



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Activity 2: Information Gathering



Lab Activities are based on **EC Council – CEH Curriculum**

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to gather information by footprinting and scanning.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Information Gathering and Reconnaissance Techniques
1. Use Windows Command Line Utility to Gather Information
2. Use Web Data Extractor tool to extract data from web pages. (Web Scraping or Web Data Mining)
3. Use Email Tracker Pro to trace and track delivered email.
4. Use TCP View tool to identify the processes running on a Machine.
5. Use Sublist3r tool to enumerate subdomains of Websites using OSINT
6. Use Recon -ng tool to gather information
7. Being Anonymous on the Internet

Part 2: Scanning your Target Network – (Virtual Lab environment – Coursework Task)
1. Use HPING to send ICMP/TCP/UPD Packets and analyse the target replies.
2. Use MegaPing to identify live hosts and open ports of the Target.
3. Use NetScanTools Pro to initiate various Scans
4. Explore various network scanning Techniques
5. Identify Target Operating System with TTL
6. Map your Network

Part 3: Enumerate your Target Network – (Virtual Lab environment – Coursework Task)
1. Enumeration using NetBIOS
2. Enumeration using Nmap and NetUse
3. Enumerate Services
4. Reflect on the above activities: (End of this Activity, you must have completed the below listed tasks with adequate evidences)
Make sure, you have recorded video snippets, documented automated reports – that includes date, and other required details to submit as evidence. Gather as many information as possible using relevant tools/ techniques in your given Virtual Lab Environment. (Not limited to the tools used in the above labs. You are free to use any tools that could help you gather further information) Use appropriate Scanning Tools/ Techniques and Mechanism to scan the Virtual Lab Network Try to enumerate different services within your Virtual Lab Network

Part 1

1. Use Windows Command Line Utility to Gather Information

Task: Gather information about the authoritative name server and its IP Address of www.itsecgames.com

Why? In future, to exploit the server to perform a DoS, DDoS, URL Redirection attacks.

How?

```
C:\Users\Administrator>ping www.itsecgames.com
```

```
Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:
```

```
Reply from 31.3.96.40: bytes=32 time=26ms TTL=128
```

```
Reply from 31.3.96.40: bytes=32 time=21ms TTL=128
```

```
Reply from 31.3.96.40: bytes=32 time=24ms TTL=128
```

```
Reply from 31.3.96.40: bytes=32 time=22ms TTL=128
```

```
Ping statistics for 31.3.96.40:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 21ms, Maximum = 26ms, Average = 23ms
```

```
C:\Users\Administrator>ping www.itsecgames.com -f -l 1500
```

```
Pinging itsecgames.com [31.3.96.40] with 1500 bytes of data:
```

```
Packet needs to be fragmented but DF set.
```

```
Packet needs to be fragmented but DF set.
```

```
Packet needs to be fragmented but DF set.
```

```
Packet needs to be fragmented but DF set.
```

```
Ping statistics for 31.3.96.40:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Administrator>ping www.itsecgames.com -f -l 1472
```

```
C:\Users\Administrator>ping www.itsecgames.com -f -l 1473
```

What is the outcome of the above two ping commands? What is the reason for the two outcomes?

```
C:\Users\nitheesh>tracert itsecgames.com
```

```
Tracing route to itsecgames.com [31.3.96.40]
over a maximum of 30 hops:

  1  1 ms   1 ms   <1 ms  ttrouter [192.168.1.1]
  2  8 ms   8 ms   7 ms  ae54-ner001.csm.as13285.net [78.144.1.17]
  3 10 ms   9 ms  12 ms ae56-scr001.slh.as13285.net [78.144.1.48]
  4 10 ms  10 ms  11 ms ae64-scr101.thw.as13285.net [78.144.1.134]
  5 20 ms  20 ms  19 ms 195.66.227.118
  6 20 ms  20 ms  20 ms te0-14.cr1.nkf.as49685.net [95.142.106.211]
  7 21 ms  23 ms  20 ms eth42.eq3-iec-rtr-002.cloudvps.nl [176.74.228.8]
  8 18 ms  18 ms  18 ms web.mmebvba.com [31.3.96.40]

Trace complete.
```

[Output may vary]

```
C:\Users\nitheesh>ping www.itsecgames.com -i 4 -n 1
```

```
Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:

Reply from 78.144.1.134: TTL expired in transit.

Ping statistics for 31.3.96.40:

    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Users\nitheesh>ping www.itsecgames.com -i 8 -n 1
```

```
Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:

Reply from 31.3.96.40: bytes=32 time=19ms TTL=54

Ping statistics for 31.3.96.40:

    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

    Approximate round trip times in milli-seconds:

        Minimum = 19ms, Maximum = 19ms, Average = 19ms
```

```
C:\Users\nitheesh>ping www.itsecgames.com -i 9 -n 1
```

```
Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:

Reply from 31.3.96.40: bytes=32 time=18ms TTL=54

Ping statistics for 31.3.96.40:

    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

    Approximate round trip times in milli-seconds:
```

Minimum = 18ms, Maximum = 18ms, Average = 18ms

By issuing the -i command, you are setting the TTL to a certain value to check the time span of the packet. By setting the TTL to 1, 2, 4, 5, 9 etc what piece of information did you gather?

