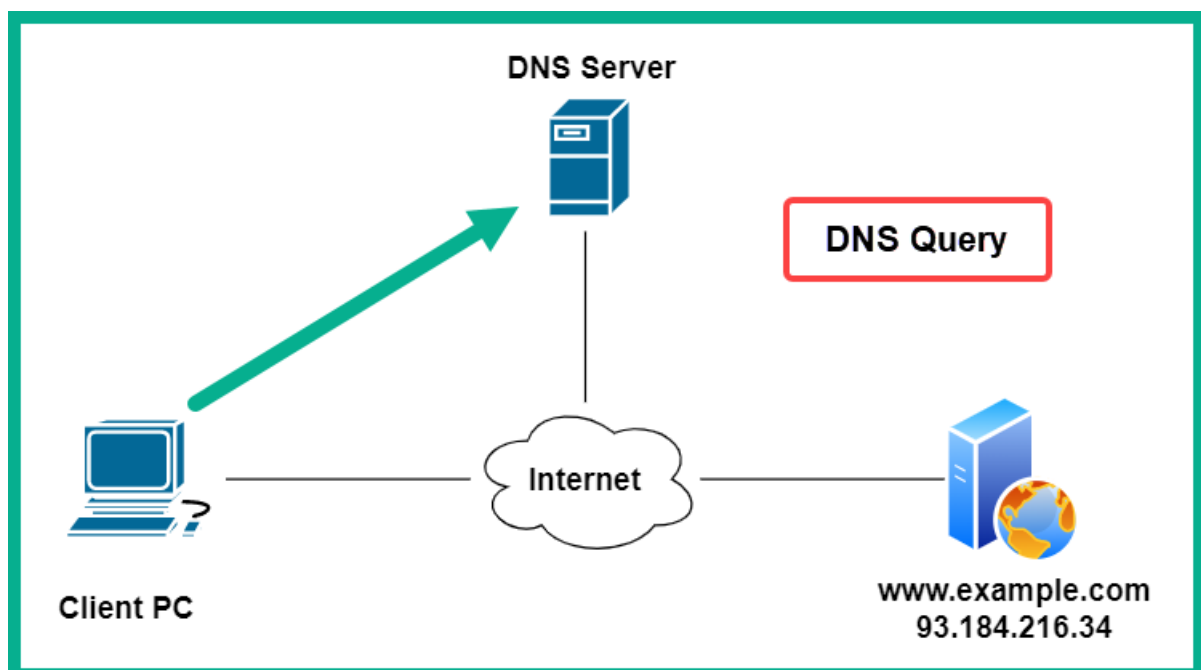
```
graph TD; Root[Root] --> com[.com]; Root --> net[.net]; Root --> org[.org]; com --> google[google]; google --> mail[mail];
```

The diagram illustrates the hierarchy of domain names. At the top is the **Root**. It branches into three **Top Level Domains (TLDs)**: **.com**, **.net**, and **.org**. From **.com**, it branches into **google**, which is a **Second Level Domain**. From **google**, it branches into **mail**, which is a **Sub-Domain**.

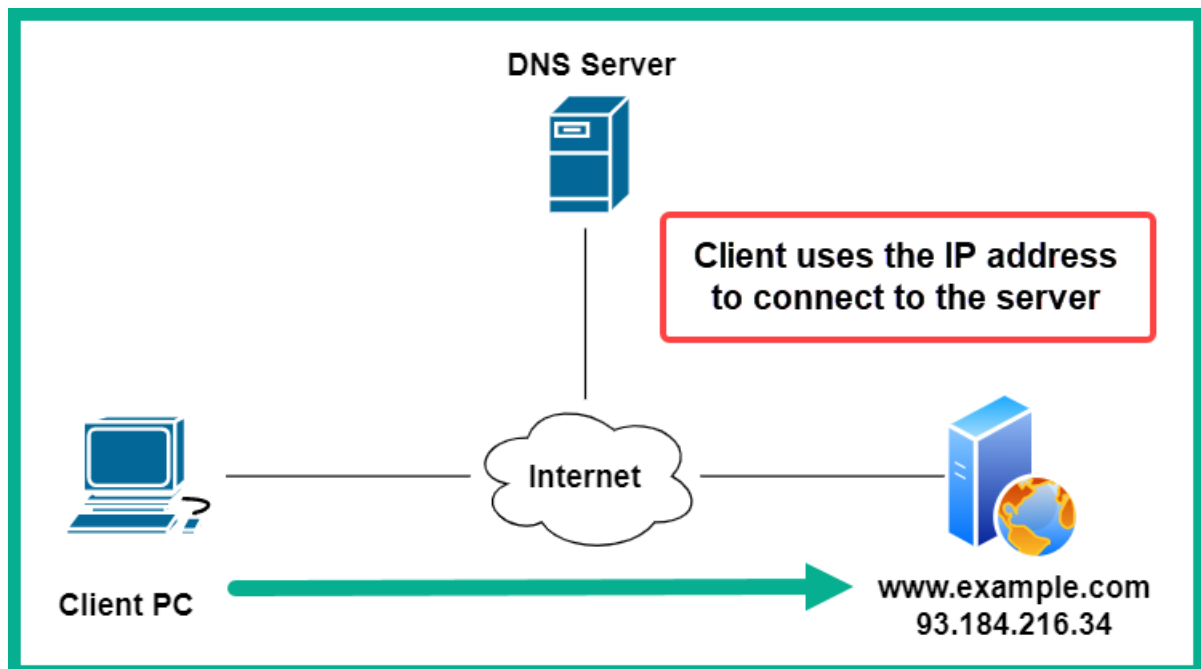
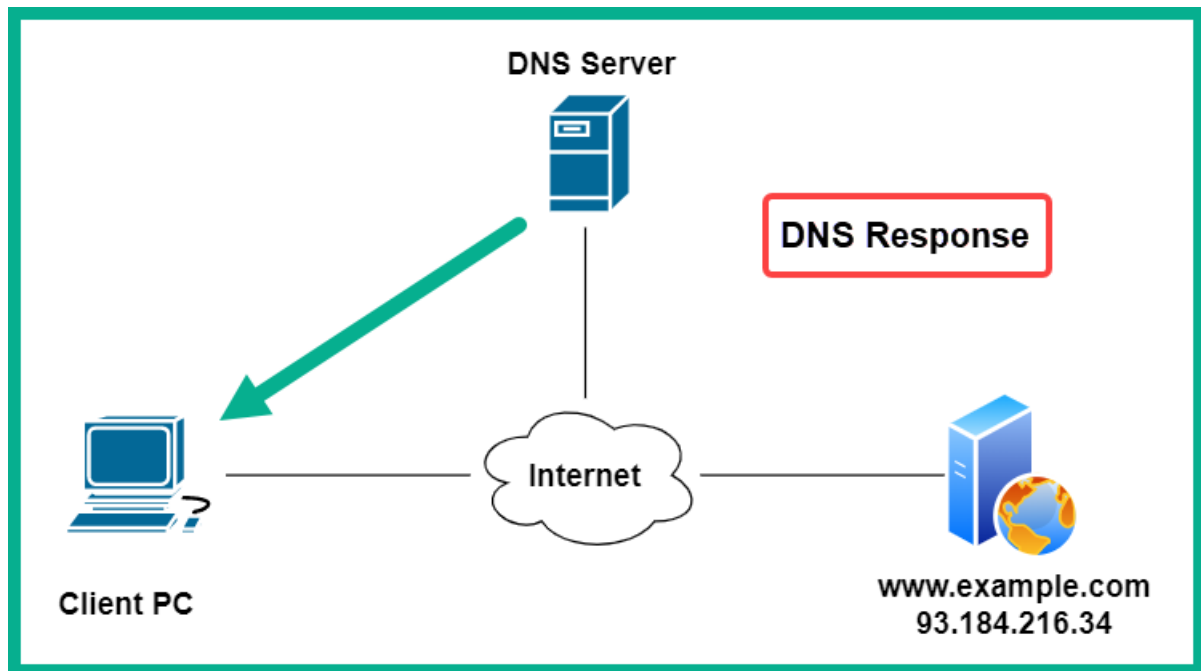


```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host

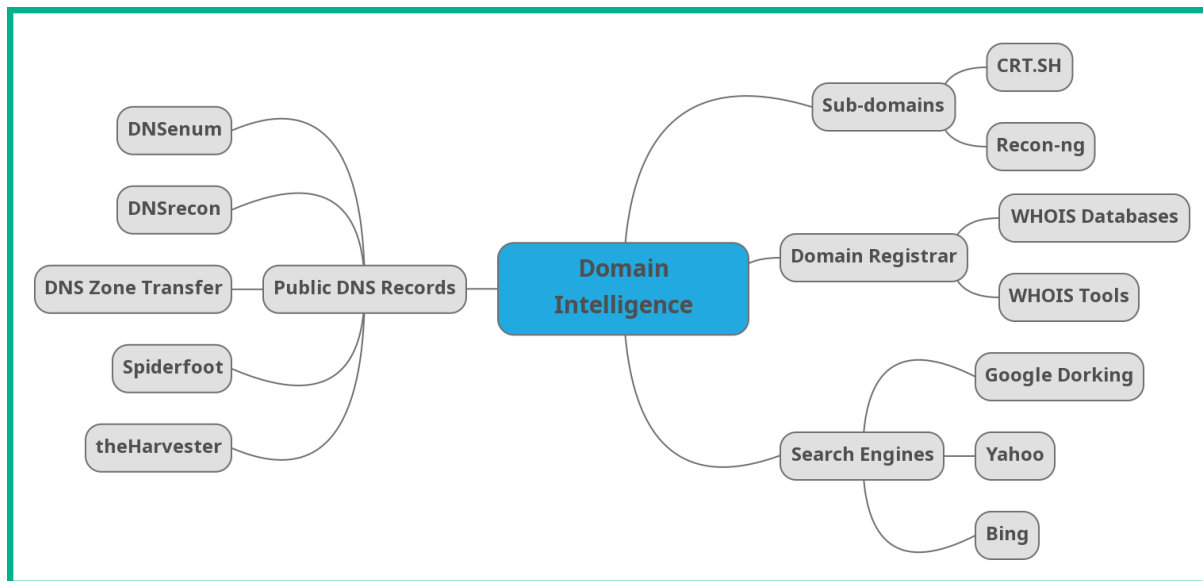
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
```











```
kali@kali:~$ whois apple.com
Domain Name: APPLE.COM
Registry Domain ID: 1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdb.com
Updated Date: 2023-02-16T06:14:38Z
Creation Date: 1987-02-19T05:00:00Z
Registry Expiry Date: 2024-02-20T05:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
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: A.NS.APPLE.COM
Name Server: B.NS.APPLE.COM
Name Server: C.NS.APPLE.COM
Name Server: D.NS.APPLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-05T20:16:21Z <<<
```

The screenshot shows the MXToolbox website interface. At the top, there's a navigation bar with "Pricing", "Tools", and "Delivery Center". Below that is a dark navigation bar with links to "SuperTool", "MX Lookup", "Blacklists", "DMARC", "Diagnostics", and "Email Health". The main section is titled "Whois Lookup" with a magnifying glass icon. It features a "Domain Name" input field containing "apple.com" and an orange "Whois Lookup" button.



apple.com

Whois Lookup

whois:apple.com

Find Problems

 whois

Name	Value
Registrar	CSC Corporate Domains, Inc.
Name Server	A.NS.APPLE.COM
Name Server	B.NS.APPLE.COM
Name Server	C.NS.APPLE.COM
Name Server	D.NS.APPLE.COM

Name	Value
Domain Name	APPLE.COM
Registry Domain ID	1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server	whois.corporatedomains.com
Registrar URL	http://cscdns.com
Updated Date	2023-02-16T06:14:38Z
Creation Date	1987-02-19T05:00:00Z
Registry Expiry Date	2024-02-20T05:00:00Z
Registrar	CSC Corporate Domains, Inc.
Registrar IANA ID	299
Registrar Abuse Contact Email	domainabuse@cscglobal.com

```
kali@kali:~$ nslookup A
>
> server 8.8.8.8 B
Default server: 8.8.8.8
Address: 8.8.8.8#53
>
> amazon.com C
;; communications error to 8.8.8.8#53: timed out
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
Name:   amazon.com
Address: 52.94.236.248
>
```



```
> set type=mx (A)
>
> amazon.com (B)
;; communications error to 8.8.8.8#53: timed out
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
amazon.com   mail exchanger = 5 amazon-smtp.amazon.com.
```

```
> set type=a (A)
>
> amazon-smtp.amazon.com (B)
;; communications error to 8.8.8.8#53: timed out
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   amazon-smtp.amazon.com
Address: 35.172.144.184 ←
>
```



## Certificate

[www.amazon.com](https://www.amazon.com)

DigiCert Global CA G2

DigiCert Global Root G2

### Subject Name

Common Name [www.amazon.com](https://www.amazon.com)

### Issuer Name

Country US  
Organization DigiCert Inc  
Common Name [DigiCert Global CA G2](#)

### Validity

Not Before Tue, 17 Jan 2023 00:00:00 GMT  
Not After Tue, 16 Jan 2024 23:59:59 GMT

### Subject Alt Names

DNS Name [amazon.com](https://amazon.com)  
DNS Name [amzn.com](https://amzn.com)  
DNS Name [uedata.amazon.com](https://uedata.amazon.com)  
DNS Name [us.amazon.com](https://us.amazon.com)  
DNS Name [www.amazon.com](https://www.amazon.com)  
DNS Name [www.amzn.com](https://www.amzn.com)

**crt.sh** Certificate Search


Enter an **Identity** (Domain Name, Organization Name, etc),  
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

[apple.com](#)

**Search**

[Advanced...](#)



crt.sh Identity Search  <a href="#">Group by Issuer</a>						
Criteria    Type: Identity   Match: ILIKE   Search: 'apple.com'						
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	
<a href="#">2382386751</a>	2020-01-27	2013-08-09	2015-08-09	Matt Martin-MPKI SSL-Premium	mattmartin@apple.com	C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network
<a href="#">2382089966</a>	2020-01-27	2013-09-23	2015-09-24	food.apple.com	food.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381996484</a>	2020-01-27	2014-07-22	2015-07-22	ecommerce-qa.apple.com	ecommerce-qa.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381996432</a>	2020-01-27	2014-05-05	2015-05-05	b2b-test.apple.com	b2b-test.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381422119</a>	2020-01-27	2014-09-11	2015-09-12	afsporal2.euro.apple.com	afsporal2.euro.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381408260</a>	2020-01-27	2011-04-11	2015-06-08	b2btest.apple.com	b2btest.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381374674</a>	2020-01-27	2013-05-01	2015-05-02	hrweb-maint.apple.com	hrweb-maint.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381374708</a>	2020-01-27	2014-07-25	2015-07-24	wdg02-uat.apple.com	sso-uat-nc.corp.apple.com wdg02-uat.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2381374659</a>	2020-01-27	2014-04-23	2015-04-24	hrweb-qa.apple.com	hrweb-qa.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2380977932</a>	2020-01-26	2014-03-04	2015-03-04	applechinawifi.apple.com	applechinawifi.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C
<a href="#">2380927914</a>	2020-01-26	2012-11-02	2014-11-02	ray.apple.com	ray.apple.com	C=US, O="Entrust, Inc.", OU=www.entrust.net/rpa is L1C

crt.sh ID	<a href="#">2382089966</a>					
Summary	Leaf certificate					
Certificate Transparency	Log entries for this certificate:					
	Timestamp	Entry #	Log Operator	Log URL		
	2020-01-27 07:04:12 UTC	991343739	Google	<a href="https://ct.googleapis.com/rocketeer">https://ct.googleapis.com/rocketeer</a>		
Revocation	Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
	OCSP	The CA	<a href="#">Check</a>	?	n/a	?
	CRL	The CA	Unknown (Expired)	n/a	n/a	2023-03-05 18:55:30 UTC
	CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
	disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
	OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a
Certificate Fingerprints	SHA-256 <a href="#">FF83F6581CCA3D4BF93B7D8CD32E3A5087F2A6C2728326170DFB621BB3F97A1D</a> SHA-1 <a href="#">363C2F0A1B6EAB7E4A77B13C72C0B985154CDC55</a>					
ASN.1   Certificate   Graph   Hierarchy   pv	Certificate:					
	Data:					
Hide metadata	Version: 3 (0x2)					
Run cabinit	Serial Number: 1277221950 (0x4c28dc3e)					
Run x509int	Signature Algorithm: sha1WithRSAEncryption					
Run zlint	Issuer: (CA ID: 57)					
Download Certificate: <a href="#">PEM</a>	commonName = Entrust Certification Authority - L1C					
	organizationalUnitName = (c) 2009 Entrust, Inc.					
	organizationalUnitName = www.entrust.net/rpa is incorporated by reference					
	organizationName = Entrust, Inc.					
	countryName = US					
	Validity (Expired)					
	Not Before: Sep 23 21:42:06 2013 GMT					
	Not After: Sep 24 04:06:54 2015 GMT					
	Subject:					
	commonName = food.apple.com					
	organizationName = Apple Inc.					
	localityName = Cupertino					
	stateOrProvinceName = California					
	countryName = US					
	Subject Public Key Info:					
	Public Key Algorithm: rsaEncryption					
	RSA Public-Key: (2048 bit)					
	Modulus:					
	00:d2:2d:11:60:4e:ad:37:3b:23:8d:30:3b:df:d2:					
	c2:63:ad:61:dc:f4:3a:a4:84:eb:06:d1:6a:14:cd:					

← **Locale Information**

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



```
[*] Reloading modules ...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
```

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

Name	Value
binaryedge_api	
bing_api	
builtwith_api	
censysio_id	
censysio_secret	
flickr_api	
fullcontact_api	
github_api	
google_api	
hashes_api	

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

Name	Value
binaryedge_api	
bing_api	
builtwith_api	ca4e249
censysio_id	dc1c645
censysio_secret	0nUWKoA
flickr_api	
fullcontact_api	
github_api	
google_api	
hashes_api	
hibp_api	
hunter_io	c895e2a
ipinfodb_api	
ipstack_api	



```
[recon-ng][target1_recon] > workspaces list
```

Workspaces	Modified
default	2023-03-06 11:58:30
target1_recon	2023-03-06 12:24:41

```
[recon-ng][target1_recon] >
```

```
[recon-ng][target1_recon] > modules search bing_domain  
[*] Searching installed modules for 'bing_domain' ...
```

#### Recon

```
recon/domains-hosts/bing_domain_api  
recon/domains-hosts/bing_domain_web
```

```
[recon-ng][target1_recon] >
```

```
[recon-ng][target1_recon] > modules load recon/domains-hosts/bing_domain_web  
[recon-ng][target1_recon][bing_domain_web] > info
```

Name: Bing Hostname Enumerator  
Author: Tim Tomes (@lanmaster53)  
Version: 1.1

#### Description:

Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.

#### Options:

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

Required Parameter

#### 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][target1_recon][bing_domain_web] >
```



```
[recon-ng][target1_recon][bing_domain_web] > run
```

```
_____
MICROSOFT.COM
_____
```

```
[*] URL: https://www.bing.com/search?first=0&q=domain%3Amicrosoft.com
[*] Country: None
[*] Host: www.microsoft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: myaccount.microsoft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
```

```
[recon-ng][target1_recon][bing_domain_web] > show hosts
```

rowid	host	ip_address	region	notes	module
1	www.microsoft.com				bing_domain_web
2	myaccount.microsoft.com				bing_domain_web
3	mysignins.microsoft.com				bing_domain_web
4	support.microsoft.com				bing_domain_web
5	account.microsoft.com				bing_domain_web
6	myaccess.microsoft.com				bing_domain_web
7	admin.microsoft.com				bing_domain_web
8	myapps.microsoft.com				bing_domain_web
9	appsource.microsoft.com				bing_domain_web
10	www.catalog.update.microsoft.com				bing_domain_web
11	learn.microsoft.com				bing_domain_web
12	setup.microsoft.com				bing_domain_web
13	developer.microsoft.com				bing_domain_web
14	apps.microsoft.com				bing_domain_web
15	client.wvd.microsoft.com				bing_domain_web



Activity Summary		
Module	Runs	
recon/companies-domains/censys_subdomains	3	
recon/domains-hosts/bing_domain_web	3	

Results Summary		
Category	Quantity	
Domains	4	
Companies	0	
Netblocks	0	
Locations	0	
Vulnerabilities	0	
Ports	0	
Hosts	74	
Contacts	0	
Credentials	0	
Leaks	0	
Pushpins	0	
Profiles	0	
Repositories	0	



```
[recon-ng][target1_recon] > modules load reporting/html A
[recon-ng][target1_recon][html] > info B

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

Description:
Creates an HTML report.

Options:
  Name                               Current Value                               Required Description
  -----                               -
CREATOR                               yes          use creator name in the report footer
CUSTOMER                             yes          use customer name in the report header
FILENAME /home/kali/.recon-ng/workspaces/target1_recon/results.html yes          path and filename for report output
SANITIZE True                         yes          mask sensitive data in the report

[recon-ng][target1_recon][html] > options set CREATOR Glen C
CREATOR => Glen
[recon-ng][target1_recon][html] > options set CUSTOMER NewCustomer1 D
CUSTOMER => NewCustomer1
[recon-ng][target1_recon][html] > options set FILENAME /home/kali/Recon-Report1.html E
FILENAME => /home/kali/Recon-Report1.html
[recon-ng][target1_recon][html] > run F
[*] Report generated at '/home/kali/Recon-Report1.html'.
[recon-ng][target1_recon][html] >
```

file:///home/kali/Recon-Report1.html

[www.recon-ng.com](http://www.recon-ng.com)

## NewCustomer1

### Recon-ng Reconnaissance Report

[-] Summary

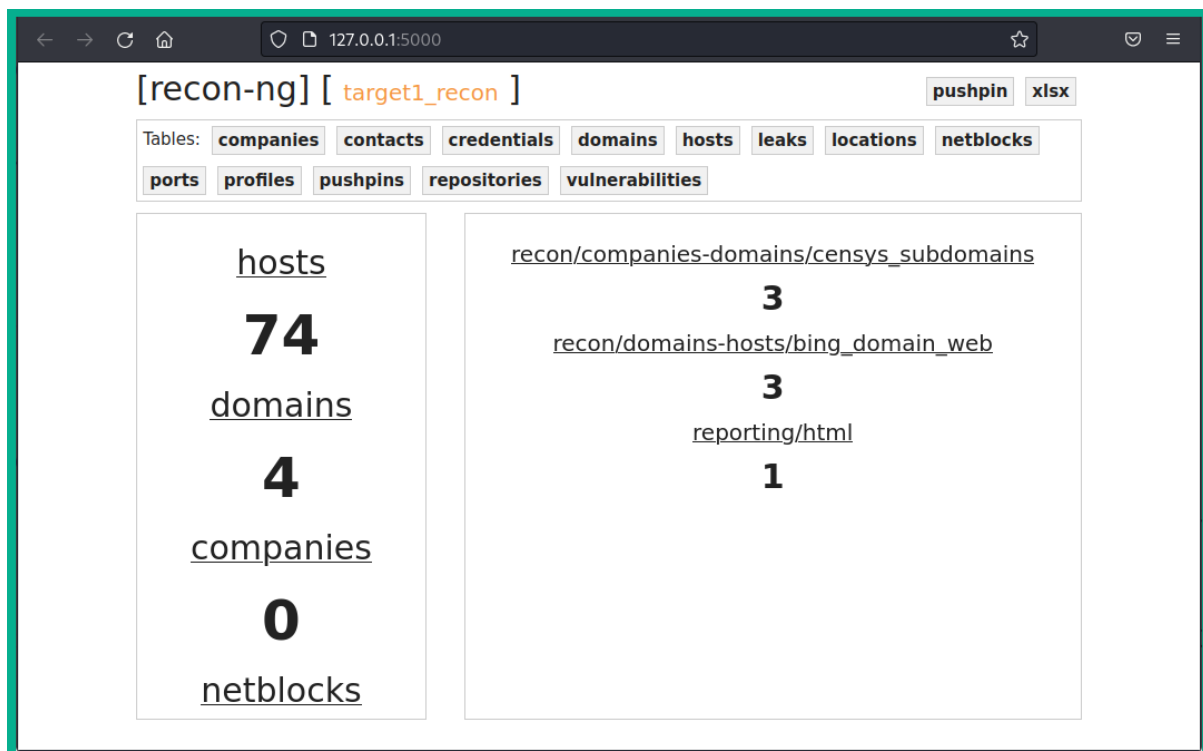
table	count
domains	4
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	74
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
account.microsoft.com							bing_domain_web
admin.microsoft.com							bing_domain_web
admin.powerplatform.microsoft.com							bing_domain_web
ads.microsoft.com							bing_domain_web





```
kali@kali:~$ dnsenum --dnsserver 8.8.8.8 apple.com
```

```
dnsenum VERSION:1.2.6
```

apple.com

#### Host's addresses:

apple.com.	453	IN	A	17.253.144.10
------------	-----	----	---	---------------

#### Name Servers:

b.ns.apple.com.	21600	IN	A	17.253.207.1
a.ns.apple.com.	21600	IN	A	17.253.200.1
c.ns.apple.com.	21401	IN	A	204.19.119.1
d.ns.apple.com.	20043	IN	A	204.26.57.1

#### Mail (MX) Servers:

mx-in.g.apple.com.	30	IN	A	17.32.222.242
mx-in-crk.apple.com.	841	IN	A	17.72.136.242
mx-in-mdn.apple.com.	2226	IN	A	17.32.222.242
mx-in-rno.apple.com.	3288	IN	A	17.179.253.242
mx-in-hfd.apple.com.	3388	IN	A	17.57.165.2
mx-in-vib.apple.com.	1630	IN	A	17.57.170.2



Brute forcing with /usr/share/dnsenum/dns.txt:

access.apple.com.	21600	IN	CNAME	www.access.apple.com.
www.access.apple.com.	21600	IN	A	17.254.3.40
ads.apple.com.	21600	IN	CNAME	ads.apple.com.akadns.net.
ads.apple.com.akadns.net.	600	IN	CNAME	ioshost.qtlcdn.com.
ioshost.qtlcdn.com.	20	IN	A	61.161.1.55
ioshost.qtlcdn.com.	20	IN	A	113.5.170.192
apps.apple.com.	117	IN	CNAME	itunes-cdn.itunes-apple.com.akadns.net.
itunes-cdn.itunes-apple.com.akadns.net.	3577	IN	CNAME	(
itunes.apple.com.edgekey.net.	7281	IN	CNAME	e673.dsce9.akamaiedge.net.
e673.dsce9.akamaiedge.net.	20	IN	A	96.17.60.35
asia.apple.com.	178	IN	A	17.253.144.10
autodiscover.apple.com.	21600	IN	CNAME	mailpex.apple.com.
mailpex.apple.com.	21600	IN	CNAME	hybridpex.v.aaplimg.com.
hybridpex.v.aaplimg.com.	30	IN	A	17.32.214.19
av.apple.com.	300	IN	CNAME	savant-bz.apple.com.
savant-bz.apple.com.	300	IN	A	17.171.99.83
savant-bz.apple.com.	300	IN	A	17.171.49.133

kali@kali:~\$ dnsrecon -d apple.com -n 8.8.8.8

```
[*] std: Performing General Enumeration against: apple.com...
[-] DNSSEC is not configured for apple.com
[*] SOA usmsc2-extxfr-001.dns.apple.com 17.47.176.10
[*] NS b.ns.apple.com 17.253.207.1
[*] NS b.ns.apple.com 2620:149:ae7::53
[*] NS a.ns.apple.com 17.253.200.1
[*] NS a.ns.apple.com 2620:149:ae0::53
[*] NS c.ns.apple.com 204.19.119.1
[*] NS c.ns.apple.com 2620:171:800:714::1
[*] NS d.ns.apple.com 204.26.57.1
[*] NS d.ns.apple.com 2620:171:801:714::1
[*] MX mx-in.g.apple.com 17.32.222.242
[*] MX mx-in-crk.apple.com 17.72.136.242
[*] MX mx-in-mdn.apple.com 17.32.222.242
[*] MX mx-in-rno.apple.com 17.179.253.242
[*] MX mx-in-hfd.apple.com 17.57.165.2
[*] MX mx-in-vib.apple.com 17.57.170.2
[*] A apple.com 17.253.144.10
[*] AAAA apple.com 2620:149:af0::10
[*] TXT apple.com 77a4a6de-da14-449c-83c4-85366e0f55f9
[*] TXT apple.com apple-domain-verification=X5Jt76bn3Dnmgzjj
```

[\*] Enumerating SRV Records

```
[+] SRV _sips._tcp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.48.136 5061
[+] SRV _sips._tcp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.71 5061
[+] SRV _sip._udp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.71 5060
[+] SRV _sip._udp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.79 5060
[+] SRV _sip._tcp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.79 5060
[+] SRV _sip._tcp.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.48.136 5060
[+] SRV _sip._tls.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.72 5060
[+] SRV _sip._tls.apple.com gslb-b2b-ext.v.aaplimg.com 17.47.49.70 5060
[+] 8 Records Found
```



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

```
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX4.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
alltcpportsoopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
```



```
Trying Zone Transfer for zonetransfer.me on nszstm2.digi.ninja ...
zonetransfer.me.      7200      IN      SOA      (
zonetransfer.me.      300      IN      HINFO     "Casio
zonetransfer.me.      301      IN      TXT      (
zonetransfer.me.      7200      IN      MX        0
zonetransfer.me.      7200      IN      MX        10
zonetransfer.me.      7200      IN      MX        10
zonetransfer.me.      7200      IN      MX        20
zonetransfer.me.      7200      IN      MX        20
zonetransfer.me.      7200      IN      MX        20
zonetransfer.me.      7200      IN      MX        20
zonetransfer.me.      7200      IN      A        5.196.105.14
zonetransfer.me.      7200      IN      NS        nszstm1.digi.ninja.
zonetransfer.me.      7200      IN      NS        nszstm2.digi.ninja.
_acme-challenge.zonetransfer.me. 301      IN      TXT      (
_acme-challenge.zonetransfer.me. 301      IN      TXT      (
_sip._tcp.zonetransfer.me. 14000    IN      SRV       0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200      IN      PTR       www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900      IN      AFSDB     1
asfdbbbox.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::
```

```
intns1.zonetransfer.me. 300      IN      A         81.4.108.41
intns2.zonetransfer.me. 300      IN      A         52.91.28.78
office.zonetransfer.me. 7200      IN      A         4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200      IN      AAAA      2001:67c:2e8:11::c100:1332
owa.zonetransfer.me. 7200      IN      A         207.46.197.32
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:~$ spiderfoot -l 0.0.0.0:1234
```

```
2023-03-12 20:35:09,884 [INFO] sf : Starting web server at 0.0.0.0:1234 ...
```

```
*****
```

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

```
*****
```

```
2023-03-12 20:35:09,906 [WARNING] sf :
```

```
*****
```

```
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
```

```
*****
```



127.0.0.1:1234/newscan#

spiderfootNew ScanScansSettingsLight ModeAbout

## New Scan

Scan Name

Recon

Scan Target

microsoft.com

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. `example.com`

IPv4 Address: e.g. `1.2.3.4`

IPv6 Address: e.g. `2606:4700:4700::1111`

Hostname/Sub-domain: e.g. `abc.example.com`

Subnet: e.g. `1.2.3.0/24`

Bitcoin Address: e.g. `1HesYJSP1QcQyPEjRQ9vzBL1wujruNGe7R`

E-mail address: e.g. `bob@example.com`

Phone Number: e.g. `+12345678901` (E.164 format)

Human Name: e.g. `"John Smith"` (must be in quotes)

Username: e.g. `"jsmith2000"` (must be in quotes)

Network ASN: e.g. `1234`

By Use Case

By Required Data

By Module

☐ All

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

☐ Footprint

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

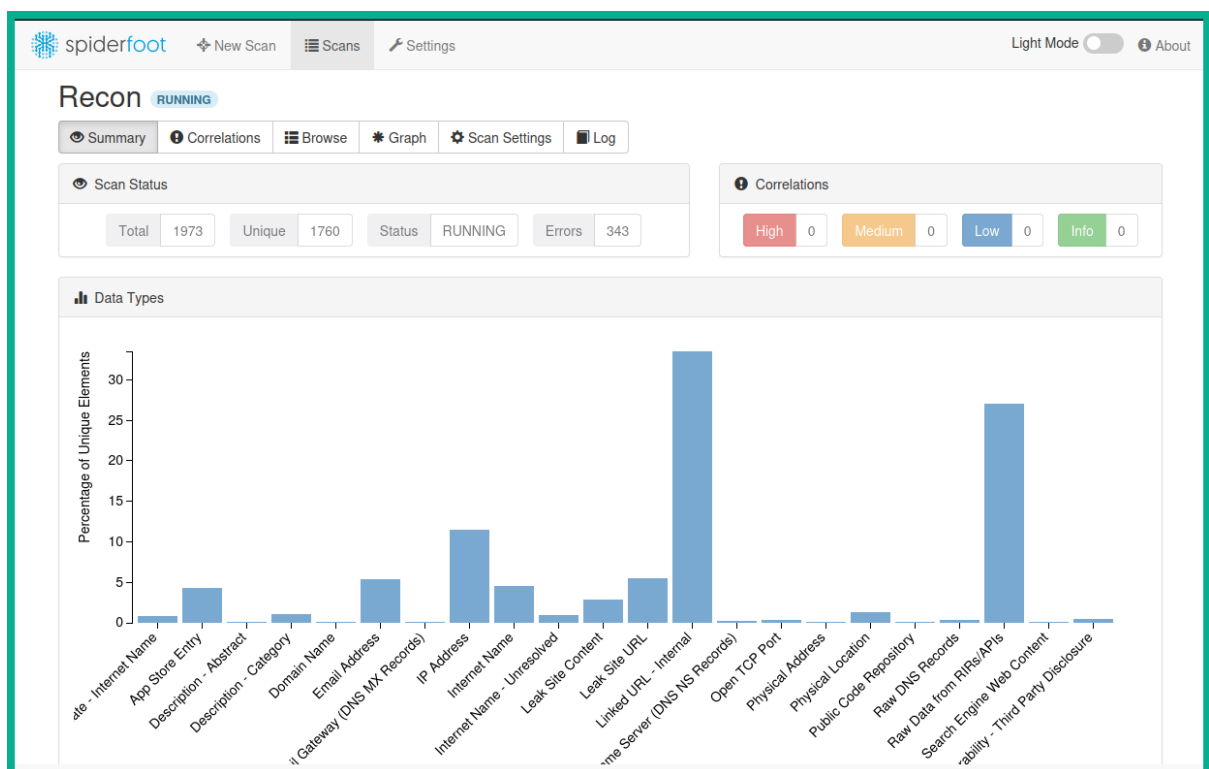
☐ Investigate

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

☒ Passive

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

Run Scan Now





New Scan

Scans

Settings

Light Mode

About

Recon

RUNNING

Summary

Correlations

Browse

Graph

Scan Settings

Log

↺

⬇

Search...

Q

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Internet Name	14	14	2023-03-06 13:19:51
App Store Entry	74	74	2023-03-06 13:20:09
Description - Abstract	1	2	2023-03-06 13:19:49
Description - Category	18	36	2023-03-06 13:19:49
Domain Name	1	4	2023-03-06 13:19:20
Email Address	94	94	2023-03-06 13:20:45
Email Gateway (DNS MX Records)	1	1	2023-03-06 13:18:11
IP Address	201	206	2023-03-06 13:19:20
Internet Name	94	106	2023-03-06 13:22:33
Internet Name - Unresolved	38	38	2023-03-06 13:22:33
Leak Site Content	50	54	2023-03-06 13:20:54
Leak Site URL	96	96	2023-03-06 13:20:56

Recon

RUNNING

Summary

Correlations

Browse

Graph

Scan Settings

Log

⌂

⌵

⌶

⌷

↺

⬇

Search...

Q

Browse

Internet Name

<input type="checkbox"/> Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/> <code>_.aks.skylight.services.microsoft.com</code>	<code>www.microsoft.com</code>	<code>sfp_mnemonic</code>	2023-03-06 13:20:03
<input type="checkbox"/> <code>_.skylight.services.microsoft.com</code>	<code>www.microsoft.com</code>	<code>sfp_mnemonic</code>	2023-03-06 13:20:05
<input type="checkbox"/> <code>aad.microsoft.com</code>	<code>www.microsoft.com</code>	<code>sfp_mnemonic</code>	2023-03-06 13:20:04
<input type="checkbox"/> <code>academic.microsoft.com</code>	<code>microsoft.com</code>	<code>sfp_flickr</code>	2023-03-06 13:19:05
<input type="checkbox"/> <code>adlab.microsoft.com</code>	<code>microsoft.com</code>	<code>sfp_flickr</code>	2023-03-06 13:19:03
<input type="checkbox"/> <code>advertising.microsoft.com</code>	<code>microsoft.com</code>	<code>sfp_flickr</code>	2023-03-06 13:19:18
<input type="checkbox"/> <code>answers.microsoft.com</code>	<code>microsoft.com</code>	<code>sfp_flickr</code>	2023-03-06 13:19:17
<input type="checkbox"/> <code>apps.microsoft.com</code>	<code>microsoft.com</code>	<code>sfp_flickr</code>	2023-03-06 13:19:18



# Recon

RUNNING

Summary

Correlations

Browse

Graph

Scan Settings

Log



Search...



Browse / Physical Location

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	Amsterdam, North Holland, Netherlands	microsoft.com	sfp_leakix	2023-03-06 13:18:15
<input type="checkbox"/>	Boynton, Virginia, United States	microsoft.com	sfp_leakix	2023-03-06 13:18:15
<input type="checkbox"/>	Campinas, Sao Paulo, Brazil	microsoft.com	sfp_leakix	2023-03-06 13:18:15
<input type="checkbox"/>	Cardiff, Cardiff, United Kingdom	microsoft.com	sfp_leakix	2023-03-06 13:18:15
<input type="checkbox"/>	Central, Central and Western District, Hong Kong	microsoft.com	sfp_leakix	2023-03-06 13:18:15
<input type="checkbox"/>	Cheyenne, Wyoming, United States	microsoft.com	sfp_leakix	2023-03-06 13:18:15



# Chapter 5: Organizational Infrastructure Intelligence

## What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://microsoft.com/

Example: https://www.netcraft.com

Look up

Background			
Site title	Microsoft – Cloud, Computers, Apps & Gaming	Date first seen	May 2004
Site rank	47874	Netcraft Risk Rating	7/10
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	Primary language	English
Network			
Site	https://microsoft.com	Domain	microsoft.com
Netblock Owner	Microsoft Corporation	Nameserver	ns1-39.azure-dns.com
Hosting company	Microsoft - US Central (Iowa) datacenter	Domain registrar	markmonitor.com
Hosting country	us	Nameserver organisation	whols.markmonitor.com
IPv4 address	20.84.181.62 (VirusTotal)	Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS8075	DNS admin	azuredns-hostmaster@microsoft.com

Organisation	Microsoft Corporation
State	WA
Country	US
Organisational unit	Not Present
Subject Alternative Name	► microsoft.com, s.microsoft.com, ga.microsoft.com, aep.microsoft.com, aer.microsoft.com, grv.microsoft.com, hup.microsoft.com, mac.microsoft.com, mkb.microsoft.com, pme.microsoft.com, pmi.microsoft.com and 117 more



## Hosting History

Netblock owner	IP address	OS	Web server	Last seen
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.112.52.29	Linux	Kestrel	15-Mar-2023
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.84.181.62	Linux	Kestrel	7-Mar-2023
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.81.111.85	Linux	Kestrel	26-Feb-2023
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.112.52.29	Linux	Kestrel	17-Feb-2023
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.81.111.85	Linux	Kestrel	9-Feb-2023
<a href="#">Microsoft Corporation One Microsoft Way Redmond WA US 98052</a>	20.112.52.29	Linux	Kestrel	26-Jan-2023

## Search Web by Domain

Explore websites visited by users of the **Netcraft** extensions [↗](#)

Site contains



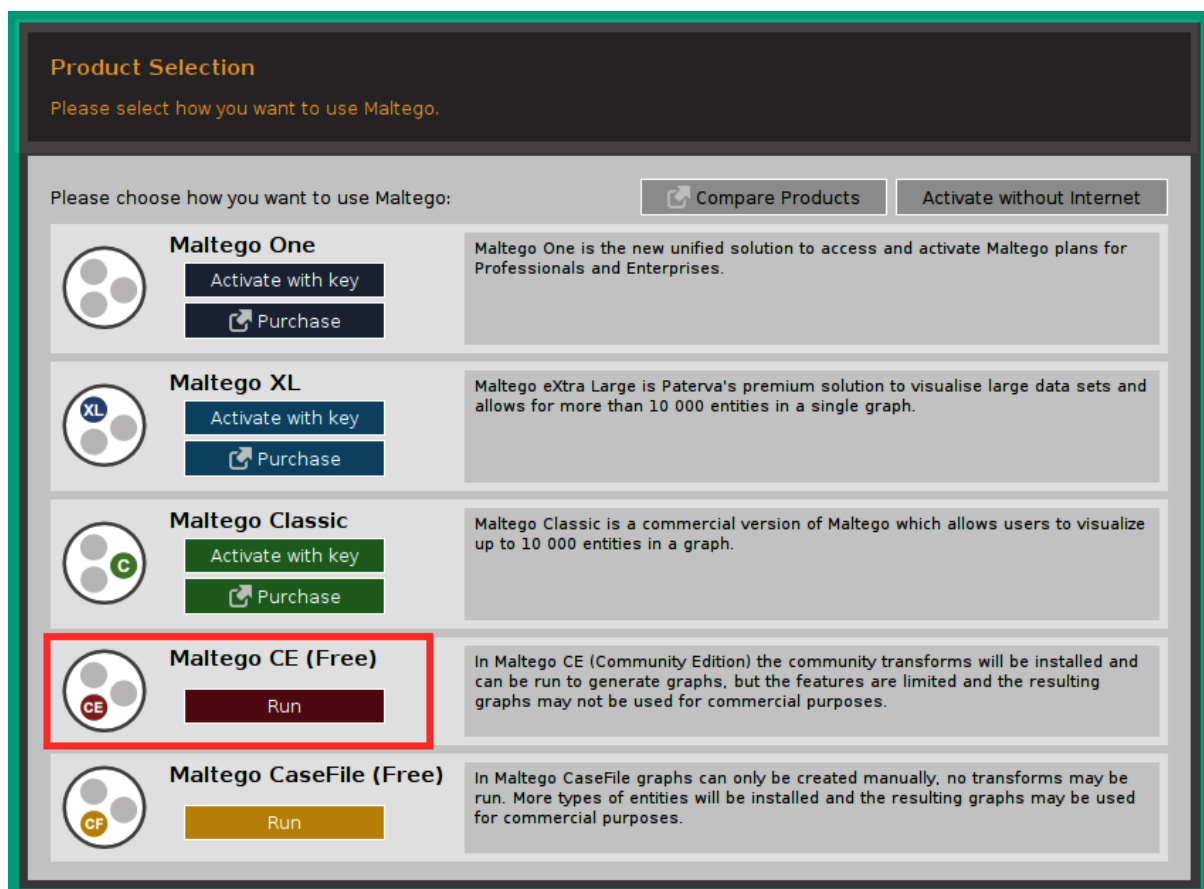
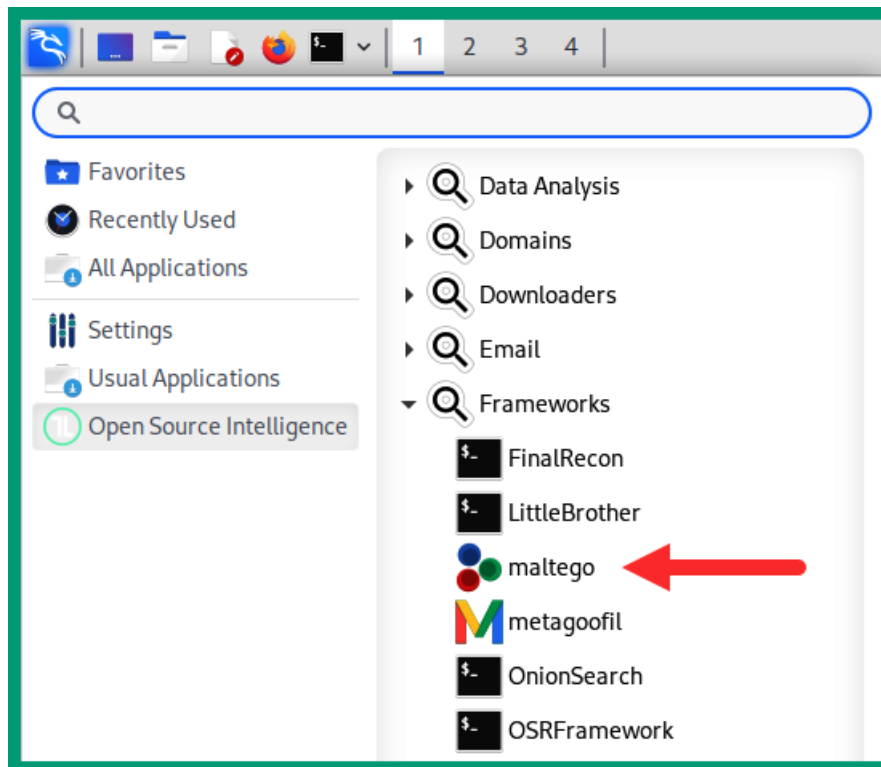
[.microsoft.com](#)

Example: site contains [.netcraft.com](#)

Search

Rank	Site	First seen	Netblock	OS	Site Report
32	<a href="#">teams.microsoft.com</a> <a href="#">↗</a>	November 2016	<a href="#">Microsoft Corporation</a>	<a href="#">Windows Server 2008</a>	<a href="#">📄</a>
40	<a href="#">learn.microsoft.com</a> <a href="#">↗</a>	July 2015	<a href="#">Akamai International, BV</a>	<a href="#">unknown</a>	<a href="#">📄</a>
66	<a href="#">support.microsoft.com</a> <a href="#">↗</a>	October 1997	<a href="#">Akamai Technologies</a>	<a href="#">unknown</a>	<a href="#">📄</a>
92	<a href="#">www.microsoft.com</a> <a href="#">↗</a>	August 1995	<a href="#">Akamai Technologies, Inc.</a>	<a href="#">Linux</a>	<a href="#">📄</a>
169	<a href="#">admin.microsoft.com</a> <a href="#">↗</a>	November 2017	<a href="#">Microsoft Corporation</a>	<a href="#">Windows Server 2008</a>	<a href="#">📄</a>
180	<a href="#">security.microsoft.com</a> <a href="#">↗</a>	December 2006	<a href="#">Microsoft Corporation</a>	<a href="#">Windows Server 2008</a>	<a href="#">📄</a>
202	<a href="#">answers.microsoft.com</a> <a href="#">↗</a>	August 2009	<a href="#">Akamai International, BV</a>	<a href="#">Linux</a>	<a href="#">📄</a>







Configure Maltego

STEPS

1. License Agreement

2. Login

3. Login Result

4. Install Transforms

5. Help Improve Maltego

6. Web Browser Options

LICENSE AGREEMENT: Please read and accept the following License Agreement.

General Terms and Conditions for Software Licenses and Accompanying Services

Effective November 2022

These General Terms and Conditions for Software Licenses and Accompanying Services ("General Terms and Conditions") apply to software distributed and accompanying services provided by Maltego Technologies GmbH, a company registered in the district court Munich, Germany under no. HRB 236523 (hereinafter referred to as "Licensor") to its customers (hereinafter referred to as "Licensee").

Unless agreed otherwise Licensor distributes software licenses by way of Subscription Plans. By subscribing to a Subscription Plan Licensee acquires temporary rights to use software and will be given access to optional Accompanying Services. The specific scope of each Subscription Plan is specified on Licensor's website. In addition, these General Terms and Condition apply. (Licensor and Licensee also referred to as "Party" and collectively the "Parties").

I. Software Licenses

1. Scope of Software Licenses

1.1. By subscribing to a Subscription Plan Licensee will be granted a worldwide, non-exclusive, non-transferrable and non-sublicensable right to temporarily use the respective Software for Licensee's

☒ Accept

< Back

Next >

Finish

Cancel

Configure Maltego

STEPS

1. License Agreement

2. Login

3. Login Result

4. Install Transforms

5. Help Improve Maltego

6. Web Browser Options

LOGIN: Please log in to use the free online version of Maltego.

Enter your details below to log in to the Maltego Community Server

Or if you have not done so yet, [register here](#)


Login

\* Email Address

\*\*\*\*\*

Password

\*\*\*\*\*



\* Solve captcha

xSAA

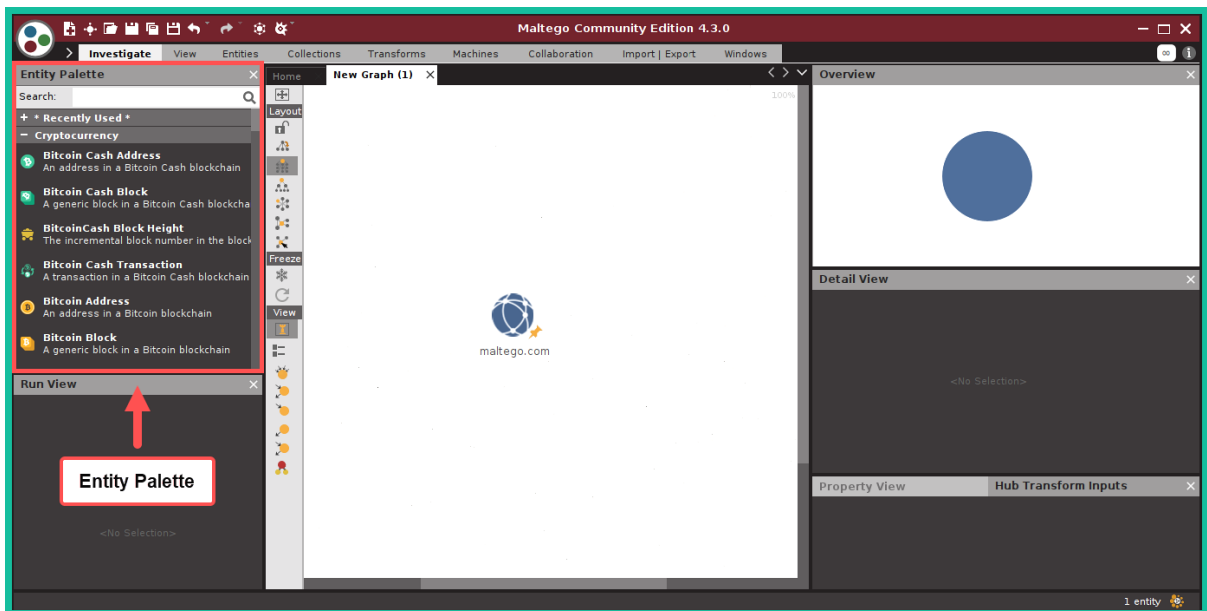
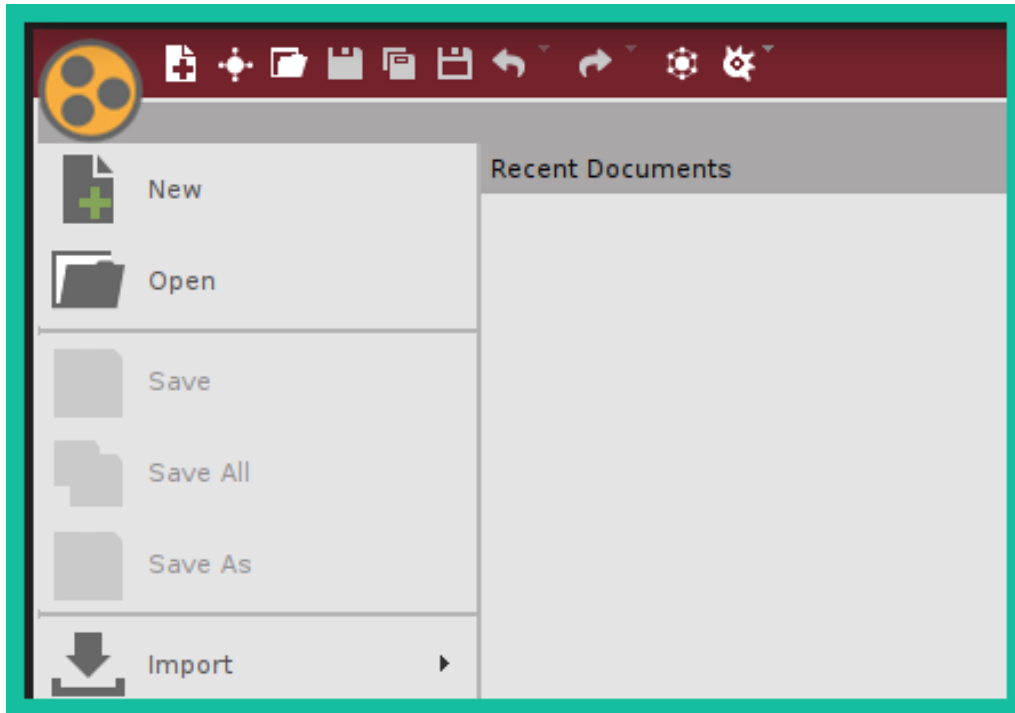
< Back

Next >

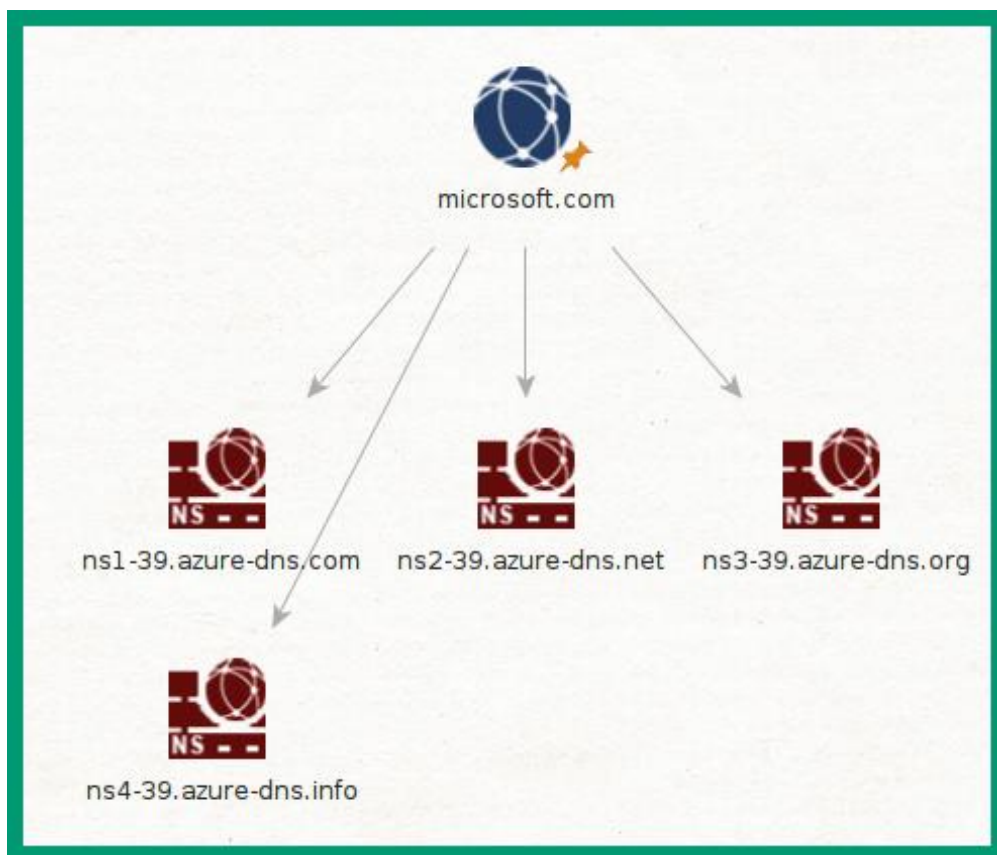
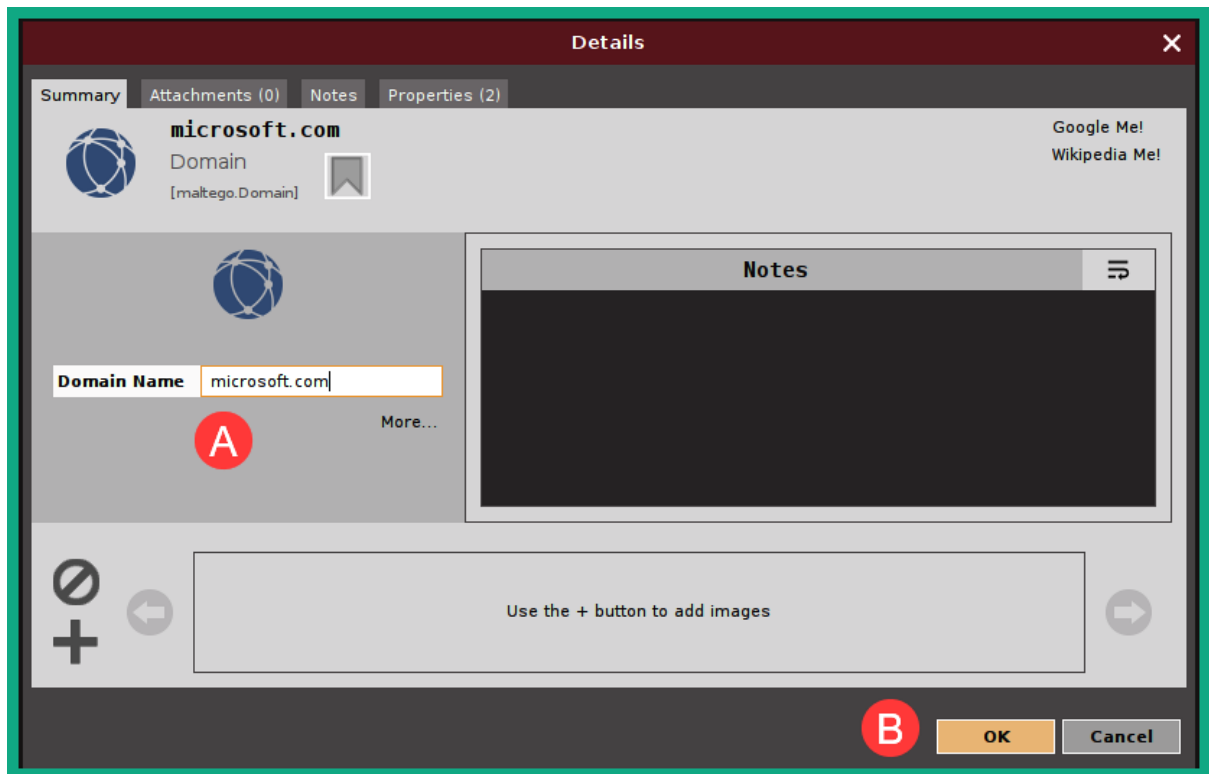
Finish

Cancel

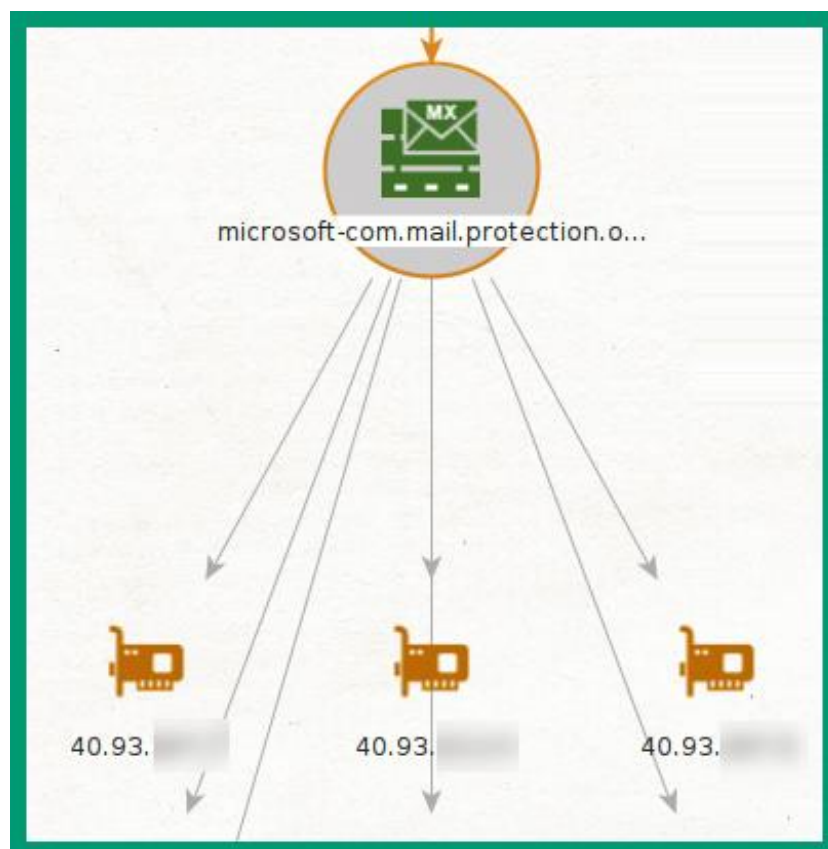
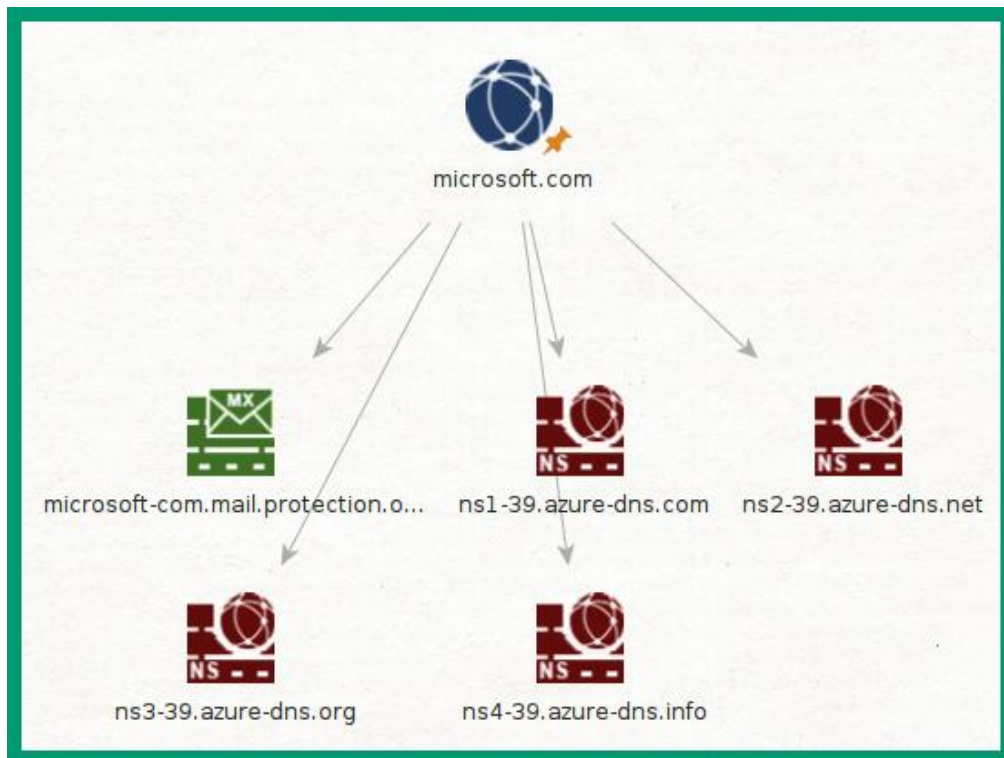




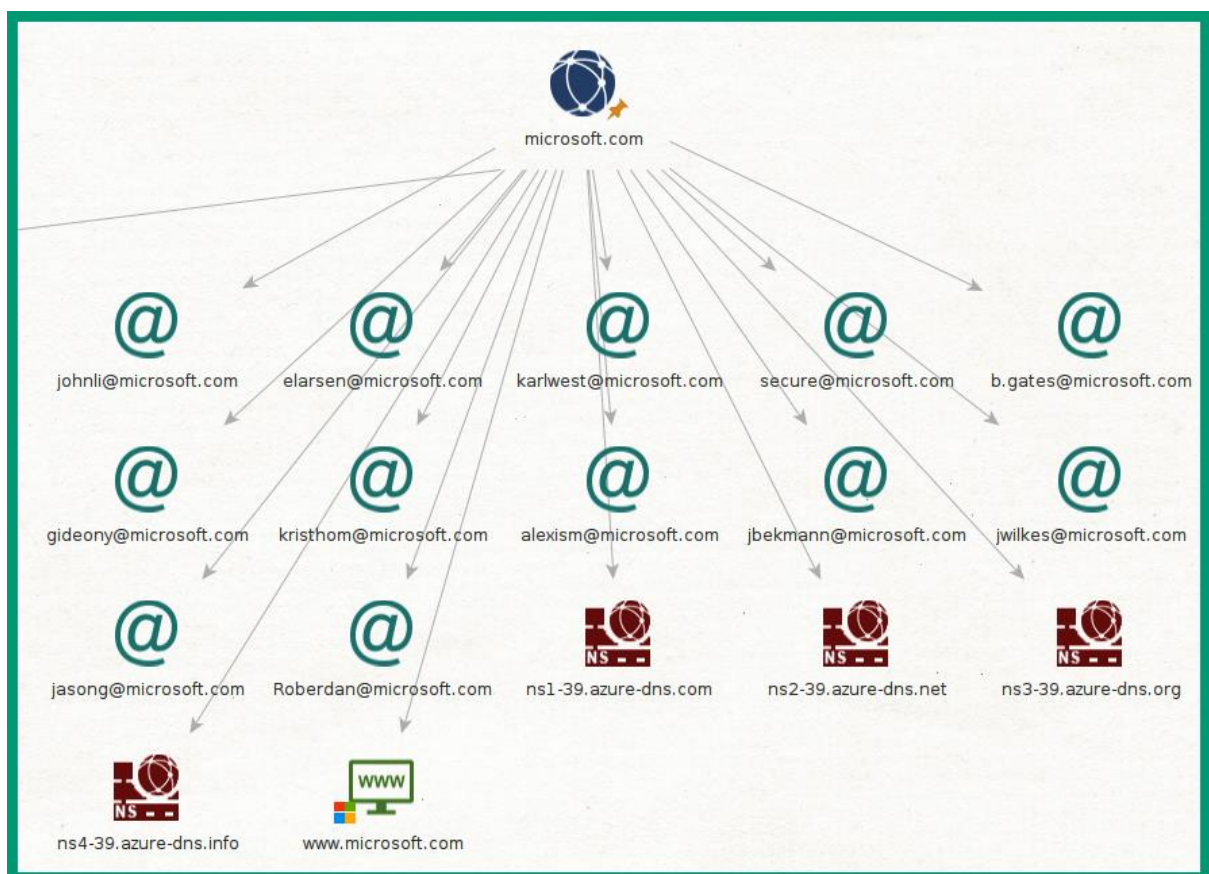
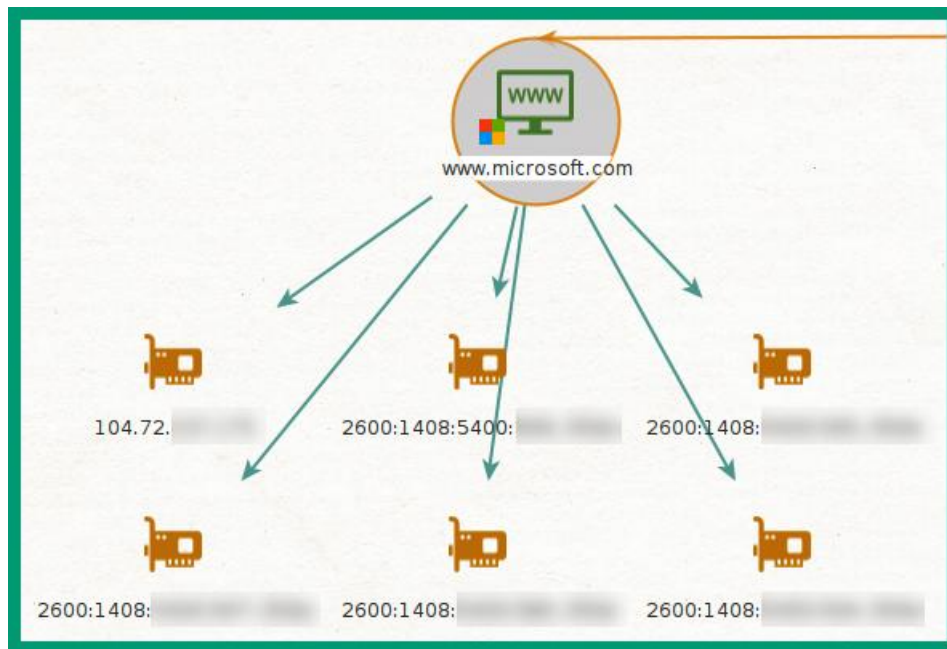




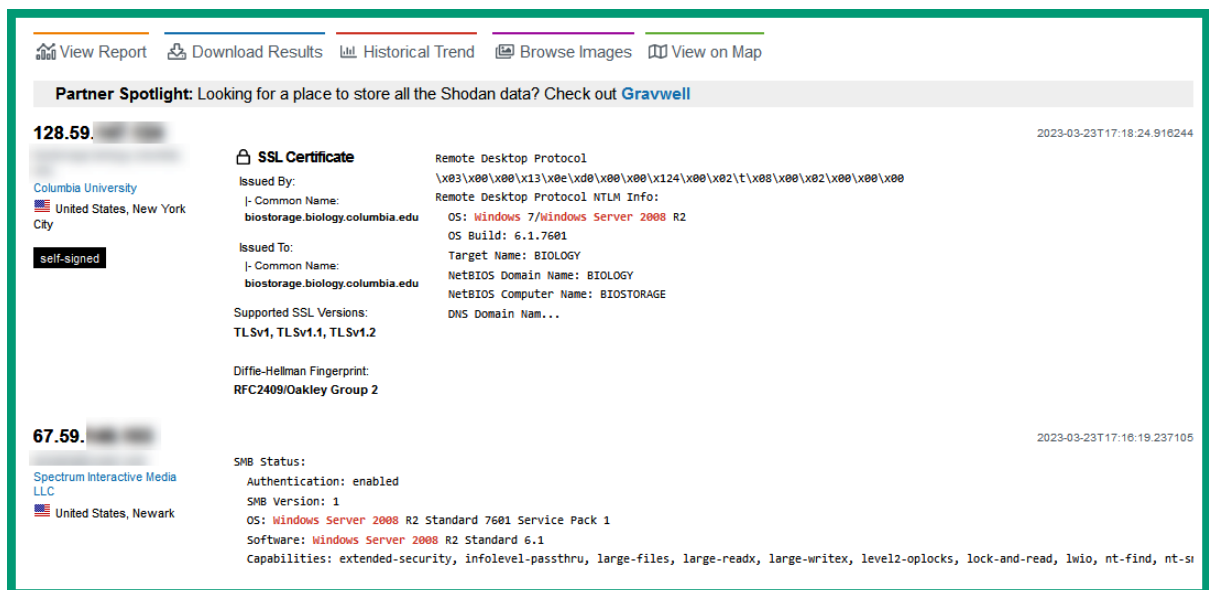
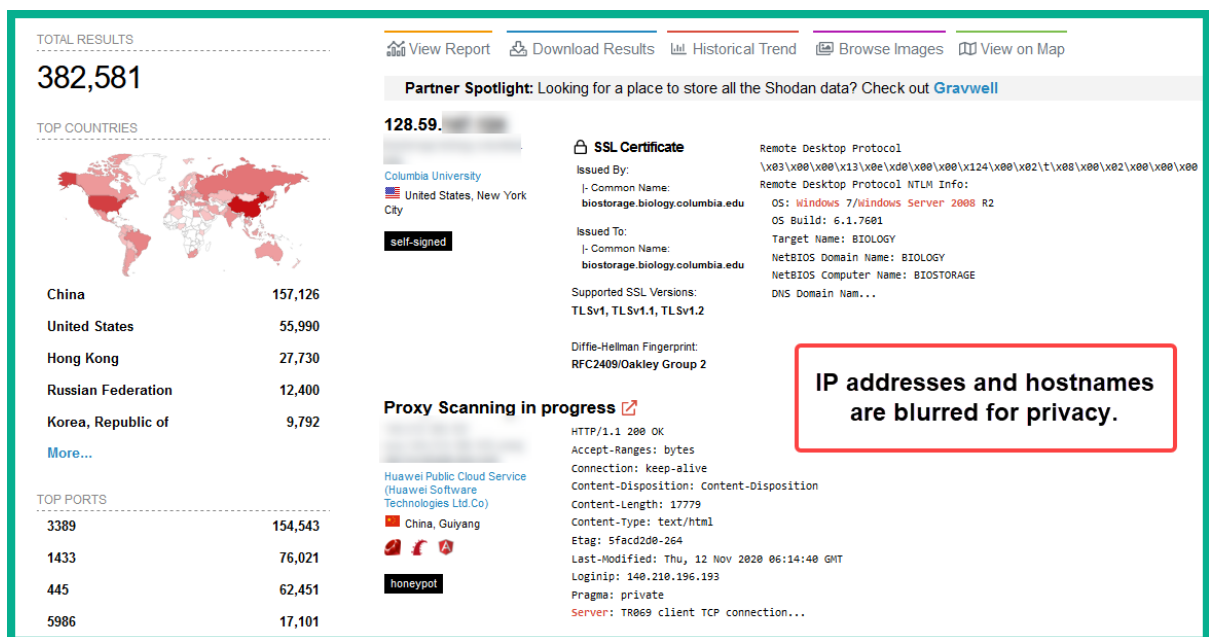
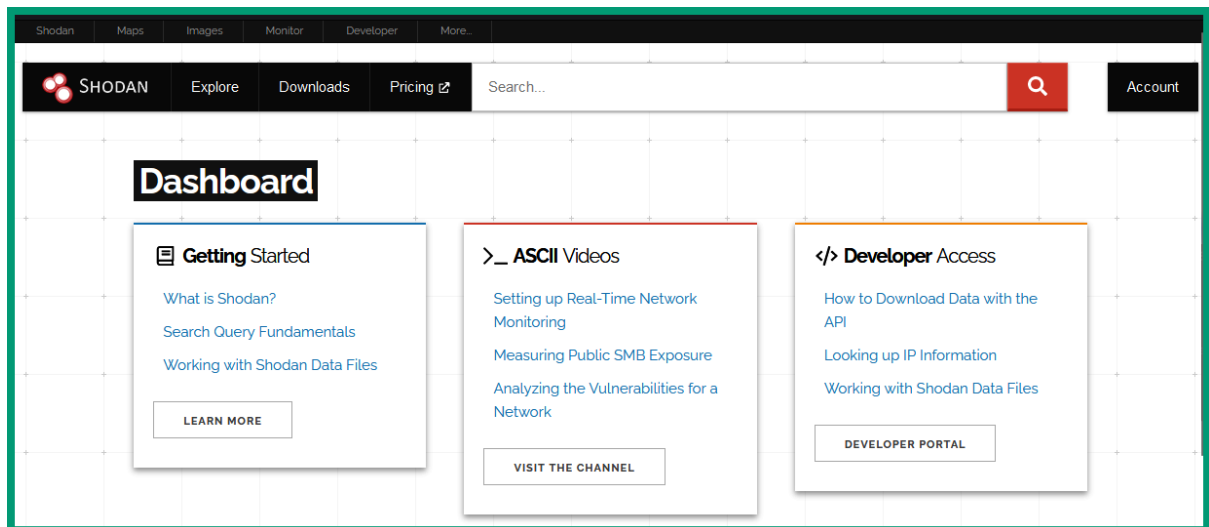














View Report

Download Results

Historical Trend

Browse Images

View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

84.40.

Hostway TPA FL

United States, Tampa

self-signed

SSL Certificate

Issued By:

- Common Name:

wtf4637.tam.us.siteprotect.com

Issued To:

- Common Name:

wtf4637.tam.us.siteprotect.com

Supported SSL Versions:

TLV1.2

Remote Desktop Protocol

Remote Desktop Protocol NTLM Info:

OS: Windows 7/Windows Server 2008 R2

OS Build: 6.1.7601

Target Name: WTF4637

NetBIOS Domain Name: WTF4637

NetBIOS Computer Name: WTF4637

DNS Domain Name...

2023-03-23T17:14:02.027947

84.40.

Beach

Largo

Regular View

Raw Data

History

// TAGS: self-signed

General Information

Hostnames

Domains

Country

United States

City

Tampa

Organization

ISP

Affinity Internet, Inc

ASN

AS3064

Operating System

Windows Server 2008 R2 Standard



## Open Ports

80

135


137

139

443

445

3389

// 80 / TCP 

-1188089910 | 2023-03-20T18:37:37.149034

### Microsoft IIS httpd 7.5

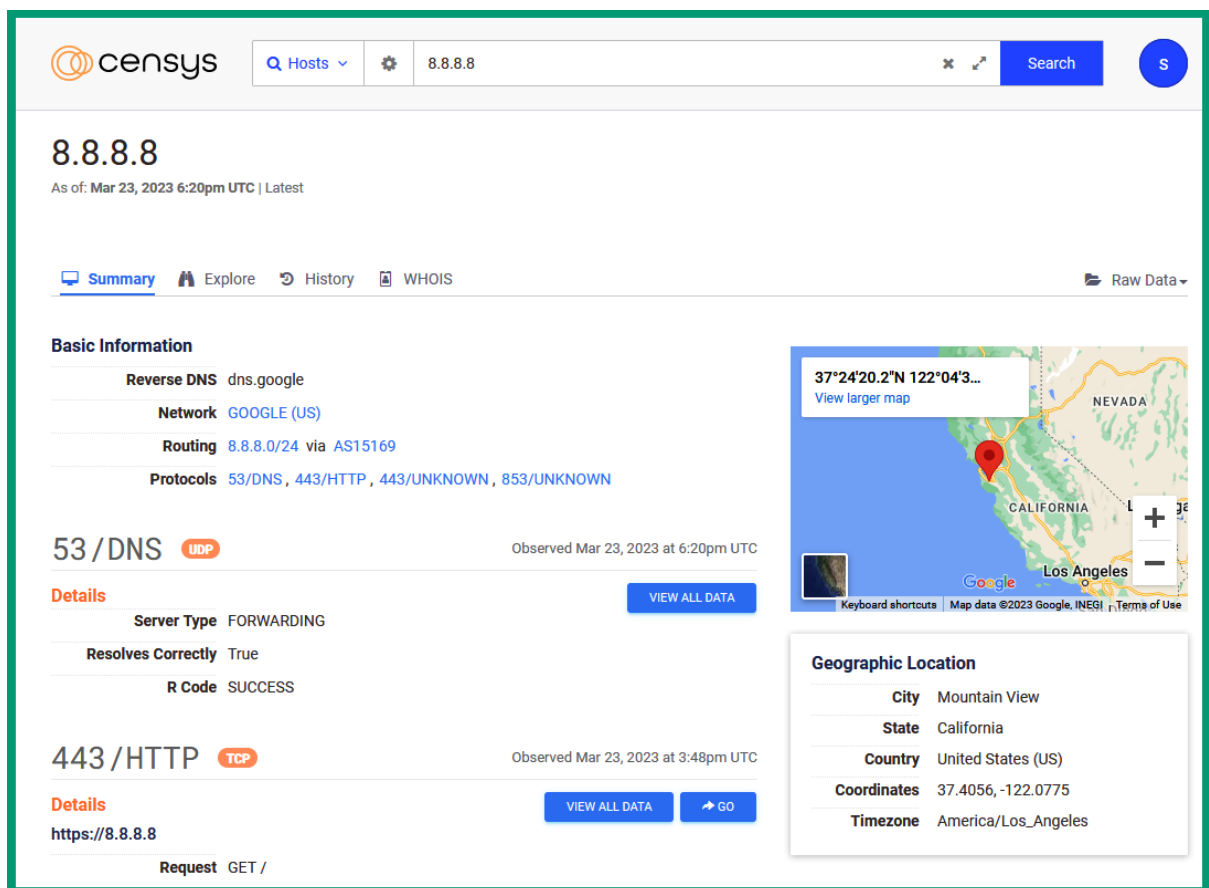
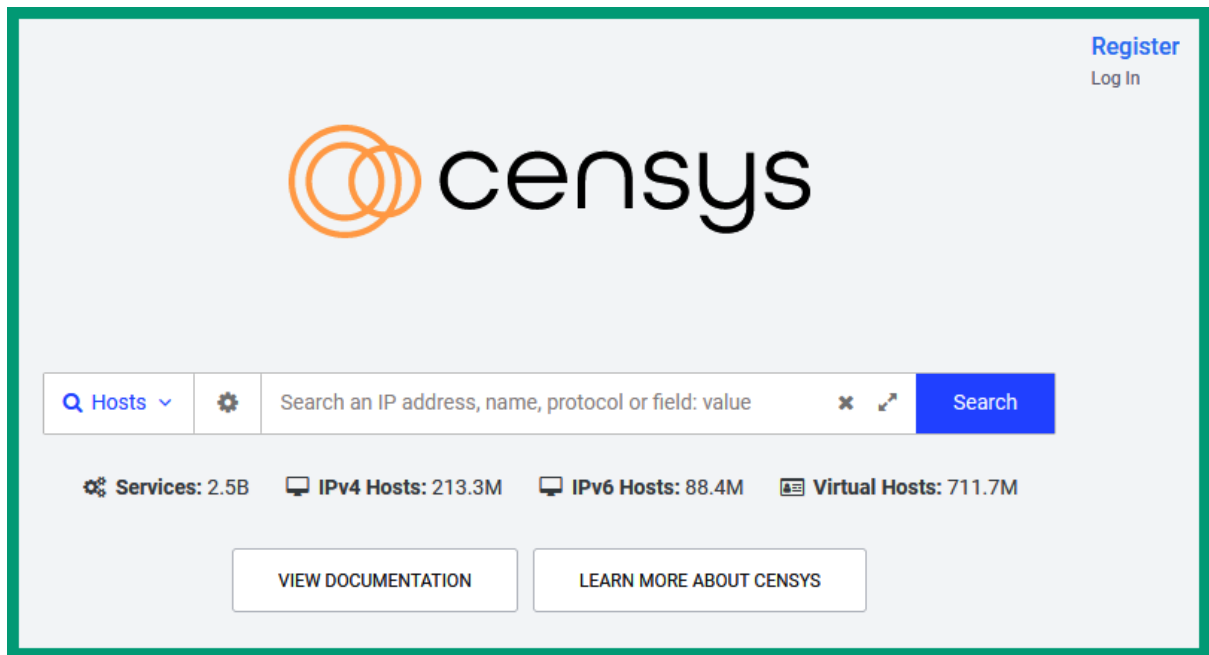
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=43ym0n45pqbbcu3fet4jqon0; path=/; HttpOnly
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Mon, 20 Mar 2023 18:37:33 GMT
Content-Length: 6558
```

## Vulnerabilities

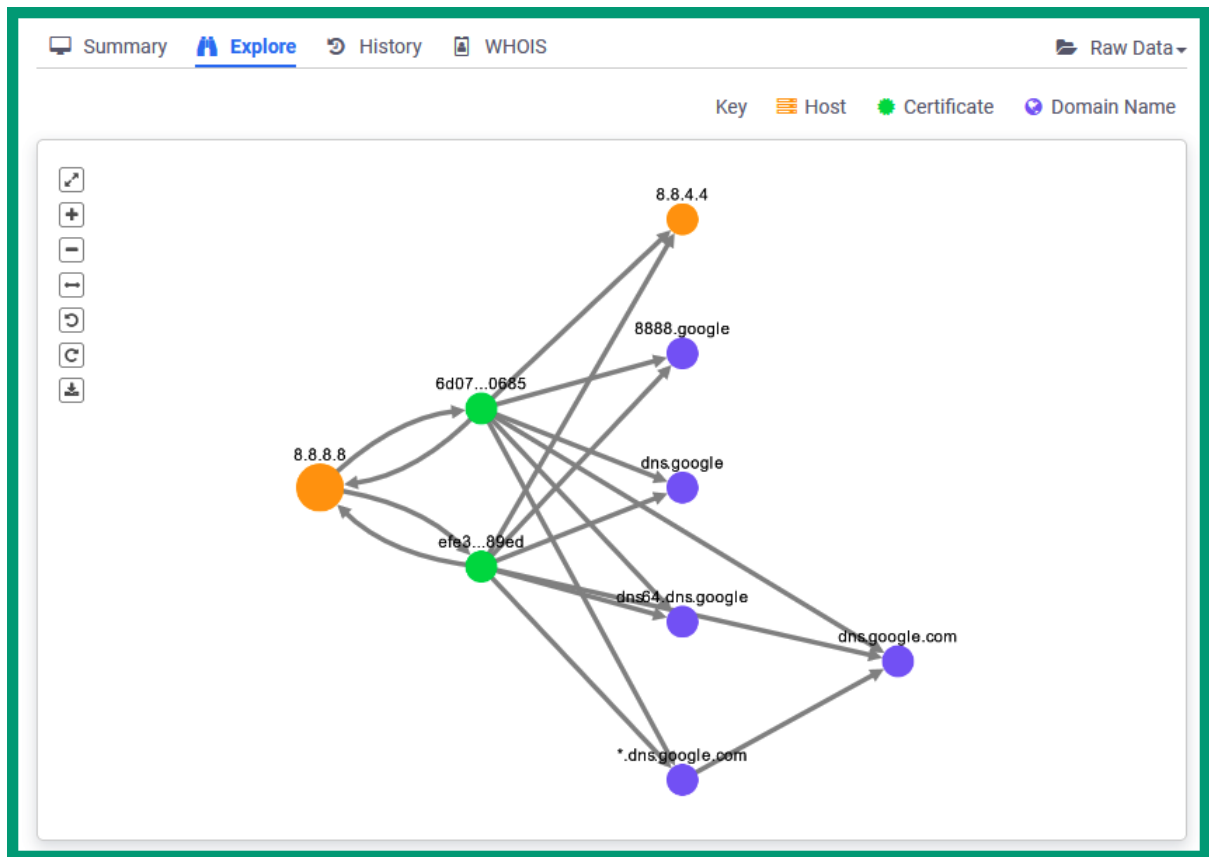
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

- |                      |  |
|----------------------|--|
| <b>CVE-2010-2730</b> | Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."   |
| <hr/>                |  |
| <b>CVE-2010-3972</b> | Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information. |
| <hr/>                |  |
| <b>CVE-2010-1899</b> | Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."  |









Summary Explore History WHOIS Raw Data

<b>Basic Information</b>	
ASN	15169
ASN CIDR	8.8.8.0/24
Entities	GOGL
ASN Country	US
Registry	arin
<b>Network</b>	
Name	LVLT-GOGL-8-8-8
Type	ALLOCATION
Handle	NET-8-8-8-0-1
Parent	NET-8-0-0-0-1
CIDR	8.8.8.0/24 (v4)
<b>Events</b>	
Last Changed	2014-03-14 16:52:05-04:00
Registration	2014-03-14 16:52:05-04:00
<b>Notices</b>	
Terms of Service	By using the ARIN RDAP/Whois service, you are agreeing to the RDAP/Whois Terms of Use

### GOGL (registrant)

<b>Contact Information</b>	
Name	Google LLC (org)
Address	1600 Amphitheatre Parkway Mountain View CA 94043 United States
<b>Other Information</b>	
Entities	ABUSE5250-ARIN, ZG39-ARIN
Remarks	<b>Registration Comments</b> Please note that the recommended way to file abuse complaints are located in the following links. To report abuse and illegal activity: <a href="https://www.google.com/contact/">https://www.google.com/contact/</a> For legal requests: <a href="http://support.google.com/legal">http://support.google.com/legal</a> Regards, The Google Team
Links	<a href="https://rdap.arin.net/registry/entity/GOGL">https://rdap.arin.net/registry/entity/GOGL</a> <a href="https://whois.arin.net/rest/org/GOGL">https://whois.arin.net/rest/org/GOGL</a>

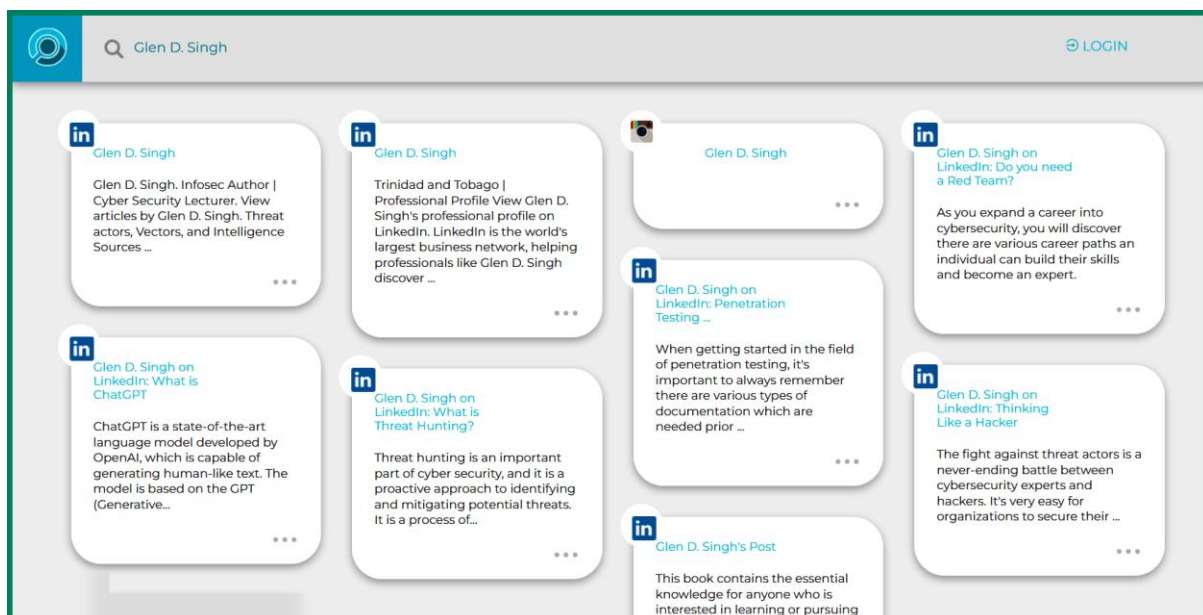


## **JOB REQUIREMENTS**

### **Knowledge/Experience:**

- Bachelor's degree in Computer Science, Information Technology or related field.
- Minimum three (3) years' experience in a supervisory or managerial role.
- Be thoroughly familiar with all aspects of the technology environment.
- Extensive knowledge of and experience with (but not limited to):

1. Cloud-based infrastructure
2. Microsoft 365 proficient including Azure AD
3. Wireless networks
4. Routing, Switching, Firewalls, VPNs
5. Windows Server Environments
6. Backup and disaster recovery systems
7. Network/workstation peripherals; print servers; firewalls, ticketing software; project and task management software and computer hardware.