Do a research in the internet and find out what are the options, you can use with ping command and what are their functionalities with suitable example?

```
C:\Users\nitheesh>nslookup
```

Default Server: ttrouter

Address: 192.168.50.10

```
> set type=a
```

```
> www.itsecgames.com
```

Server: ttrouter

Address: 192.168.50.10

Non-authoritative answer:

Name: itsecgames.com

Address: 31.3.96.40

Aliases: www.itsecgames.com

```
> set type=cname
```

```
> www.itsecgames.com
```

Server: ttrouter

Address: 192.168.50.10

Non-authoritative answer:

www.itsecgames.com canonical name = itsecgames.com

```
> set query=ns
```

```
> www.itsecgames.com
```

Server: ttrouter

Address: 192.168.50.10

Non-authoritative answer:

www.itsecgames.com canonical name = itsecgames.com

itsecgames.com nameserver = ns53.domaincontrol.com

itsecgames.com nameserver = ns54.domaincontrol.com

ns53.domaincontrol.com internet address = 97.74.106.27

ns53.domaincontrol.com AAAA IPv6 address = 2603:5:21a2::1b

ns54.domaincontrol.com internet address = 173.201.74.27

ns54.domaincontrol.com AAAA IPv6 address = 2603:5:22a2::1b

```
> set type=a
```

```
> ns53.domaincontrol.com
```

Server: ttrouter

Address: 192.168.50.10

Non-authoritative answer:

Name: ns53.domaincontrol.com

Address: 97.74.106.27

```
C:\Users\nitheesh>ping ns53.domaincontrol.com
```

Pinging ns53.domaincontrol.com [97.74.106.27] with 32 bytes of data:

Reply from 97.74.106.27: bytes=32 time=25ms TTL=52

Reply from 97.74.106.27: bytes=32 time=25ms TTL=52

Reply from 97.74.106.27: bytes=32 time=25ms TTL=52

Reply from 97.74.106.27: bytes=32 time=26ms TTL=52

Ping statistics for 97.74.106.27:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 25ms, Maximum = 26ms, Average = 25ms

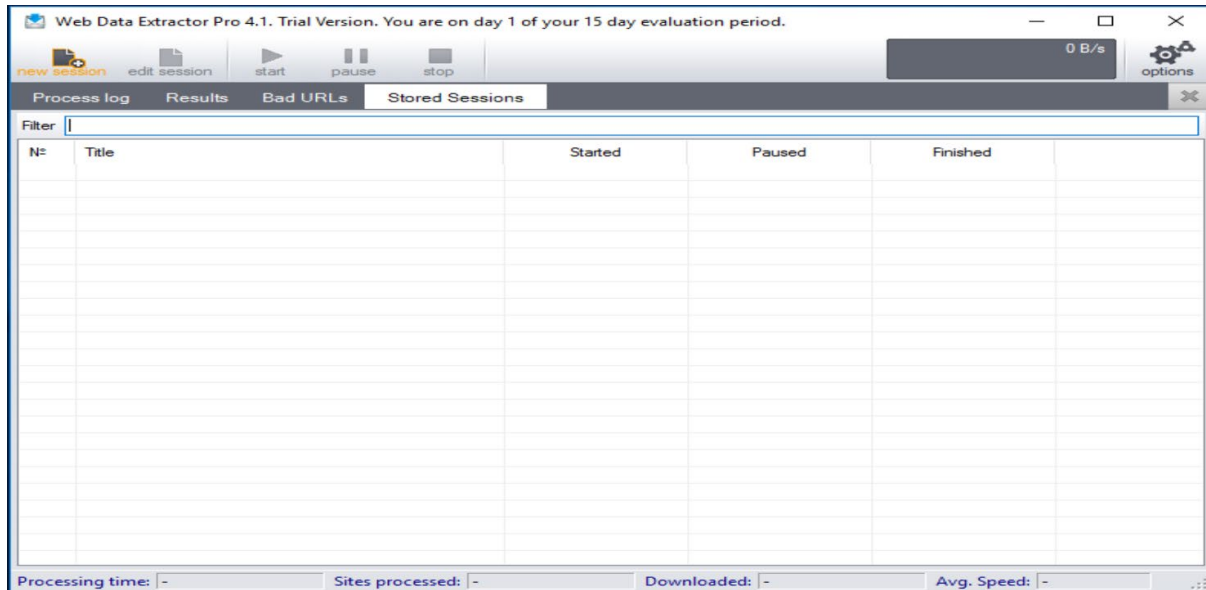
By issuing the above steps, you may get the records of domain from an authoritative server. What is so important in getting the information like this?

How can we prevent our Infrastructure from these kinds of attack? Could you reflect your reviews in a short description with appropriate citations? Why do we get an output like this?

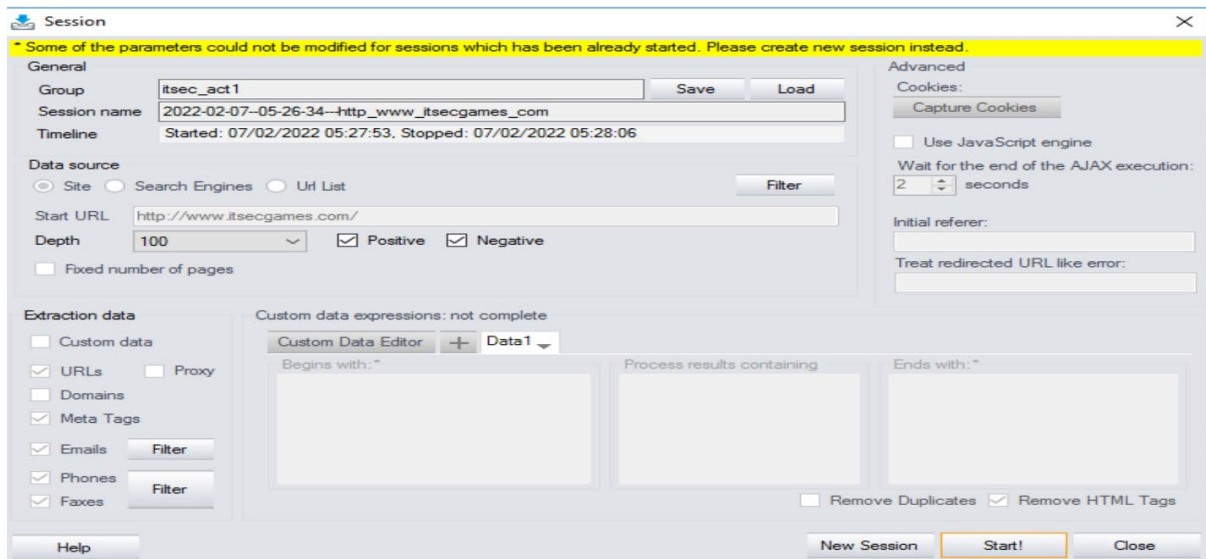
This Page is
intentionally left blank

2. Use Web Data Extractor tool to extract data from web pages. (Web Scraping or Web Data Mining)

Download Web Data Extractor



Start a scan to extract information like Emails, Data, Phone number etc.