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

+ 3dnews: http://forum.3dnews.ru/member.php?username=microsoft
+ 7Cups: https://www.7cups.com/@microsoft
+ 8tracks: https://8tracks.com/microsoft
+ 9GAG: https://www.9gag.com/u/microsoft
+ About.me: https://about.me/microsoft
+ Academia.edu: https://independent.academia.edu/microsoft
+ Alik.cz: https://www.alik.cz/u/microsoft
+ AllMyLinks: https://allmylinks.com/microsoft
+ Anilist: https://anilist.co/user/microsoft/
```

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

kali@kali:~/sherlock$ cat microsoft.txt
http://forum.3dnews.ru/member.php?username=microsoft
https://www.7cups.com/@microsoft
https://8tracks.com/microsoft
https://www.9gag.com/u/microsoft
https://about.me/microsoft
https://independent.academia.edu/microsoft
https://www.alik.cz/u/microsoft
https://allmylinks.com/microsoft
https://anilist.co/user/microsoft/
https://developer.apple.com/forums/profile/microsoft
```



facebook

Log In



**Mark Zuckerberg** ✓

Friends   Photos   Videos

...

```
{ "__dr": "ProfileCometRoot.react" }, "resource":
{ "__dr": "ProfileCometLoggedOutRoot.react" }, "props":
{ "collectionToken": "YXBwX2NvbGx1Y3Rpb246NDoyMzI3MTU4MjI3OjIwMg==", "userID": "4", "userVanity": "zuck", "viewerID": "0", "eligibleForProfilePlusEntityMenu": false, "cometLoginUpsellType": null }, "entryPoint":
{ "__dr": "ProfileCometLoggedOutRouteRoot.entrypoint" }, "tracePolicy": "comet.profile.logged_out", "meta": { "title": "Mark Zuckerberg", "accessory": null, "favicon": null }, "prefetchable": true, "timeSpentConfig": { "has_profile_session_id": true }, "entityKeyConfig": { "entity_type": { "source": "constant", "value": "profile", "entity_id": { "source": "prop", "value": "userID", "section": { "source": "constant", "value": "timeline" } }, "hostableView": { "allResources": [ { "__dr": "ProfileCometLoggedOutRoot.react" }, { "__dr": "ProfileCometLoggedOutRouteRoot.entrypoint" }, { "__dr": "ProfileCometRoot.react" } ], "resource": { "__dr": "ProfileCometLoggedOutRoot.react" }, "props": { "collectionToken": "YXBwX2NvbGx1Y3Rpb246NDoyMzI3MTU4MjI3OjIwMg==", "userID": "4", "userVanity": "zuck", "viewerID": "0", "eligibleForProfilePlusEntityMenu": false, "cometLoginUpsellType": null }, "entryPoint":
```



IntelligenceX

[About](#) [Product](#) [Blog](#) [Tools](#) [Integrations](#) [Login](#) [Sign up](#)

Third Party Search:

[General](#)  
[Email](#)  
[Domain](#)  
[IP](#)  
[Bitcoin](#)  
[Image](#)  
[Username](#)  
[Person](#)  
[Phone Number](#)  
[Location 2 Map](#)  
[File](#)  
[VIN](#)  
[Hash](#)  
[Google Analytics](#)  
[Google AdSense](#)

## Facebook Graph Searcher

Note: You need to be logged in at Facebook!

### Posts in a particular date

[Search](#)

### Posts in a particular month

[Search](#)

### Posts in an interval

From  to  [Search](#)

### Posts from someone posting about something

ID of the user

Talking about

[Search](#)

Enter the userID value and a keyword.

IntelX Tools:


new york - Facebook Search

[All](#) [Posts](#) [People](#) [Photos](#) [Videos](#) [Pages](#) [Places](#) [Groups](#) [Events](#)

Mark Zuckerberg

October 17, 2016 at 4:29 PM · 🌐

Swoon, New York.



577 comments 710 shares

[Like](#) [Comment](#) [Share](#)

Mark Zuckerberg

May 17, 2016 at 4:12 PM · 🌐

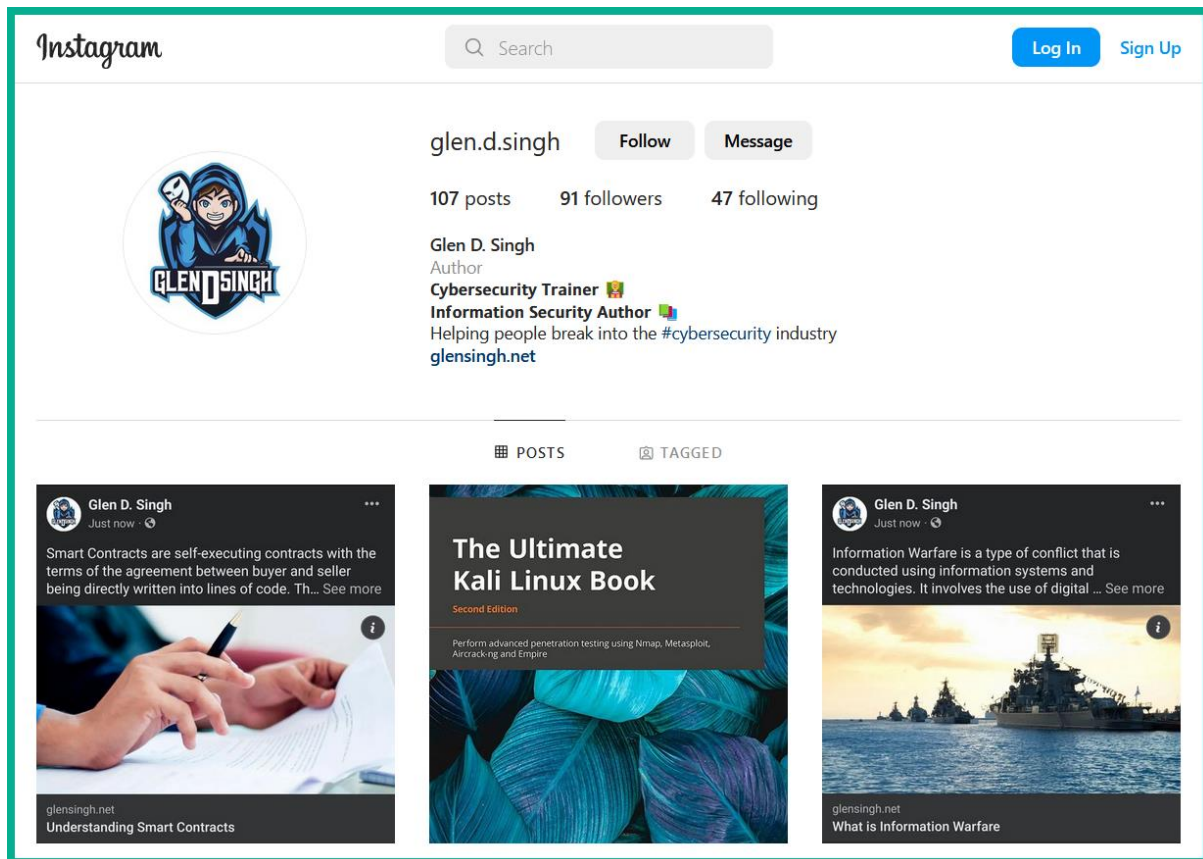
Check out this 360 video of Grand Central Terminal in New York City. It's the first 360 video that we produced and filmed ourselves using our new Surround 360 camera. You can tilt your phone to experience... [More](#)

HELP.FACEBOOK.COM  
360 Video is not yet available for this device.

29K comments 90K shares

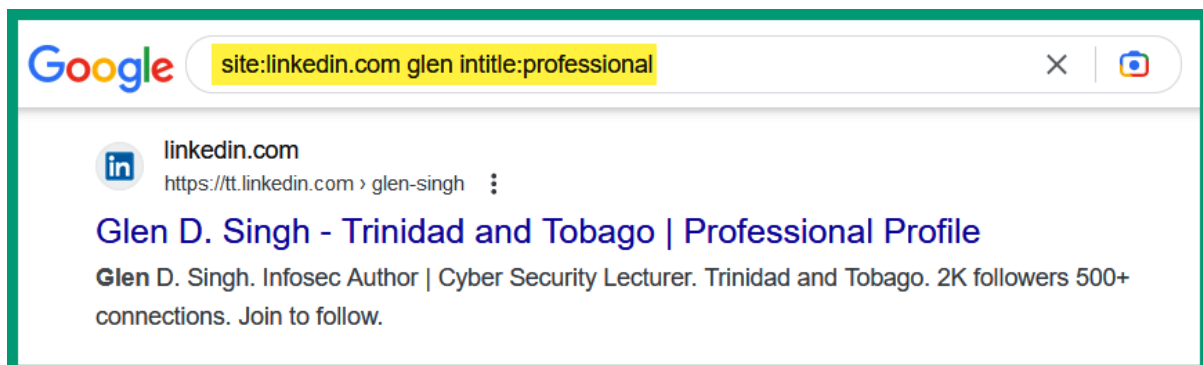
[Like](#) [Comment](#) [Share](#)





```
osint@osint:~$ pwd
/home/osint

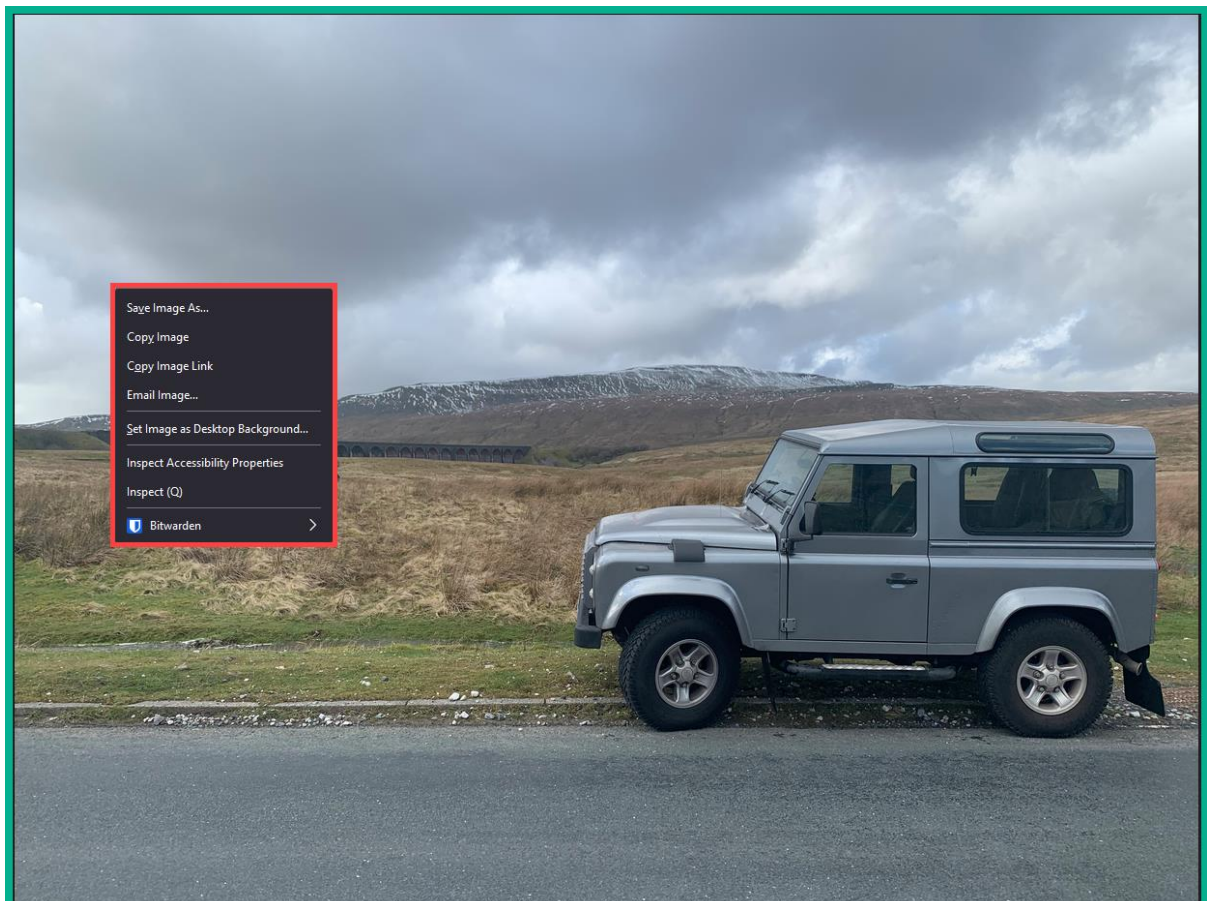
osint@osint:~$ ls /home/osint/zuck
2022-10-17_13-57-43.UTC.json.xz      2022-12-02_15-01-03.UTC.mp4
2022-10-17_13-57-43.UTC.txt        2022-12-02_15-01-03.UTC.txt
2022-10-17_13-57-43.UTC.webp      2022-12-13_15-59-27.UTC.json.xz
2022-10-18_14-34-04.UTC_profile_pic.jpg 2022-12-13_15-59-27.UTC.txt
2022-10-19_15-08-54.UTC.jpg        2022-12-13_15-59-27.UTC.webp
```





## Chapter 6: Imagery, People, and Signals Intelligence

Downloads
Exercise
<b>Exif Example 1</b>
Exif Example 2
Glossary
Image Search Exercise





```
osint@osint:~$ exiftool Downloads/exif1.jpg
ExifTool Version Number      : 12.40
File Name                    : exif1.jpg
Directory                   : Downloads
File Size                   : 5.9 MiB
File Modification Date/Time  : 2023:03:27 11:23:06-04:00
File Access Date/Time       : 2023:03:27 11:23:06-04:00
File Inode Change Date/Time  : 2023:03:27 11:23:06-04:00
File Permissions             : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Make                        : Apple
Camera Model Name           : iPhone XS Max
Orientation                 : Horizontal (normal)
X Resolution                 : 72
Y Resolution                 : 72
```

```
@0x0000792=1938 : <GPS IFD> (in IFD 0) 13 entries starting at file offset 0x794=1940
@0x0000794=1940 : <0x0001= 1> LatitudeRef [2 =ASCII 2] = 'N'
@0x00007a0=1952 : <0x0002= 2> Latitude [5 =RATIONAL 3] = @0x834=2100
@0x00007ac=1964 : <0x0003= 3> LongitudeRef [2 =ASCII 2] = 'W\000'
@0x00007b8=1976 : <0x0004= 4> Longitude [5 =RATIONAL 3] = @0x84c=2124
@0x00007c4=1988 : <0x0005= 5> AltitudeRef [1 =BYTE 1] = 0
@0x00007d0=2000 : <0x0006= 6> Altitude [5 =RATIONAL 1] = @0x864=2148
@0x00007dc=2012 : <0x000c= 12> SpeedRef [2 =ASCII 2] = 'K\000'
@0x00007e8=2024 : <0x000d= 13> Speed [5 =RATIONAL 1] = @0x86c=2156
@0x00007f4=2036 : <0x0010= 16> DirectionRef [2 =ASCII 2] = 'T\000'
@0x0000800=2048 : <0x0011= 17> Direction [5 =RATIONAL 1] = @0x874=2164
@0x000080c=2060 : <0x0017= 23> BearingRef [2 =ASCII 2] = 'T\000'
@0x0000818=2072 : <0x0018= 24> Bearing [5 =RATIONAL 1] = @0x87c=2172
@0x0000824=2084 : <0x001f= 31> GPS_0x001f [5 =RATIONAL 1] = @0x884=2180
@0x0000830=2096 : **** next IFD offset 0
@0x0000834=2100 : ===== VALUES, GPS IFD =====
@0x0000834=2100 : Latitude = 54,12,30.67
@0x000084c=2124 : Longitude = 2,21,41.53
@0x0000864=2148 : Altitude = 280.202
@0x000086c=2156 : Speed = 0
@0x0000874=2164 : Direction = 311.281
@0x000087c=2172 : Bearing = 311.281
@0x0000884=2180 : GPS_0x001f = 4.57993
-0x000088b=2187 : </GPS IFD>
```




FotoForensics

Submit a picture for Forensic Analysis

Image URL:

or

Upload File:  exif1.jpg



FotoForensics

Analysis:

- Digest
- ELA
- Games
- Hidden Pixels
- ICC+
- JPEG %
- Metadata**
- Strings
- Source





## File

File Type	JPEG
File Type Extension	.jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	4032
Image Height	3024
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

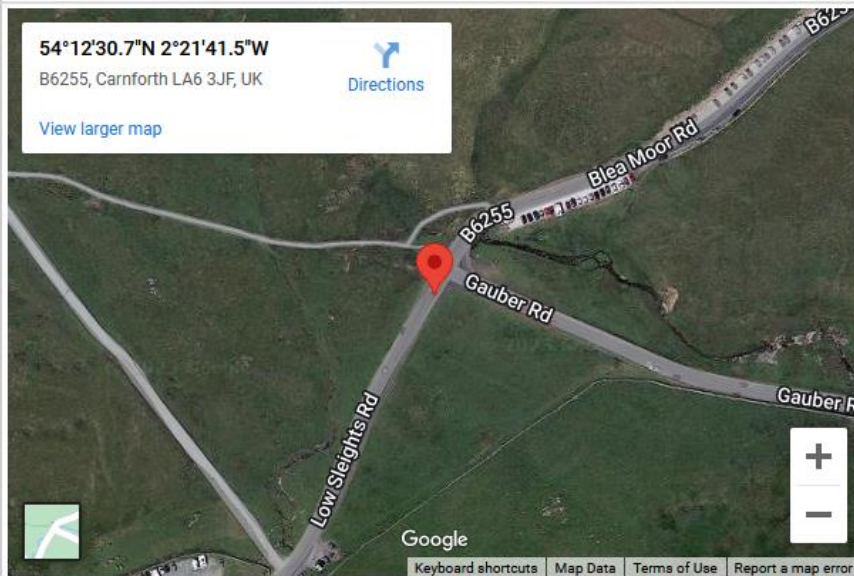
## EXIF

Make	Apple
Camera Model Name	iPhone XS Max
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	13.3.1
Modify Date	2020:02:29 14:37:44
Y Cb Cr Positioning	Centered
Exposure Time	1/1032
F Number	1.8
Exposure Program	Program AE
ISO	25
Exif Version	0231
Date/Time Original	2020:02:29 14:37:44
Create Date	2020:02:29 14:37:44

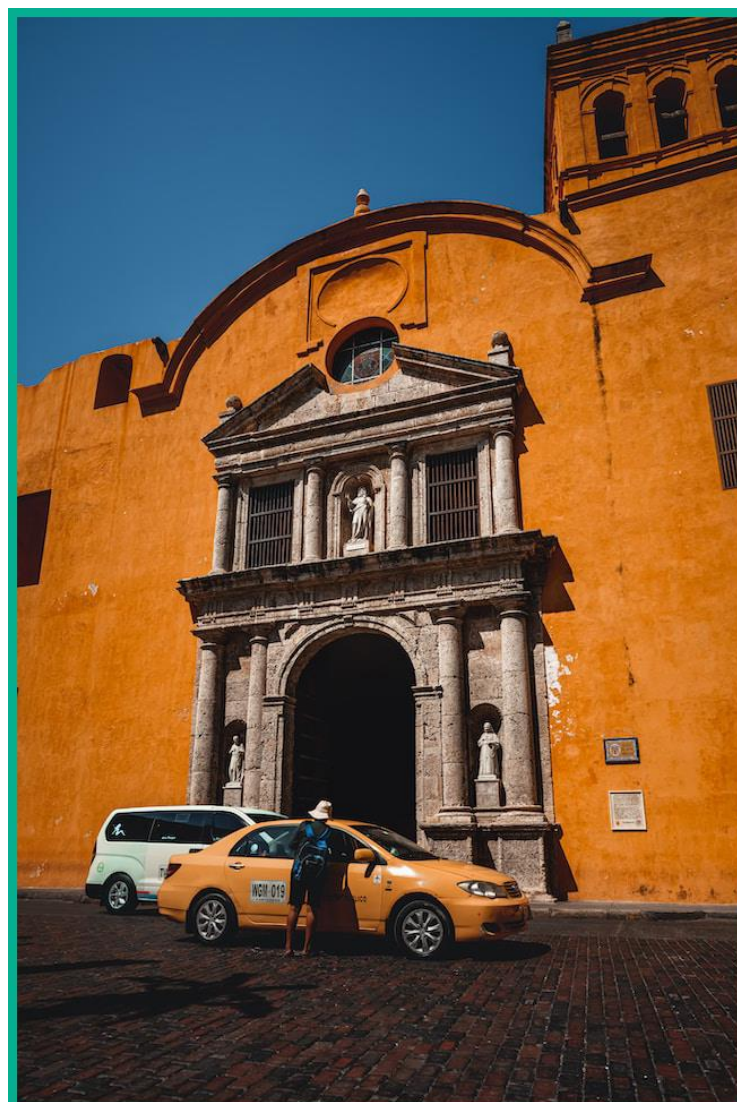
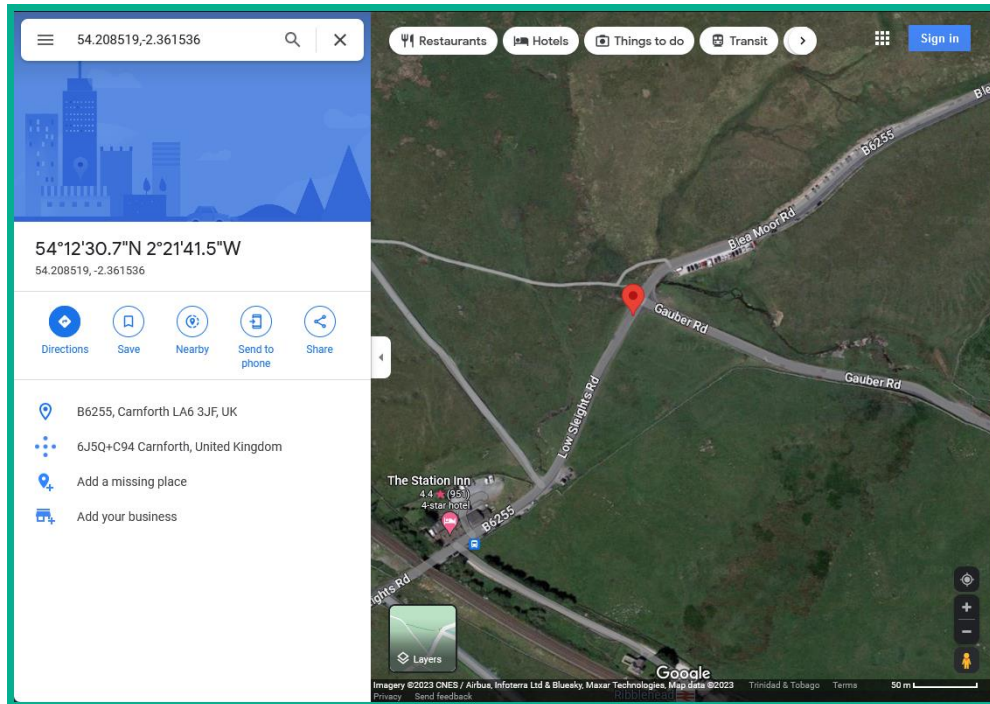
## Approximate GPS Location

This information is interpreted from the GPS metadata. **Locations are approximate.** Although the coordinates appear precise, mobile devices typically have low accuracy.

Approximate Coordinates	54.208519,-2.361536
Approximate Location	5.75 miles (9.25 km) ENE of Ingleton, ENG, GB
Approximate Range	+/- 4.579930861 meters (15 feet)











Cleanup.pictures

[Use cases](#)

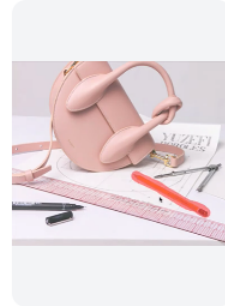
[Pricing](#)

[FAQ](#)

[API](#)



Remove any unwanted **object**, **defect**, **people** or **text** from your pictures in seconds



[Click here](#) or drag an image file







Google

Find image source

Search Text Translate

Convento de Santo Domingo, Cartagena  
Convent

Search

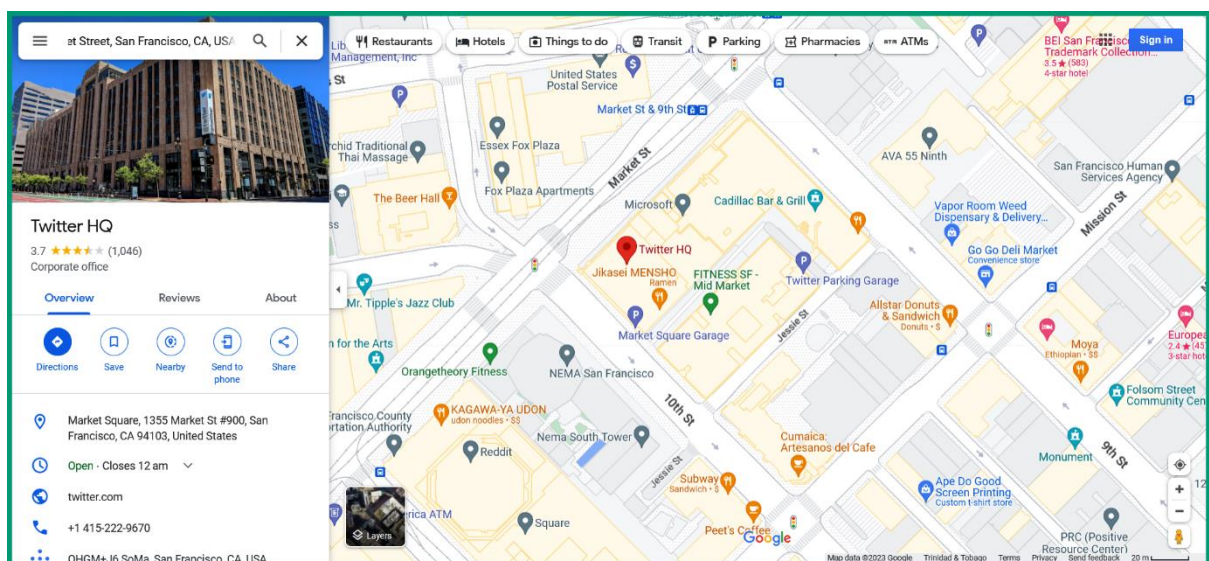
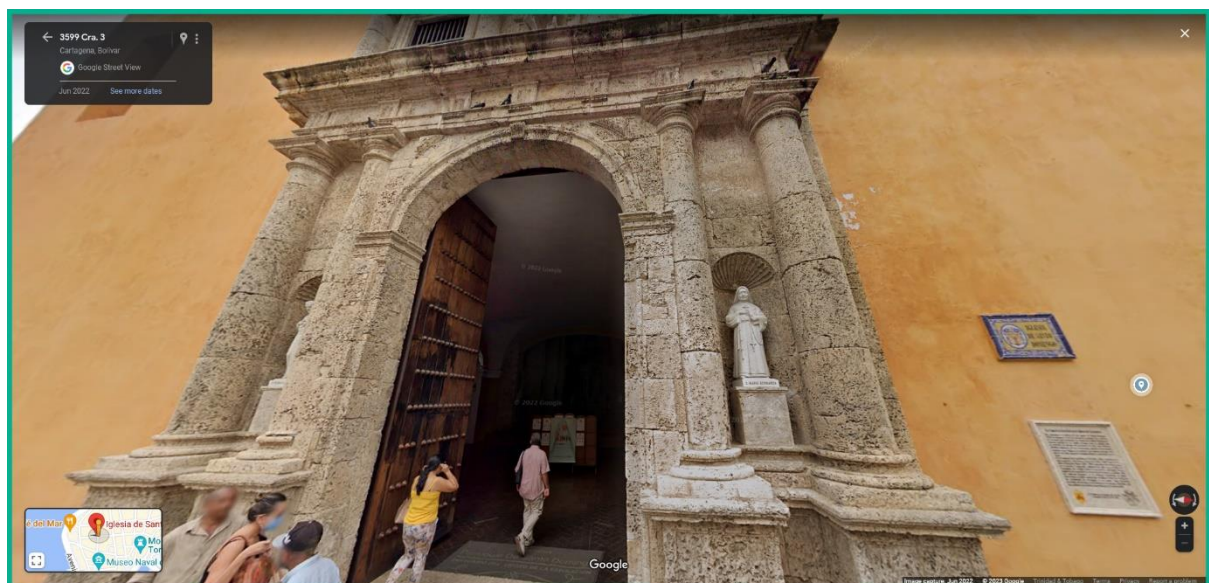
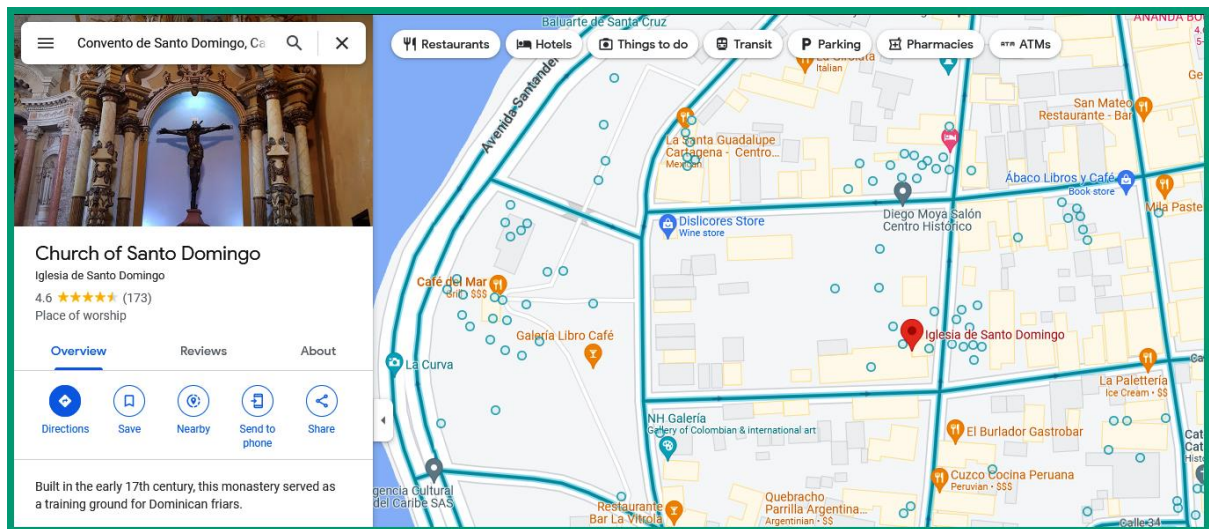
More images

Visual matches

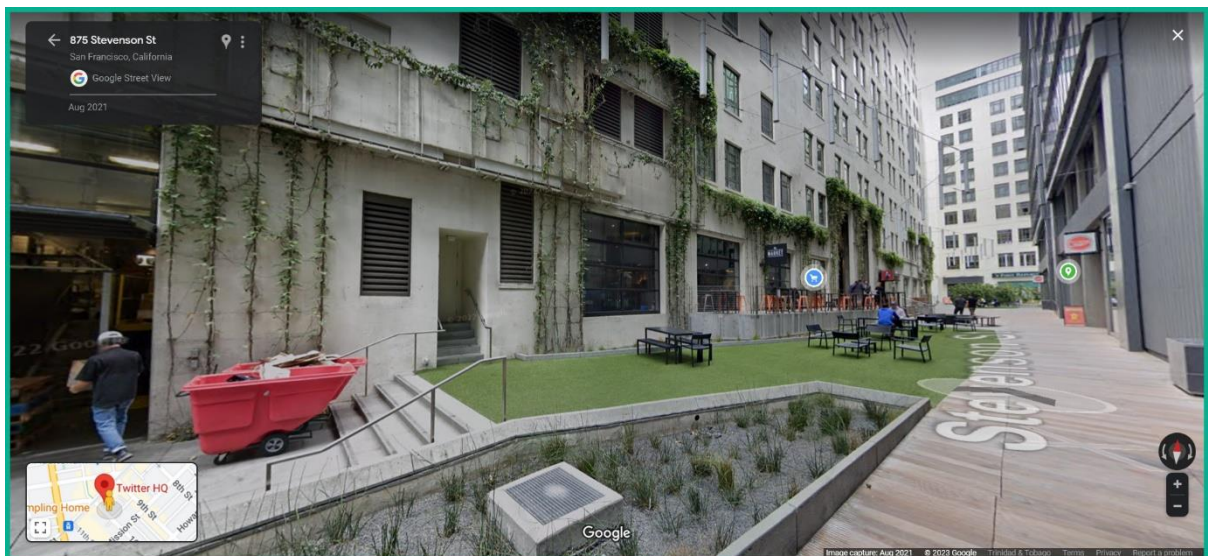
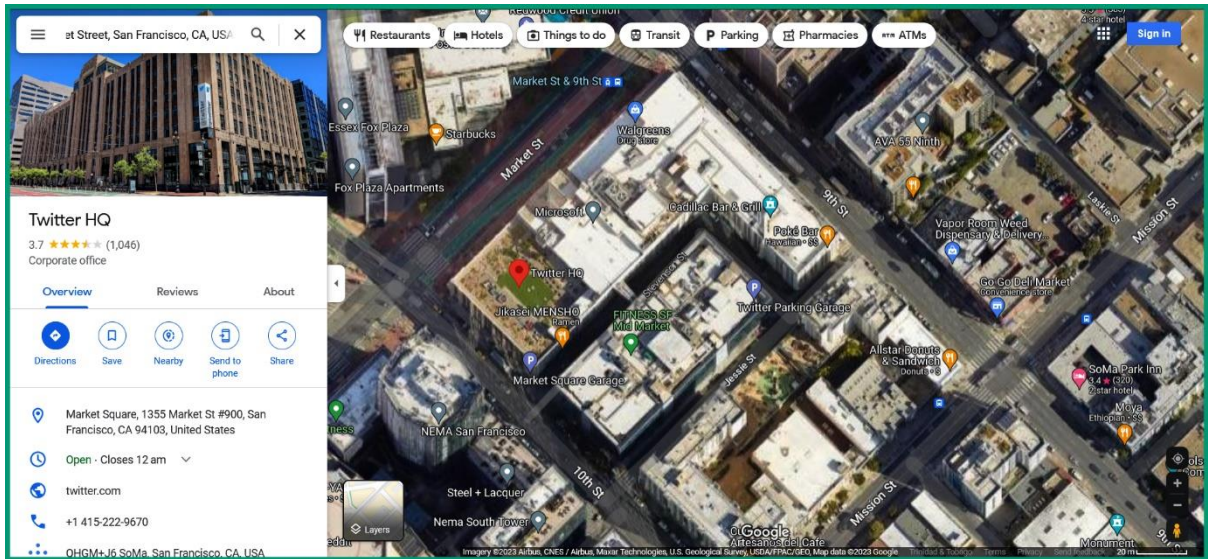
alamy.com  
The church of Santo Domingo, Cartagena,...

alamy.com  
Plaza santo domingo cartagena colombia hi...













microsoft.com


microsoft.com



Type 0 ▾ Department 0 ▾ Show only results with 0 ▾

30,893 results


Find by name ▾

  
@microsoft.com

Save

99%

▾

  
@microsoft.com

Save

99%

Sales Representative

▾



Follow

**Bill Gates** 

@BillGates

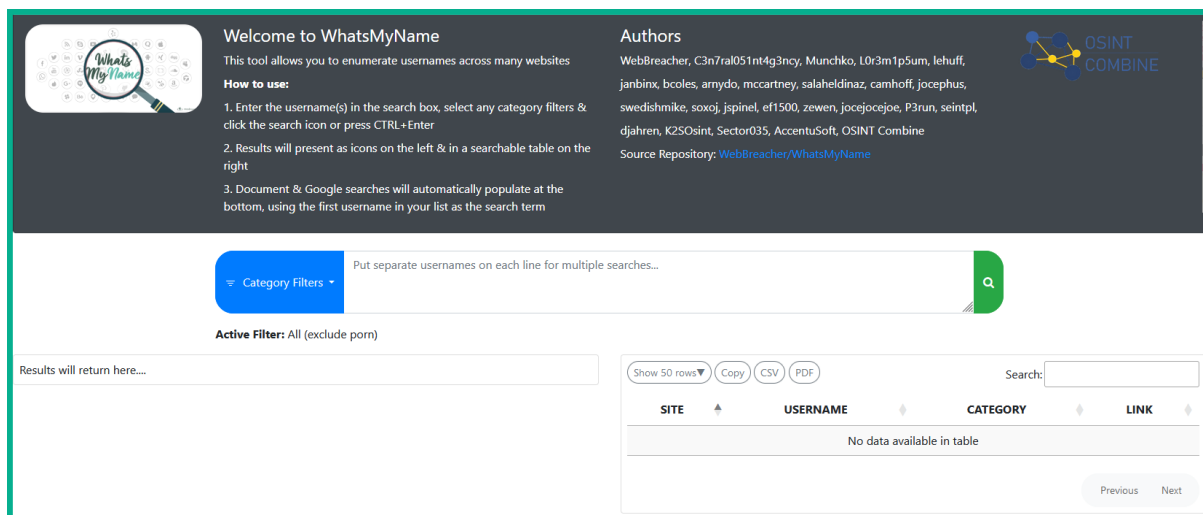
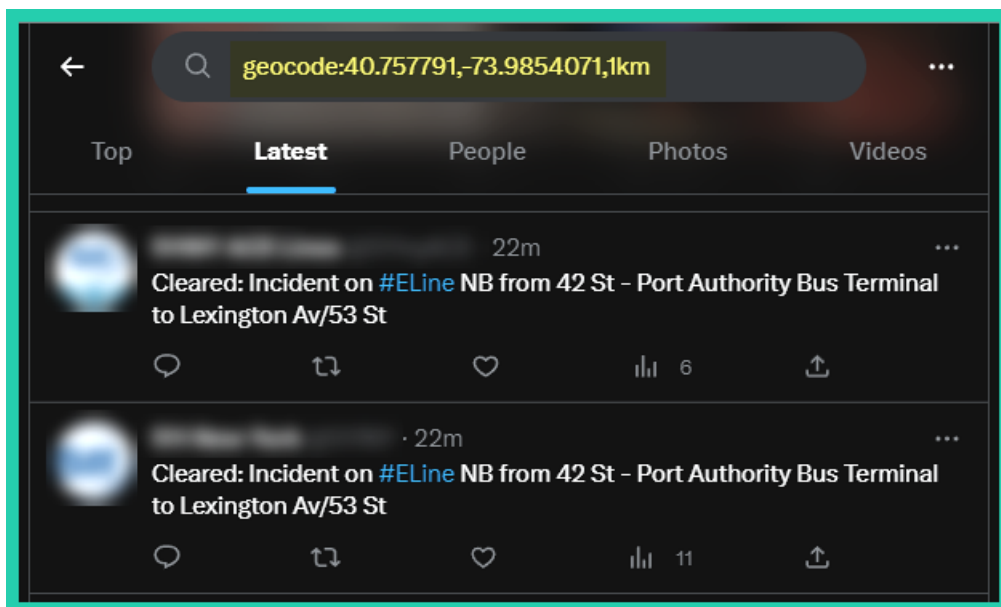
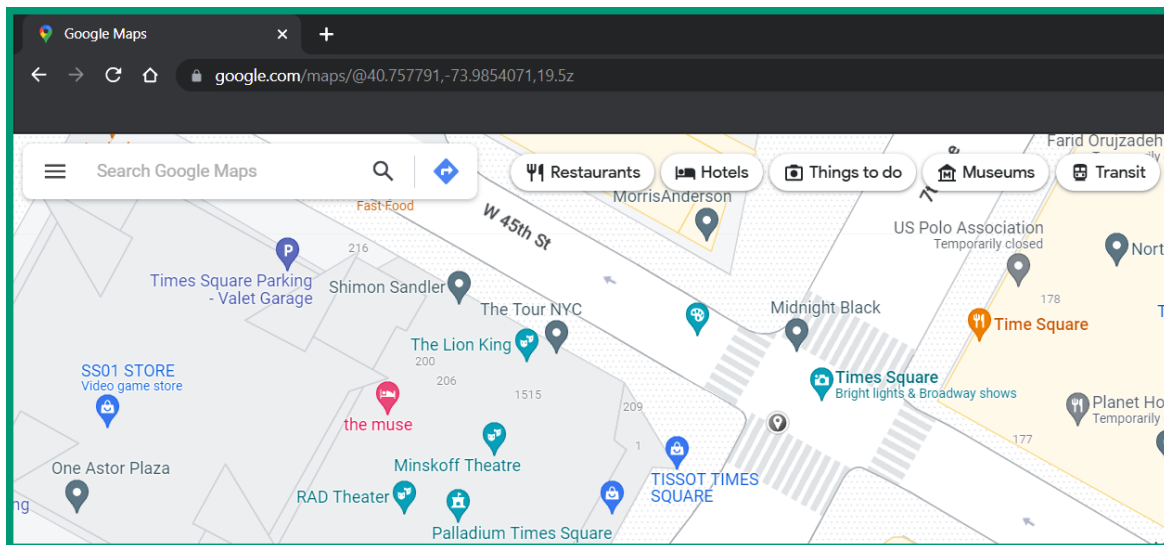
Sharing things I'm learning through my foundation work and other interests.