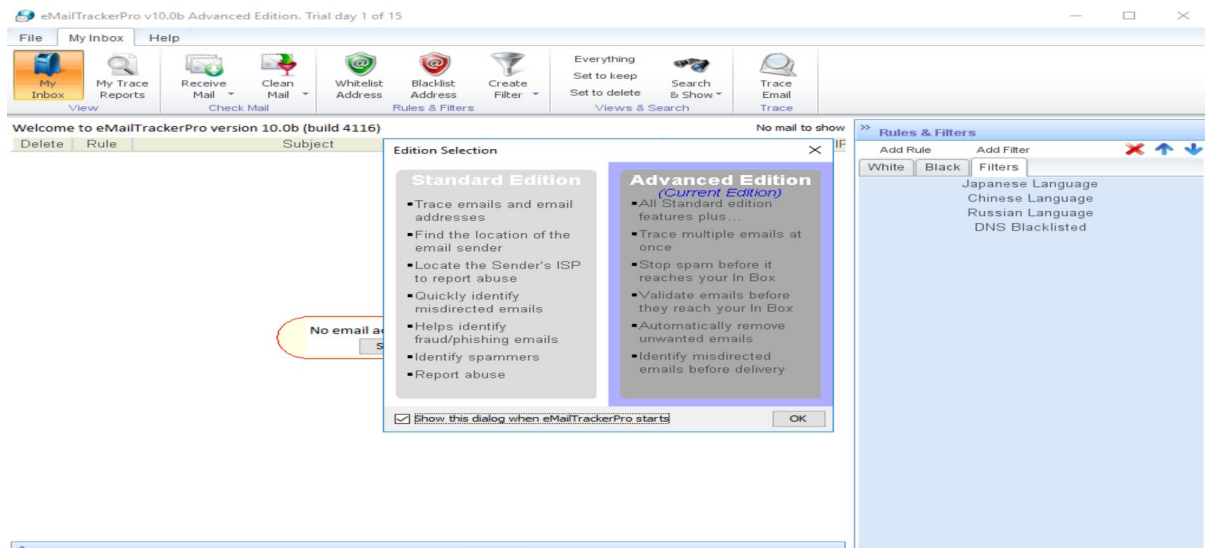
What information did you gather? Did you get the below result? If so, why? If not, what would be the reason for an outcome like the below one?

This Page is
intentionally left blank

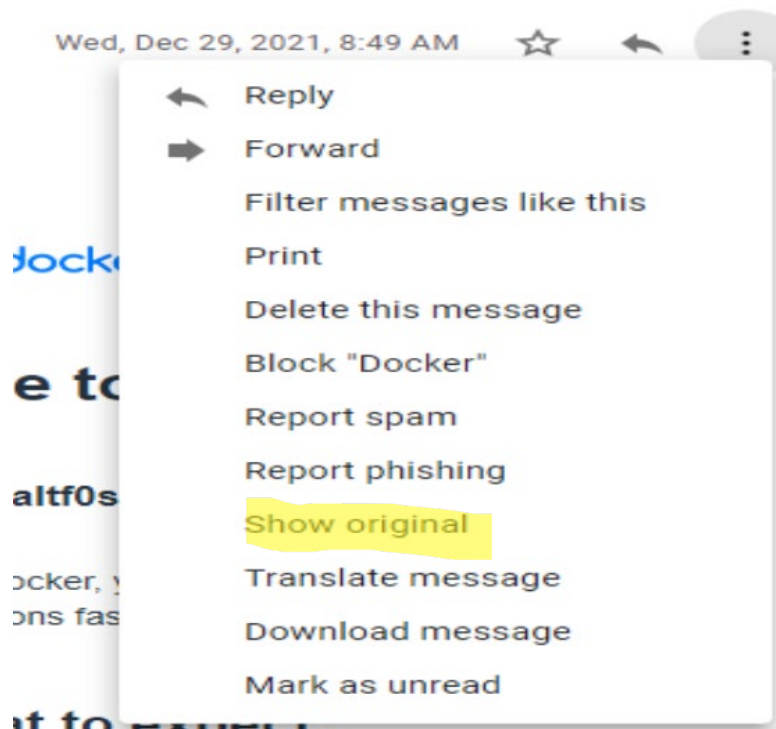
3. Use Email Tracker Pro to trace and track delivered email

Email Tracking helps you identifying the details of an email like when it was received, read, location of the recipient, time spent in the email, links, attachments etc.

Download eMailTracker Pro. Install along with its dependencies. Work in Windows Machine.



Select My Trace Reports, Trace Headers. Select Trace an email I have received and enter the email header you wish to track



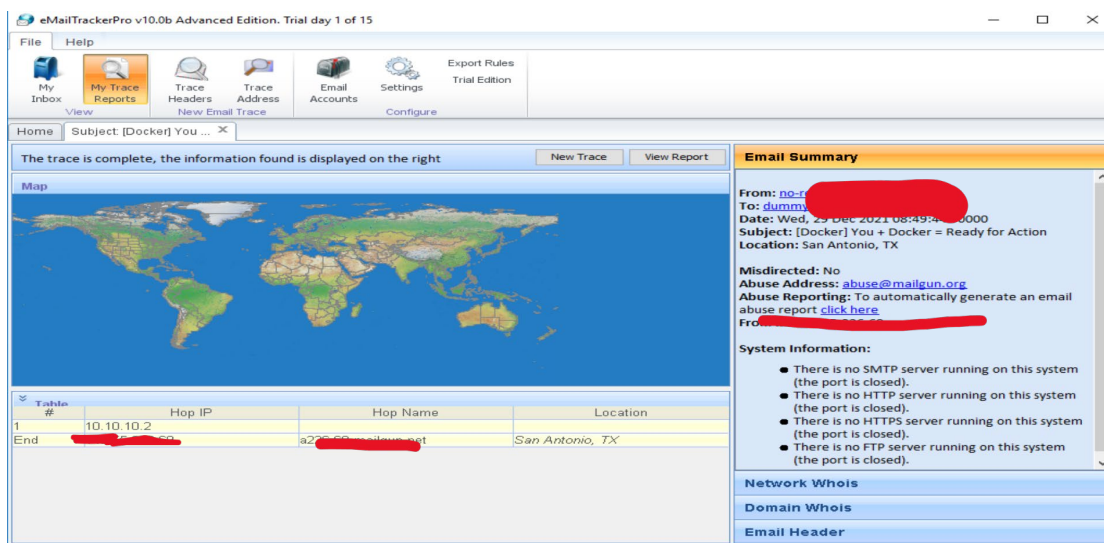
Enter Details

To proceed, paste the email headers in the box below ([how do I find the headers?](#)).

Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

Trace Cancel



What information did you gather?

Do research on the internet and find out similar tools used? Document them with their operations, functions, and screenshots.

This Page is
intentionally left blank

4. Use TCP View tool to identify the processes running on a Machine.

Identify the processes running on a computer, the protocol they are using, and their local and remote port addresses.

Download and install the TCPView software.

Use a browser and observe the TCPView window.

Description

For a hacker to establish a connection to a remote computer, a port must be listening on that device. This may be due to infection by malware, or a vulnerability in a legitimate piece of software. A utility, such as TCPView, can be used to detect open ports, monitor them in real-time, and close active ports and processes using them.

1. Download and install the TCPView software.

Search internet for TCPView Software. List out the websites which offers a download.

Which website/ link do you think is safe to download the software? Why?

2. Create a folder on the desktop named TCPView.
3. Extract the contents of the zip to this new folder.
4. Start the Tcpview Application.
5. Finally, agree to the software license terms.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
lsass.exe	476	TCP	pi	58702	pi	0	LISTENING				
lsass.exe	476	TCPV6	pi	58702	pi	0	LISTENING				
services.exe	468	TCP	pi	49155	pi	0	LISTENING				
services.exe	468	TCPV6	pi	49155	pi	0	LISTENING				
svchost.exe	716	TCP	pi	epmap	pi	0	LISTENING				
svchost.exe	768	TCP	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCP	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDP	pi.cisco.com	ssdp	*	*		36	17,142	462	91,080
svchost.exe	1408	UDP	pi	ssdp	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	1408	UDP	pi	ws-discovery	*	*					
svchost.exe	312	UDP	pi	ws-discovery	*	*					
svchost.exe	972	UDP	pi	llmnr	*	*					
svchost.exe	972	UDP	pi	54649	*	*					
svchost.exe	1408	UDP	pi	61427	*	*					
svchost.exe	312	UDP	pi	61464	*	*					
svchost.exe	1408	UDP	pi.cisco.com	63677	*	*					
svchost.exe	1408	UDP	pi	63678	*	*					
svchost.exe	716	TCPV6	pi	epmap	pi	0	LISTENING				
svchost.exe	2300	TCPV6	pi	3587	pi	0	LISTENING				
svchost.exe	768	TCPV6	pi	49153	pi	0	LISTENING				
svchost.exe	924	TCPV6	pi	49154	pi	0	LISTENING				
svchost.exe	1408	UDPV6	[0:0:0:0:0:1]	1900	*	*					
svchost.exe	1408	UDPV6	pi.cisco.com	1900	*	*					

Endpoints: 55 Established: 1 Listening: 24 Time Wait: 0 Close Wait: 0

How many Endpoints are listed?

How many are Listening?

How many Endpoints are Established?

Set your TCPView to “Always on Top”. Use a browser and observe the TCPView window.

Note: Use the Help section of the program to help you answer the following questions.

Open any browser and browse any website. Eg: google.com, cisco.com etc

What happens in the TCPView window?

You could see a lot of colors highlighting in the tool. What is represented by the colors?

Close a process (my choice would be the web browser) and see what happens?

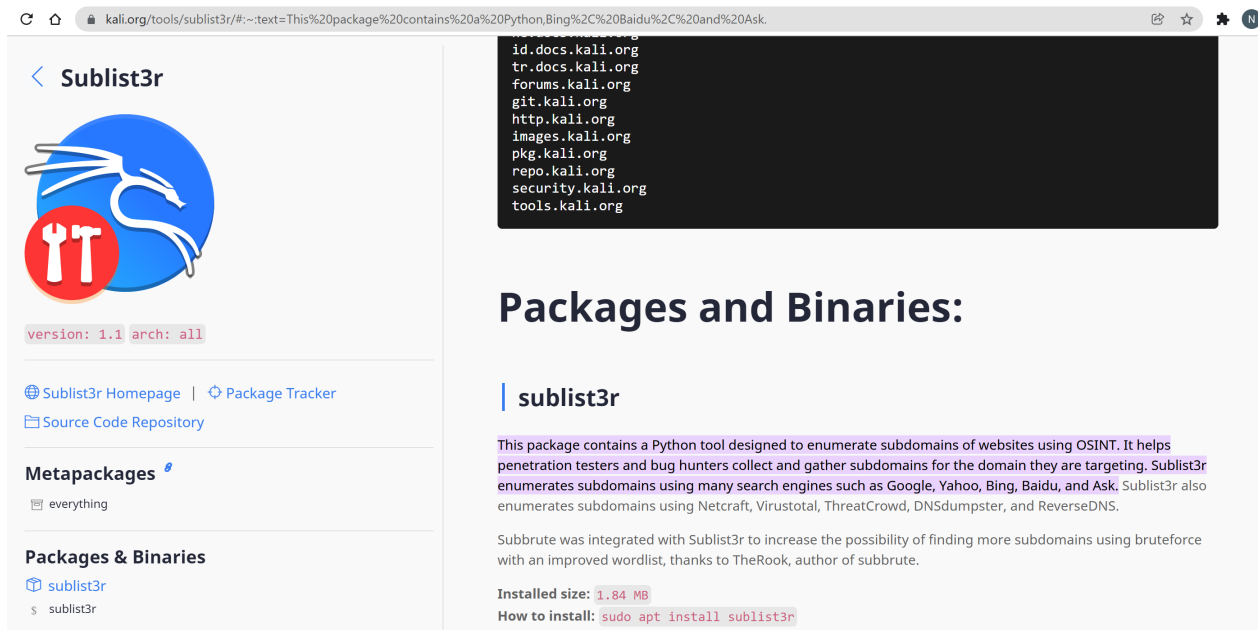
Note:

To close a process directly, right-click the process and choose End Process. Using this method can cause a program or the operating system to become unstable. Only end processes that you know are safe to end.