Seattle, WA  [gatesnot.es/blog](https://gatesnot.es/blog)  Joined June 2009

544 Following 62.2M Followers

Tweets Replies Media Likes









## 13 results

Searched over 59.2 billion images in 0.4 seconds for: Picture 2.jpg

☐ Show only 1 result found in collections

Sort by best match

Filter by website / collection



[svetlanasmith.medium.com/](#) - First found on Jan 14, 2021

[svetlanasmith.medium.com/](#) - First found on Jan 14, 2021

[view all 3 matches](#)

Filename: [1\\*dG6Du-zmZR3MaIKoRG-0IA.jpeg](#) (1024 x 1024, 170.7 kB)



[mentalism-and-mind-reading-tricks/](#) - First found on Jan 12, 2023

Filename: [6c0785b6e972e291b21aaa7b0d9d91c4-256.jpg](#) (256 x 256, 12.3 kB)



Free Search

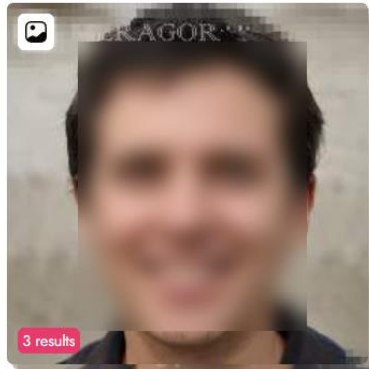
About 181 results in 3.16s



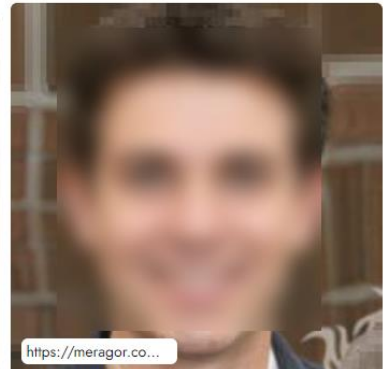
New Search



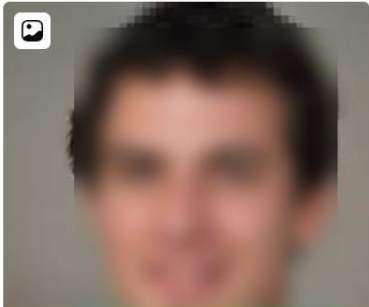
2 results



3 results



<https://meragor.co...>





# ';--have i been pwned?

Check if your email or phone is in a data breach

johndoe@gmail.com

pwned?

Oh no — pwned!

Pwned in 205 [data breaches](#) and found 75 [pastes](#) ([subscribe](#) to search sensitive breaches)

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



**000webhost:** In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

**Compromised data:** Email addresses, IP addresses, Names, Passwords



**123RF:** In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone numbers and passwords stored as MD5 hashes. The data was provided to HIBP by [dehashed.com](#).

**Compromised data:** Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames



**17:** In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a [Tor hidden service marketplace](#). The data contained over 4 million unique email addresses along with IP addresses, usernames and passwords stored as unsalted MD5 hashes.

**Compromised data:** Device information, Email addresses, IP addresses, Passwords, Usernames



## Pastes you were found in

A paste is information that has been published to a publicly facing website designed to share content and is often an early indicator of a data breach. Pastes are automatically imported and often removed shortly after having been posted. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Paste title	Date	Emails
<a href="#">siph0n.in</a>	Unknown	7,842
<a href="#">siph0n.in</a>	Unknown	59,437
<a href="#">balockae.online</a>	Unknown	178,410
<a href="#">pred.me</a>	Unknown	4,788,657
<a href="#">pxahb.xyz</a>	Unknown	4,161
<a href="#">www.pemiblanco.com</a>	Unknown	2,909,066
<a href="#">xn--e1alhsoq4c.xn--p1ai</a>	Unknown	4,788,657
<a href="#">is-bad-at.tech</a>	Unknown	1,878,845

\_IntelligenceX



Search Tor, I2P, data leaks, public web...

johndoe@gmail.com

Search

[Advanced](#)

\_IntelligenceX



[Collection 1/Collection #1\\_Games combos.tar.gz/Collection #1\\_Games](#)

**PREVIEW** 2019-01-17 21:20:53

a1@hotmail.com;45494549  
s.w.ampyyn.ua@gmail.com;30di15ngx8  
stonehead12121212@yahoo.com;coolio123  
paul@gmail.com;160884  
sasha7828@yandex.ru;sasha2014  
manfredlaterner@hotmail.com;Nokia3310  
jimmy@hotmail.com;123456ta  
lordray101@hotmail.com;locokid

[Full Data](#)

[gamerzplanet.net\\_15.10.23.rar/gamerzplanet.net\\_15-10-23.txt \[Part 16](#)

**PRO** 2022-09-23 11:05:18

[REDACTED]

[Full Data](#)



[← Back to results](#)



Collection 1/Collection #1\_Games

combos.tar.gz/Collection #1\_Games combos/Личный

Игровой АП [70% Гудов UPLAY].txt [Part 633 of 683]

2019-01-17 21:20:53

[Signup](#) or [Login](#) to view redacted documents.

Document

Tree View

Metadata

Selectors

Actions

Search:

a1@hotmail.com;45494549  
s.w.ampyyn.ua@gmail.com;30di15ngxB  
stonehead1212121212@yahoo.com;coolio123  
paul@gmail.com;160884  
sasha7828@yandex.ru;sasha2014  
manfredlaterner@hotmail.com;Nokia3310  
jimmy@hotmail.com;123456ta  
lordray101@hotmail.com;locokid  
frisovk@gmail.com;Quint111  
danielmarco777@gmail.com;criswell7  
beni@yahoo.com;221852s  
ratodainternet@hotmail.com;104458  
rocknroll\_cowboy@hotmail.com;caliber1  
axnis@hotmail.com;kukkel  
chris2000poker@yahoo.com;cocacola  
flufnpanda@gmail.com;FlufnPanda  
kingdoom14@hotmail.com;999  
brycebgar@aol.com;coolguy

**Enter the email address**

**Alfa AWUS036NHA**



**Raspberry Pi**



**Laptop**



**GPS Dongle**

**Signal Intelligence  
Infrastructure**





# ARM

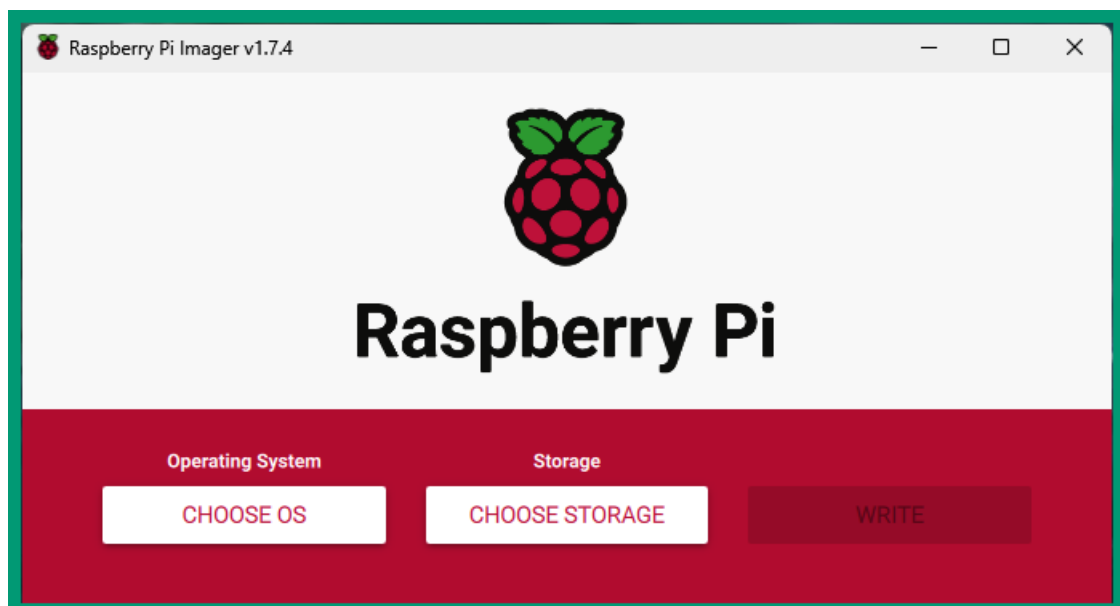
Are you looking for **Kali Linux ARM** images? We have generated flavours of Kali using the same build infrastructure as the official Kali releases for **ARM architecture**.

These images have a [default credentials](#) of "kali/kali".

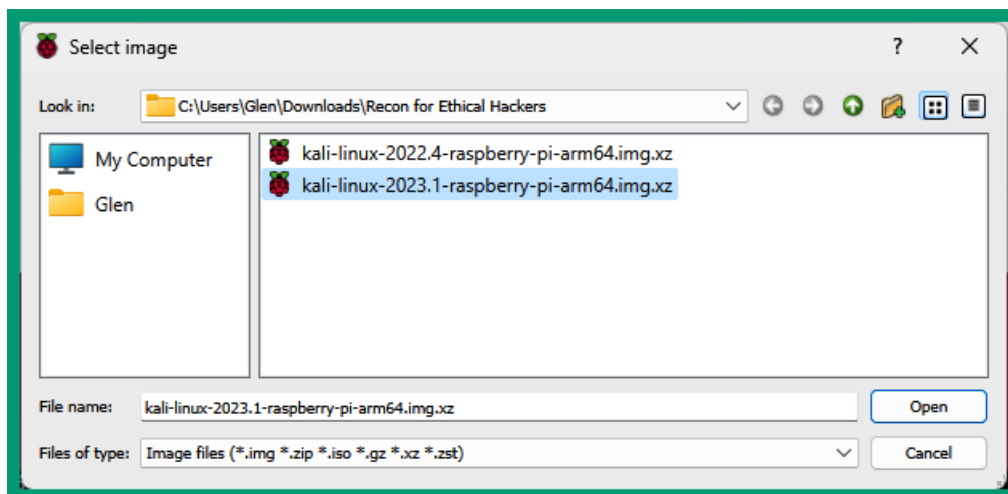
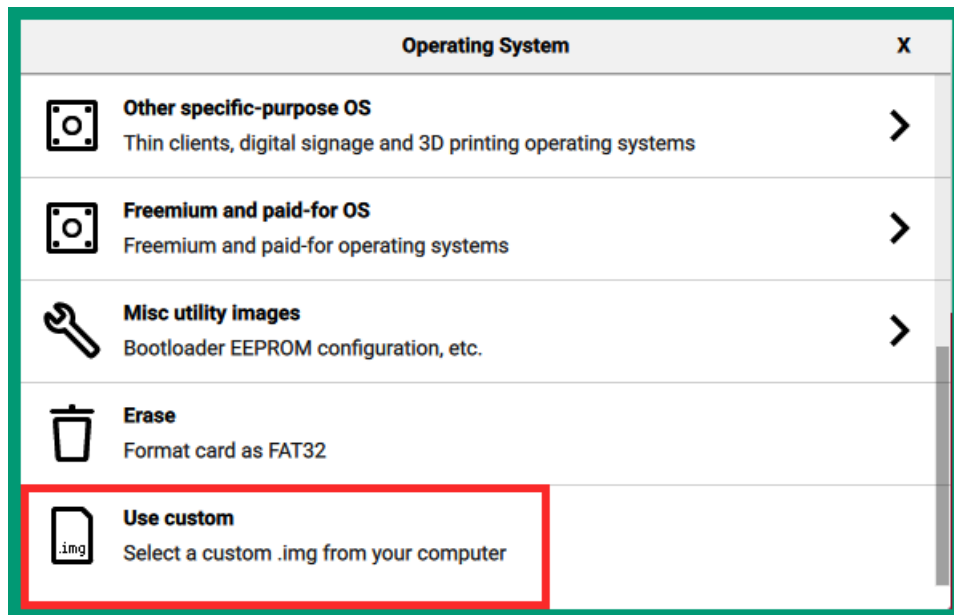
[Kali-ARM Documentation >](#)

## raspberrypi

Raspberry Pi 2, 3, 4 and 400 (32-bit)	↓ 2.2G	torrent	📄	sum
🔑 Recommended				
Raspberry Pi 2 (v1.2), 3, 4 and 400 (64-bit)	↓ 2.3G	torrent	📄	sum
Raspberry Pi 1 (Original)	↓ 2.1G	torrent	📄	sum
Raspberry Pi Zero 2 W	↓ 2.2G	torrent	📄	sum
🔑 Recommended				









Advanced options

X

Image customization options for this session only

☐ Set hostname: raspberrypi.local

☒ Enable SSH

☒ Use password authentication

☐ Allow public-key authentication only

Set authorized\_keys for 'kali':


☒ Set username and password

Username: kali

Password: ●●●●

SAVE

Raspberry Pi Imager v1.7.4



Raspberry Pi


Operating System

KALI-LINUX-2022.4-RASPBERRY-PI-ARM64.IMG.XZ

Storage

SABRENT S...

WRITE





```
kali@kali-raspberry-pi: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Glen> ssh kali@192.168.20.222
The authenticity of host '192.168.20.222 (192.168.20.222)' can't be established.
ED25519 key fingerprint is SHA256:vm/6w2VZSu4NX48tVjmOkVEagWnVTaFvgIUL7Im+rtM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.20.222' (ED25519) to the list of known hosts.
kali@192.168.20.222's password:
Linux kali-raspberry-pi 5.15.44-Re4son-v8+ #1 SMP PREEMPT Debian kali-pi (2022-07-03) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 2 16:14:40 2023 from 192.168.20.156
kali@kali-raspberry-pi:~$
kali@kali-raspberry-pi:~$
```

```
# For more information about the GPS types, see the documentation at:
# https://www.kismetwireless.net/docs/readme/gps/
#
# gps=serial:device=/dev/ttyUSB0,name=laptop
# gps=tcp:host=1.2.3.4,port=4352
# gps=gpsd:host=localhost,port=2947
# gps=virtual:lat=123.45,lon=45.678,alt=1234
# gps=web:name=gpsweb
gps=gpsd:host=localhost,port=2947,reconnect=true
```

Time: 2023-03-31T15:17:33.000Z (0)		Seen 14/Used 5				
Latitude:	N	GNSS	PRN	Elev	Azim	SNR Use
Longitude:	W	GP	1			Y
Alt (HAE, MSL):	ft	GP	4			Y
Speed: 0.04 mph		GP	7			Y
Track (true, var):	deg	GP	8			Y
Climb: -7.09 ft/min		GP	9			Y
Status: DGPS FIX (3 secs)		GP	26			N
Long Err (XDOP, EPX):	ft	GP	27			N
Lat Err (YDOP, EPY):	ft	GP	31			N
Alt Err (VDOP, EPV):	ft	SB	120			N
2D Err (HDOP, CEP):	ft	SB	133			N
3D Err (PDOP, SEP):	ft	SB	138			N
Time Err (TDOP):		QZ	1			N
Geo Err (GDOP):		QZ	2			N
ECEF X, VX:	m/s	QZ	5			N
ECEF Y, VY:	m/s					
ECEF Z, VZ:	m/s					
Speed Err (EPS):	+/- 0.8 mph					
Track Err (EPD):	+/- 0.0 deg					
Time offset:	0.065177906 s					
Grid Square:						



```
kali@kali-raspberry-pi: ~
GNU nano 7.2
interface=wlan0
driver=nl80211
ssid=MyNetwork
hw_mode=g
channel=7
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=Password123
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
|
```

```
interface wlan0
static ip_address=192.168.4.1/24
nohook wpa_supplicant
|
```

```
kali@kali-raspberry-pi: ~
GNU nano 7.2
interface=wlan0
dhcp-range=192.168.4.2,192.168.4.20,255.255.255.0,24h
|
```

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

eth0        no wireless extensions.

wlan0       IEEE 802.11  ESSID:"!|>_<|!"
            Mode:Managed  Frequency:2.442 GHz  Access Point: 
            Bit Rate=24 Mb/s   Tx-Power=31 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Power Management:on
            Link Quality=70/70  Signal level=-31 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-raspberry-pi:~$ sudo airmon-ng start wlan1
```

Found 3 processes that could cause trouble.  
Kill them using 'airmon-ng check kill' before putting  
the card in monitor mode, they will interfere by changing channels  
and sometimes putting the interface back in managed mode

```
PID Name
391 dhclient
601 NetworkManager
676 wpa_supplicant
```

PHY	Interface	Driver	Chipset
phy0	wlan0	brcmfmac	Broadcom 43430
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-raspberry-pi:~$ iwconfig
```

```
lo          no wireless extensions.
```

```
eth0        no wireless extensions.
```

```
wlan0       IEEE 802.11  ESSID:"!|>_<|!"
Mode:Managed  Frequency:2.442 GHz  Access Point: 
Bit Rate=24 Mb/s   Tx-Power=31 dBm
Retry short limit:7  RTS thr:off   Fragment thr:off
Power Management:on
Link Quality=70/70  Signal level=-31 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
```

```
wlan1mon    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-raspberry-pi: ~/war  X + v
```

KISMET - Point your browser to <http://localhost:2501> (or the address of this system) for the Kismet UI

```
INFO: (GPS) Connected to gpsd server [::1]:2947
INFO: (GPS) Connected to a JSON-enabled GPSD (3.22), enabling JSON mode
INFO: Could not open system plugin directory (/usr/lib/aarch64-linux-gnu/ki
smet/), skipping: No such file or directory
INFO: Did not find a user plugin directory (/home/kali/.kismet//plugins/),
skipping: No such file or directory
INFO: Found type 'linuxwifi' for 'wlan1mon'
INFO: wlan1mon interface 'wlan1mon' is already in monitor mode
INFO: wlan1mon finished configuring wlan1mon, ready to capture
INFO: Data source 'wlan1mon' launched successfully
INFO: Detected new 802.11 Wi-Fi access point 38:4C:4F:58:EC:AC
INFO: 802.11 Wi-Fi device 38:4C:4F:58:EC:AC advertising SSID
'Digicel_WiFi_T28R'
INFO: 802.11 Wi-Fi device 38:4C:4F:58:EC:AC advertising SSID
```



Kismet

GPS Data Collected

Search:

Devices

Alerts

SSIDs

ADSB Live

All devices

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID
00:AD:D5:...	Wi-Fi Bridged	IEEE802.11	n/a	n/a	1	53.55 KB		0	38:4C:4F:...
00:F3:61:...	Wi-Fi Bridged	IEEE802.11	n/a	n/a	7	903 B		0	9C:3D:CF:...
02:00:00:...	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	38:4C:4F:...
02:79:08:...	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	BC:E2:65:...
2C:9D:1E:...	Wi-Fi Bridged	IEEE802.11	n/a	n/a	6	336 B		0	9C:3D:CF:...

26 devices

Kismet

Devices

Alerts

SSIDs

ADSB Live

All devices

All devices

Wi-Fi

Wi-Fi Access Points

Phy types

IEEE802.11 devices

RTL433 devices

Z-Wave devices

Bluetooth devices

UAV devices

Type

Wi-Fi Bridged

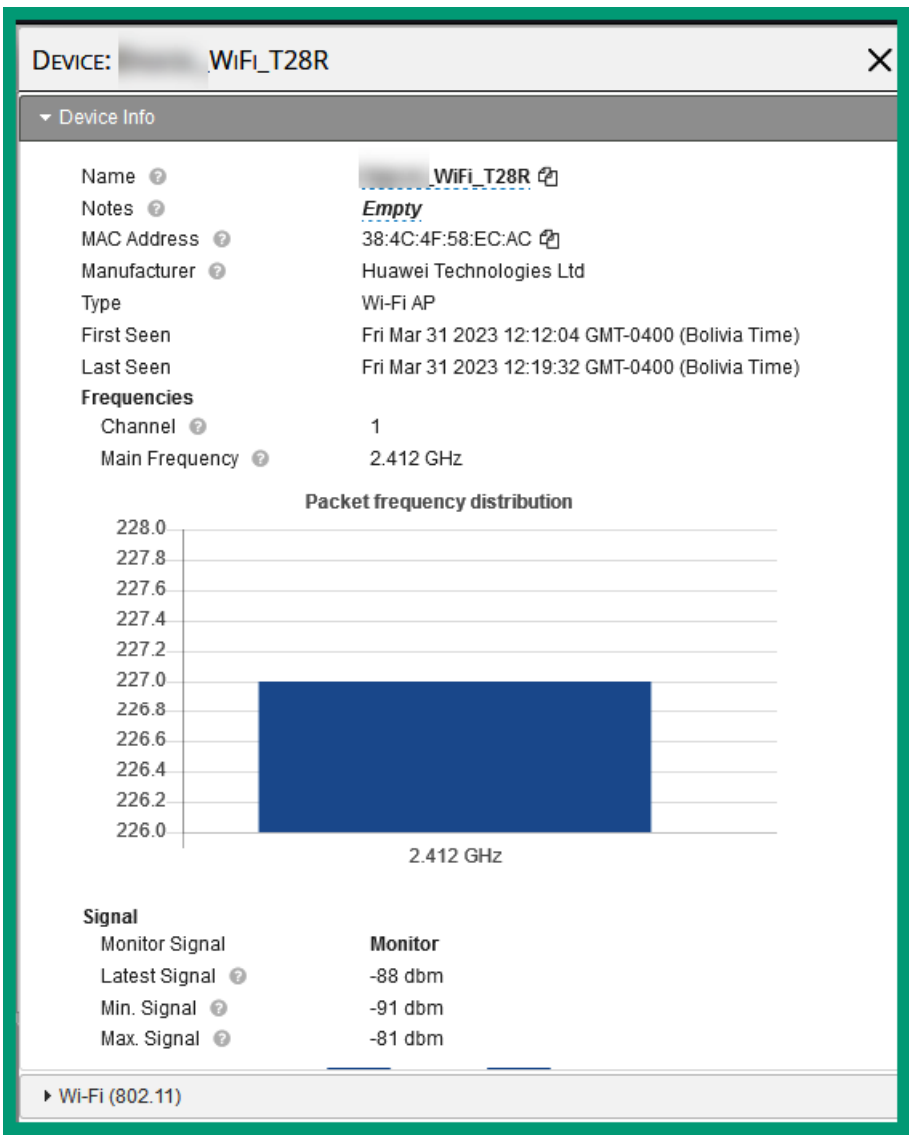
Wi-Fi Bridged

Wi-Fi Client

Wi-Fi Client

Wi-Fi Bridged











#### Associated Clients ?

- ▶ CA:EB:1C:71:59:4E
- ▶ 84:9A:40:40:7D:38
- ▶ 40:A9:CF:DE:14:1E
- ▶ 00:AD:D5:3D:2E:F3
- ▶ 2C:C5:46:11:3A:62
- ▶ E6:AA:21:18:13:46
- ▶ 38:4C:4F:58:EC:A4
- ▼ E2:F2:14:96:19:6D

##### Client Info

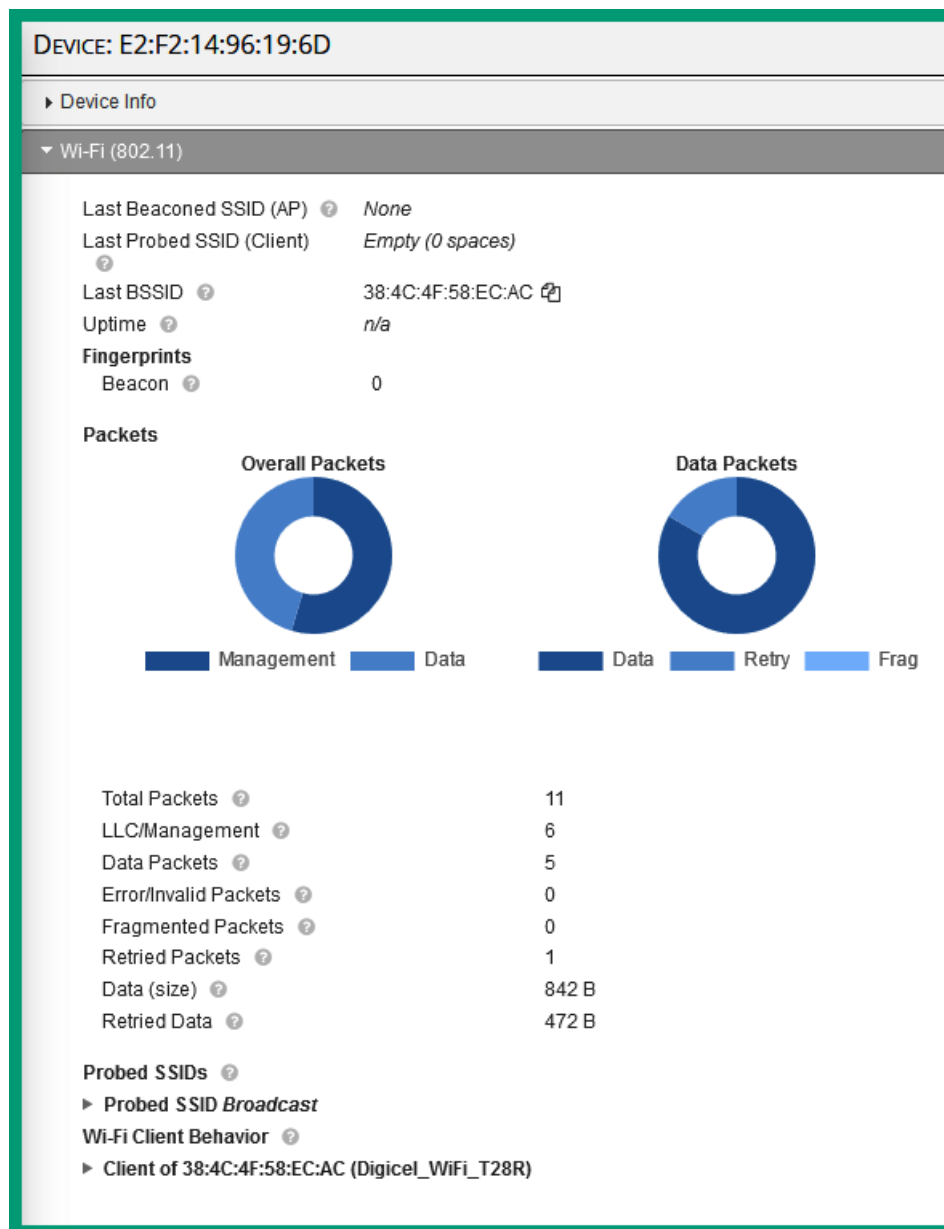
Name  
Type  
Manufacturer  
First Connected  
Last Connected  
Data  
Retried Data

##### View Client Details

E2:F2:14:96:19:6D  
Wi-Fi Client  
Unknown  
Mar 31 2023 12:14:57  
Mar 31 2023 12:14:57  
0 B  
0 B

- ▶ 12:85:BA:82:6F:BA





```
kali@kali-raspberry-pi: ~/war x + v
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for the Kismet UI
INFO: Detected new 802.11 Wi-Fi device 02:00:00:
INFO: Detected new 802.11 Wi-Fi access point B4:39:39:
INFO: 802.11 Wi-Fi device B4:39:39:2A:94:96 advertising SSID 'Hyundai E504'
INFO: Detected new 802.11 Wi-Fi device CA:EB:1C:
INFO: Detected new 802.11 Wi-Fi device 40:A9:CF:
INFO: 802.11 Wi-Fi device B4:39:39: advertising SSID 'Hyundai E504'
INFO: Detected new 802.11 Wi-Fi device FC:49:2D:
INFO: Detected new 802.11 Wi-Fi device 12:85:BA:
INFO: Detected new 802.11 Wi-Fi device 98:09:CF:
INFO: Detected new 802.11 Wi-Fi device 94:83:C4:
INFO: Detected new 802.11 Wi-Fi device 9C:8E:CD:
```



```
*** KISMET IS SHUTTING DOWN ***
Shutting down plugins...
WARNING: Kismet changes the configuration of network devices.
        In most cases you will need to restart networking for
        your interface (varies per distribution/OS, but
        typically one of:
        sudo service networking restart
        sudo /etc/init.d/networking restart
        or
        nmcli device set [device] managed true

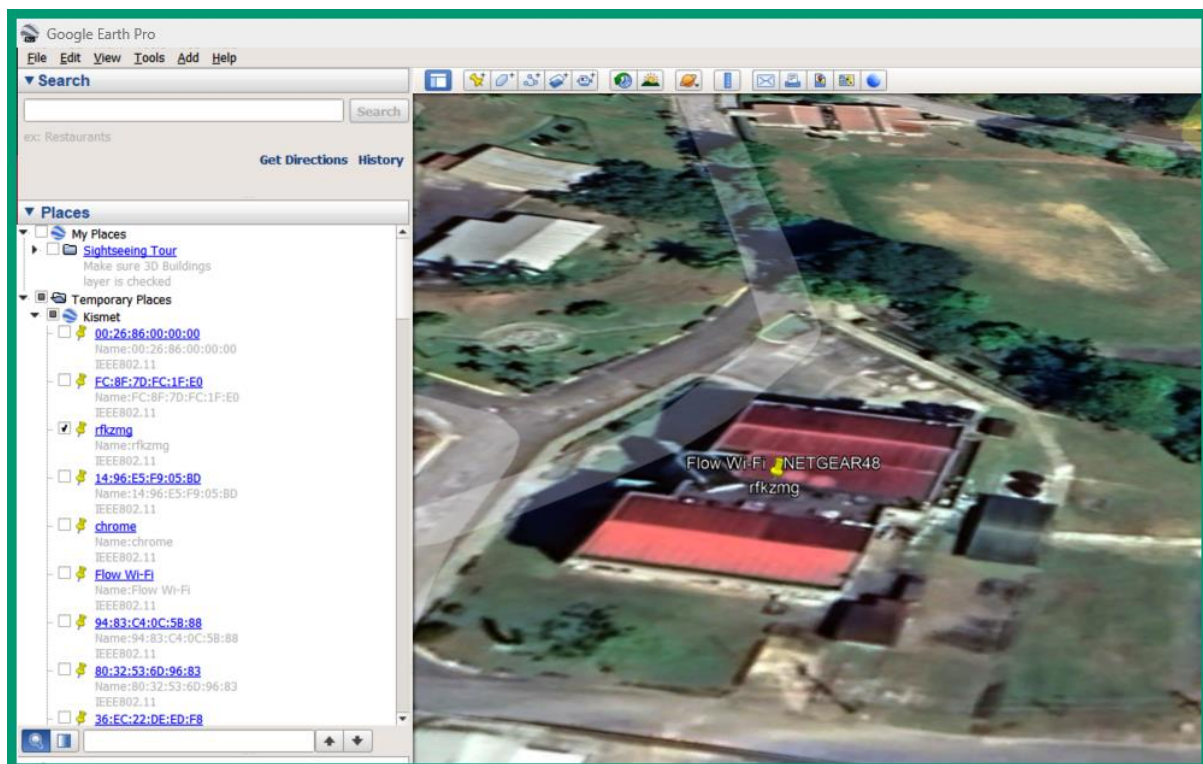
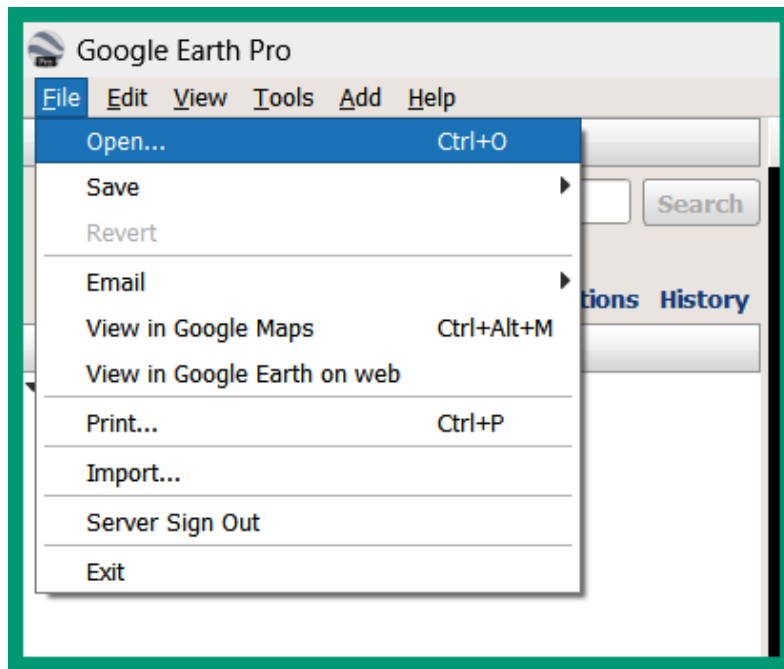
Kismet exiting.
EXITING: Signal service thread complete.
```

```
kali@kali-raspberry-pi:~/wardrive$ ls
Kismet-20230302-16-15-13-1.kismet
```

```
kali@kali-raspberry-pi:~/wardrive$ sudo kismetdb_to_kml --in Kismet-20230302-16-15-13-1.kismet --out wardrive1.kml
WARNING: No packets with GPS info for 'B8:8A:60:...', skipping
WARNING: No packets with GPS info for '80:30:49:...', skipping
WARNING: No packets with GPS info for '44:1E:98:...', skipping
WARNING: No packets with GPS info for 'E0:37:17:...', skipping
WARNING: No packets with GPS info for 'DA:CD:74:...', skipping
WARNING: No packets with GPS info for '6E:63:9C:...', skipping
WARNING: No packets with GPS info for '7C:1C:68:...', skipping
WARNING: No packets with GPS info for 'DA:FC:8F:...', skipping
WARNING: No packets with GPS info for '40:0D:10:...', skipping
WARNING: No packets with GPS info for '40:0D:10:...', skipping
WARNING: No packets with GPS info for '4A:78:5E:...', skipping
WARNING: No packets with GPS info for '22:96:2B:...', skipping
WARNING: No packets with GPS info for '44:1E:98:...', skipping
WARNING: No packets with GPS info for '9E:9A:9B:...', skipping
WARNING: No packets with GPS info for '46:91:91:...', skipping
WARNING: No packets with GPS info for 'A4:77:33:...', skipping

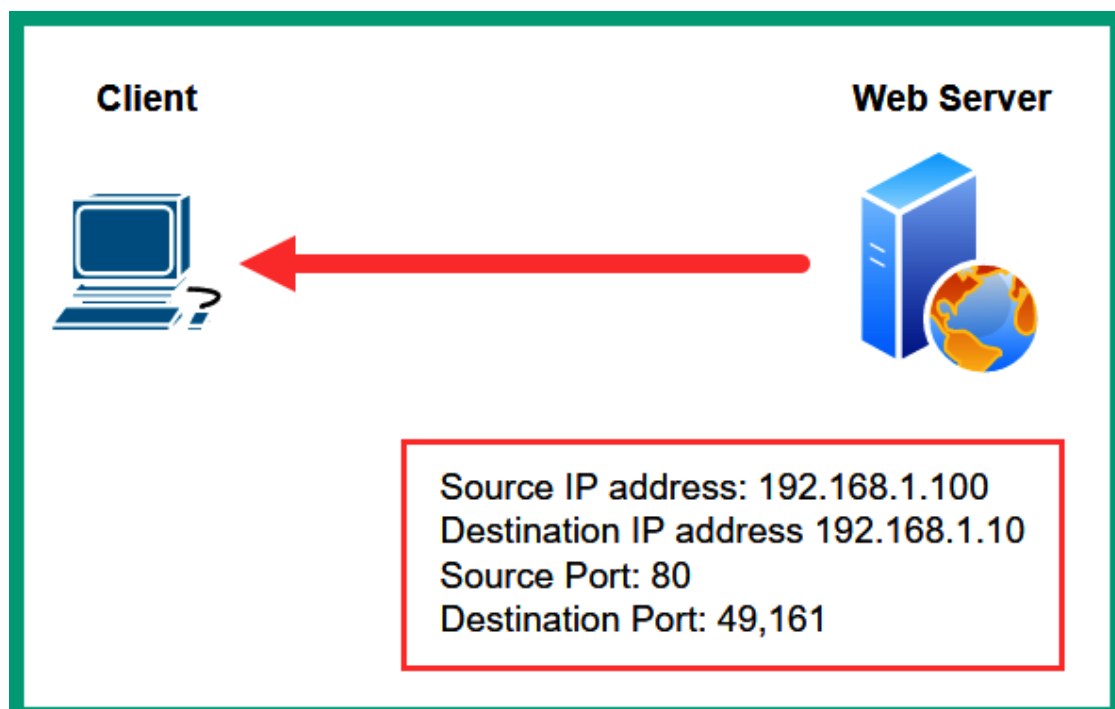
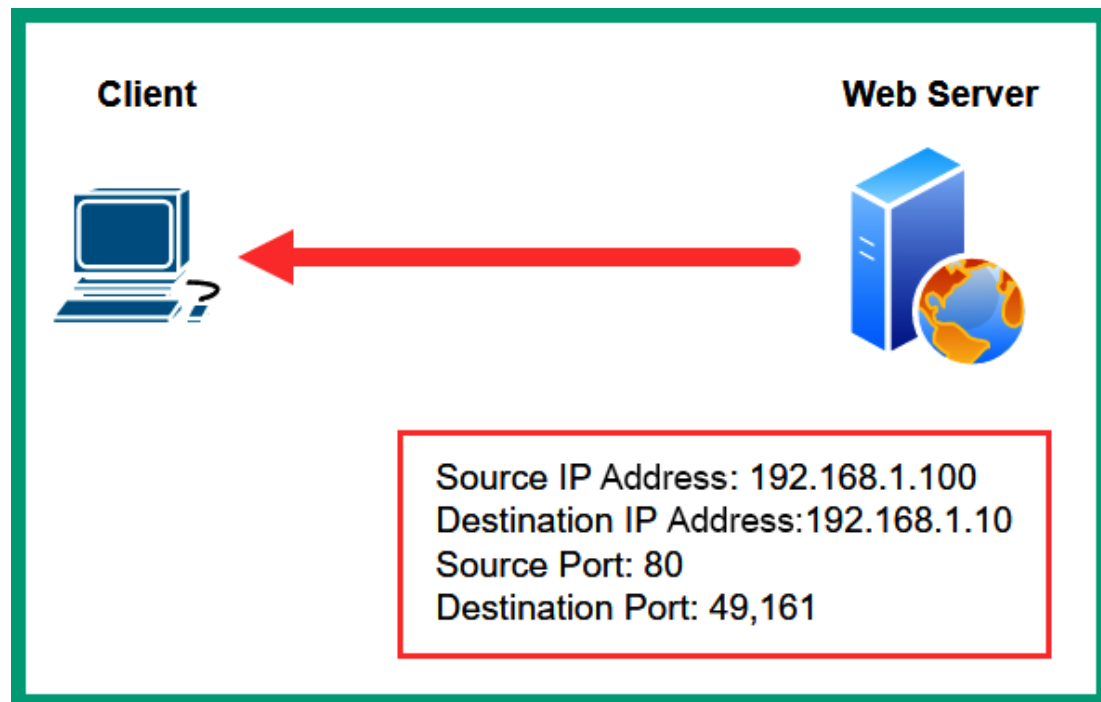
kali@kali-raspberry-pi:~/wardrive$ ls
Kismet-20230302-16-15-13-1.kismet  wardrive1.kml
```







## Chapter 7: Working with Active Reconnaissance





Port Range	Category
0 - 1,023	Well-known ports
1,024 - 49,151	Registered ports
49,152 - 65,535	Private/Dynamic ports

```
kali@kali:~$ ip address show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 08:00:27:7d:98:8e brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.44/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
        valid_lft 409sec preferred_lft 409sec

kali@kali:~$
```

```
kali@kali:~$ sudo 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 eth1
Current MAC: 08:00:27:7d:98:8e (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:7d:98:8e (CADMUS COMPUTER SYSTEMS)
New MAC: 00:e0:cd:97:15:74 (SAAB SENSIS CORPORATION)
```



```
kali@kali:~$ ip address show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 00:e0:cd:97:15:74 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:7d:98:8e
    inet 172.30.1.49/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
        valid_lft 587sec preferred_lft 587sec

kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.1.49 netmask 255.255.255.0 broadcast 172.30.1.255
    ether 00:e0:cd:97:15:74 txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 5140 (5.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 4153 (4.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
kali@kali:~$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 00:e0:cd:97:15:74 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:7d:98:8e
    inet 172.30.1.49/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
        valid_lft 120sec preferred_lft 120sec
```

Currently scanning: (passive) | 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
172.30.1.45	08:00:27:bf:3e:9c	3	180	PCS Systemtechnik GmbH
172.30.1.1	08:00:27:2f:d8:4a	2	120	PCS Systemtechnik GmbH

No.	Time	Source	Destination	Protocol	Length	Info
163	9.878252	172.16.17.65	8.8.8.8	ICMP	74	Echo (ping) request
164	9.927742	8.8.8.8	172.16.17.65	ICMP	74	Echo (ping) reply
166	10.895600	172.16.17.65	8.8.8.8	ICMP	74	Echo (ping) request
167	10.944807	8.8.8.8	172.16.17.65	ICMP	74	Echo (ping) reply
169	11.904669	172.16.17.65	8.8.8.8	ICMP	74	Echo (ping) request
170	11.953887	8.8.8.8	172.16.17.65	ICMP	74	Echo (ping) reply
172	12.922175	172.16.17.65	8.8.8.8	ICMP	74	Echo (ping) request
173	12.971113	8.8.8.8	172.16.17.65	ICMP	74	Echo (ping) reply

```
kali@kali:~$ ./ping-sweep.sh
Enter the network ID you want to scan (e.g. 192.168.1.0):
172.30.1.0
Enter the subnet mask in CIDR notation (e.g. 24):
24
172.30.1.1 is up
172.30.1.45 is up
172.30.1.49 is up
```



*eth1						
icmp						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000226479	172.30.1.49	172.30.1.1	ICMP	98	Echo (ping) request
4	0.000524646	172.30.1.1	172.30.1.49	ICMP	98	Echo (ping) reply
134	43.290568291	172.30.1.49	172.30.1.45	ICMP	98	Echo (ping) request
137	43.291630131	172.30.1.45	172.30.1.49	ICMP	98	Echo (ping) reply

```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 11:36 AST
Nmap scan report for 172.30.1.45
Host is up (0.0035s latency).
Nmap done: 255 IP addresses (1 host up) scanned in 18.96 seconds
```

*eth1						
ip.addr==172.30.1.49 && ip.addr==172.30.1.45						
No.	Time	Source	Destination	Protocol	Length	Info
177	18.896530093	172.30.1.49	172.30.1.45	TCP	74	36038 → 443 [SYN] Seq=0
181	18.897178127	172.30.1.45	172.30.1.49	TCP	60	443 → 36038 [RST, ACK]
603	20.867170284	172.30.1.49	172.30.1.45	TCP	74	36044 → 443 [SYN] Seq=0
604	20.867712274	172.30.1.45	172.30.1.49	TCP	60	443 → 36044 [RST, ACK]

```
kali@kali:~$ nmap 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 11:51 AST
Nmap scan report for 172.30.1.45
Host is up (0.0017s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
```

← Top 1000 open TCP ports



```
kali@kali:~$ nmap -T4 -p- 172.30.1.45
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 11:53 AST
```

```
Nmap scan report for 172.30.1.45
```

```
Host is up (0.0015s latency).
```

```
Not shown: 65497 closed tcp ports (conn-refused)
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
1617/tcp	open	nimrod-agent
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server
3700/tcp	open	lrs-paging
4848/tcp	open	appserv-http

**Scanned all 65,535  
TCP ports**

```
kali@kali:~$ nmap -PN 172.30.1.45
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 12:12 AST
```

```
Nmap scan report for 172.30.1.45
```

```
Host is up (0.0041s latency).
```

```
Not shown: 980 closed tcp ports (conn-refused)
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server

**Don't Ping Scan**



```
kali@kali:~$ sudo nmap -sU 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 12:16 AST
Nmap scan report for 172.30.1.45
Host is up (0.00069s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE      SERVICE
137/udp    open       netbios-ns
138/udp    open|filtered netbios-dgm
161/udp    open       snmp
500/udp    open|filtered isakmp
4500/udp   open|filtered nat-t-ike
5353/udp   open|filtered zeroconf
5355/udp   open|filtered llmnr
MAC Address: 08:00:27:BF:3E:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1105.24 seconds
```

UDP scan

```
kali@kali:~$ sudo nmap -sV 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 12:38 AST
Nmap scan report for 172.30.1.45
Host is up (0.00092s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp     open  ftp              Microsoft ftpd
22/tcp     open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp     open  http             Microsoft IIS httpd 7.5
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp   open  mysql            MySQL 5.5.20-log
3389/tcp   open  ms-wbt-server?

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