This method can be used to stop malware from communicating.

This Page is
intentionally left blank

5. Use Sublist3r tool to enumerate subdomains of Websites using OSINT



Sublist3r

version: 1.1 arch: all

[Sublist3r Homepage](#) | [Package Tracker](#)
[Source Code Repository](#)

Metapackages

everything

Packages & Binaries

sublist3r

id.docs.kali.org
tr.docs.kali.org
forums.kali.org
git.kali.org
http.kali.org
images.kali.org
pkg.kali.org
repo.kali.org
security.kali.org
tools.kali.org

Packages and Binaries:

sublist3r

This package contains a Python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

Subbrute was integrated with Sublist3r to increase the possibility of finding more subdomains using brute force with an improved wordlist, thanks to TheRook, author of subbrute.

Installed size: 1.84 MB
How to install: `sudo apt install sublist3r`

Open Terminal in Kali Linux

```
$ apt update && apt -y install sublist3r
```

```
Reading package lists... Done
```

```
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
```

```
E: Unable to lock directory /var/lib/apt/lists/
```

```
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
```

```
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)
```

```
—(kali@kali)~
```

```
└─$ sudo su
```

```
100 x
```

```
[sudo] password for kali:
```

```
—(root@kali)~
```

```
└─# whoami
```

```
root
```

```
—(root@kali)~
```

```
└─# apt update && apt -y install sublist3r
```

```
sublist3r -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python3 /usr/lib/python3/dist-packages/sublist3r.py -d google.com
```

Sublist3r will give you information about any subdomains. -d is to search subdomains, -t 3 with 3 threads, -e bing is to search in the bing platform

```
sublist3r -d google.com -t 3 -e bing

Sublist3r

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Bing..
[-] Total Unique Subdomains Found: 17
careers.google.com
chrome.google.com
status.cloud.google.com
developers.google.com
docs.google.com
drive.google.com
fi.google.com
groups.google.com
images.google.com
ipv6test.google.com
news.google.com
colab.research.google.com
safebrowsing.google.com
santatracker.google.com
sites.google.com
store.google.com
support.google.com
```

More commands could be used to gather further information. Here is only to find out which subdomain has port 80 open.

```
# sublist3r -d google.com -p 80 -e bing

File System Home
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Bing..
[-] Total Unique Subdomains Found: 27
[-] Start port scan now for the following ports: 80
drive.google.com - Found open ports: 80
chrome.google.com - Found open ports: 80
docs.google.com - Found open ports: 80
mail.google.com - Found open ports: 80
answers.google.com - Found open ports: 80
news.google.com - Found open ports: 80
meet.google.com - Found open ports: 80
duo.google.com - Found open ports: 80
get.google.com - Found open ports: 80
developers.google.com - Found open ports: 80
careers.google.com - Found open ports: 80
explorer.earthengine.google.com - Found open ports: 80
mapsplatform.google.com - Found open ports: 80
merchants.google.com - Found open ports: 80
desktop.google.com - Found open ports: 80
groups.google.com - Found open ports: 80
picasa.google.com - Found open ports: 80
code.google.com - Found open ports: 80
images.google.com - Found open ports: 80
ipv6test.google.com - Found open ports: 80
colab.research.google.com - Found open ports: 80
remotedesktop.google.com - Found open ports: 80
support.google.com - Found open ports: 80
santatracker.google.com - Found open ports: 80
sb.google.com - Found open ports: 80
store.google.com - Found open ports: 80
vr.google.com - Found open ports: 80

(root🐼 kali)-[/home/kali]
#
```

Do research on the internet and find out similar tools used? Document them with their operations, functions, and screenshots.

This Page is
intentionally left blank

6. Use Recon -ng tool

It is another information gathering tool, like Metasploit. It is a collection of many features to gather information. Use Kali Linux.

Install Recon -ng

Install Marketplace

Do research on the internet and find out the purpose, functionality of this tool. In relation to this tool, find out what Market place is?

```
└─$ recon-ng
[*] Version check disabled.

  _____
 /         \
/   recon-ng   \
 \         /
  _____

Sponsored by ...

  _____
 /         \
/   recon-ng   \
 \         /
  _____
  www.blackhillsinfosec.com

  _____
 /         \
/   recon-ng   \
 \         /
  _____
  www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > show modules
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpi

[recon-ng][default] > help

Commands (type [help!?] <topic>):
back          Exits the current context
dashboard     Displays a summary of activity
db            Interfaces with the workspace's database
exit          Exits the framework
help          Displays this menu
index         Creates a module index (dev only)
keys          Manages third party resource credentials
marketplace   Interfaces with the module marketplace
modules       Interfaces with installed modules
options       Manages the current context options
pdb           Starts a Python Debugger session (dev only)
script        Records and executes command scripts
```

Walkthrough Commands and its features (make yourself familiar)

[recon-ng] > help

workspaces (create workspaces) Creating a user space.

```
[recon-ng][default] > workspaces create ACCB6000
[recon-ng][ACCB6000] > workspaces list
```

Workspaces	Modified
ACCB6000	2022-02-07 01:29:35
default	2022-02-07 01:27:22

workspaces load ACCB6000**workspaces remove ACCB6000****Snapshots (saves the work)**

```
[recon-ng][default] > snapshots take
[*] Snapshot created: snapshot_20220207020751.db
[recon-ng][default] > snapshots list
```

Snapshots
snapshot_20220207020751.db

```
[recon-ng][default] > snapshots load
Loads an existing database snapshot
```