```
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```



```
kali@kali:~$ sudo nmap -A 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 12:44 AST
Nmap scan report for 172.30.1.45
Host is up (0.00066s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 a5702aacb0ab784fbc1efc053623de38 (RSA)
|_  521 4aa1db4e864943fe0eb86a337fa97882 (ECDSA)
80/tcp    open  http             Microsoft IIS httpd 7.5
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Microsoft-HTTPAPI/2.0
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Windows Server 2008 R2 Standard 7601 Service Pack 1
3306/tcp  open  mysql            MySQL 5.5.20-log
```

```
Host script results:
| smb2-time:
|   date: 2023-04-06T16:46:39
|_  start_date: 2023-04-06T15:46:29
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 1h45m00s, deviation: 3h30m00s, median: 0s
|_ nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 080027bf3e9c
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-04-06T09:46:37-07:00
```



```
kali@kali:~$ sudo nmap -sT -PN --spoof-mac 0 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 13:09 AST
Spoofing MAC address AB:A4:7A:56:A5:E3 (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 172.30.1.45
Host is up (0.0012s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
```

```
kali@kali:~$ sudo nmap -sT -PN --spoof-mac dell 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 13:10 AST
Spoofing MAC address 00:00:97:47:11:CD (Dell EMC)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 172.30.1.45
Host is up (0.0012s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
```

```
kali@kali:~$ sudo nmap -sT -PN --spoof-mac 12:34:56:78:9A:BC 172.30.1.45
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 13:11 AST
Spoofing MAC address 12:34:56:78:9A:BC (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 172.30.1.45
Host is up (0.0018s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```



ip.src == 172.30.1.44						
No.	Time	Source	Destination	Protocol	Length	Info
30	108160748	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
40	108256655	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
50	108344032	172.30.1.44	172.30.1.45	TCP	42	64350 → 22 [SYN] Seq=0
60	108510165	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
70	108524088	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
80	108532087	172.30.1.44	172.30.1.45	TCP	42	64350 → 199 [SYN] Seq=0
90	108558400	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
100	108568704	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
110	108576763	172.30.1.44	172.30.1.45	TCP	42	64350 → 80 [SYN] Seq=0
120	108660562	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol
140	108817604	172.30.1.44	172.30.1.45	TCP	54	64350 → 22 [RST] Seq=1
150	108851735	172.30.1.44	172.30.1.45	IPv4	42	Fragmented IP protocol

```
kali@kali:~$ nbtscan -r 172.30.1.45
```

Doing NBT name scan for addresses from 172.30.1.45

IP address	NetBIOS Name	Server	User	MAC address
172.30.1.45	VAGRANT-2008R2	<server>	<unknown>	08:00:27:bf:3e:9c

```
kali@kali:~$ nmap -A -T4 -Pn -n -p 445 172.30.1.45
```

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-14 12:28 AST

Nmap scan report for 172.30.1.45

Host is up (0.00037s latency).

PORT	STATE	SERVICE	VERSION
445/tcp	open	microsoft-ds	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds

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

MAC Address: 08:00:27:BF:3E:9C (Oracle VirtualBox virtual NIC)

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

Host script results:

| nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 080027bf3e9c

| Names:

| VAGRANT-2008R2<00> Flags: <unique><active>

| WORKGROUP<00> Flags: <group><active>

|\_ VAGRANT-2008R2<20> Flags: <unique><active>

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 108.31 seconds

```
kali@kali:~$ smbclient -L //172.30.1.45 -U vagrant
```

Password for [WORKGROUP\vagrant]:

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC

Reconnecting with SMB1 for workgroup listing.

do\_connect: Connection to 172.30.1.45 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

Unable to connect with SMB1 -- no workgroup available



```
kali@kali:~$ smbmap -H 172.30.1.45 -u vagrant -p vagrant
```

[+] IP: 172.30.1.45:445 Name: 172.30.1.45		
Disk	Permissions	Comment
ADMIN\$	READ, WRITE	Remote Admin
C\$	READ, WRITE	Default share
IPC\$	NO ACCESS	Remote IPC
Users	READ, WRITE	

```
kali@kali:~$ sudo nmap -p139,445 --script=smb-enum-shares.nse 172.30.1.45
```

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-15 11:01 AST  
Nmap scan report for 172.30.1.45  
Host is up (0.00015s latency).

PORT STATE SERVICE  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
MAC Address: 08:00:27:BF:3E:9C (Oracle VirtualBox virtual NIC)

Host script results:

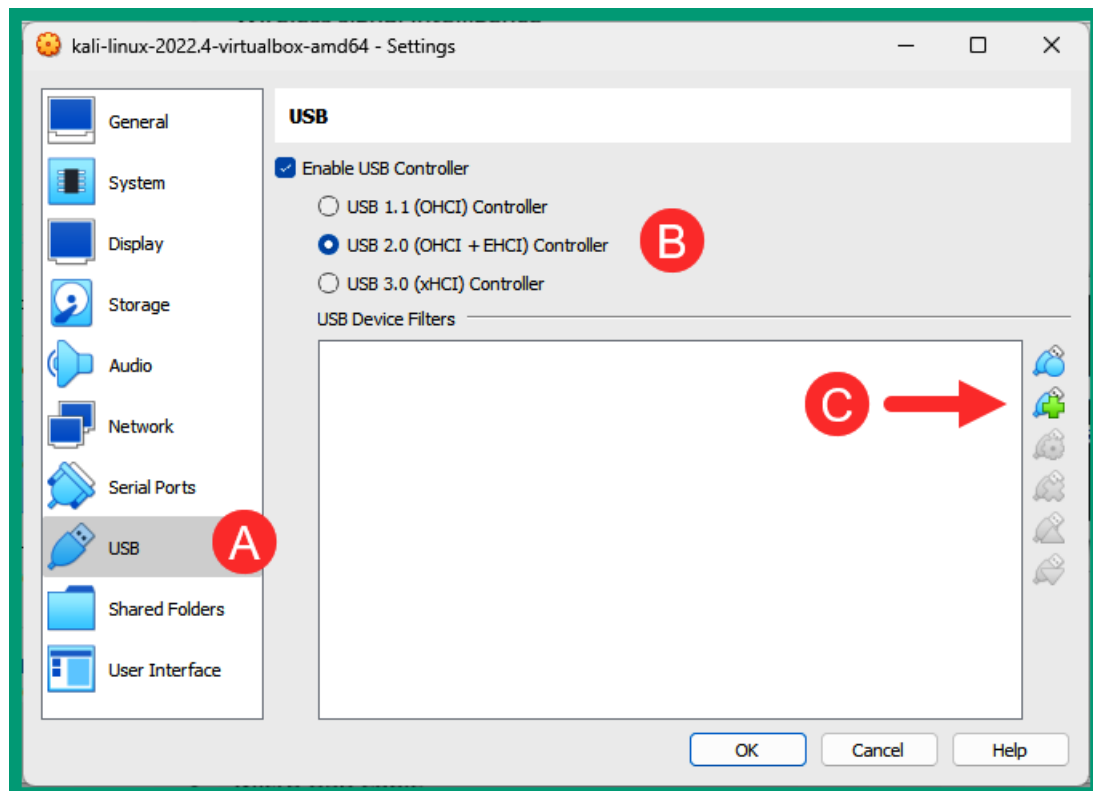
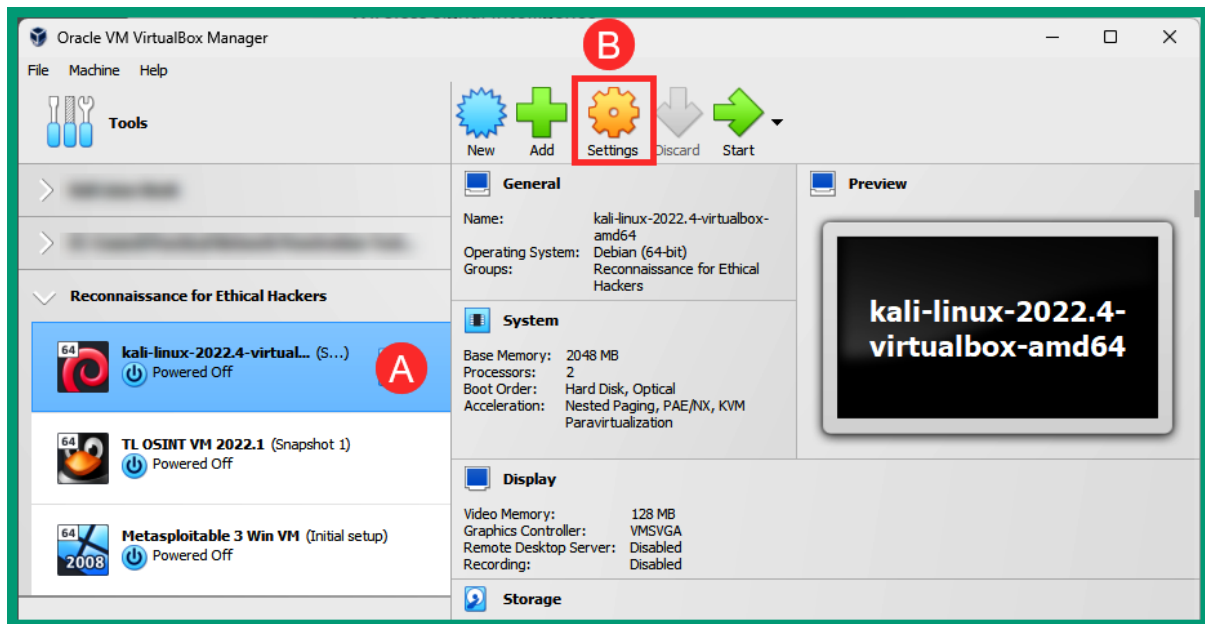
```
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\172.30.1.45\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\172.30.1.45\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\172.30.1.45\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\172.30.1.45\USERS:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: <none>
```

Host script results:

```
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

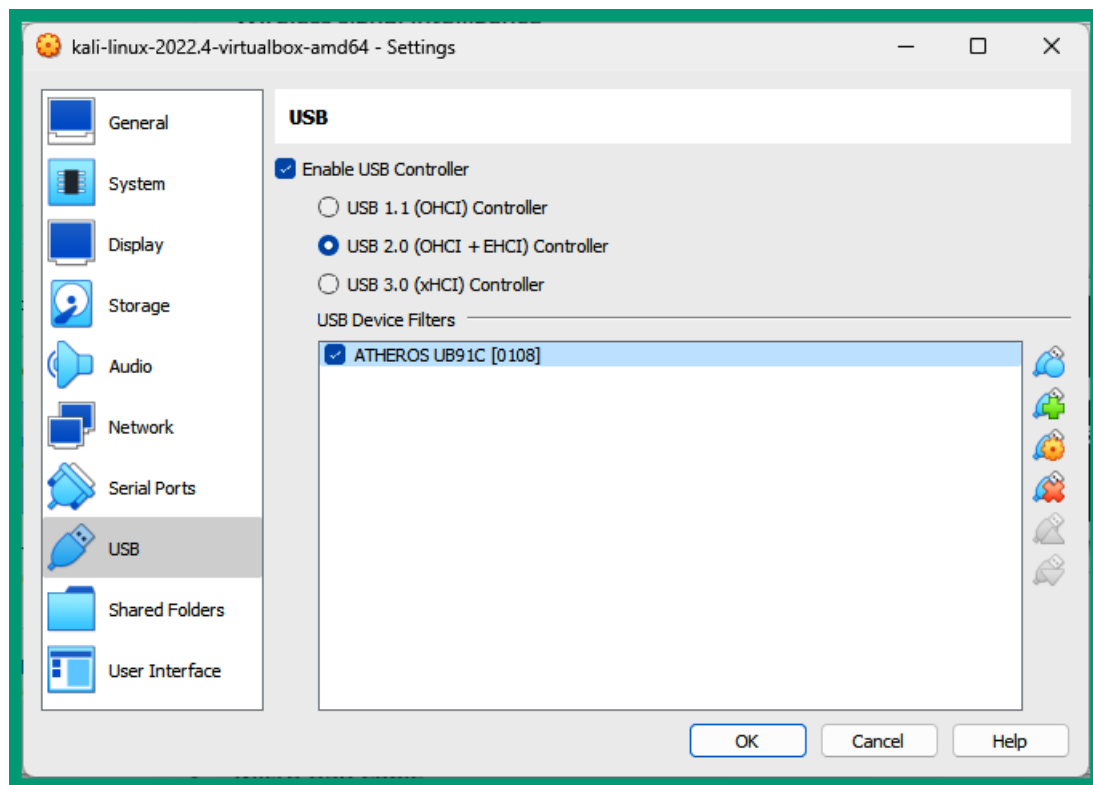
Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds





Blue Microphones Yeti Stereo Microphone [0100]  
Intel Corp. [0001]  
SINOWEALTH Wired Gaming Mouse [0101]  
Elgato Stream Deck  
**ATHEROS UB91C [0108]** ←  
ASUSTek Computer Inc. N-KEY Device [4022]  
Wacom Co.,Ltd. Intuos S [0111]  
Logitech, Inc. C922 Pro Stream Webcam [0016]





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

eth0        no wireless extensions.

eth1        no wireless extensions.

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

docker0     no wireless extensions.
```

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


Killing these processes:

```
PID Name
771 wpa_supplicant
```



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

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



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

```
lo        no wireless extensions.
```

```
eth0      no wireless extensions.
```

```
eth1      no wireless extensions.
```

```
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:...	F8:54:B8:...	-45	24e- 1e	0	11		
9C:3D:CF:...	78:BD:BC:...	-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:...	B0:C0:90:...	-82	24e- 1	0	20		
38:4C:4F:...	E4:C8:01:...	-83	5e- 1	0	47		
38:4C:4F:...	88:9F:6F:...	-84	24e- 1	0	52		
38:4C:4F:...	B8:C3:85:...	-89	24e- 1	0	146		
38:4C:4F:...	2C:C5:46:...	-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:██████	-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		

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]

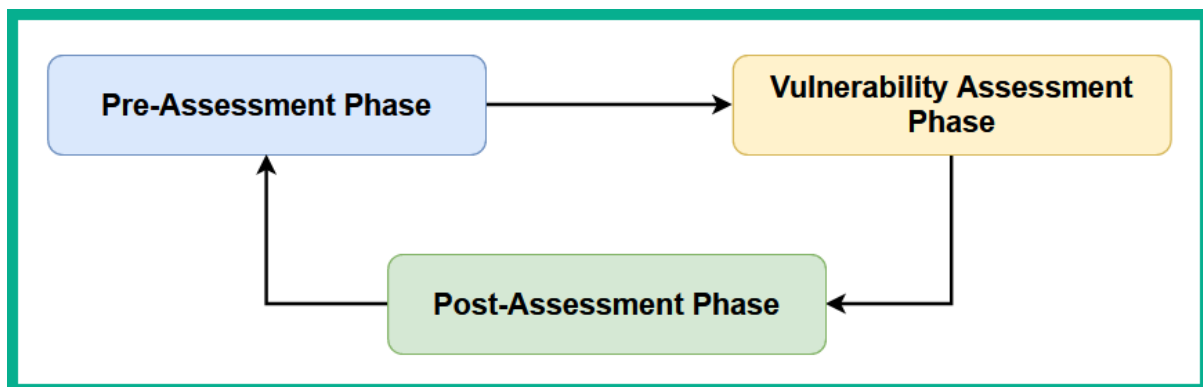
CH 6 ][ Elapsed: 2 mins ][ 2021-09-12 13:30 ][ PMKID found: 68:7F:74:01:28:E1

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	



## Chapter 8: Performing Vulnerability Assessments



```
kali@kali:~$ curl --request GET \
--url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.5.1-debian10_amd64.deb' \
--output 'Nessus-10.5.1-debian10_amd64.deb'
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100	61.2M	0	9117k	0	--:--:--	0:00:06	--:--:-- 12.7M

```
kali@kali:~$ ls
```

Desktop	Nessus-10.5.1-debian10_amd64.deb	'Ping Sweep using bash script.pcapng'	sherlock
Documents	'Nmap fragment packets.pcapng'	'Ping Sweep using Nmap SN.pcapng'	Sublist3r
Downloads	Pictures	Public	Templates
Music	ping-sweep.sh	Recon-Report1.html	Videos

```
kali@kali:~$ sudo dpkg -i Nessus-10.5.1-debian10_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 395753 files and directories currently installed.)
Preparing to unpack Nessus-10.5.1-debian10_amd64.deb ...
Unpacking nessus (10.5.1) ...
Setting up nessus (10.5.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
```





## 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 \(Recommended\)](#)

[Advanced...](#)

A

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 \(Recommended\)](#)

[Accept the Risk and Continue](#)

B



# nessus®

## Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

☐ Register Offline

[Settings](#)

[Continue](#)





## Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- ☐ Set up a purchased instance of Nessus
- ☐ Start a trial of Nessus Expert
- ☐ Start a trial of Nessus Professional
- ☒ Register for Nessus Essentials **A**
- ☐ Link Nessus to another Tenable product

[Back](#)

**B**

[Continue](#)



## Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

First Name

Last Name

Email

Already have activation code? Skip this step to enter it manually.

[Back](#)

[Skip](#)

[Register](#)





---

## Register Nessus

Enter your activation code.

Activation Code

Back

Continue

---



---

## License Information

Activation Code:

Continue

---



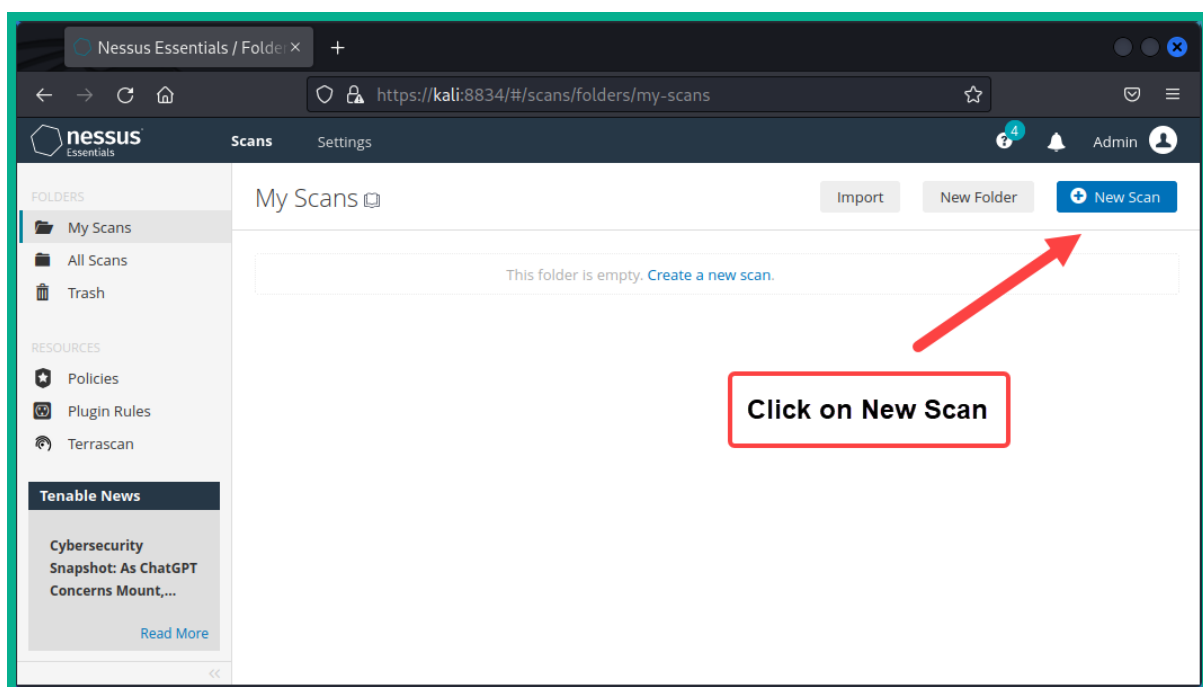
 **nessus**

Create a user account

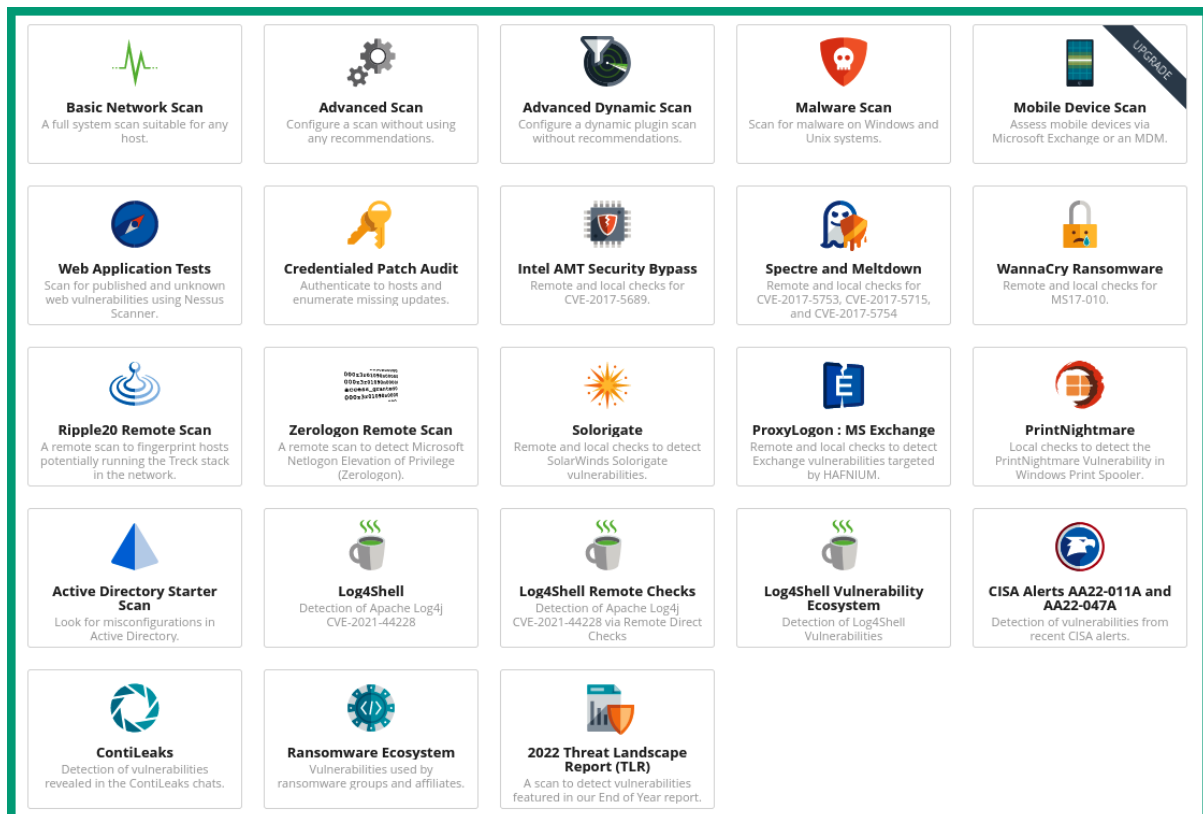
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username \*

Password \*







Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

My First Scan

A

Description

First Vulnerability Scan

B

Folder

My Scans

Targets

172.30.1.45

C

Upload Targets

Add File

Save

Cancel

Launch

D



nessus Essentials Scans Settings

My Scans

Search Scans 1 Scan

Scan in progress

Name	Schedule	Last Scanned
My First Scan	On Demand	Today at 11:56 AM

My Scans

Search Scans 1 Scan

Scan Completed

Name	Schedule	Last Scanned
My First Scan	On Demand	Today at 12:06 PM

My First Scan

Back to My Scans

Configure Audit Trail Launch Report

Hosts 1 Vulnerabilities 42 Remediations 3 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
172.30.1.45	14 17 25 101

Column that shows the number of security vulnerabilities found

Doughnut chart shows an overview of vulnerabilities based on their severity rating

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 11:56 AM  
End: Today at 12:06 PM  
Elapsed: 10 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (14), High (17), Medium (25), Low (101), Info (0).



<div>Vulnerabilities 42</div>								
<div> <div>Filter</div> <div>Search Vulnerabilities</div> <div>42 Vulnerabilities</div> </div>								
<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	MIXED	...	...	15 PHP (...)	CGI abuses	15		
<input type="checkbox"/>	MIXED	...	...	10 Apach...	Web Servers	10		
<input type="checkbox"/>	MIXED	...	...	7 Micro...	Windows	7		
<input type="checkbox"/>	CRITICAL	...	...	6 Apach...	Web Servers	6		
<input type="checkbox"/>	MIXED	...	...	13 SSL (...)	General	20		
<input type="checkbox"/>	MIXED	...	...	7 SNMP...	SNMP	7		

<div>Vulnerabilities 42</div>								
<div> <div>Search Vulnerabilities</div> <div>6 Vulnerabilities</div> </div>								
<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache 2.4...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.8	7.4	Apache < 2...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.8	7.4	Apache 2.4...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.8	7.4	Apache 2.4...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.0	8.1	Apache < 2...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.0	7.3	Apache 2.4...	Web Servers	1		



CRITICAL

## Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

>

### Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod\_rewrite and mod\_proxy: Some mod\_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod\_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.\*) http://example.com:8080/elsewhere?\$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod\_proxy\_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod\_proxy\_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client. Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

### Solution

Upgrade to Apache version 2.4.56 or later.

### Risk Information

Vulnerability Priority Rating (VPR): 9.0

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

CVSS v3.0 Temporal Score: 8.5

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 7.4

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

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

IAVM Severity: I



Base Score

9.8  
(Critical)

Attack Vector (AV)

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

Attack Complexity (AC)

Low (L)High (H)

Privileges Required (PR)

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

User Interaction (UI)

None (N)Required (R)

Scope (S)

Unchanged (U)Changed (C)

Confidentiality (C)

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

Integrity (I)

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

Availability (A)

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

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

Generate Report - 1 Vulnerability Selecte

Report Format: HTMLPDFCSV

Select a Report Template:

SYSTEM

Complete List of Vulnerabilities by Host

Detailed Vulnerabilities By Host

Detailed Vulnerabilities By Plugin

Vulnerability Operations

Template Description:

This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:

None

Formatting Options:

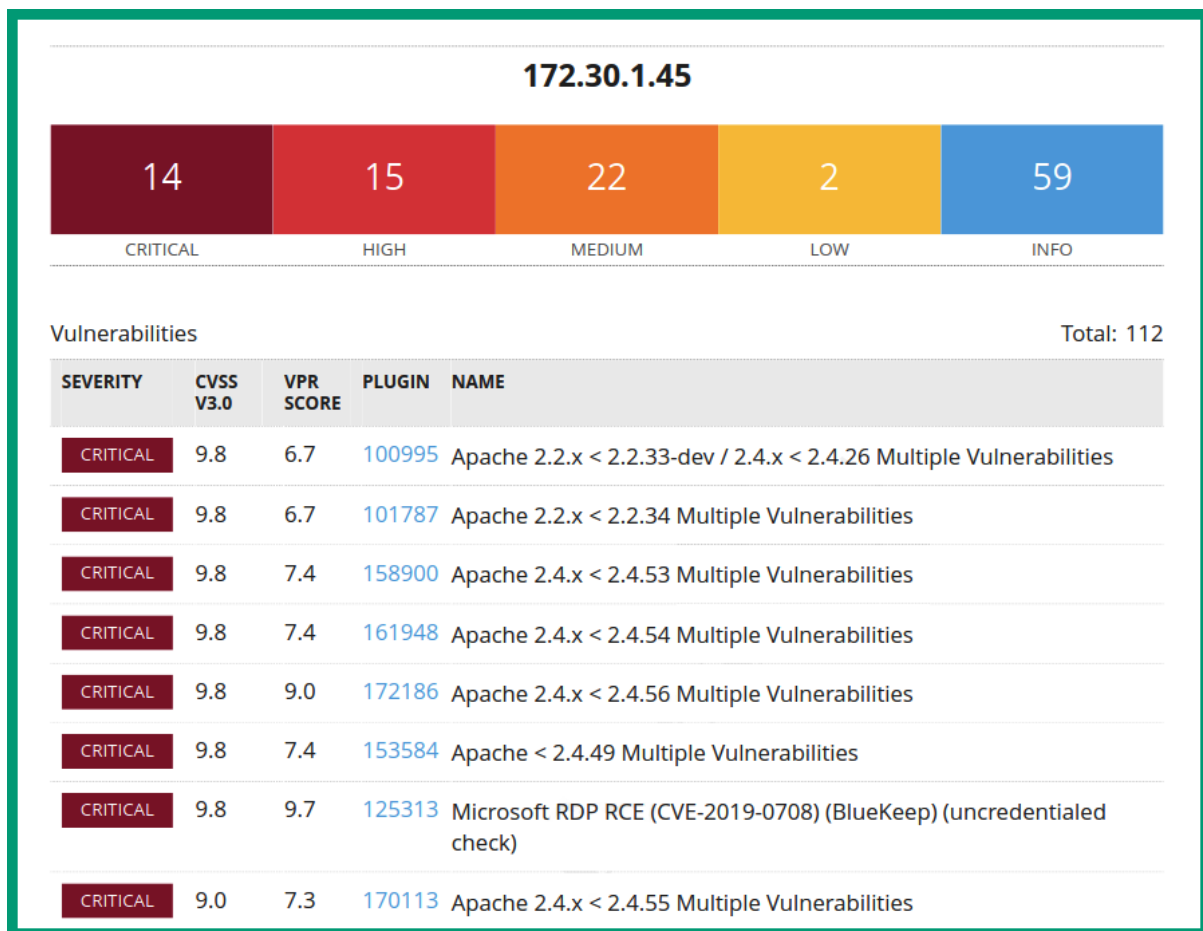
☒ Include page breaks between vulnerability results

Generate Report

Cancel

☐ Save as default






```
[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '3beaebb7-3ab3-4673-ab65-f2fe92417c29'.

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

User Credentials







# Greenbone

## Sign in to your account

Username

admin

Password

.....

Sign In



Configuration

Administration

A

Help

Users

Groups

Roles

Permissions

Performance

Trashcan

Feed Status


B

LDAP

RADIUS



## Feed Status

Type	Content	Origin	Version	Status
NVT	 NVTs	Greenbone Community Feed	20230418T1011	Current
SCAP	 CVEs  CPEs	Greenbone Community SCAP Feed	20230418T0510	Update in progress...
CERT	 CERT-Bund Advisories  DFN-CERT Advisories	Greenbone Community CERT Feed	20230418T0406	Update in progress...
GVM_DATA	 Compliance Policies  Port Lists  Report Formats  Scan Configs	Greenbone Community gvm Data Feed	20230418T1004	Update in progress...



Dashboards

Scans

Assets

Resilience

?

Feed Status

Type	Content	Origin	Version	Status
NVT	<div><div></div><div>NVTs</div></div>	Greenbone Community Feed	20230418T1011	Current
SCAP	<div><div><div></div><div>CVEs</div></div><div><div></div><div>CPEs</div></div></div>	Greenbone Community SCAP Feed	20230418T0510	Current
CERT	<div><div><div></div><div>CERT-Bund Advisories</div></div><div><div></div><div>DFN-CERT Advisories</div></div></div>	Greenbone Community CERT Feed	20230418T0406	Current
GVMD_DATA	<div><div><div></div><div>Compliance Policies</div></div><div><div></div><div>Port Lists</div></div><div><div></div><div>Report Formats</div></div><div><div></div><div>Scan Configs</div></div></div>	Greenbone Community gvmd Data Feed	20230418T1004	Current

Configuration

Administration

Targets

Port Lists

Credentials

Scan Configs

Alerts

Schedules

Report Formats

Scanners

Filters

Tags

☐

New Target

Name

First Scan 1

Comment

Scanning Metasploitable 3

Hosts

☒ Manual 

172.30.1.45

☐ 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 ar

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

--

on port

22

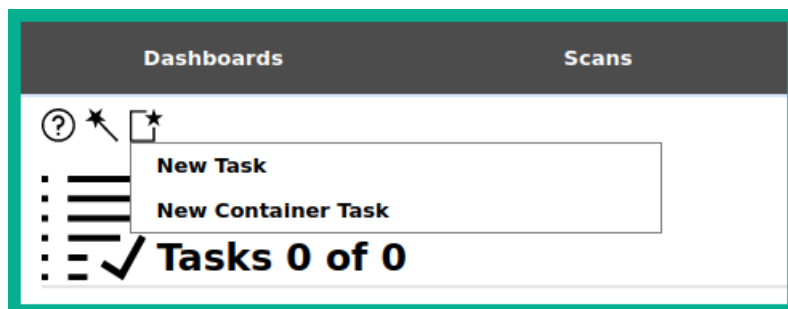
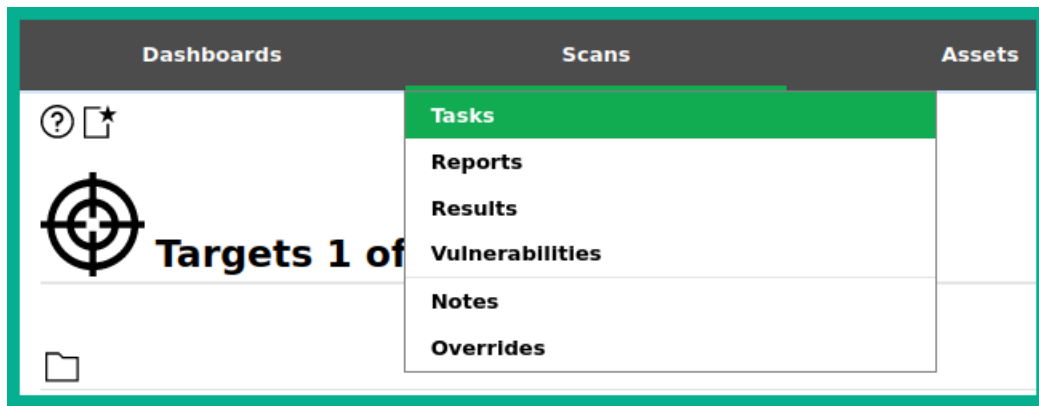
SMB

--

Cancel

Save





**New Task** [X]

**Name**

**Comment**

**Scan Targets**  [X]

**Alerts**  [X]

**Schedule**  ☐ Once [X]

**Add results to Assets** ☒ Yes ☐ No

**Apply Overrides** ☒ Yes ☐ No

**Min QoD**  %

**Alterable Task** ☐ Yes ☒ No

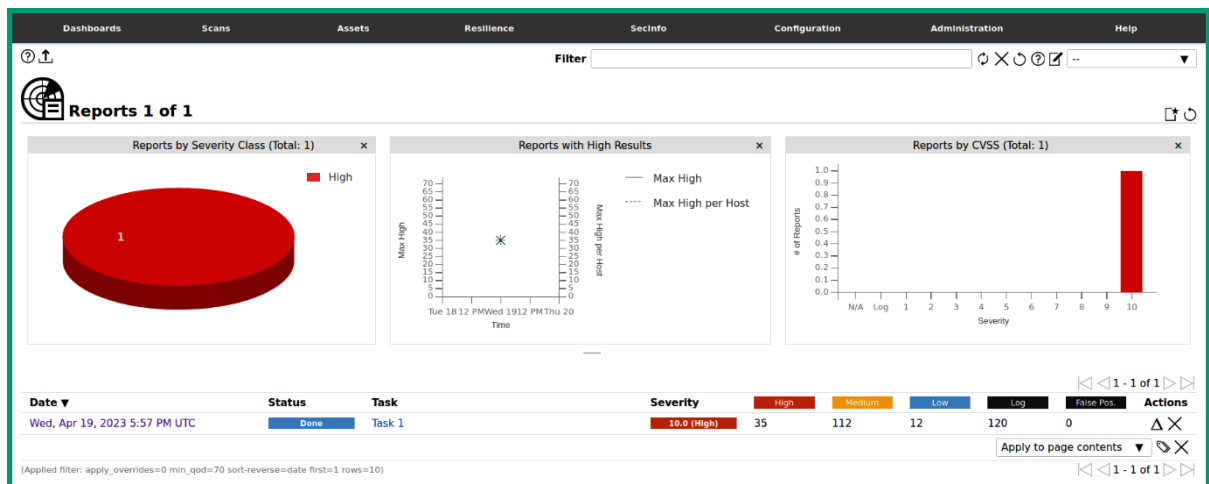
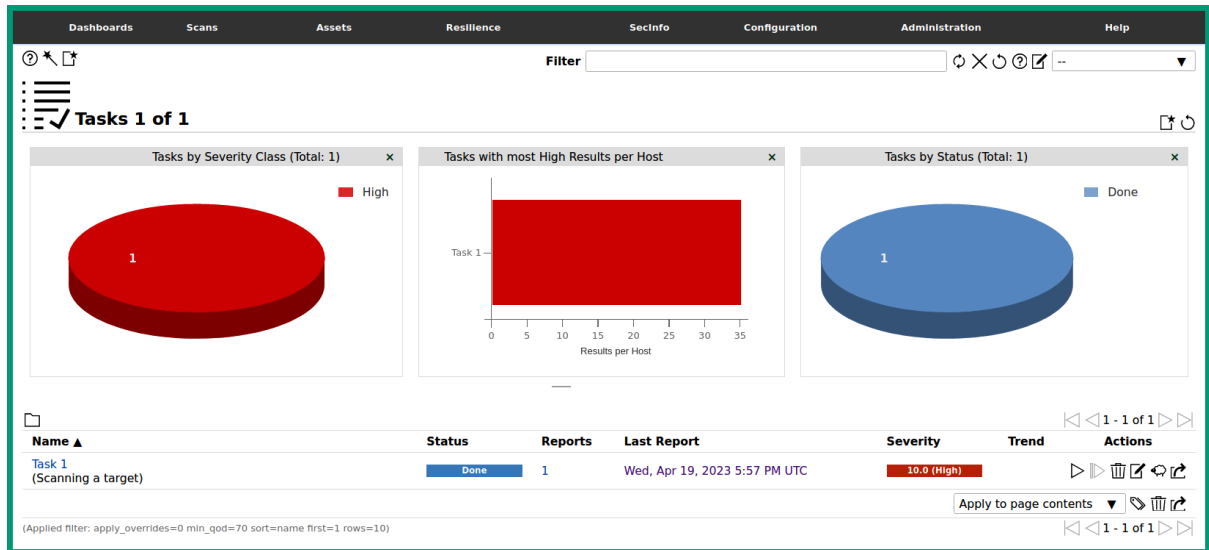
**Auto Delete Reports** ☒ Do not automatically delete reports  
☐ Automatically delete oldest reports but always keep newest  reports

**Scanner**

**Scan Config**



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Task 1 (Scanning a target)	New					<div>Click Play Button</div> <div>Apply to page contents ▼</div>







Report: Wed, Apr 19, 2023 5:57 PM UTC

Done

ID: e051727c-41eb-4cb1-ba25-2fcb9b48c05

Created: Wed, Apr 19, 2023 5:57 PM UTC

Modified: Wed, Apr 19, 2023 6:29 PM UTC

Owner: admin

Information

Results

(159 of 309)

Hosts

(1 of 1)

Ports

(12 of 20)

Applications

(10 of 10)

Operating Systems

(1 of 1)

CVEs

(141 of 141)

Closed CVEs

(16 of 16)

TLS Certificates

(4 of 4)

Error Messages

(1 of 1)

User Tags

(0)

1 - 100 of 159

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows	10.0 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	172.30.1.45		9200/tcp	Wed, Apr 19, 2023 6:13 PM UTC
MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)	10.0 (High)	95 %	172.30.1.45		80/tcp	Wed, Apr 19, 2023 6:28 PM UTC
Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)	9.8 (High)	80 %	172.30.1.45		9200/tcp	Wed, Apr 19, 2023 6:13 PM UTC
OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)	9.8 (High)	80 %	172.30.1.45		22/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows	9.8 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Oracle Mysql Security Update (cpuoct2018 - 02) - Windows	9.8 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpuju12022) - Windows	9.8 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Oracle MySQL Server <= 5.5.52 / 5.6 <= 5.6.33 / 5.7 <= 5.7.15 Security Update (cpuoct2016) - Windows	9.8 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC
Oracle MySQL Server Multiple Vulnerabilities-01 Nov12 (Windows)	9.0 (High)	80 %	172.30.1.45		3306/tcp	Wed, Apr 19, 2023 6:10 PM UTC

## Vulnerability

Name	MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)
Severity	10.0 (High)
QoD	95 %
Host	172.30.1.45
Location	80/tcp

## Summary

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

## Detection Result

Vulnerability was detected according to the Detection Method.

## Product Detection Result

Product `cpe:/a:microsoft:internet_information_services:7.5`

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

Log [View details of product detection](#)



## Detection Method

Send a special crafted HTTP GET request and check the response

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

Version used: 2022-12-05T10:11:03Z


## Affected Software/OS

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

## Impact

Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

## Solution

**Solution Type:**  Vendorfix

The vendor has released updates. Please see the references for more information.