Usage: snapshots load <name>

```
[recon-ng][default] > snapshots
Manages workspace snapshots
```

Usage: snapshots <list|load|remove|take> [...]

```
[recon-ng][default] > █
```

```
[recon-ng][default] > snapshots remove snapshot_20220207020751.db
[*] Snapshot removed: snapshot_20220207020751.db
[recon-ng][default] > snapshots list
[*] This workspace has no snapshots.
[recon-ng][default] > █
```

Show (Shows various framework items)**Shell (Execute shell commands)****pdb (As a developer if you wish to check your codes, use pdb – python debugger)****Options (Setting of the framework)**

```
[recon-ng][default] > options
Manages the current context options

Usage: options <list|set|unset> [ ... ]

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

Name	Current Value	Required	Description
NAMESERVER	8.8.8.8	yes	default nameserver for the resolver mixin
PROXY		no	proxy server (address:port)
THREADS	10	yes	number of threads (where applicable)
TIMEOUT	10	yes	socket timeout (seconds)
USER-AGENT	Recon-ng/v5	yes	user-agent string
VERBOSITY	1	yes	verbosity level (0 = minimal, 1 = verbose, 2 = debug)

```
[recon-ng][default] > options set THREADS 11
THREADS ⇒ 11
[recon-ng][default] > options list
```

Name	Current Value	Required	Description
NAMESERVER	8.8.8.8	yes	default nameserver for the resolver mixin
PROXY		no	proxy server (address:port)
THREADS	11	yes	number of threads (where applicable)
TIMEOUT	10	yes	socket timeout (seconds)
USER-AGENT	Recon-ng/v5	yes	user-agent string
VERBOSITY	1	yes	verbosity level (0 = minimal, 1 = verbose, 2 = debug)

```
[recon-ng][default] > options unset THREADS 11
THREADS ⇒ None
[recon-ng][default] > options list
```

Name	Current Value	Required	Description
NAMESERVER	8.8.8.8	yes	default nameserver for the resolver mixin
PROXY		no	proxy server (address:port)
THREADS		yes	number of threads (where applicable)
TIMEOUT	10	yes	socket timeout (seconds)
USER-AGENT	Recon-ng/v5	yes	user-agent string
VERBOSITY	1	yes	verbosity level (0 = minimal, 1 = verbose, 2 = debug)

Marketplaces (Interface with the module marketplace – many tools using for hacking could be found here)

```
[recon-ng][default] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

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

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
discovery/info_disclosure/interesting_files	1.2	not installed	2021-10-04		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		
import/nmap	1.1	not installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache	1.0	not installed	2019-06-24		*
recon/companies-contacts/censys_email_address	2.0	not installed	2021-05-11	*	*
recon/companies-contacts/pen	1.1	not installed	2019-10-15		
recon/companies-domains/censys_subdomains	2.0	not installed	2021-05-10	*	*
recon/companies-domains/pen	1.1	not installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois	1.1	not installed	2021-08-24		
recon/companies-domains/whoxy_dns	1.1	not installed	2020-06-17		*

Dependencies and API keys. Tools will work only if all dependencies and API keys are installed.

```
[recon-ng][default] > marketplace search netcraft
[*] Searching module index for 'netcraft' ...
```

Path	Version	Status	Updated	D	K
recon/domains-hosts/netcraft	1.1	not installed	2020-02-05		

```

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

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

All the tools installed are saved/ located in modules

```
[recon-ng][default] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [ ... ]
```

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

Recon
-----
recon/domains-hosts/netcraft

[recon-ng][default] > █
```

Index [Gives the module index]

```
[recon-ng][default] > index
Creates a module index (dev only)

Usage: index <module|all> <index>

[recon-ng][default] > index recon/domains-hosts/netcraft
[*] Building index markup ...
- author: thrapt (thrapt@gmail.com)
  dependencies: []
  description: Harvests hosts from Netcraft.com. Updates the 'hosts' table with the
    results.
  files: []
  last_updated: '2022-02-07'
  name: Netcraft Hostname Enumerator
  path: recon/domains-hosts/netcraft
  required_keys: []
  version: '1.1'

[recon-ng][default] > █
```

Using Recon-ng (Add Workspace, Domain Names)

```
[recon-ng][default] > workspaces load ACCB6000
[recon-ng][ACCB6000] > db domain
Interfaces with the workspace's database

Usage: db <delete|insert|notes|query|schema> [ ... ]

[recon-ng][ACCB6000] > db domain schema
Interfaces with the workspace's database

Usage: db <delete|insert|notes|query|schema> [ ... ]

[recon-ng][ACCB6000] > show domains

+-----+-----+-----+-----+
| rowid | domain          | notes | module      |
+-----+-----+-----+-----+
| 2     | itsecgames.com  |       | user_defined |
| 3     | bmw.com         |       | user_defined |
| 4     | certifiedhacker.com | tutorial | user_defined |
+-----+-----+-----+-----+

[*] 3 rows returned
```

Let us use Recon-ng with available modules to gather information about our target.

Our Target:

<http://www.itsecgames.com/>

<http://www.certifiedhacker.com/>

You may also use other vulnerable sites discussed during our lectures.

Use Netcraft

1. Load Netcraft module in recon-ng

```
[recon-ng][ACCB6000] > modules load recon/domains-hosts/netcraft
[recon-ng][ACCB6000][netcraft] > run

-----
ITSECGAMES.COM
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith%0host=itsecgames.com
[*] No results found.

-----
BMW.COM
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith%0host=bmw.com
[*] No results found.

-----
CERTIFIEDHACKER.COM
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith%0host=certifiedhacker.com
[*] No results found.
```

In this screenshot, no results were found. However, outcomes may vary.