## References

CVE [CVE-2015-1635](#)

CERT [DFN-CERT-2015-0545](#)  
[CB-K15/0527](#)

```
kali@kali:~$ ls -l /usr/share/nmap/scripts
```

```
total 4936
```

```
-rw-r--r-- 1 root root 3901 Oct 6 2022 acarsd-info.nse
-rw-r--r-- 1 root root 8749 Oct 6 2022 address-info.nse
-rw-r--r-- 1 root root 3345 Oct 6 2022 afp-brute.nse
-rw-r--r-- 1 root root 6463 Oct 6 2022 afp-ls.nse
-rw-r--r-- 1 root root 7001 Oct 6 2022 afp-path-vuln.nse
-rw-r--r-- 1 root root 5600 Oct 6 2022 afp-serverinfo.nse
-rw-r--r-- 1 root root 2621 Oct 6 2022 afp-showmount.nse
-rw-r--r-- 1 root root 2262 Oct 6 2022 ajp-auth.nse
-rw-r--r-- 1 root root 2983 Oct 6 2022 ajp-brute.nse
```

```
kali@kali:~$ ls -l /usr/share/nmap/scripts/http-vuln*
```

```
-rw-r--r-- 1 root root 3273 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2006-3392.nse
-rw-r--r-- 1 root root 6610 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2009-3960.nse
-rw-r--r-- 1 root root 2957 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2010-0738.nse
-rw-r--r-- 1 root root 5607 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2010-2861.nse
-rw-r--r-- 1 root root 4527 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2011-3192.nse
-rw-r--r-- 1 root root 5851 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2011-3368.nse
-rw-r--r-- 1 root root 4403 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2012-1823.nse
-rw-r--r-- 1 root root 4831 Oct 6 2022 /usr/share/nmap/scripts/http-vuln-cve2013-0156.nse
```



```
kali@kali:~$ ls -l /usr/share/nmap/scripts/smb-vuln*
-rw-r--r-- 1 root root 7524 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-conficker.nse
-rw-r--r-- 1 root root 6402 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root 6545 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root 5386 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root 5688 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root 5647 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root 7214 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root 7344 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root 4400 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root 6586 Oct 6 2022 /usr/share/nmap/scripts/smb-vuln-webexec.nse
```

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_
```



## Chapter 9: Delving into Website Reconnaissance

```
kali@kali:~$ host microsoft.com
microsoft.com has address 20.112.52.29
microsoft.com has address 20.103.85.33
microsoft.com has address 20.53.203.50
microsoft.com has address 20.84.181.62
microsoft.com has address 20.81.111.85
```

```
kali@kali:~$ nslookup microsoft.com 8.8.8.8
Server:                8.8.8.8
Address:                8.8.8.8#53

Non-authoritative answer:
Name:   microsoft.com
Address: 20.81.111.85
Name:   microsoft.com
Address: 20.84.181.62
Name:   microsoft.com
Address: 20.103.85.33
```

```
kali@kali:~$ dig @8.8.8.8 microsoft.com

; <>> DiG 9.18.12-1-Debian <>> @8.8.8.8 microsoft.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 11397
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
microsoft.com.      526      IN      A       20.81.111.85
microsoft.com.      526      IN      A       20.84.181.62
microsoft.com.      526      IN      A       20.103.85.33
microsoft.com.      526      IN      A       20.53.203.50
microsoft.com.      526      IN      A       20.112.52.29

;; Query time: 91 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Apr 28 14:07:52 AST 2023
;; MSG SIZE rcvd: 122
```



```
kali@kali:~$ dig @8.8.8.8 microsoft.com NS
```

```
; <<>> DiG 9.18.12-1-Debian <<>> @8.8.8.8 microsoft.com NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 14671
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;microsoft.com.                IN      NS
```

Name Servers



```
;; ANSWER SECTION:
```

```
microsoft.com.      21548   IN      NS
microsoft.com.      21548   IN      NS
microsoft.com.      21548   IN      NS
microsoft.com.      21548   IN      NS
```

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

```
kali@kali:~$ dnsrecon -d microsoft.com -n 8.8.8.8
```

```
[*] std: Performing General Enumeration against: microsoft.com...
```

```
[-] DNSSEC is not configured for microsoft.com
```

```
[*]      SOA ns1-39.azure-dns.com 150.171.10.39
[*]      SOA ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns1-39.azure-dns.com 150.171.10.39
[*]      NS ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns2-39.azure-dns.net 150.171.16.39
[*]      NS ns2-39.azure-dns.net 2620:1ec:8ec:10::27
[*]      NS ns3-39.azure-dns.org 13.107.222.39
[*]      NS ns3-39.azure-dns.org 2a01:111:4000:10::27
[*]      NS ns4-39.azure-dns.info 13.107.206.39
```

```
kali@kali:~$ wafw00f cloudflare.com
```



~ WAFW00F : v2.2.0 ~

```
[*] Checking https://cloudflare.com
```

```
[+] The site https://cloudflare.com is behind Cloudflare (Cloudflare Inc.) WAF.
```

```
[~] Number of requests: 2
```



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

```
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-04-01T11:51:08Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2024-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
```

## What's that site running?


Find out the infrastructure and technologies used by any site using results from our **internet data mining**

microsoft.com

Example: <https://www.netcraft.com>

Look up

### Network

Site	<a href="http://microsoft.com">http://microsoft.com</a>	Domain	<a href="http://microsoft.com">microsoft.com</a>
Netblock Owner	<a href="#">Microsoft Corporation</a>	Nameserver	ns1-39.azure-dns.com
Hosting company	Microsoft - Europe West (Netherlands) datacenter	Domain registrar	markmonitor.com
Hosting country	 <a href="#">nl</a>	Nameserver organisation	whois.markmonitor.com
IPv4 address	20.112.52.29 ( <a href="#">VirusTotal</a> )	Organisation	Microsoft Corporation, One Microsoft Way., Redmond, 98052, United States
IPv4 autonomous systems	<a href="#">AS8075</a>	DNS admin	azuredns-hostmaster@microsoft.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	unknown		



IP delegation

IPv4 address (20.112.52.29)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
📶 20.0.0.0-20.255.255.255	United States	NET20	American Registry for Internet Numbers
📶 20.33.0.0-20.128.255.255	United States	MSFT	Microsoft Corporation
📶 20.112.52.29	United States	MSFT	Microsoft Corporation

dns recon & research, find & lookup dns records

microsoft.com

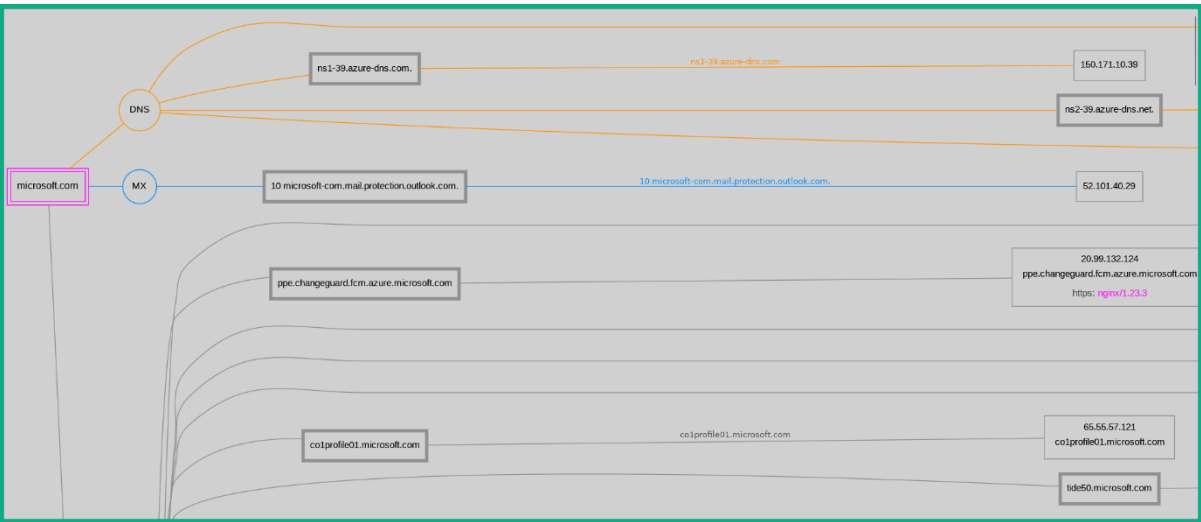
Search ➔

DNS Servers

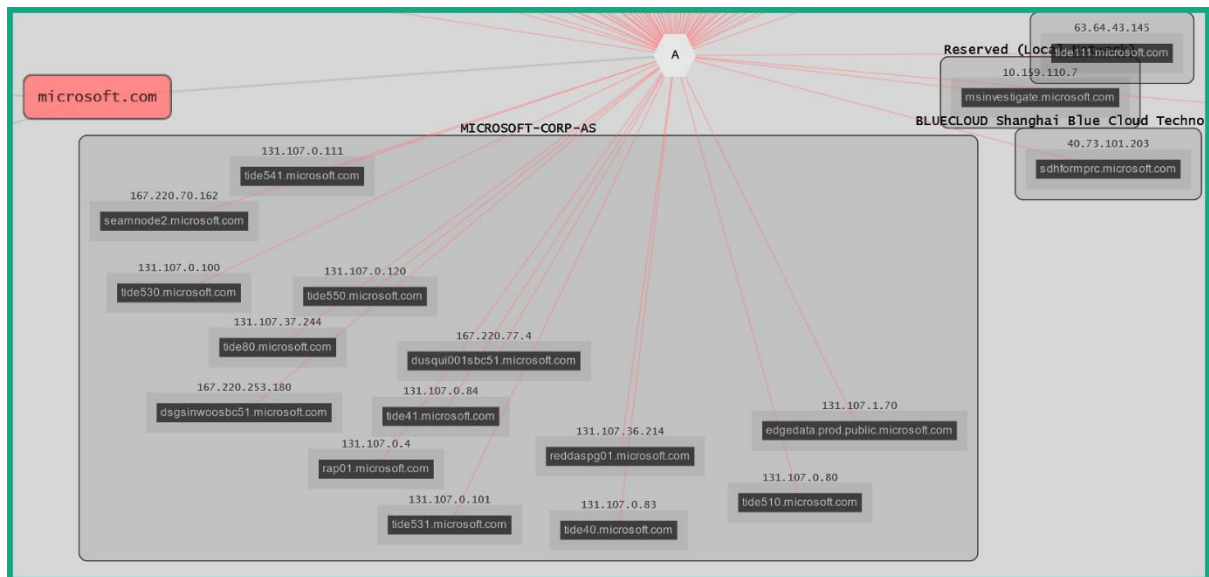
ns1-39.azure-dns.com. 	150.171.10.39 ns1-39.azure-dns.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns2-39.azure-dns.net. 	150.171.16.39 ns2-39.azure-dns.net	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns3-39.azure-dns.org. 	13.107.222.39 ns3-39.azure-dns.org	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns4-39.azure-dns.info. 	13.107.206.39 ns4-39.azure-dns.info	MICROSOFT-CORP-MSN-AS-BLOCK United States

MX Records \*\* This is where email for the domain goes...

10 microsoft-com.mail.protection.outlook.com. 	52.101.40.29	MICROSOFT-CORP-MSN-AS-BLOCK United States
---	--------------	--







```
kali@kali:~$ whatweb https://github.com
https://github.com [200 OK] Content-Language[en-US], Cookies[_gh_sess,octo
,logged_in], Country[UNITED STATES][US], HTML5, HTTPServer[GitHub.com], Htt
pOnly[_gh_sess,logged_in], IP[140.82.114.4], Open-Graph-Protocol[object][14
01488693436528], OpenSearch[/opensearch.xml], Script[application/javascript
], Strict-Transport-Security[max-age=31536000; includeSubdomains; preload],
Title[GitHub: Let's build from here • GitHub], UncommonHeaders[x-content-t
ype-options,referer-policy,content-security-policy,x-github-request-id], X
-Frame-Options[deny], X-XSS-Protection[0]
```

Firefox Browser

# ADD-ONS

Extensions Themes More... ▾

## Wappalyzer

by Wappalyzer

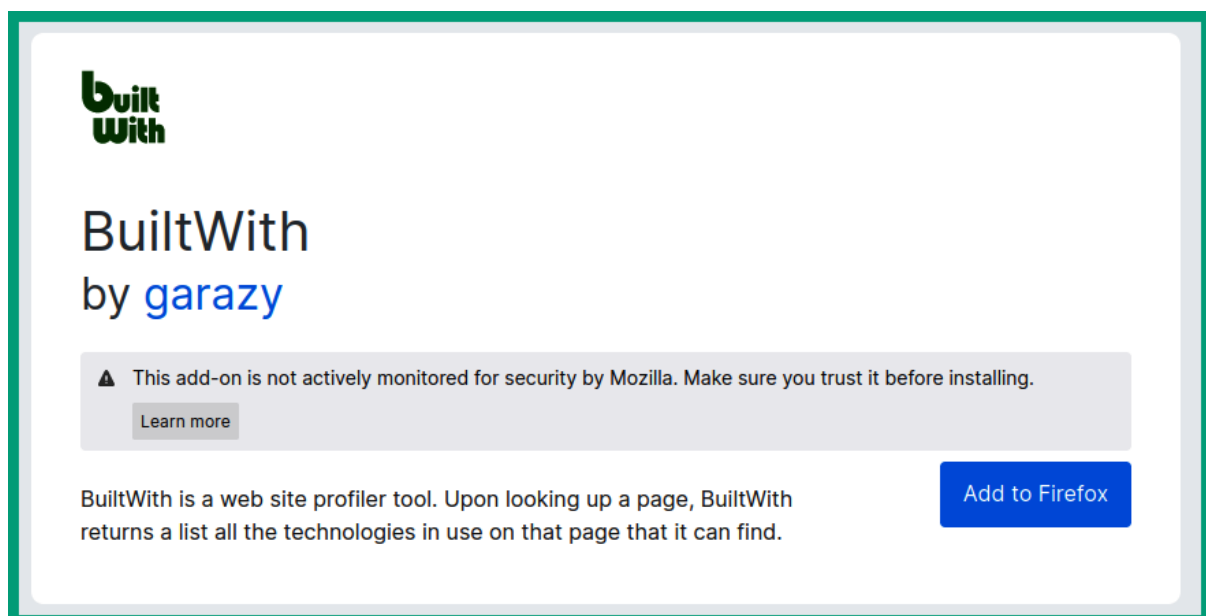
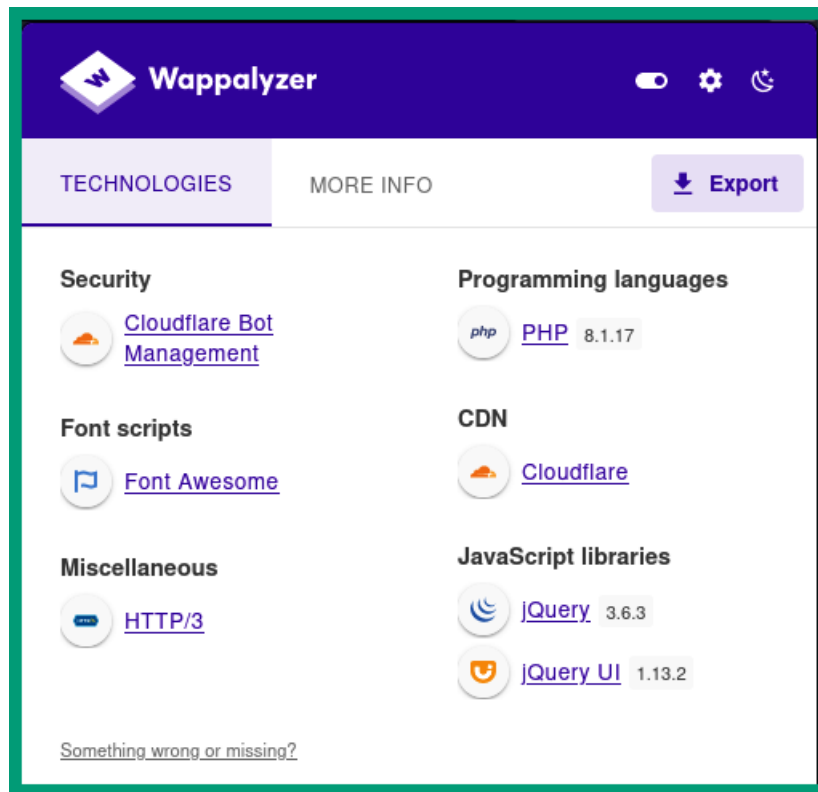
⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

[Learn more](#)

Identify technologies on websites

[Add to Firefox](#)







Widgets

[View Global Trends](#)

## Google Tag Manager

Google Tag Manager Usage Statistics · Download List of All Websites using Google Tag Manager

Tag management that lets you add and update website tags without changes to underlying website code.

Tag Management

Language

[View Global Trends](#)

## English HREF LANG

English HREF LANG Usage Statistics · Download List of All Websites using English HREF LANG

This webpage has alternate versions available in English via the use of the hreflang tag.

## Portuguese HREF LANG

Portuguese HREF LANG Usage Statistics · Download List of All Websites using Portuguese HREF LANG

This webpage has alternate versions available in

```
kali@kali:~$ cd Sublist3r
```

```
kali@kali:~/Sublist3r$ sudo pip install -r requirements.txt
```

```
Collecting argparse
```

```
Using cached argparse-1.4.0-py2.py3-none-any.whl (23 kB)
```

```
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages
```

```
Requirement already satisfied: requests in /usr/lib/python3/dist-packages
```

```
Installing collected packages: argparse
```


```
Successfully installed argparse-1.4.0
```



```

[-] Enumerating subdomains now for [REDACTED].com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 6
www.[REDACTED].com
autodiscover.[REDACTED].com
cpanel.[REDACTED].com
mail.[REDACTED].com
webdisk.[REDACTED].com
webmail.[REDACTED].com

```



**Sub-Domains**

```

options:
-h, --help                show this help message and exit
-d DOMAIN, --domain DOMAIN
                           Company name or domain to search.
-l LIMIT, --limit LIMIT   Limit the number of search results, default=500.
-S START, --start START   Start with result number X, default=0.
-p, --proxies              Use proxies for requests, enter proxies in proxies.yaml.
-s, --shodan               Use Shodan to query discovered hosts.
--screenshot SCREENSHOT   Take screenshots of resolved domains specify output directory: --screenshot output_directory
-v, --virtual-host         Verify host name via DNS resolution and search for virtual hosts.
-e DNS_SERVER, --dns-server DNS_SERVER
                           DNS server to use for lookup.
-r, --take-over            Check for takeovers.
-n, --dns-lookup           Enable DNS server lookup, default False.
-c, --dns-brute            Perform a DNS brute force on the domain.
-f FILENAME, --filename FILENAME
                           Save the results to an XML and JSON file.
-b SOURCE, --source SOURCE
                           anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverrun, censys, certspotter, crtsh,
                           dnsdumpster, duckduckgo, fullhunt, github-code, hackertarget, hunter, intelx, omnisint, otx,
                           pentesttools, projectdiscovery, qwant, rapiddns, rocketreach, securityTrails, sublist3r,
                           threatcrowd, threatminer, urlscan, virustotal, yahoo, zoomeye

```



[\*] Hosts found: 109

assessment.changeguard.fcm.azure.microsoft.com:20.69.174.99  
auditboard-ppe.microsoft.com:52.143.78.92  
awsuiu1.microsoft.com:13.77.211.251  
bayprofile10.microsoft.com:64.4.17.21  
bayprofile11.microsoft.com:64.4.17.22  
bn1vlscstest01.microsoft.com:134.170.22.43  
changeguard.fcm.azure.microsoft.com:20.69.174.99  
changemanager.fcm.azure.microsoft.com:20.69.145.220  
cmsbn1test01.microsoft.com:134.170.22.53  
cmsco2test60.microsoft.com:134.170.184.45  
colprofile01.microsoft.com:65.55.57.121  
comm-image.microsoft.com:13.88.11.232  
cus.dlsppe.microsoft.com:52.154.223.20  
dsgsinwoosbc51.microsoft.com:167.220.253.180

Ip address	Code	Subdomain	Real hostname	Server
(ctrl+c)   1.15%   6d75338fc909107.twitter.com				
104.244.42.131	400	0.twitter.com	s.twitter.com	tsa_b
104.244.42.195	200	2012.twitter.com	s.twitter.com	tsa_b
104.244.42.67	200	2013.twitter.com	s.twitter.com	tsa_b
104.244.42.131	200	2010.twitter.com	s.twitter.com	tsa_b
104.244.42.67	200	2011.twitter.com	s.twitter.com	tsa_b
104.244.42.67	200	2014.twitter.com	s.twitter.com	tsa_b



```
[+] Domain:      microsoft.com
[+] Threads:     10
[+] Timeout:     1s
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
```

```
2023/04/26 13:03:28 Starting gobuster in DNS enumeration mode
```

```
Found: academic.microsoft.com
```

```
Found: account.microsoft.com
```

```
Found: accountants.microsoft.com
```

```
Found: accounts.microsoft.com
```

```
Found: activate.microsoft.com
```

```
Found: activex.microsoft.com
```

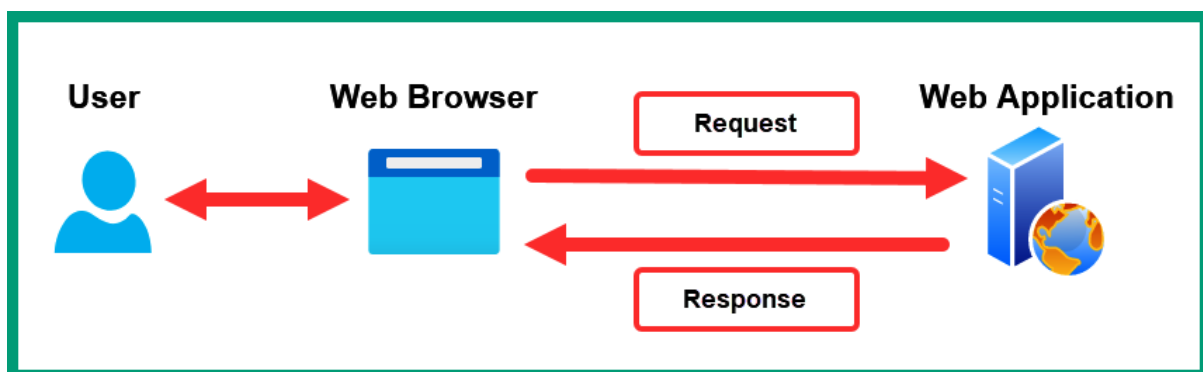
```
Found: admin.microsoft.com
```

**Enumerated Sub-Domains**

```
/~administrator (Status: 301)
/~amanda (Status: 301)
/~ftp (Status: 301)
/~apache (Status: 301)
/~bin (Status: 301)
/~guest (Status: 301)
/~httpd (Status: 301)
/~www (Status: 301)
/08 (Status: 200)
/04 (Status: 200)
/02 (Status: 200)
/01 (Status: 200)
```



```
--- Scanning URL: http://127.0.0.1:3000/ ---
+ http://127.0.0.1:3000/assets (CODE:301|SIZE:179)
+ http://127.0.0.1:3000/ftp (CODE:200|SIZE:11062)
+ http://127.0.0.1:3000/profile (CODE:500|SIZE:1243)
+ http://127.0.0.1:3000/promotion (CODE:200|SIZE:6586)
+ http://127.0.0.1:3000/redirect (CODE:500|SIZE:3119)
+ http://127.0.0.1:3000/robots.txt (CODE:200|SIZE:28)
+ http://127.0.0.1:3000/snippets (CODE:200|SIZE:683)
```



```
kali@kali:~$ nikto -h http://127.0.0.1:3000
- Nikto v2.1.6

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 3000
+ Start Time: 2023-04-26 13:15:50 (GMT-4)

+ Server: No banner retrieved
+ Retrieved access-control-allow-origin header: *
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
+ Uncommon header 'x-recruiting' found, with contents: /#/jobs
+ Uncommon header 'feature-policy' found, with contents: payment 'self'
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/ftp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ /site.jks: Potentially interesting archive/cert file found.
```



## RUNNING TCP PORT SCAN

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-30 11:20 AST
Nmap scan report for [REDACTED].com (172.67.168.43)
Host is up (0.065s latency).
Other addresses for [REDACTED].com (not scanned): [REDACTED]
Not shown: 59 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

## RUNNING COMMON FILE/DIRECTORY BRUTE FORCE

 v0.4.2

**Target:** [http://\[REDACTED\].com:80/](http://[REDACTED].com:80/)

**[11:21:42] Starting:**

```
[11:21:44] 200 -      3KB - /1.txt
[11:21:45] 200 -      3KB - /123.txt
[11:21:45] 200 -      3KB - /2.txt
[11:21:46] 200 -      3KB - /access.txt
[11:21:46] 200 -      3KB - /accounts.txt
[11:21:46] 200 -      3KB - /admin/access.txt
[11:21:47] 200 -      3KB - /admin/error.txt
[11:21:49] 200 -      3KB - /admins/log.txt
[11:21:49] 200 -      3KB - /admin/_logs/login.txt
[11:21:49] 200 -      3KB - /admin/logs/login.txt
```



```
kali@kali:~$ amass enum -d microsoft.com
tide510.microsoft.com
mail-db9lp0239.outbound.messaging.microsoft.com
wus2-stagingretrieval-dcatbackend-int.staging.bigcatalog-int.commerce.microsoft.com
tide530.microsoft.com
52-114-125-40.relay.teams.microsoft.com
52-114-124-131.relay.teams.microsoft.com
order.rest.store.internal.colc.microsoft.com
52-114-124-248.relay.teams.microsoft.com
52-114-125-41.relay.teams.microsoft.com
52-114-125-25.relay.teams.microsoft.com
52-114-124-41.relay.teams.microsoft.com
spteam2010.microsoft.com
```

38 names discovered - scrape: 29, api: 6, archive: 1, cert: 2

```
ASN: 262589 - INTERNEXA BRASIL OPERADORA DE TELECOMUNICACOES S.A
    23.219.152.0/22      2      Subdomain Name(s)
ASN: 20940 - AKAMAI-ASN1
    23.33.40.0/21       2      Subdomain Name(s)
    23.56.5.0/24        4      Subdomain Name(s)
    23.50.8.0/24        2      Subdomain Name(s)
ASN: 0 - Not routed
    64.5.32.0/19        1      Subdomain Name(s)
ASN: 3598 - MICROSOFT-CORP-AS - Microsoft Corporation
    131.107.0.0/17      5      Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
    213.199.128.0/18    3      Subdomain Name(s)
    52.112.0.0/14       11     Subdomain Name(s)
    70.37.128.0/18      1      Subdomain Name(s)
    20.64.0.0/10        9      Subdomain Name(s)
```

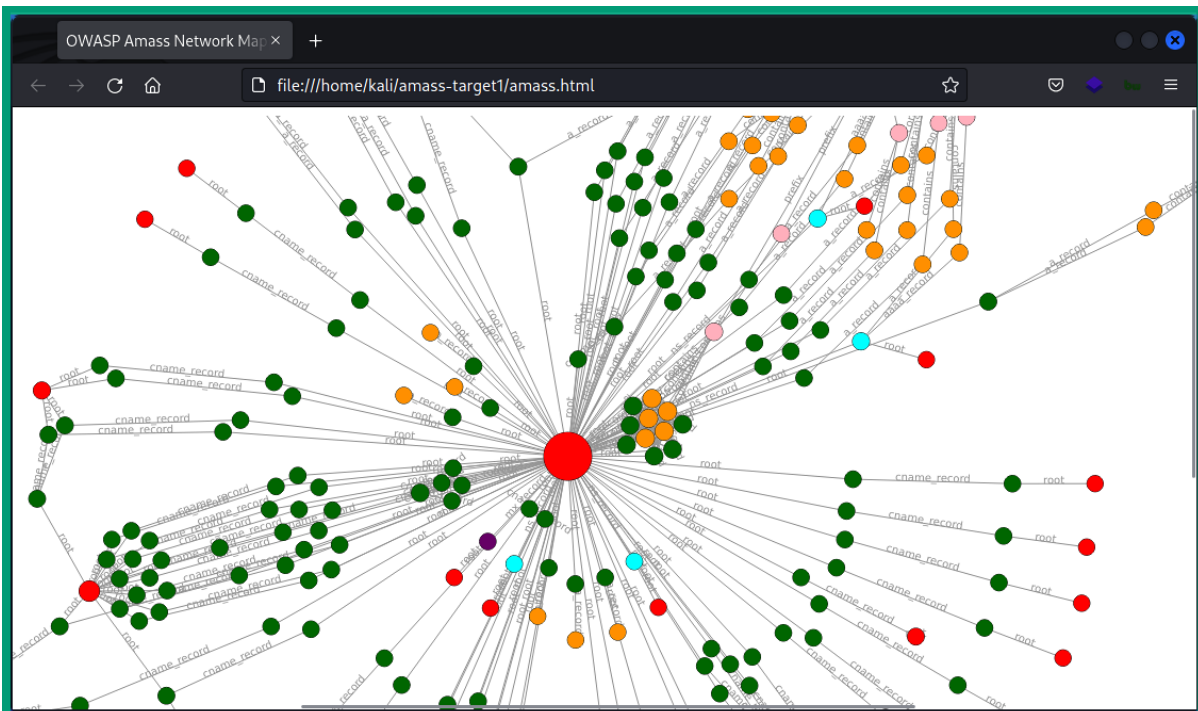
```
kali@kali:~$ amass intel -whois -d microsoft.com -dir /home/kali/amass-target1
0fficeteam.com
1-800-microsoft.com
121hotmailhelp.com
123hotmail.com
123hotmail.net
123lovehotmail.com
123xbox.com
1drive.com
1drive.net
1drv.com
1hotmail.com
1xbox.com
```



```
kali@kali:~$ amass enum -passive -d microsoft.com -src
[ RapidDNS ]      wus2-frontdoor-displaycatalog-int.bigcatalog.microsoft.com
[ AnubisDB ]      000dco2o40pl1.redmond.corp.microsoft.com
[ AnubisDB ]      accountservices.microsoft.com
[ AnubisDB ]      globalmigration.partners.extranet.microsoft.com
[ AnubisDB ]      servicedeliveryws.microsoft.com
[ RapidDNS ]      36-usce.noam.prn.audience.teams.microsoft.com
[ AnubisDB ]      dns11.one.microsoft.com
[ RapidDNS ]      reportingapi.bingads.microsoft.com
```

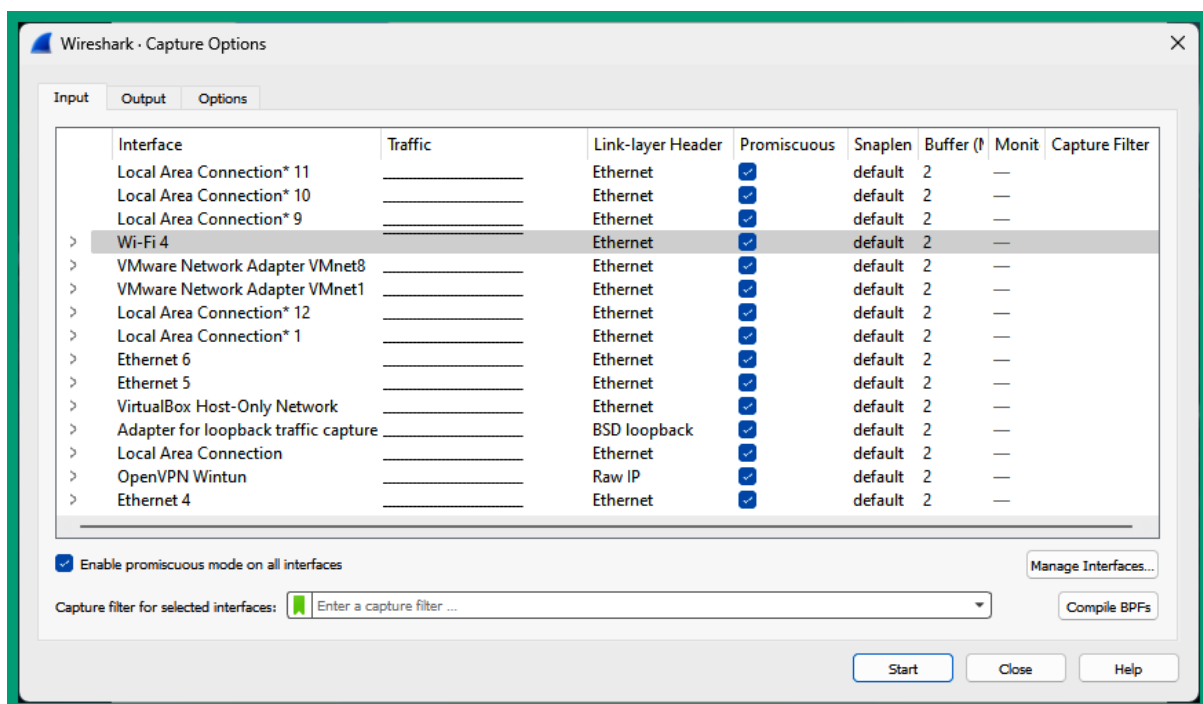
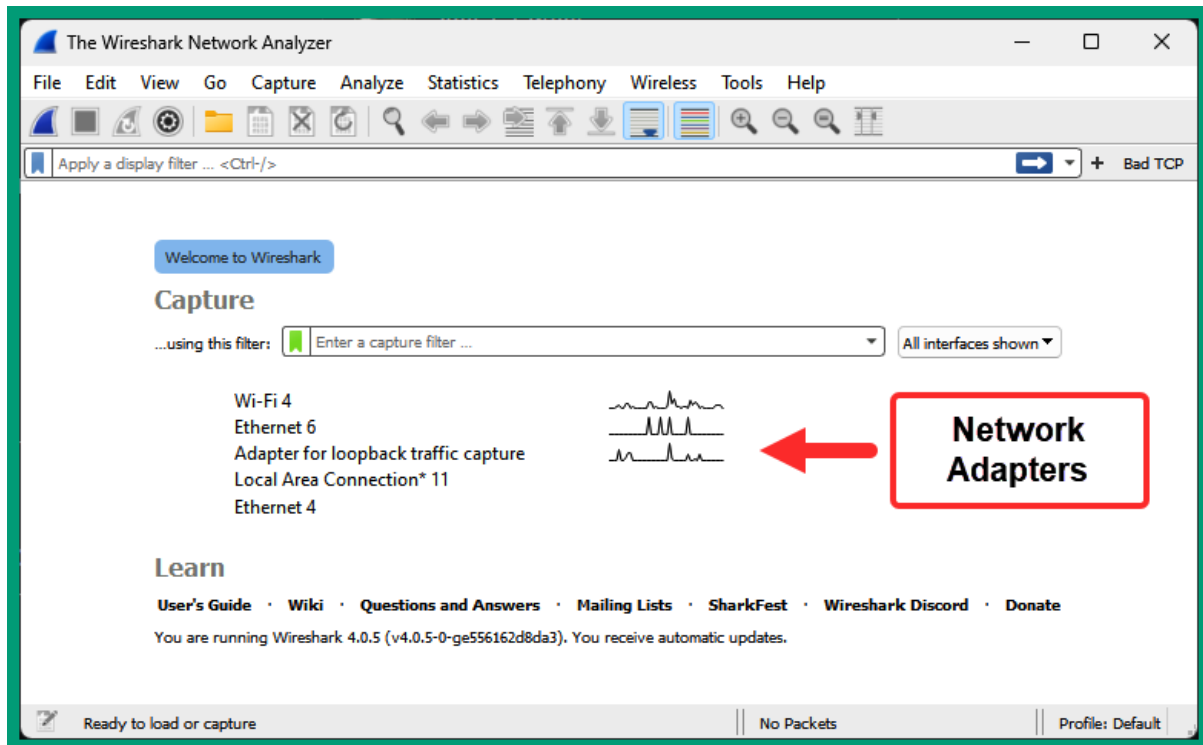
```
kali@kali:~$ amass enum -d microsoft.com -src -ip -brute -dir /home/kali/amass-target1
[ Brute Forcing ] broadcast.microsoft.com 209.240.199.60
[ DNS ]           microsoft.com 20.112.52.29,20.103.85.33,20.84.181.62,20.81.111.85
[ Brute Forcing ] demo.microsoft.com 20.112.52.29,20.84.181.62,20.103.85.33,20.81.111.85
[ Brute Forcing ] mail2.microsoft.com 131.107.115.215
[ DNSSpy ]        mail6.microsoft.com 205.248.106.32
[ Brute Forcing ] mail.microsoft.com 167.220.71.19
[ Brute Forcing ] shop.microsoft.com 20.84.181.62,20.81.111.85,20.103.85.33,20.112.52.29
[ Brute Forcing ] mi.microsoft.com 20.84.181.62,20.81.111.85,20.112.52.29,20.103.85.33
[ DNS ]           epqdata.microsoft.com 209.240.199.60
```

```
kali@kali:~$ amass db -dir /home/kali/amass-target1 -list
1) 04/30 17:22:19 2023 UTC → 04/30 17:25:21 2023 UTC: adobe.com, windows.n
et, microsoft.com, azure.com, akadns.net, azure-dns.org, mktoweb.com, azure
-dns.com, office.com, 1eslivesecrets.azurewebsites.net, azure-dns.info, a-m
sedge.net, wpeproxy.com, azurefd.net, dispositionjournalfd-eastus2-commerci
al.azurewebsites.net, azure-dns.net, sharepoint.com, lync.com, b-msedge.net
, nsatc.net, ost-thirdpartycode-prod.azurewebsites.net, audience-prd-noam-u
sce-14.cloudapp.net, trafficmanager.net, edgekey.net, dynamitecdn.com, best
practice-prod.azurewebsites.net, outlook.com, office.net, p.azurewebsites.n
et
```

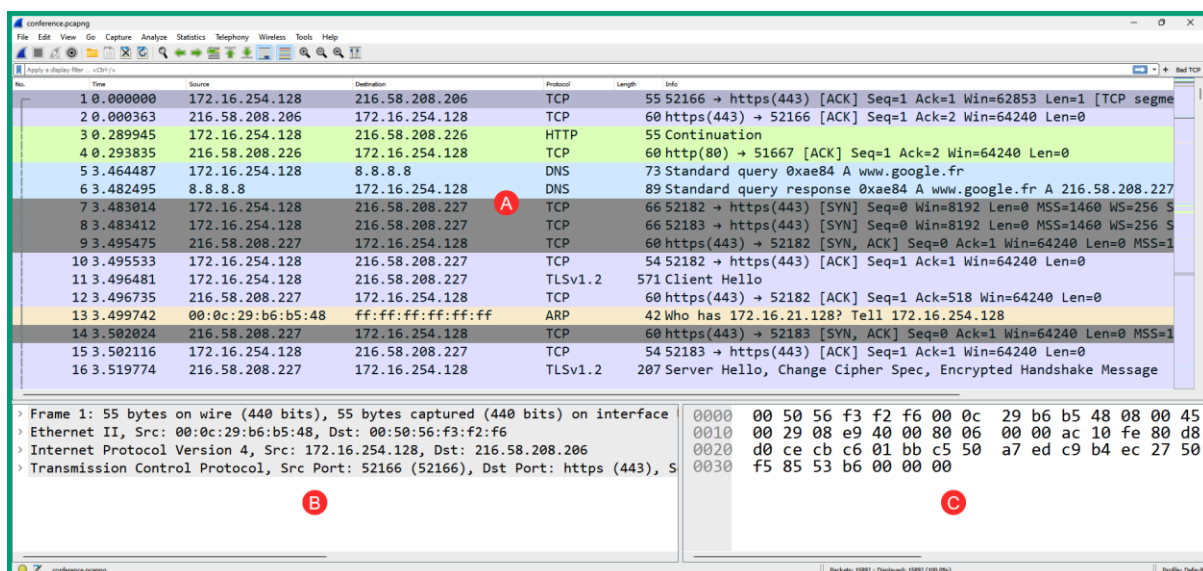
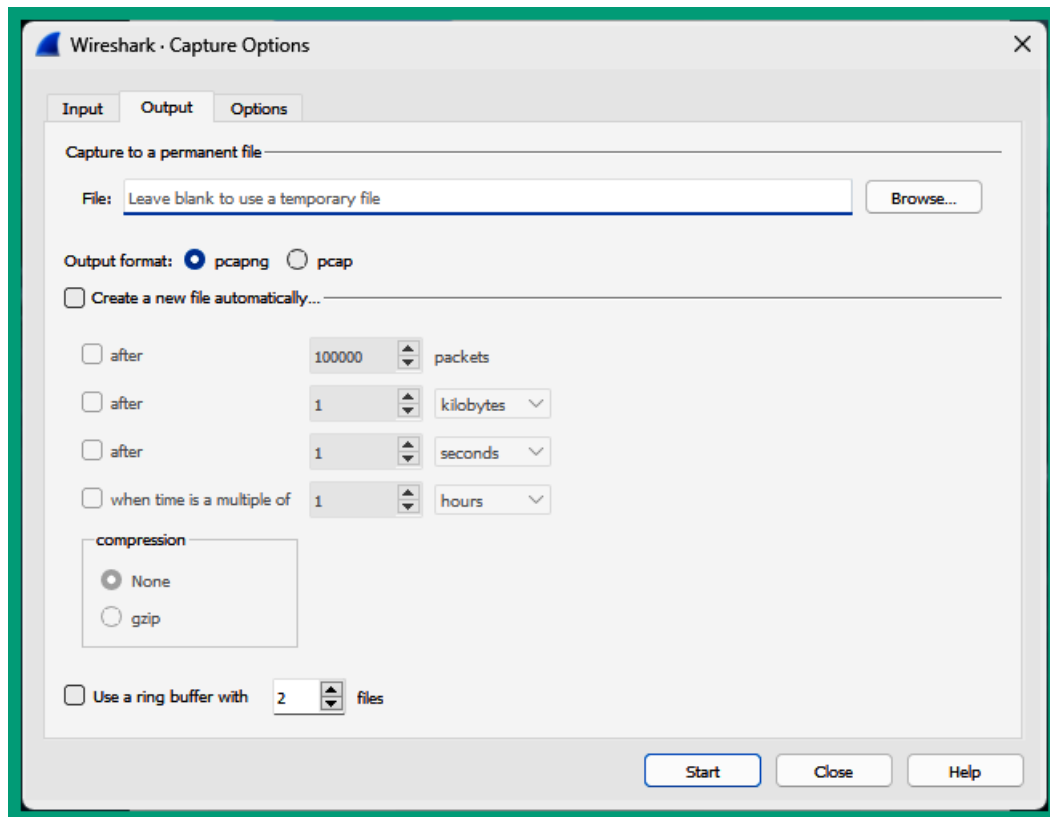




# Chapter 10: Implementing Recon Monitoring and Detection Systems



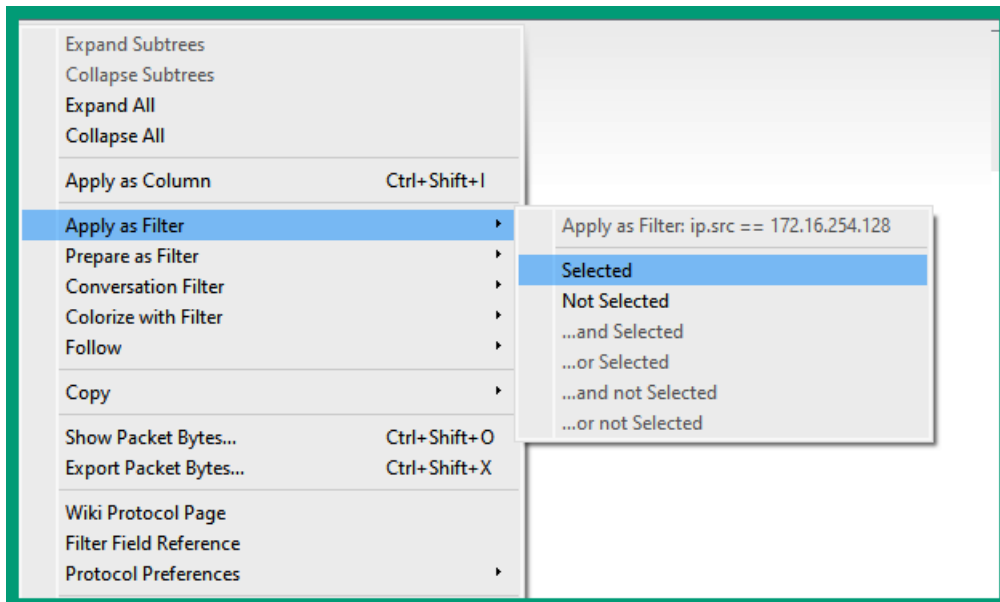






- > Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface
- > Ethernet II, Src: 00:0c:29:b6:b5:48, Dst: 00:50:56:f3:f2:f6
- > Internet Protocol Version 4, Src: 172.16.254.128, Dst: 8.8.8.8
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 59
  - Identification: 0x08eb (2283)
  - > 000. .... = Flags: 0x0
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: UDP (17)
  - Header Checksum: 0x0000 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 172.16.254.128
  - Destination Address: 8.8.8.8
  - > [Destination GeoIP: Los Angeles, US, ASN 15169, GOOGLE]
- > User Datagram Protocol, Src Port: 61125 (61125), Dst Port: domain (53)

Right-click on the IP address



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.254.128	216.58.208.206	TCP	55	52166 → https(443) [ACK]
3	0.289945	172.16.254.128	216.58.208.226	HTTP	55	Continuation
5	3.464487	172.16.254.128	8.8.8.8	DNS	73	Standard query 0xae84 A w
7	3.483014	172.16.254.128	216.58.208.227	TCP	66	52182 → https(443) [SYN]
8	3.483412	172.16.254.128	216.58.208.227	TCP	66	52183 → https(443) [SYN]
10	3.495533	172.16.254.128	216.58.208.227	TCP	54	52182 → https(443) [ACK]
11	3.496481	172.16.254.128	216.58.208.227	TLSv1.2	571	Client Hello
15	3.502116	172.16.254.128	216.58.208.227	TCP	54	52183 → https(443) [ACK]
17	3.561668	172.16.254.128	216.58.208.227	TLSv1.2	270	Change Cipher Spec, Encry
19	3.562470	172.16.254.128	216.58.208.227	TLSv1.2	571	Client Hello
23	3.582387	172.16.254.128	216.58.208.227	TCP	54	52182 → https(443) [ACK]



No.	Time	Source	Destination	Protocol	Length	Info
5	3.464487	172.16.254.128	8.8.8.8	DNS	73	Standard query 0xae84 A www.google.fr
63	3.932662	172.16.254.128	8.8.8.8	DNS	75	Standard query 0xfec2 A ssl.gstatic.com
204	4.398457	172.16.254.128	8.8.8.8	DNS	74	Standard query 0xc9f8 A www.reddit.com
462	5.853759	172.16.254.128	8.8.8.8	DNS	75	Standard query 0x7ff9 A www.gstatic.com
525	6.026648	172.16.254.128	8.8.8.8	DNS	75	Standard query 0x391b A apis.google.com
970	7.861516	172.16.254.128	8.8.8.8	DNS	84	Standard query 0x1553 A www.google-analytics.com
971	7.861831	172.16.254.128	8.8.8.8	DNS	76	Standard query 0x00d0 A en.wikipedia.org
978	7.881850	172.16.254.128	8.8.8.8	DNS	74	Standard query 0x2b60 A soundcloud.com
1048	8.227485	172.16.254.128	8.8.8.8	DNS	71	Standard query 0x18df A i.imgur.com
1049	8.227771	172.16.254.128	8.8.8.8	DNS	69	Standard query 0x0dd0 A imgur.com

Wireshark · Preferences

Appearance

Columns

Font and Colors

Layout

Capture

Expert

Filter Buttons

Name Resolution

Protocols

RSA Keys

Statistics

Advanced

Name Resolution

☐ Resolve MAC addresses
 ☒ Resolve transport names
 ☐ Resolve network (IP) addresses
 ☒ Use captured DNS packet data for name resolution
 ☒ Use your system's DNS settings for name resolution
 ☐ Use a custom list of DNS servers for name resolution

DNS Servers
 

Edit...

Maximum concurrent requests
 

500

☐ Only use the profile "hosts" file
 ☐ Resolve VLAN IDs
 ☐ Resolve SS7 PCs
 ☐ Enable OID resolution
 ☐ Suppress SMI errors

SMI (MIB and PIB) paths
 

Edit...

SMI (MIB and PIB) modules
 

Edit...

OK

Cancel

Help

Wireshark · Conversations · conference.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Ethernet · 5IPv4 · 52IPv6 · 1TCP · 149UDP · 100

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:0c:29:b6:b5:48	00:50:56:f3:f2:f6	15,829	13,606 MiB	4,522	4,350 MiB	11,307	9,256 MiB	0.000000	191.0991	186.489 KiB	396.768 KiB
00:0c:29:b6:b5:48	01:00:5e:00:00:fc	2	128 bytes	2	128 bytes	0	0 bytes	31.924809	0.1000	10.003 KiB	0 bytes
00:0c:29:b6:b5:48	33:33:00:01:00:03	2	168 bytes	2	168 bytes	0	0 bytes	31.924562	0.1000	13.118 KiB	0 bytes
00:0c:29:b6:b5:48	ff:ff:ff:ff:ff:ff	53	2,467 KiB	53	2,467 KiB	0	0 bytes	3.499742	146.1293	138 bytes	0 bytes
00:50:56:c0:00:08	ff:ff:ff:ff:ff:ff	6	996 bytes	6	996 bytes	0	0 bytes	27.474104	156.9633	50 bytes	0 bytes



Wireshark · Conversations · conference.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

Filter list for specific type

Ethernet · 5

IPv4 · 52

IPv6 · 1

TCP · 149

UDP · 100

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.254.1	172.16.254.255	6	996 bytes	6	996 bytes	0	0 bytes	27.474104	156.9633	50 bytes	0 bytes
172.16.254.128	8.8.8.8	195	22.566 KiB	97	7.261 KiB	98	15.306 KiB	3.464487	157.7660	377 bytes	794 bytes
172.16.254.128	23.21.60.15	60	35.608 KiB	23	11.482 KiB	37	24.126 KiB	9.197825	17.6576	5.202 KiB	10.930 KiB
172.16.254.128	23.192.162.171	27	7.734 KiB	12	1.950 KiB	15	5.784 KiB	51.592620	60.3368	264 bytes	785 bytes
172.16.254.128	23.205.82.104	29	14.088 KiB	12	2.286 KiB	17	11.802 KiB	38.202987	0.0989	184.964 KiB	954.844 KiB
172.16.254.128	23.205.92.118	55	55.388 KiB	17	1.225 KiB	38	54.163 KiB	36.354561	0.1545	63.397 KiB	2.738 MiB
172.16.254.128	31.13.93.3	134	49.380 KiB	55	8.016 KiB	79	41.364 KiB	38.190018	90.2123	727 bytes	3.668 KiB
172.16.254.128	37.252.163.152	28	23.482 KiB	8	3.966 KiB	20	19.517 KiB	39.260294	0.7001	45.319 KiB	223.028 KiB
172.16.254.128	37.252.163.209	11	3.874 KiB	5	1.174 KiB	6	2.700 KiB	40.778490	0.3395	27.657 KiB	63.621 KiB
172.16.254.128	54.192.79.107	402	389.323 KiB	121	10.040 KiB	281	379.283 KiB	34.833362	0.5677	141.477 KiB	5.219 MiB
172.16.254.128	54.225.150.134	14	816 bytes	8	456 bytes	6	360 bytes	14.078783	19.8989	183 bytes	144 bytes
172.16.254.128	54.227.250.135	69	16.025 KiB	33	5.121 KiB	36	10.904 KiB	9.154900	24.8366	1.649 KiB	3.512 KiB
172.16.254.128	54.230.78.45	284	256.475 KiB	87	13.257 KiB	197	243.218 KiB	34.812413	6.5728	16.135 KiB	296.030 KiB
172.16.254.128	54.231.10.92	450	270.724 KiB	172	33.991 KiB	278	236.732 KiB	50.375404	104.3052	2.606 KiB	18.156 KiB
172.16.254.128	54.231.32.188	12	690 bytes	6	330 bytes	6	360 bytes	15.156664	0.9305	2.771 KiB	3.022 KiB
172.16.254.128	54.241.5.77	11	1.689 KiB	6	972 bytes	5	758 bytes	34.817583	0.6394	11.876 KiB	9.261 KiB
172.16.254.128	54.241.33.115	12	4.888 KiB	6	721 bytes	6	4.184 KiB	36.749203	0.5050	11.154 KiB	66.279 KiB
172.16.254.128	81.166.122.238	10,124	9.549 MiB	2,570	4.082 MiB	7,554	5.467 MiB	66.066809	125.0323	267.459 KiB	358.161 KiB

Close

Help

Wireshark · Conversations · conference.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

Filter list for specific type

Ethernet · 5IPv4 · 52IPv6 · 1TCP · 149UDP · 100

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bit
172.16.254.128	52164	23.21.60.15	80	60	35.608 KiB	31	23	11.482 KiB	37	24.126 KiB	9.197825	17.6576	
172.16.254.128	52404	23.192.162.171	443	27	7.734 KiB	141	12	1.950 KiB	15	5.784 KiB	51.592620	60.3368	
172.16.254.128	52242	23.205.82.104	443	21	12.887 KiB	97	8	1.485 KiB	13	11.401 KiB	38.202987	0.0989	
172.16.254.128	52243	23.205.82.104	443	8	1.201 KiB	98	4	820 bytes	4	410 bytes	38.203291	0.0437	
172.16.254.128	52094	23.205.92.118	80	55	55.388 KiB	80	17	1.225 KiB	38	54.163 KiB	36.354561	0.1545	
172.16.254.128	52240	31.13.93.3	80	8	2.688 KiB	95	4	1.021 KiB	4	1.668 KiB	38.190018	0.2707	
172.16.254.128	52241	31.13.93.3	80	3	180 bytes	96	2	120 bytes	1	60 bytes	38.190321	0.0327	
172.16.254.128	52253	31.13.93.3	443	33	14.065 KiB	109	12	2.430 KiB	21	11.636 KiB	39.227831	1.9469	
172.16.254.128	52254	31.13.93.3	443	11	1.548 KiB	110	5	915 bytes	6	670 bytes	39.228773	0.2043	
172.16.254.128	52399	31.13.93.3	80	7	408 bytes	136	4	228 bytes	3	180 bytes	50.755226	10.2825	
172.16.254.128	52400	31.13.93.3	80	14	2.274 KiB	137	7	963 bytes	7	1.334 KiB	50.946738	70.0672	
172.16.254.128	52401	31.13.93.3	443	58	28.229 KiB	138	21	2.392 KiB	37	25.838 KiB	51.161444	77.2409	
172.16.254.128	52255	37.252.163.152	80	28	23.482 KiB	111	8	3.966 KiB	20	19.517 KiB	39.260294	0.7001	
172.16.254.128	52269	37.252.163.209	80	11	3.874 KiB	126	5	1.174 KiB	6	2.700 KiB	40.778490	0.3395	
172.16.254.128	52220	54.192.79.107	80	85	80.108 KiB	69	27	2.153 KiB	58	77.955 KiB	34.833362	0.3822	
172.16.254.128	52221	54.192.79.107	80	53	50.937 KiB	70	16	1.573 KiB	37	49.363 KiB	34.833739	0.4241	
172.16.254.128	52222	54.192.79.107	80	68	66.482 KiB	71	20	1.424 KiB	48	65.059 KiB	34.834253	0.5668	

Close

Help

Wireshark · Export · HTTP object list

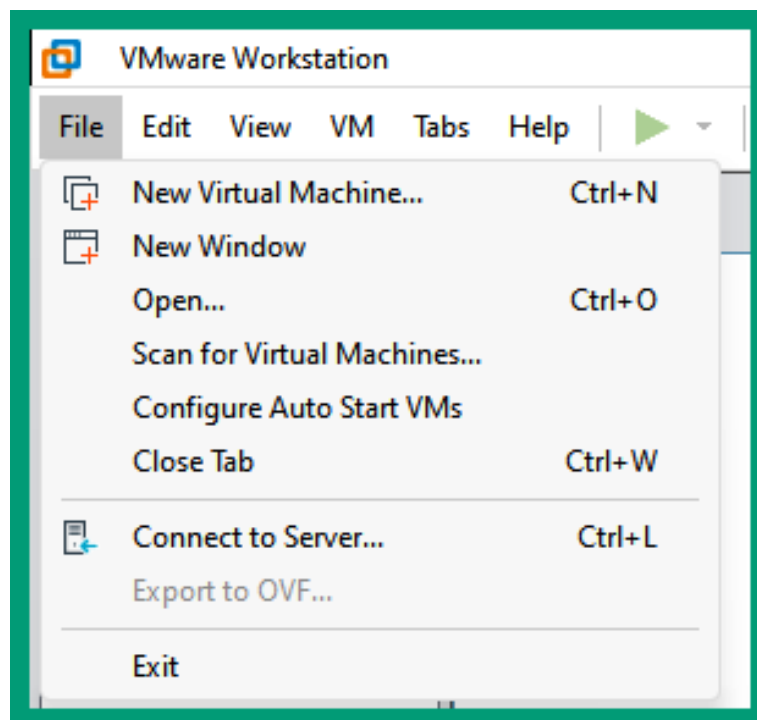
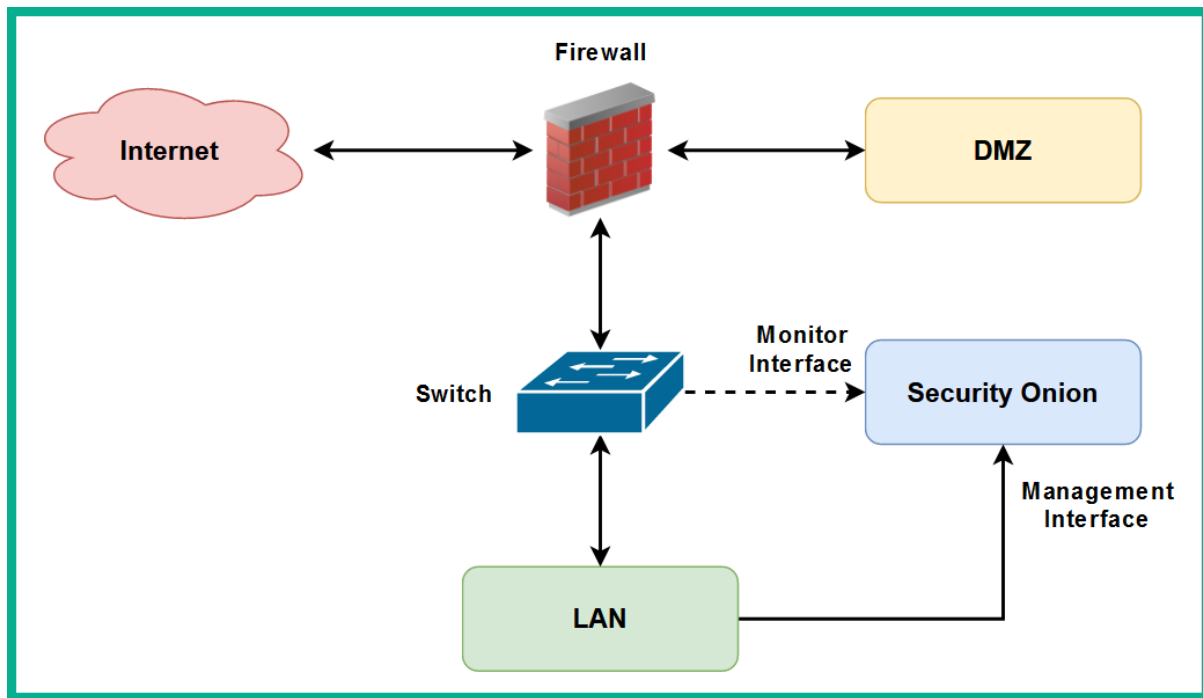
Text Filter:

Content Type: All Content-Types

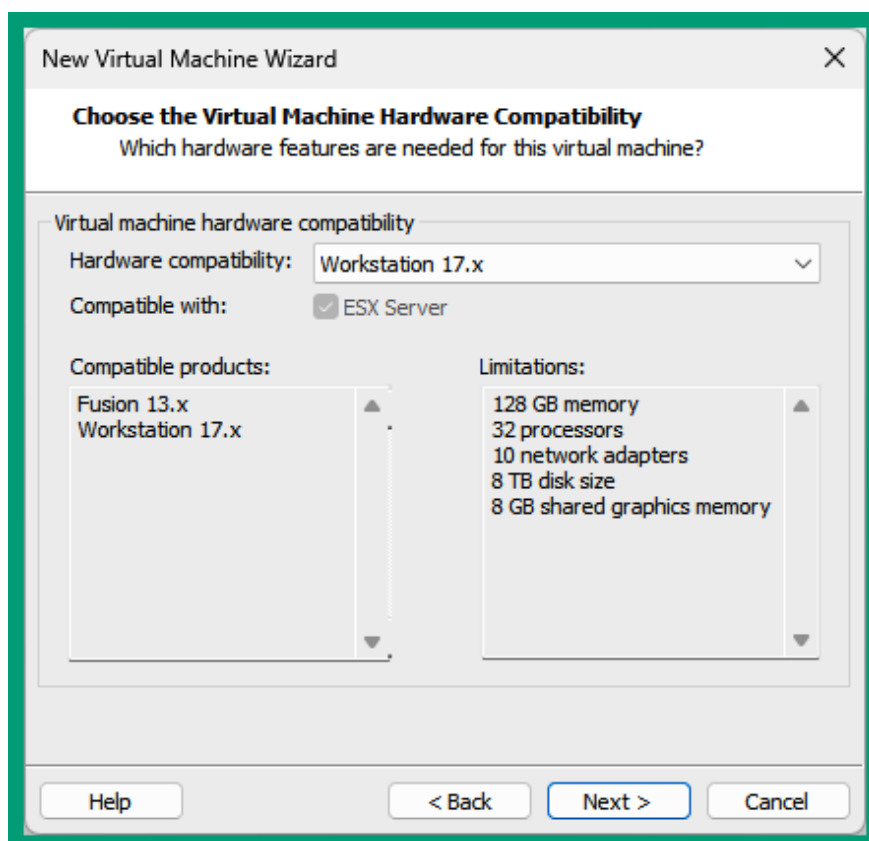
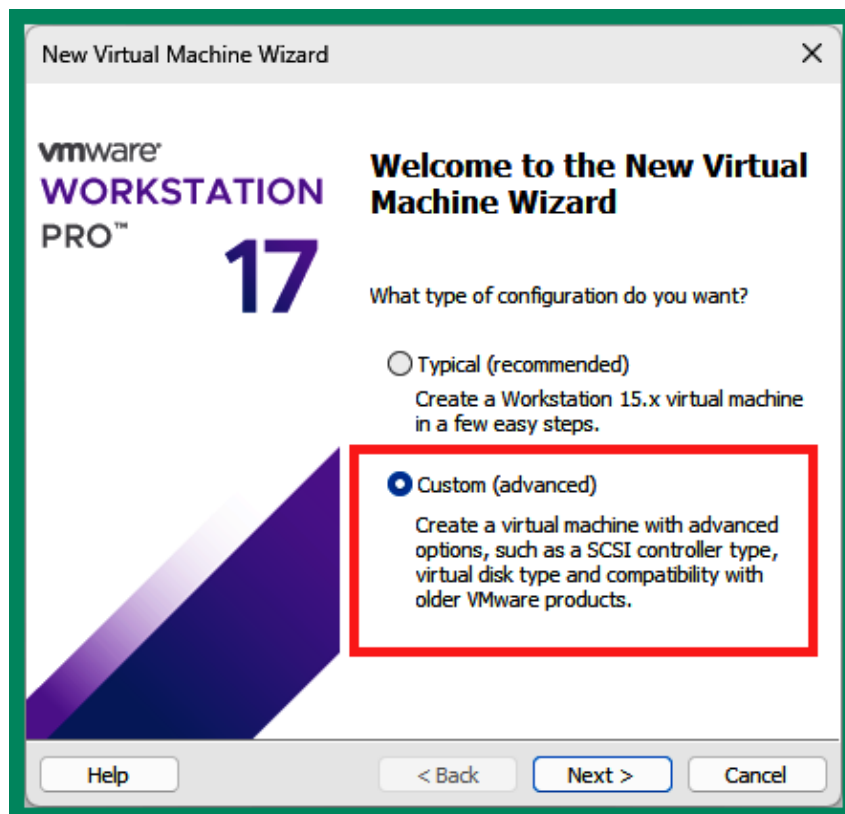
Packet	Hostname	Content Type	Size	Filename
619	www.reddit.com	text/html	114 kB	\
631	b.thumbs.redditmedia.com	text/css	711 b...	ba_fm376ctS_mGlZGAbqddmkhth3jqncUyhKW7iGBo.css
646	b.thumbs.redditmedia.com	image/png	2509 ...	WnWL9Elap8UCXn12wtaLaNrDSQgM4Dfirtammyb88RMU.p
682	b.thumbs.redditmedia.com	image/jpeg	6639 ...	9FkUjylHkmm-P0jauXAc2Qvl56nz1CfXK023PGWB5mA.jpg
725	www.redditstatic.com	text/css	221 kB	reddit.IXjlj0Z6Dgc.css
730	www.redditstatic.com	application/javascript	105 kB	reddit.fr.vf-uApcZRS4.js
736	b.thumbs.redditmedia.com	image/jpeg	5701 ...	fTMgRASiBOAIHNGuCVuGxX8GpnGta4d5Dal6vGgkKpg.jpg
746	b.thumbs.redditmedia.com	image/jpeg	5134 ...	aM3AbbkvSo8SNRYCjrodJtF6nKWUiBb8EQLevbdMXA.jpg
755	b.thumbs.redditmedia.com	image/jpeg	6686 ...	lpBctkQaLEFDz9KU9uSuD5mY4aKs5gEV-DAHJtIgFME.jpg
818	b.thumbs.redditmedia.com	image/jpeg	3338 ...	OZduv5qenmcDxw16CRs9NU8c1Q1E_izY5e2KrfCAH-A.jpg
827	www.redditstatic.com	application/javascript	199 kB	reddit-init.fr.c7gGq8YZfSo.js
846	b.thumbs.redditmedia.com	image/jpeg	4339 ...	Hxt2j1-aiDvJY_eZTpsxfkVMwcy38lxtmk2u6Xs_M.jpg
859	b.thumbs.redditmedia.com	image/jpeg	6596 ...	6pTyv9LJM9fdw1Dis_QKTFY7FE7VNWKsmFhkq8bxZUY.jpg

Save Save All Preview Close Help











New Virtual Machine Wizard

**Guest Operating System Installation**

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\Users\Glen\Downloads\Recon for Ethical Hackers\si v Browse...

⚠ Could not detect which operating system is in this disc image.  
You will need to specify which operating system will be installed.

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

New Virtual Machine Wizard

**Select a Guest Operating System**

Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows

☒ Linux

☐ VMware ESX

☐ Other

Version

CentOS 8 64-bit

Help < Back Next > Cancel



New Virtual Machine Wizard ✕

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

The default location can be changed at Edit > Preferences.

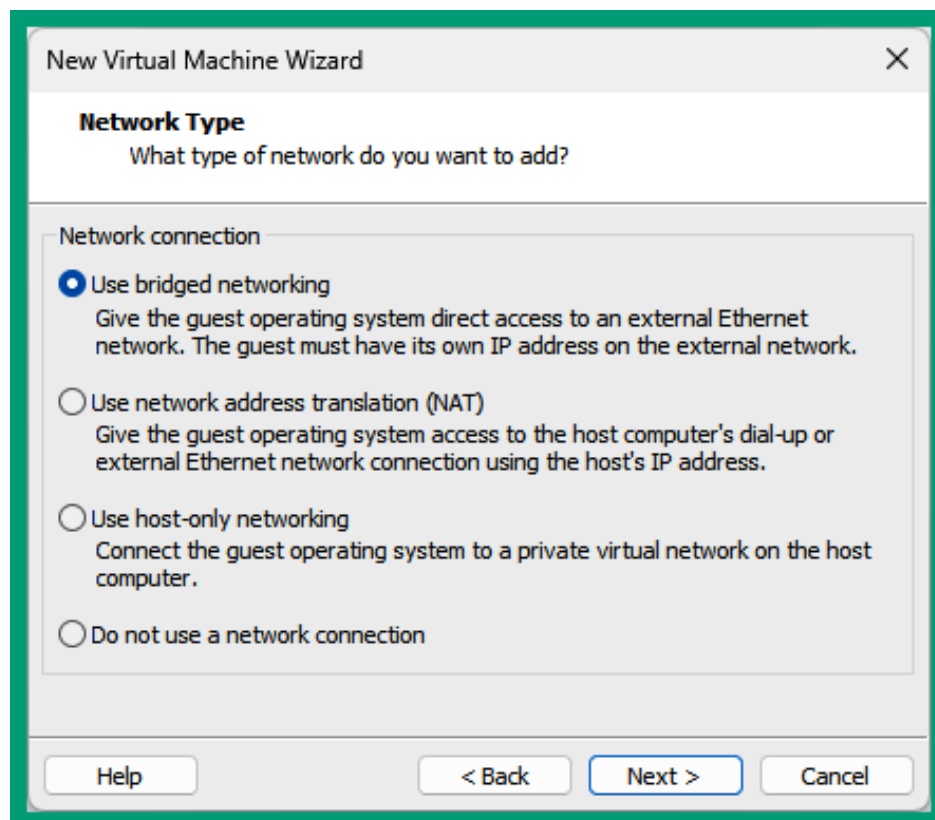
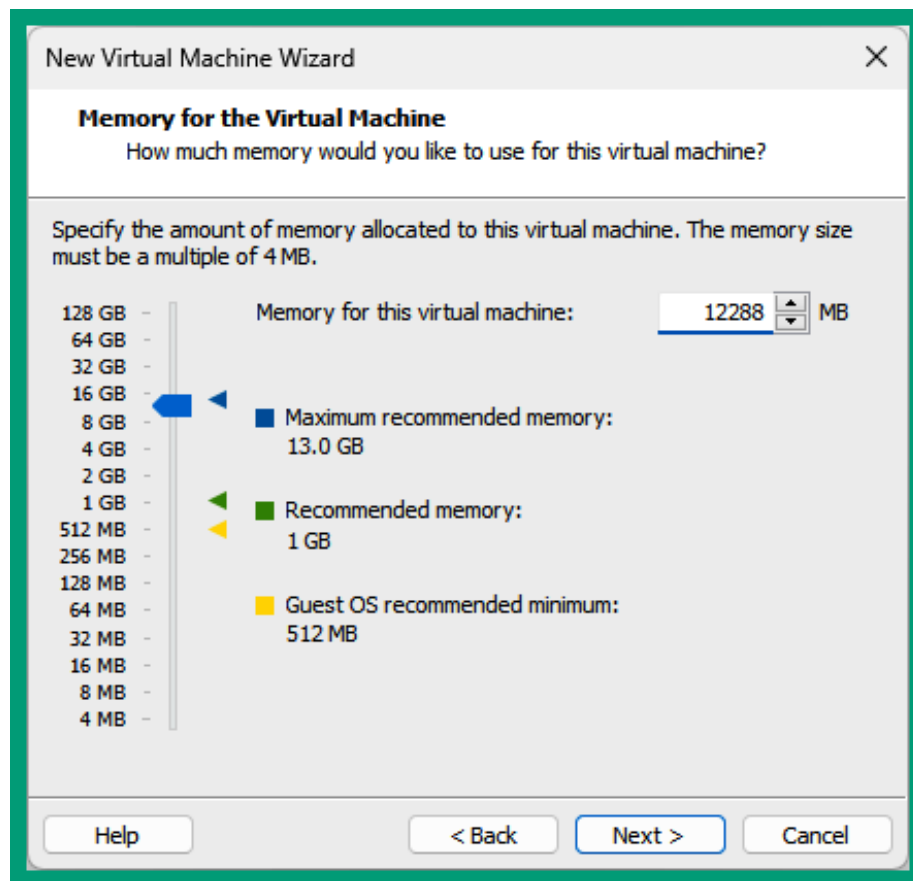
New Virtual Machine Wizard ✕

**Processor Configuration**  
Specify the number of processors for this virtual machine.

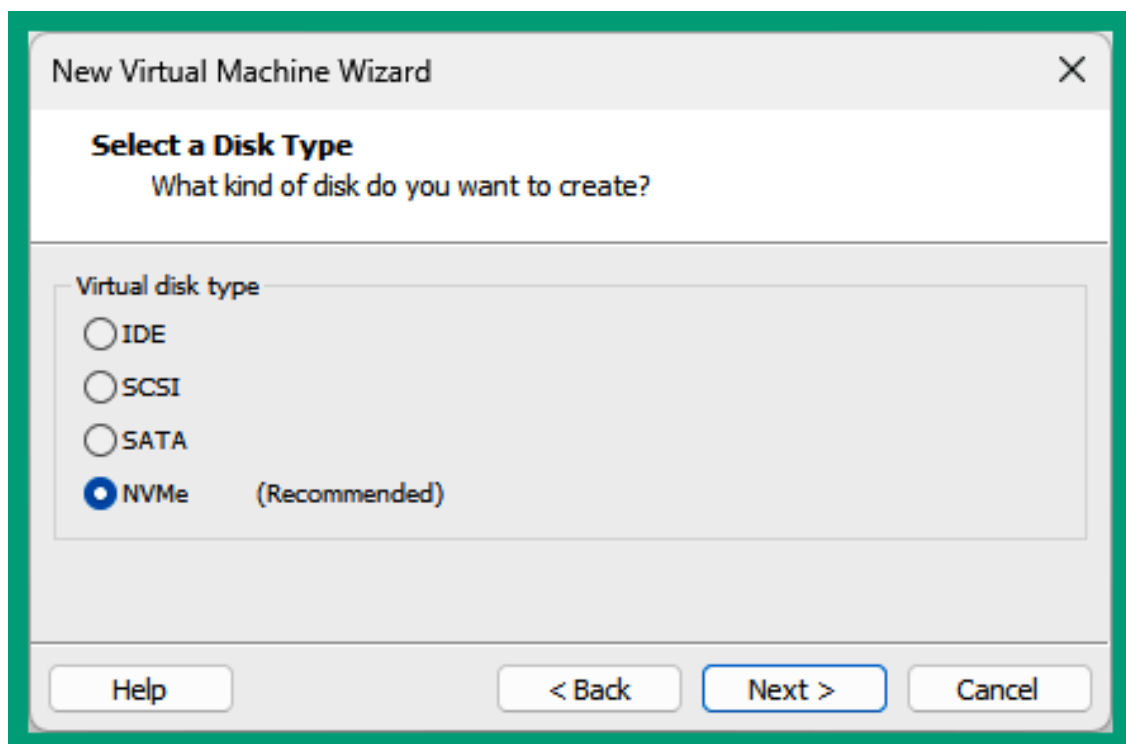
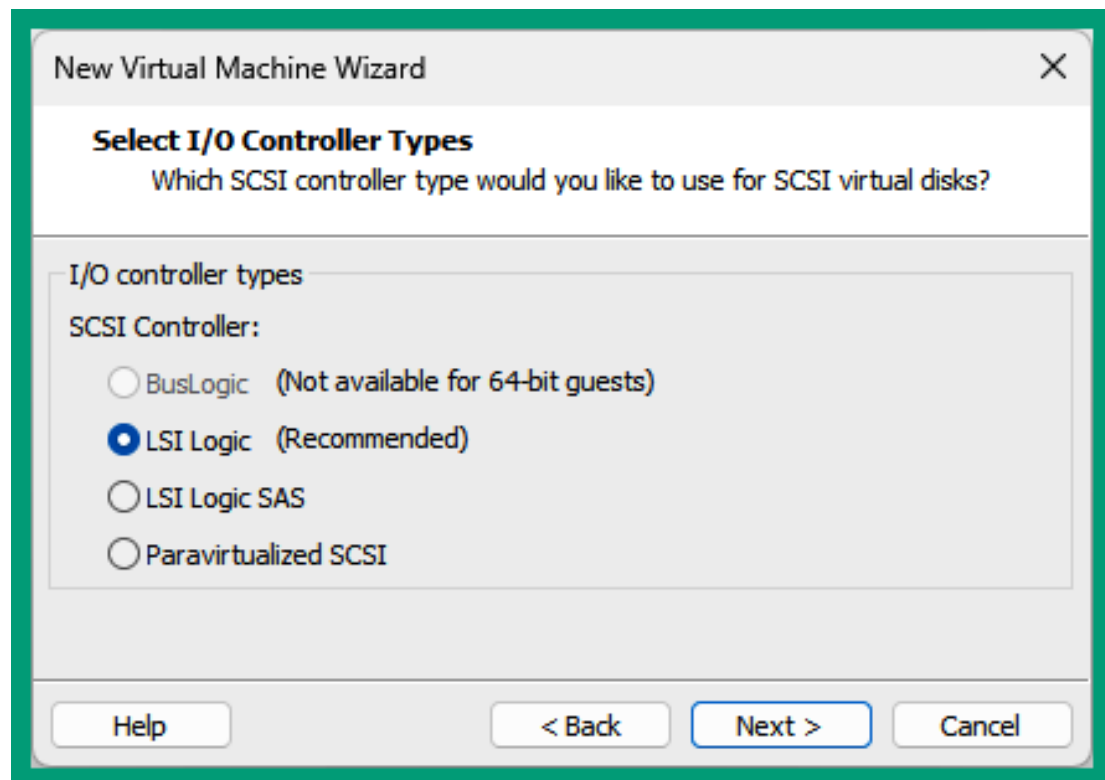
Processors

Number of processors:	<input type="text" value="1"/>
Number of cores per processor:	<input type="text" value="4"/>
Total processor cores:	4

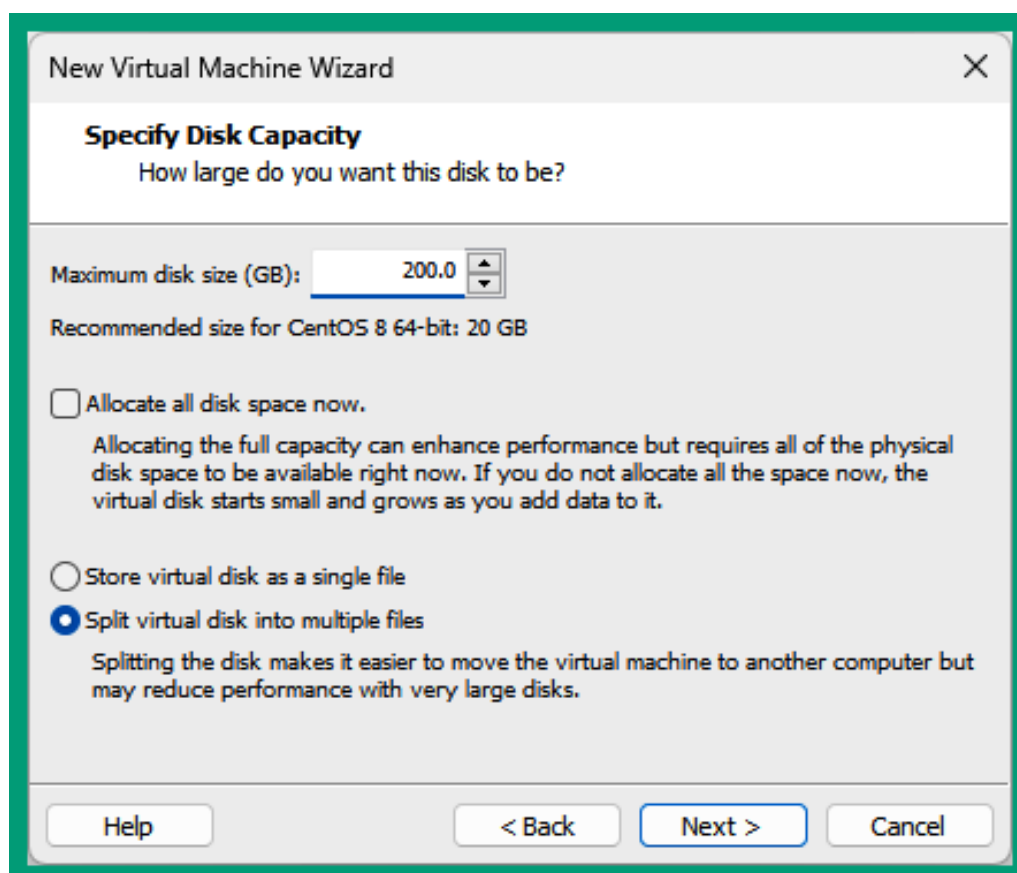
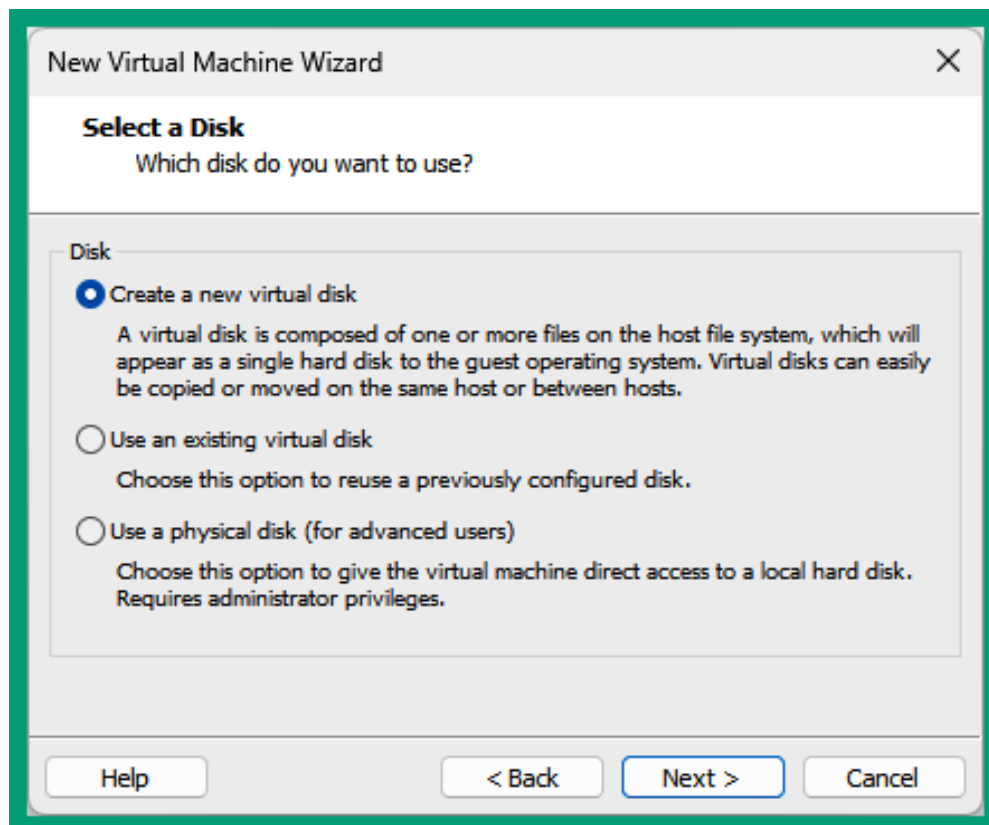




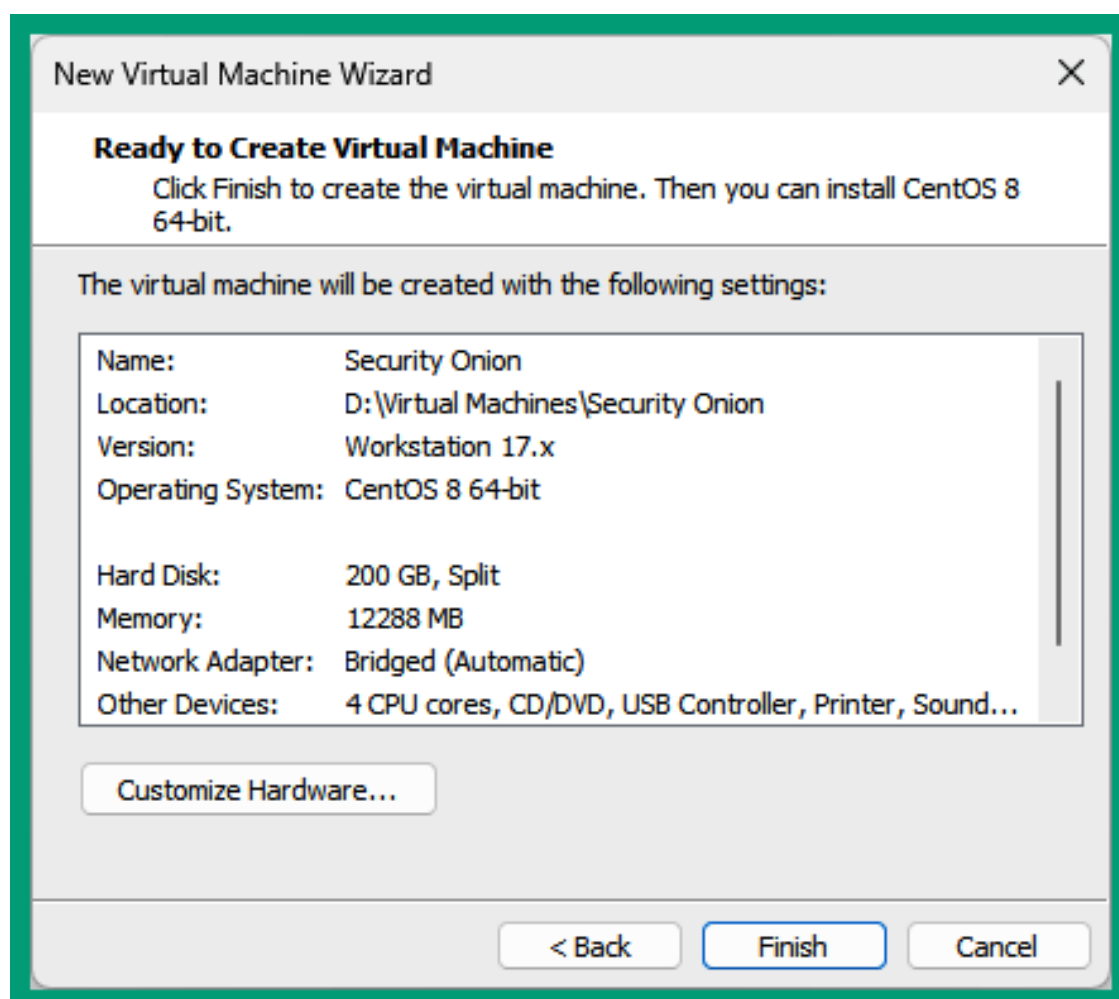
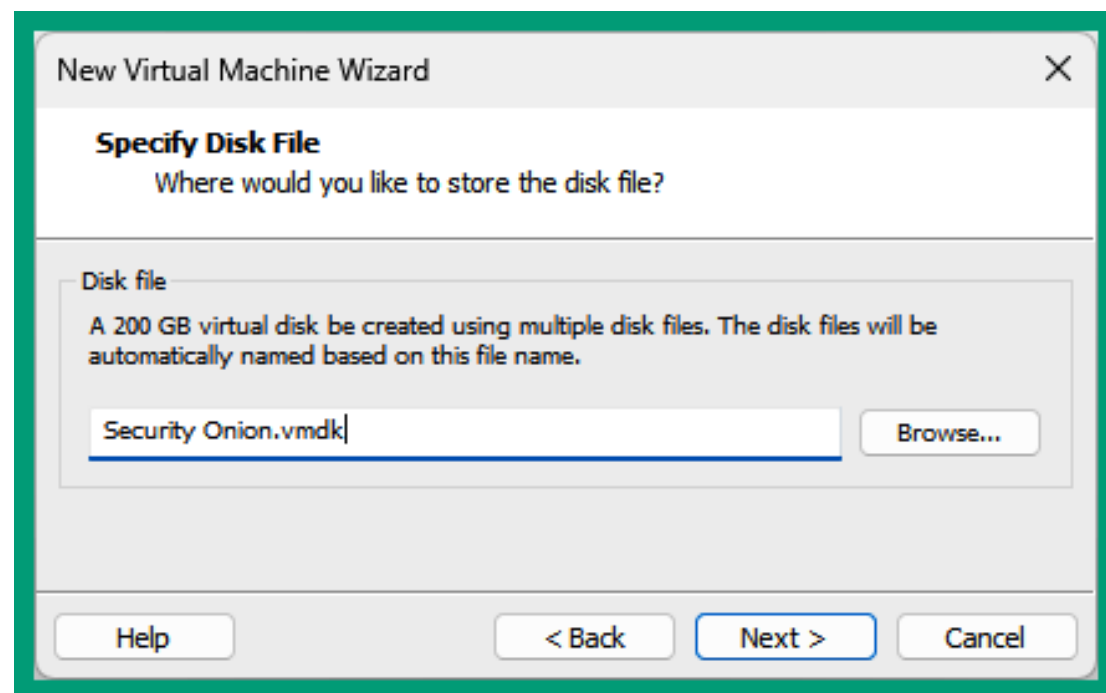




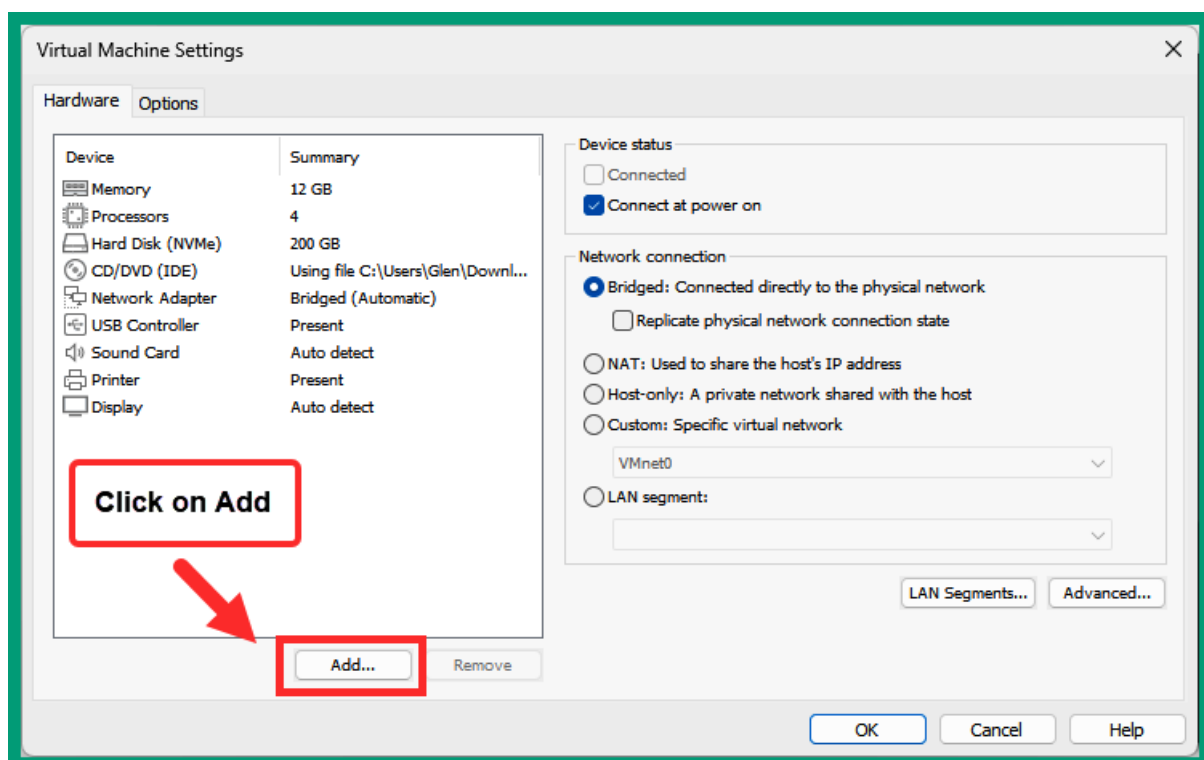
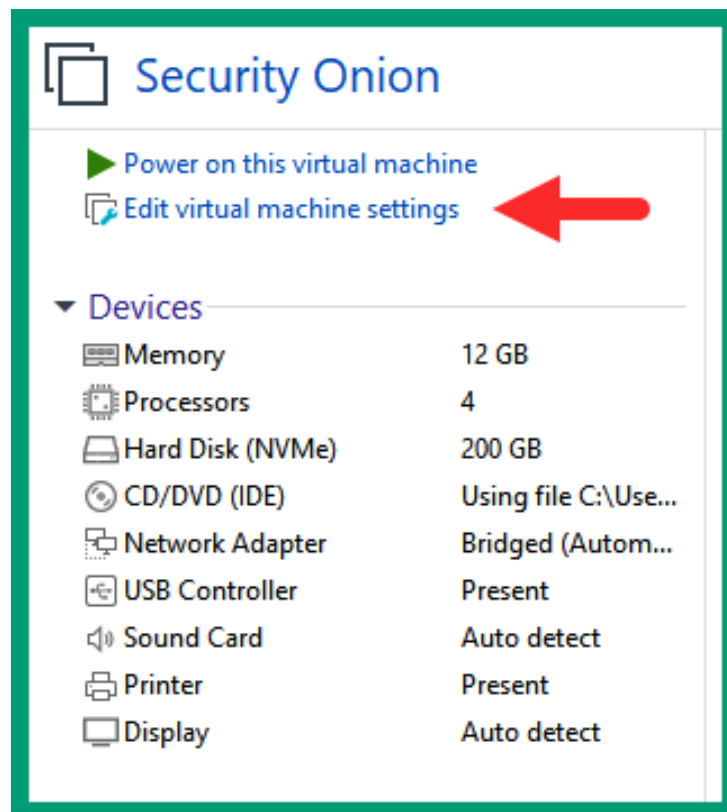




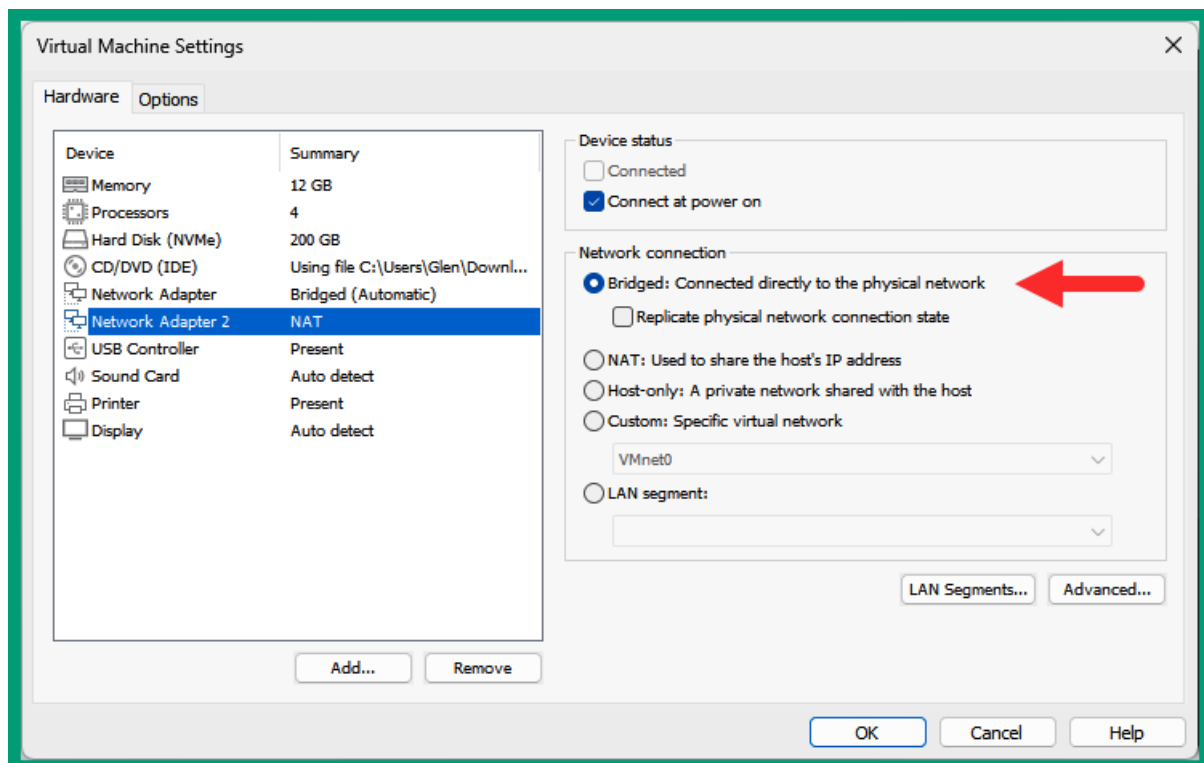
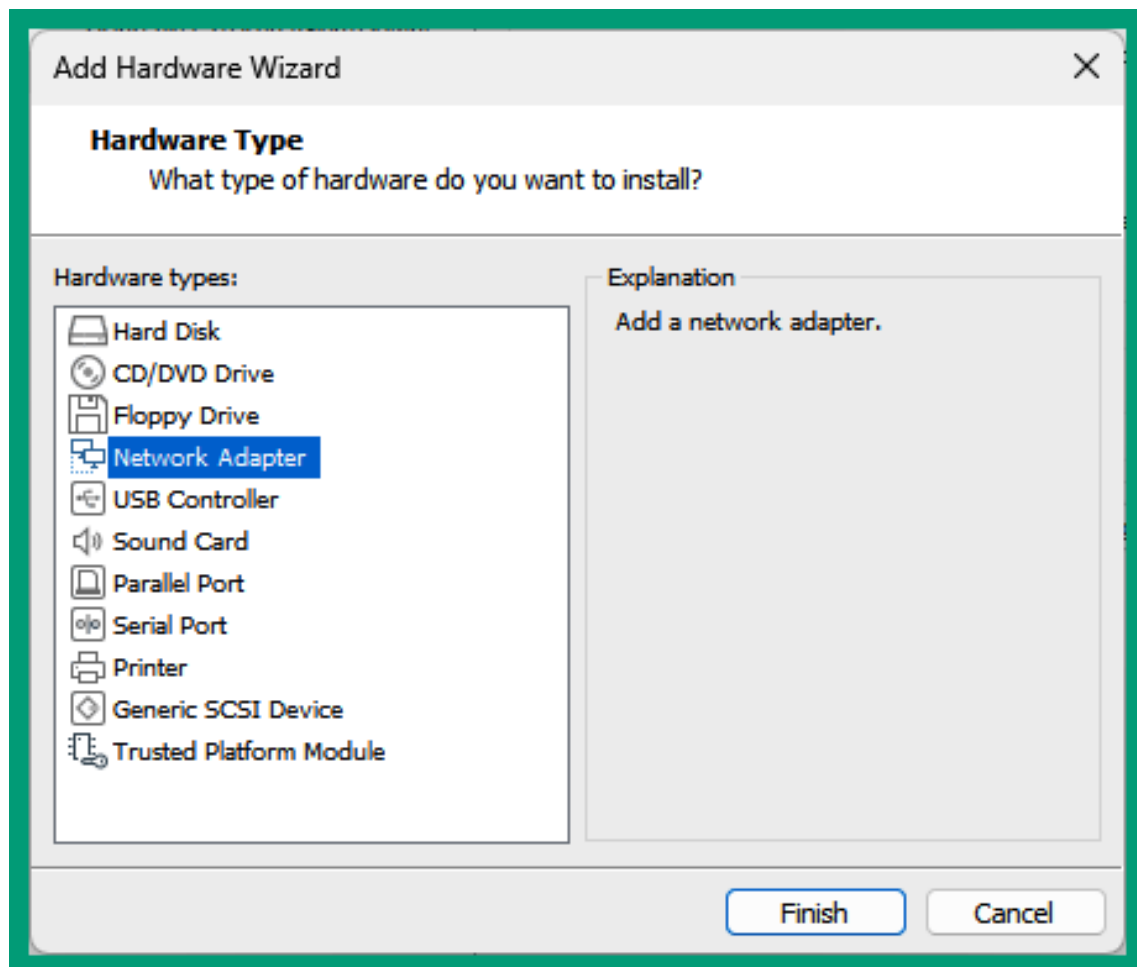














Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.38.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.146.0
VMnet19	Custom	-	-	-	192.168.126.0

Add Network... Remove Network Rename Network...

VMnet Information

☒ Bridged (connect VMs directly to the external network)

Bridged to: Intel(R) Wi-Fi 6 AX200 160MHz #2 Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet0

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: . . . Subnet mask: . . .

Restore Defaults Import... Export... OK Cancel Apply Help





- Press the <ENTER> key to begin the installation process.