2. Load Bing. – Select `bing_domain_web` module as it is more suitable for the task we are doing.

```
[recon-ng][ACCB6000][netcraft] > modules load bing
[*] Multiple modules match 'bing'.

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

[recon-ng][ACCB6000][netcraft] > modules load recon/domains-hosts//bing_domain_web
[!] Invalid module name.
[recon-ng][ACCB6000][netcraft] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][ACCB6000][bing_domain_web] > run

ITSECGAMES.COM
-----
[*] URL: https://www.bing.com/search?first=0&q=domain%3Aitsecgames.com
[*] Country: None
[*] Host: www.itsecgames.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Aitsecgames.com+-domain%3Awww.itsecgames.com

CERTIFIEDHACKER.COM
-----
[*] URL: https://www.bing.com/search?first=0&q=domain%3Acertifiedhacker.com
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Acertifiedhacker.com+-domain%3Awww.certifiedhacker.com
[*] Country: None
[*] Host: cpanel.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Acertifiedhacker.com+-domain%3Awww.certifiedhacker.com+-domain%3Acpanel.certifiedhacker.com

SUMMARY
-----
[*] 58 total (58 new) hosts found.
```

Using the above methods to gather information, as per this screenshot, 58 new hosts are found. However, you may use different modules to identify more hosts.

What information did you gather?

Do research on the internet and find out other modules to find out more hosts. Document them with their operations, functions, and screenshots.

Similar to Bing_domain_web, we could also use, Brute_hosts

1. Search for Module Brute Hosts and run

SUMMARY

```
[*] 58 total (58 new) hosts found.
[recon-ng][ACCB6000][bing_domain_web] > modules load brute
[*] Multiple modules match 'brute'.
```

Exploitation

```
exploitation/injection/xpath_bruter
```

Recon

```
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts
```

```
[recon-ng][ACCB6000][bing_domain_web] > modules load recon/domains-hosts/brute_hosts
[recon-ng][ACCB6000][brute_hosts] > run
```

```
[*] www.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] www01.certifiedhacker.com ⇒ No record found.
[*] www1.certifiedhacker.com ⇒ No record found.
[*] www2.certifiedhacker.com ⇒ No record found.
[*] www3.certifiedhacker.com ⇒ No record found.
[*] wwwchat.certifiedhacker.com ⇒ No record found.
[*] wwwdev.certifiedhacker.com ⇒ No record found.
[*] wy.certifiedhacker.com ⇒ No record found.
[*] wyoming.certifiedhacker.com ⇒ No record found.
[*] www02.certifiedhacker.com ⇒ No record found.
[*] wwwmail.certifiedhacker.com ⇒ No record found.
[*] xi.certifiedhacker.com ⇒ No record found.
[*] x-ray.certifiedhacker.com ⇒ No record found.
[*] xlogan.certifiedhacker.com ⇒ No record found.
[*] xmail.certifiedhacker.com ⇒ No record found.
[*] xml.certifiedhacker.com ⇒ No record found.
[*] x.certifiedhacker.com ⇒ No record found.
[*] yankee.certifiedhacker.com ⇒ No record found.
[*] ye.certifiedhacker.com ⇒ No record found.
[*] xp.certifiedhacker.com ⇒ No record found.
[*] y.certifiedhacker.com ⇒ No record found.
[*] yellow.certifiedhacker.com ⇒ No record found.
[*] yt.certifiedhacker.com ⇒ No record found.
[*] z-log.certifiedhacker.com ⇒ No record found.
[*] za.certifiedhacker.com ⇒ No record found.
[*] young.certifiedhacker.com ⇒ No record found.
[*] yu.certifiedhacker.com ⇒ No record found.
[*] zebra.certifiedhacker.com ⇒ No record found.
[*] z.certifiedhacker.com ⇒ No record found.
[*] zera.certifiedhacker.com ⇒ No record found.
[*] zeus.certifiedhacker.com ⇒ No record found.
[*] zm.certifiedhacker.com ⇒ No record found.
[*] zlog.certifiedhacker.com ⇒ No record found.
[*] zulu.certifiedhacker.com ⇒ No record found.
[*] zw.certifiedhacker.com ⇒ No record found.
```

SUMMARY

```
[*] 181 total (144 new) hosts found.
[recon-ng][ACCB6000][brute_hosts] > █
```

As per the screenshot, 144 new hosts found. Now, we shall do a reverse lookup for the IP Address to know the Hostnames.

2. Search for Module Reverse Lookup

```
[recon-ng][ACCB6000][brute_hosts] > modules load reverse
[*] Multiple modules match 'reverse'.

Recon
-----
recon/companies-domains/viewdns_reverse_whois
recon/hosts-hosts/reverse_resolve
recon/locations-locations/reverse_geocode
recon/netblocks-hosts/reverse_resolve

[recon-ng][ACCB6000][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][ACCB6000][reverse_resolve] > █
```

```
[*] Country: None
[*] Host: a2-22-225-186.deploy.static.akamaitechnologies.com
[*] Ip_Address: 2.22.225.186
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: yours-customised-nasfree.mini.com
[*] Ip_Address: 160.46.231.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] 195.27.218.61 ⇒ No record found.
[*] 193.23.38.30 ⇒ No record found.
[*] 193.23.33.6 ⇒ No record found.
[*] Country: None
[*] Host: live01.iconmobile.com
[*] Ip_Address: 62.220.6.131
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] 160.46.238.41 ⇒ No record found.
[*] 4.26.228.254 ⇒ No record found.
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] 127.0.0.1 ⇒ No record found.
```

SUMMARY

```
[*] 36 total (33 new) hosts found.
[recon-ng][ACCB6000][reverse_resolve] > █
```

As per the screenshot, 33 new hosts are found.