```
[ 0.000000] Detected CPU family 19h model 80
[ 0.000000] Warning: AMD Processor - this hardware has not undergone upstream
testing. Please consult http://wiki.centos.org/FAQ for more information
[ 1.291062] core perfctr but no constraints; unknown hardware!
```

```
#####
##          ** W A R N I N G **          ##
##          _____                    ##
## Installing the Security Union ISO      ##
## on this device will DESTROY ALL DATA ##
## and partitions!                       ##
##          ** ALL DATA WILL BE LOST **  ##
#####
```

Do you wish to continue? (Type the entire word 'yes' to proceed.) yes

A new administrative user will be created. This user will be used for setting up and administering S  
ecurity Union.

Enter an administrative username: glen

Let's set a password for the glen user:

Enter a password:

Re-enter the password: \_

Passwords are invisible

### Security Union Setup - 2.3.240

Welcome to Security Union Setup!

You can use Setup for several different use cases, from a small  
standalone installation to a large distributed deployment for your  
enterprise. Don't forget to review the documentation at:  
<https://docs.securityunion.net>

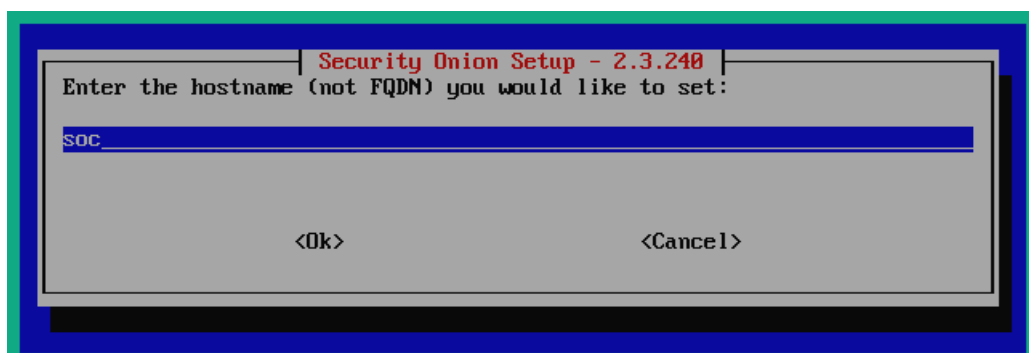
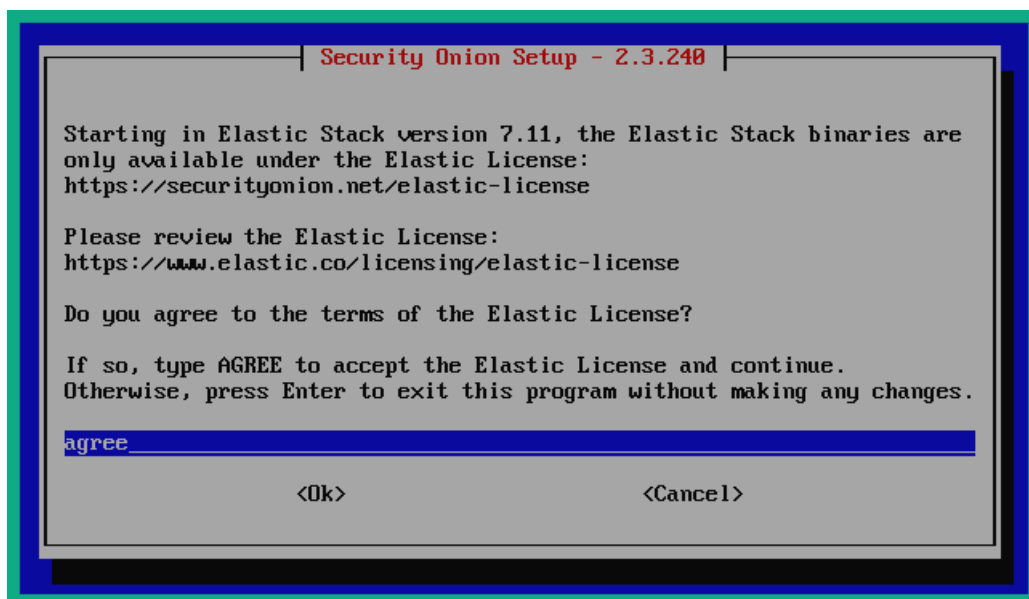
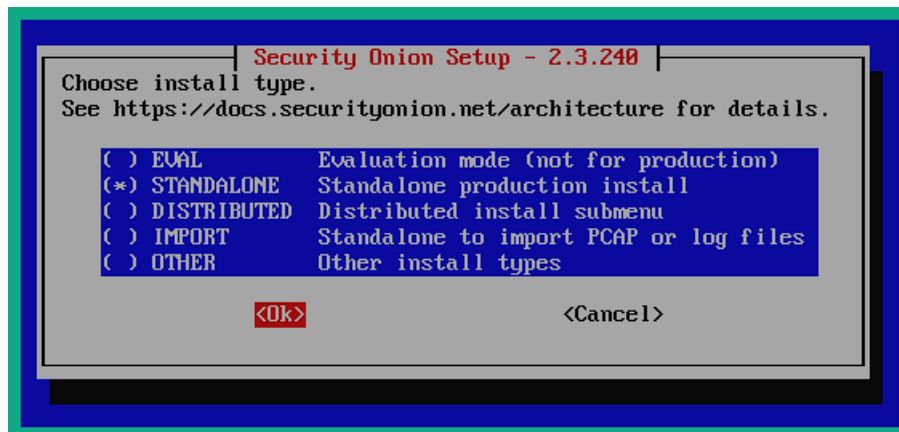
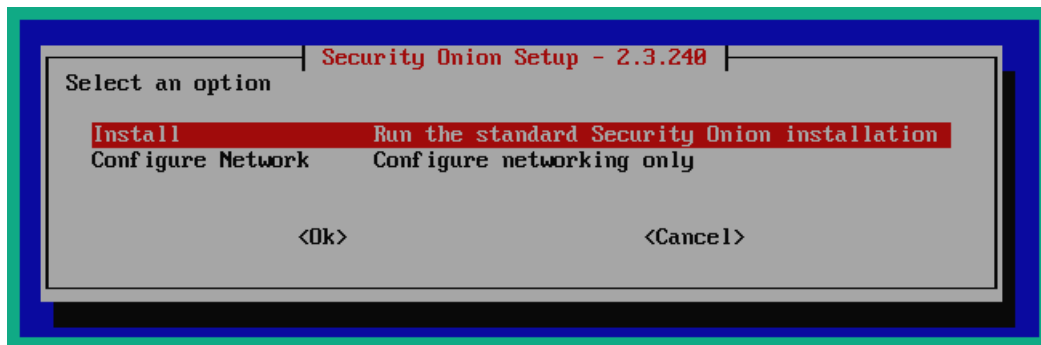
Setup uses keyboard navigation and you can use arrow keys to move  
around. Certain screens may provide a list and ask you to select one  
or more items from that list. You can use [SPACE] to select items and  
[ENTER] to proceed to the next screen.

Would you like to continue?

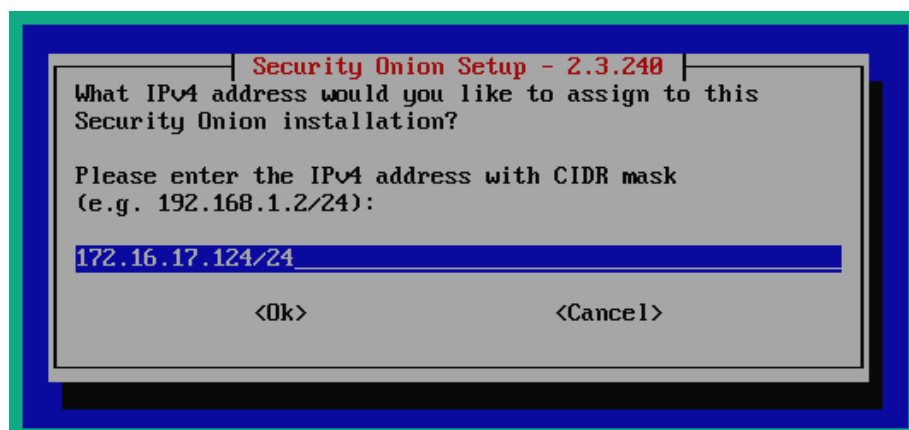
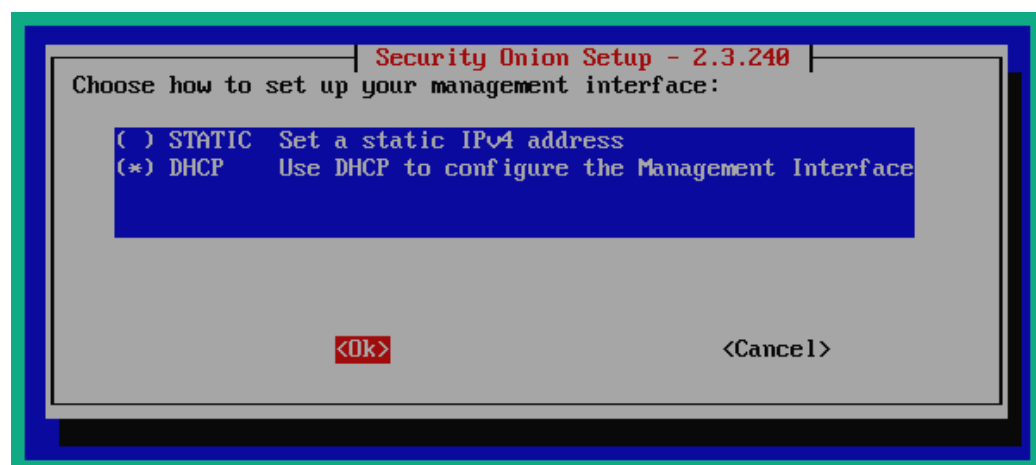
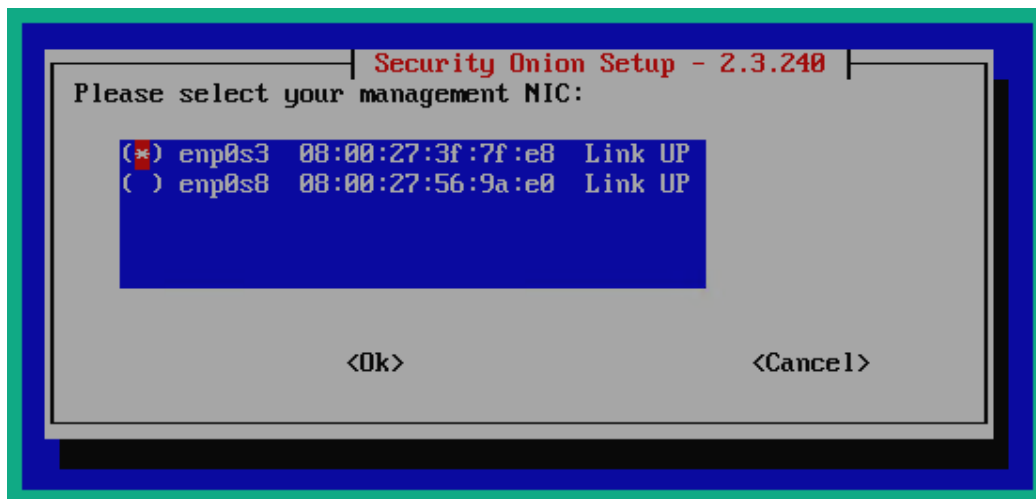
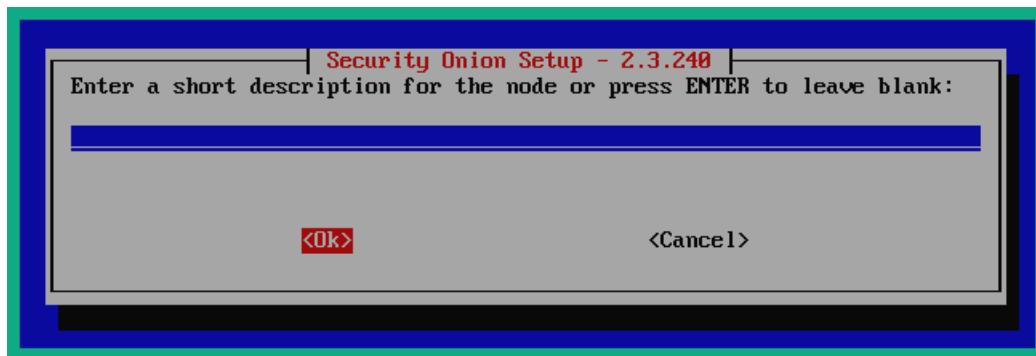
<Yes>

<No>

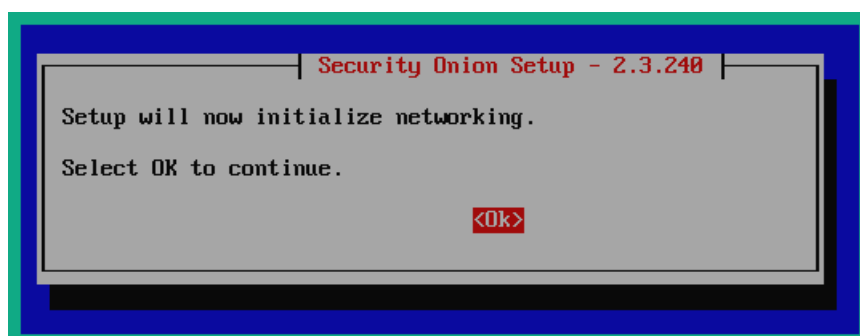
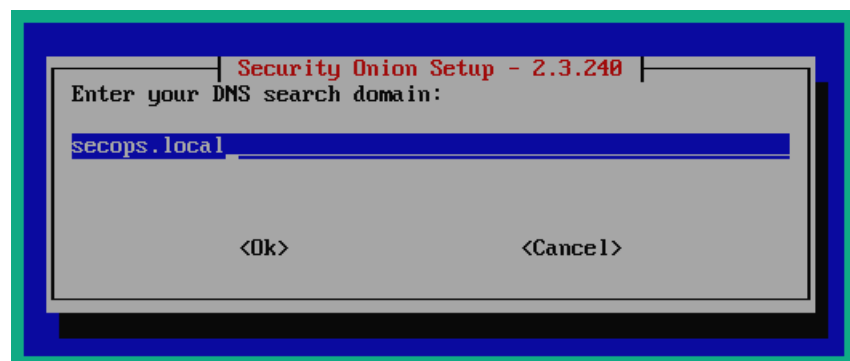
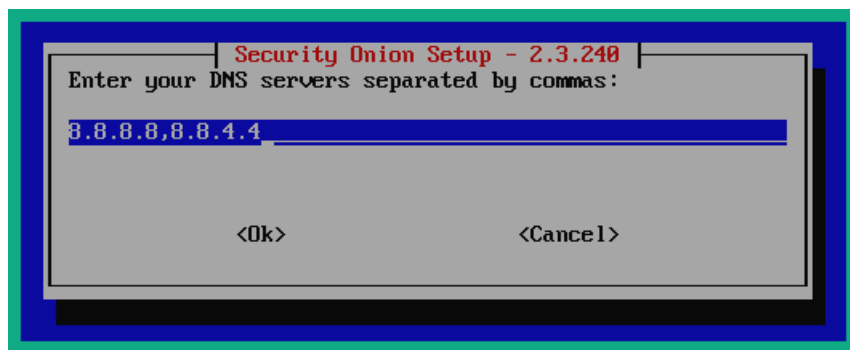
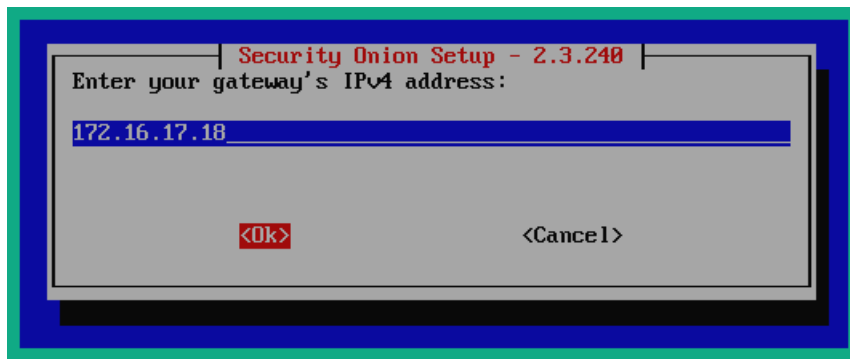














```
glen@soc:~$ sudo so-status

Checking Docker status

Docker ----- [ OK ]

Checking container statuses

so-aptcacherng ----- [ OK ]
so-curator ----- [ OK ]
so-dockerregistry ----- [ OK ]
so-elastalert ----- [ OK ]
so-elasticsearch ----- [ OK ]
so-filebeat ----- [ OK ]
so-fleet ----- [ OK ]
so-grafana ----- [ OK ]
so-idstools ----- [ OK ]
so-influxdb ----- [ OK ]
```

Overview

Alerts A

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

FleetDM

Navigator

Q Group By Name, Module

Last 24 hours

REFRESH

Fetch Limit 500

Filter Results

B

	Count	rule.name	event.module	event.severity_label
	136	ET USER_AGENTS Suspicious Win32 User Agent	suricata	high
	23	ET INFO ZeroTier Related Activity (udp)	suricata	medium
	15	PAM: Login session opened.	ossec	low
	14	PAM: Login session closed.	ossec	low
	13	Successful sudo to ROOT executed.	ossec	low
	7	System Audit event.	ossec	low
	3	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
	3	ET USER_AGENTS Go HTTP Client User-Agent	suricata	low
	1	sshd: authentication success.	ossec	low
	1	Ossec server started.	ossec	low
	1	Ossec agent started.	ossec	low

Rows per page: 50 1-11 of 11



Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

absolute time

Fetch Limit500Filter Results

Count	rule.name	event.module	event.severity_label
136	ET USER_AGENTS Suspicious Win32 User Agent	suricata	high
23	ET INFO ZeroTier Related Activity (udp)	suricata	medium
15	PAM: Login session opened.	ossec	low
14	PAM: Login session closed.	ossec	low
13	Successful sudo to ROOT executed.	ossec	
7	System Audit event.	ossec	
3	Listened ports status (netstat) changed (new)	ossec	low
3	ET USER_AGENTS Go HTTP Client User-Agent	suricata	low
1	sshd: authentication success.	ossec	low
1	Ossec server started.	ossec	low
1	Ossec agent started.	ossec	low

Rows per page:501-11 of 11

Include

Exclude

Only

Drilldown

Group By

New Group By

Clipboard

Actions

Select Drilldown

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Timestamp	rule.name	event.severity_label	source.ip	source.port
> 2023-05-04 14:40:29.177 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64193				
> 2023-05-04 14:40:29.175 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64192				
> 2023-05-04 14:40:29.174 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64191				
> 2023-05-04 14:40:29.172 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64190				
> 2023-05-04 14:40:29.170 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64189				
> 2023-05-04 14:40:29.169 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64188				
> 2023-05-04 14:40:29.167 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64187				

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

FleetDM

Navigator

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip
> 2023-05-04 14:40:29.177 -04:00 ET USER_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64193 172.16.17.18					
@timestamp2023-05-04T18:40:29.177Z					
@version1					
destination.ip172.16.17.18					
destination.port49153					
ecs.version8.0.0					
event.categorynetwork					
event.datasetalert					
event.ingested2023-05-04T18:40:35.418Z					
event.modulesuricata					
event.severity3					
event.severity_labelhigh					
host.namesoc					
log.file.path/nsm/suricata/eve-2023-05-04-18:02.json					
log.id.uid245483085606772					
log.offset92310					
message{"timestamp":"2023-05-04T18:40:29.177384+0000","flow_id":"245483085606772","in_iface":"ens34","event_type":"alert","src_ip":"172.16.17.16","src_port":"64193","community_id":"1:oEpn0NeHDFHYwBMonwEVL1kfzw-","tx_id":"0","alert":{"action":"allowed","gid":"1","signature_id":"2012249","rev":"5","signature":"ET USER_AGENT Suspicious Win32 User Agent","created_at":"2011_02_02","updated_at":"2020_04_23"},"rule":{"alert http \$HOME_NET 1024 -> \$EXTERNAL_NET any (msg:\"ET USER_AGENTS Suspicious Win32 User Agent\"; classtype:trojan-activity; sid:2012249; rev:5; metadata:created_at 2011_02_02, updated_at 2020_04_23);"},"app_proto":"http","payload_printable":"GE2,UPnP/1.1,MiniUPnPc/2.0\\r\\n\\r\\n","stream":"1","packet":"nD3P7nzqHG911ASCCABFAAAok65AAIAG7N6sEBEQrBAREvBwAHSHmJX2jsJrVARIBBCXgAAA\\filebeat"}					
metadata.beatfilebeat					



Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

FleetDM

Navigator

Timestamp


rule.name


event.severity\_label


source.ip


source.port


destination.ip


>  2023-05-04 14:40:29.177 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64193 172.16.17.18


>  2023-05-04 14:40:29.175 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64192 172.16.17.18


>  2023-05-04 14:40:29.174 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64191 172.16.17.18


>  2023-05-04 14:40:29.172 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64190 172.16.17.18


>  2023-05-04 14:40:29.170 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64189 172.16.17.18


>  2023-05-04 14:40:29.169 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64188 172.16.17.18


>  2023-05-04 14:40:29.167 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64187 172.16.17.18


>  2023-05-04 14:40:29.165 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64186 172.16.17.18

>  2023-05-04 14:35:19.905 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64034 172.16.17.18

>  2023-05-04 14:35:19.905 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64033 172.16.17.18

>  2023-05-04 14:35:19.903 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64032 172.16.17.18

>  2023-05-04 14:35:19.902 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent 172.16.17.16 64031 172.16.17.18

>  2023-05-04 14:35:19.900 -04:00 ET USER\_AGENTS Suspicious Win32 User Agent high 172.16.17.16 64030 172.16.17.18

Include

Exclude

Only

Group By

New Group By

Clipboard

Actions

Hunt

Correlate

PCAP

CyberChef

Google

VirusTotal

Select Correlate

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana


CyberChef


Playbook


Count

event.module

event.dataset

 1 suricata alert

 1 zeek http

 1 zeek conn

Rows per page: 10 1-3 of 3

Events

Fetch Limit 100 Filter Results

Timestamp

source.ip


source.port


destination.ip


destination.port

rule.name

rule

>  2023-05-04 14:40:29.177 -04:00 172.16.17.16 64193 172.16.17.18 49153 ET USER\_AGENTS Suspicious Win32 User Agent A N

>  2023-05-04 14:40:29.176 -04:00 172.16.17.16 64193 172.16.17.18 49153

>  2023-05-04 14:40:29.175 -04:00 172.16.17.16 64193 172.16.17.18 49153

Rows per page: 10 1-3 of 3


Timestamp


source.ip


source.port

destination.ip

destination.port


>  2023-05-04 14:40:29.177 -04:00 172.16.17.16 64193 172.16.17.18 49153

>  2023-05-04 14:40:29.176 -04:00 172.16.17.16 64193 172.16.17.18 49153

>  172.16.17.18 49153

+ Escalate to new case

Attach event to a recently viewed case:

 Case title not yet provided - click here to update this title

The backend data fetch took 0.087 seconds. The total round trip took 0.091 seconds.



Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

FleetDM

Navigator

Timestamp

source.ip


source.port


destination.ip


destination.port


rule.name


rule.category


>  2023-05-04 15:11:17.362 -04:00 172.16.17.16 65179 172.16.17.18 49153 ET in32 User Agent A Network Trojan was detected


>  2023-05-04 15:11:17.356 -04:00 172.16.17.16 65178 172.16.17.18 49153 ET in32 User Agent A Network Trojan was detected


>  2023-05-04 15:11:17.356 -04:00 172.16.17.16 65177 172.16.17.18 49153 ET in32 User Agent A Network Trojan was detected


>  2023-05-04 15:11:17.352 -04:00 172.16.17.16 65176 172.16.17.18 49153 ET in32 User Agent A Network Trojan was detected


>  2023-05-04 15:11:17.350 -04:00 172.16.17.16 65175 172.16.17.18 49152 ET in32 User Agent A Network Trojan was detected

>  2023-05-04 15:11:17.347 -04:00 172.16.17.16 65174 172.16.17.18 49152 ET in32 User Agent A Network Trojan was detected

>  2023-05-04 15:11:17.345 -04:00 172.16.17.16 65173 172.16.17.18 49152 ET in32 User Agent A Network Trojan was detected

>  2023-05-04 15:11:17.342 -04:00 172.16.17.16 65172 172.16.17.18 49152 ET in32 User Agent A Network Trojan was detected

>  2023-05-04 15:06:09.082 -04:00 172.16.17.16 6501 49153 ET in32 User Agent A Network Trojan was detected

>  2023-05-04 15:06:09.080 -04:00 172.16.17.16 6501 49152 ET in32 User Agent A Network Trojan was detected

Page 10 1-10 of 100

The backend data fetch took 0.1 seconds. The total round trip took 0.138 seconds.

Include

Exclude

Only

Group By

New Group By

Clipboard

Actions

Hunt

Correlate

PCAP

CyberChef

Google

VirusTotal

Select PCAP

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

FleetDM

Filter Results

HEX

Num

Timestamp

Type

Source IP

Source Port

Destination IP

Destination Port

Flags

Length

0 2023-05-04 15:11:17.357 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 SYN 66

1 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 SYN ACK 66

2 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 ACK 60

3 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 PSH ACK 175

4 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 ACK 60

5 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 PSH ACK 1175

6 2023-05-04 15:11:17.362 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 FIN ACK 60

7 2023-05-04 15:11:17.362 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 ACK 60

8 2023-05-04 15:11:17.362 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 FIN ACK 60

9 2023-05-04 15:11:17.362 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 ACK 60

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

Filter Results

HEX

Num

Timestamp

Type

Source IP

Source Port

Destination IP

Destination Port

Flags

Length

0 2023-05-04 15:11:17.357 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 SYN 66

0000 9C 3D CF EE 7C EA 1C 6F 65 D4 04 82 08 00 45 00 .=.].oe.....E.  
0016 00 34 A2 88 40 00 80 06 D0 F8 AC 10 11 10 AC 10 .4..@.....  
0032 11 12 FE 9B C0 01 80 4A FE D8 00 00 00 80 02 .....J.....  
0048 FA F0 BC 1B 00 00 02 04 05 B4 01 03 03 08 01 01 .....  
0064 04 02 ..

1 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.18 49153 172.16.17.16 65179 SYN ACK 66

0000 1C 6F 65 D4 04 82 9C 3D CF EE 7C EA 08 00 45 00 .oe.....].E.  
0016 00 34 00 00 40 00 06 C0 81 AC 10 11 12 AC 10 .4..@.....  
0032 11 10 C0 01 FE 9B A2 BD CF A5 80 4A FE D9 80 12 .....J.....  
0048 39 08 08 92 00 00 02 04 05 B4 01 01 04 02 01 03 9.....  
0064 03 06 ..

2 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 ACK 60

0000 9C 3D CF EE 7C EA 1C 6F 65 D4 04 82 08 00 45 00 .=.].oe.....E.  
0016 00 28 A2 89 40 00 06 DE 03 AC 10 11 10 AC 10 .(.@.....  
0032 11 12 FE 9B C0 01 80 4A FE D9 A2 BD CF A6 50 10 .....J.....P.  
0048 04 02 81 69 00 00 00 00 00 00 00 00 .....

3 2023-05-04 15:11:17.361 -04:00 TCP 172.16.17.16 65179 172.16.17.18 49153 PSH ACK 175



Count	source.ip	Count	destination.ip
9,242	172.16.17.16	6,794	172.16.17.18
4,254	172.16.17.123	6,592	172.16.17.16
3,369	172.16.17.18	4,016	8.8.8.8
3,237	172.16.17.3	1,615	172.16.17.3
578	2803:1500:1202::	264	172.16.17.123
339	172.16.17.65	161	2a02:6ea0::
128	2001:19f0:6001::	159	2803:1500:1202::
113	fe80::4e66:6010:6197:64b2	151	104.194.8.134
85	fe80::1	133	50.7.252.138
83	2803:1500:1202::	131	239.255.255.250

Count	destination.port	Count	destination_geo.organization_name
4,098	53	4,109	Google LLC
3,412	49152	489	ReliableSite.Net LLC
3,355	49153	266	Datacamp Limited
2,332	56639	249	NTT America, Inc.

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

Administration

Tools

Kibana

Grafana

CyberChef

Playbook

## Downloads

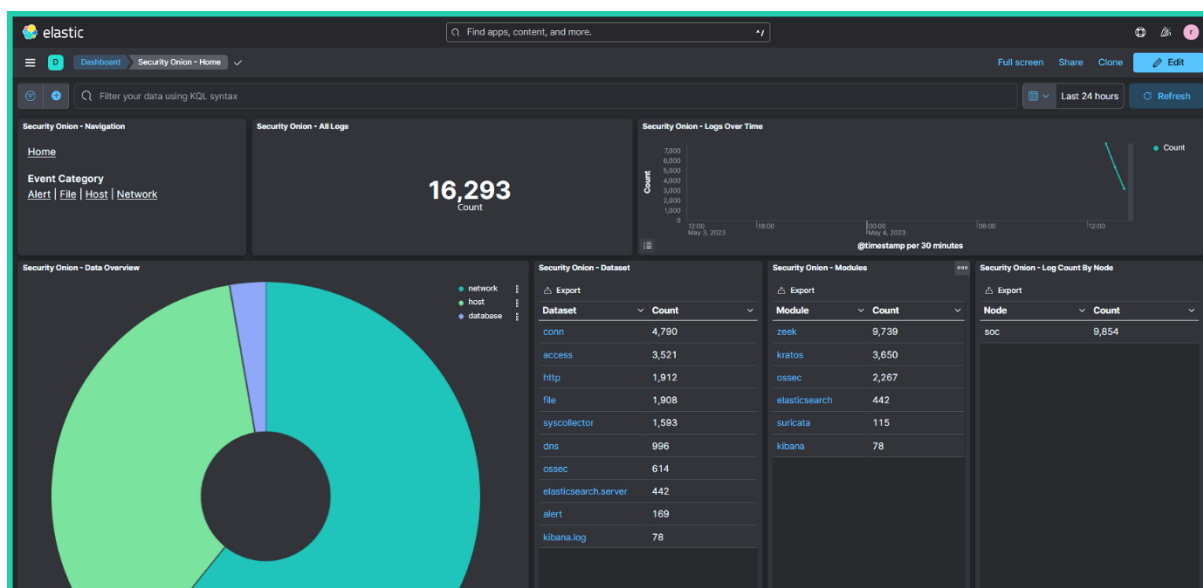
When installing packages such as osquery or beats onto remote systems be sure to run `so-allow`

### Elasticsearch Utilities (8.6.2)

- [Winlogbeat](#) (Windows)
- [Filebeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Filebeat RPM](#) (Linux [x86\_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [Metricbeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Metricbeat RPM](#) (Linux [x86\_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [Auditbeat DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [Auditbeat RPM](#) (Linux [x86\_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)

### Wazuh Agents (3.13.1-1)

- [MSI](#) (Windows)
- [DEB](#) (Linux [amd64]: Debian, Ubuntu)
- [RPM](#) (Linux [x86\_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- [PKG](#) (MacOS)





Security Onion - Dataset

Export

Dataset	Count
conn	1,618
file	828
http	827
syscollector	733
elasticsearch.server	426
dns	334

DashboardSecurity Onion - Indicator

Full screenShareCloneEdit

event.dataset.keyword: conn

Security Onion - Navigation

Home

Event Category

AlertFileHostNetwork

Security Onion - All Logs

4,859

Count

Security Onion - Top Network Protocols

ntpsslhttpdns

Security Onion - Dataset

Export

Dataset	Count
conn	4,859

Security Onion - Source IPs

Export

Source IP	Count
172.16.17.16	2,167
172.16.17.3	1,109
172.16.17.123	1,009
2803:1500:1202:1e75:c891:e7a...	261
172.16.17.65	87
2001:19f0:6001:2c59:beef:d1:58...	72
fe80::1	46
172.16.17.18	40
2803:1500:1202:1e75:c88b:2dd...	23
fe80::4e66:6010:6197:64b2	19

Security Onion - Destination IPs

Export

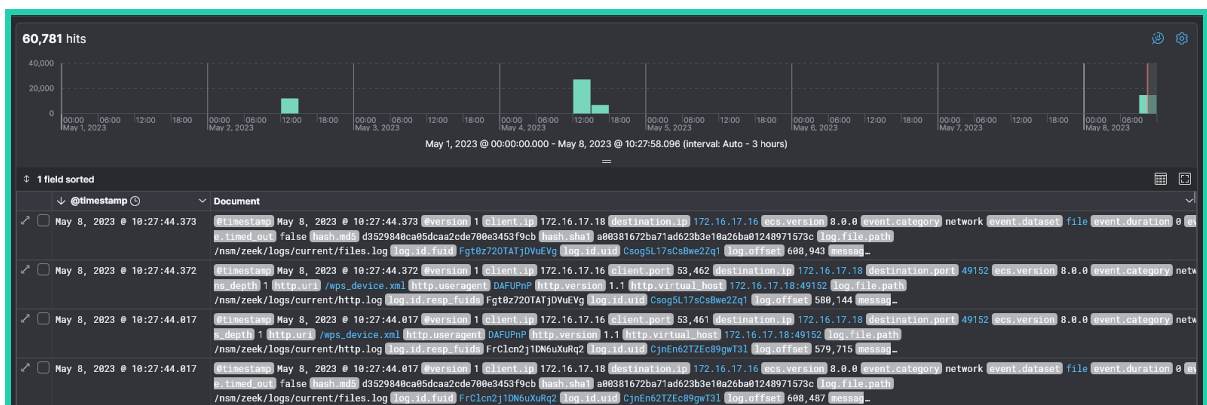
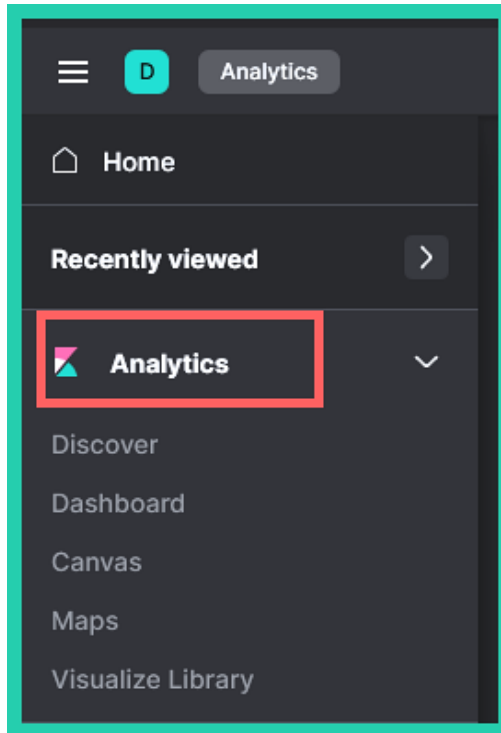
Destination IP	Count
172.16.17.18	1,530
172.16.17.16	1,134
8.8.8.8	934
172.16.17.3	374
2803:1500:1202:1e75:c891:e7a...	86
2a02:6ea0:d405::9993	73
104.194.8.134	72
239.255.255.250	63
50.7.252.138	59
2001:49f0:d0db:2::2	54

Security Onion - Destination Ports

Export

Destination Port	Count
56639	1,074
53	954
49152	776
49153	742
9993	441
9080	366
443	83
1900	61
136	43
62128	40





# Visualize Library

Create visualization

Search... Recently updated Tags

Name, description, tags	Type	Last updated	Actions
Security Onion - Alerts Over Time	Line	6 days ago	
Security Onion - Rule - Name	Data table	6 days ago	
Security Onion - Rule - Severity	Pie	6 days ago	
Security Onion - Rule - Category	Data table	6 days ago	
Security Onion - Destination Ports	Data table	6 days ago	