3. Let's look at the hosts

```
[recon-ng][ACCB6000][reverse_resolve] > show hosts
```

rowid	module	host	ip_address	region	country	latitude	longitude
1	www.itsecgames.com						
2	static.bmw.com						
3	lifestyle.bmw.com						
4	...						
223	reverse_resolve	server-13-224-132-83.lhr3.r.cloudfront.net	13.224.132.83				
224	reverse_resolve	a104-96-173-40.deploy.static.akamaitechnologies.com	104.96.173.40				
225	reverse_resolve	ec2-3-126-241-72.eu-central-1.compute.amazonaws.com	3.126.241.72				
226	reverse_resolve	ec2-3-69-83-113.eu-central-1.compute.amazonaws.com	3.69.83.113				
227	reverse_resolve	host-62-245-246-210.customer.m-online.net	62.245.246.210				
228	reverse_resolve	a2-22-225-202.deploy.static.akamaitechnologies.com	2.22.225.202				
229	reverse_resolve	a23-62-3-203.deploy.static.akamaitechnologies.com	23.62.3.203				
230	reverse_resolve	iucp.bmw.com	194.55.91.208				
231	reverse_resolve	a23-62-3-208.deploy.static.akamaitechnologies.com	23.62.3.208				
232	reverse_resolve	a2-22-225-186.deploy.static.akamaitechnologies.com	2.22.225.186				
233	reverse_resolve	yours-customised-nasfree.mini.com	160.46.231.230				
234	reverse_resolve	live01.iconmobile.com	62.220.6.131				
235	reverse_resolve	box5331.bluehost.com	162.241.216.11				

```
[*] 235 rows returned
[recon-ng][ACCB6000][reverse_resolve] >
```

4. Use Reporting module to gather the information and analyse them for further attacks.

```
[recon-ng][ACCB6000][html] > back
[recon-ng][ACCB6000] > modules load reporting/html
[recon-ng][ACCB6000][html] > options set FILENAME /home/kali/Desktop/ACCB6000 output.html
FILENAME => /home/kali/Desktop/ACCB6000 output.html
[recon-ng][ACCB6000][html] > options set CREATOR Nitheesh
CREATOR => Nitheesh
[recon-ng][ACCB6000][html] > options set CUSTOMER ACB
CUSTOMER => ACB
[recon-ng][ACCB6000][html] > run
[*] Report generated at '/home/kali/Desktop/ACCB6000 output.html'.
[recon-ng][ACCB6000][html] >
```

5. Report

ACB

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	3
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	235
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Hosts

Created by: Nitheesh
Mon, Feb 07 2022 04:11:09

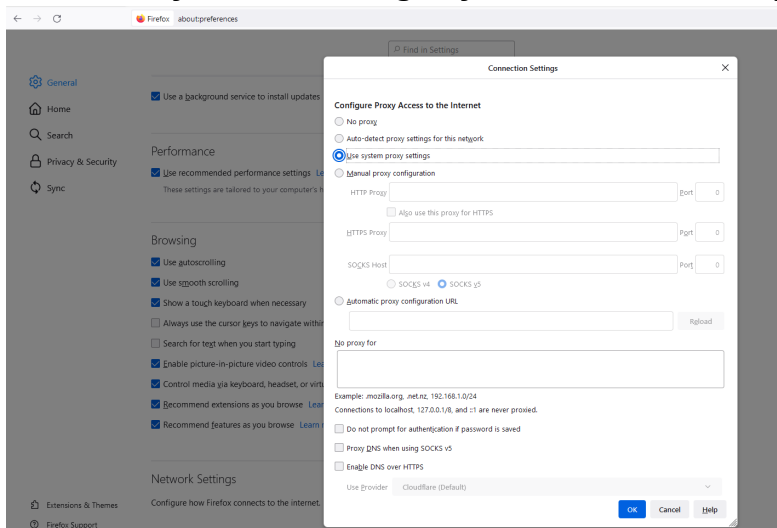
Note: Similar to Recon-ng, there are several tools that help you with an automated Report. Try to use tools like this to generate reports in your Virtual Lab Network. Use those reports as evidences during your demonstration to support your information gathering activity.

This Page is
intentionally left blank

7. Use Proxy Switcher to browse anonymously.

+ Machine: Windows Client

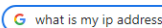
1. Download Proxy Switcher.
2. Install Proxy Switcher in Windows 10. **USE ONLY IN LAB ENVIRONMENT**
3. Make sure you have changed your Browser's Proxy settings.



(This is in Firefox. Options varies in each browser. Look for Settings → Network Settings → Proxy)

 Use system proxy settings

4. Look at your public IP Address.

 what is my ip address

Google

Search Google or type a URL



Web Store



Add shortcut

whatismyip.com/my-ip-information/

WhatsMyIP.com IP Lookup Speed Test Change IP Hide IP Search ... Sign Up Login

WhatsMyIP.com » Tools » My IP Information

My IP Information

Holidays just got easier
Book now

My Public IPv4 is:
2.96.16.17
Your IPv6 is: Not Detected

Stay safe, browse fast.
Get Special Deal

My IP Location Info ?	My IP Hostname
City: Bristol	ISP: TalkTalk Communications Limited
State: England	Host Name: host-2-96-16-17.as13285.net
Country: United Kingdom of Great Britain and Northern Ireland	ASN: 13285

IP Tools

- Internet Speed Test
- IP Address Lookup
- IP Address Hostname Lookup
- IP WHOIS Lookup
- Server Headers Check
- Email Header Analyzer
- Blacklist Check
- User Agent Info
- DNS Lookup
- Reverse DNS Lookup
- Proxy Check
- Port Scanner
- Password Strength Test

How To Knowledge Base Resources

What is your IP Address?

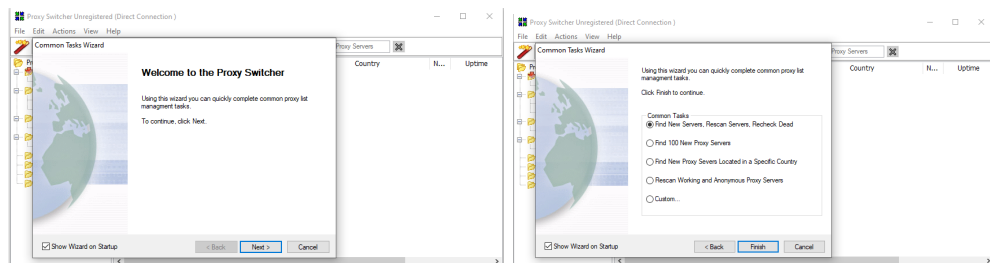
What is your location?

Could you locate/see any proxy detected?

Which tool did you use to find the above information?

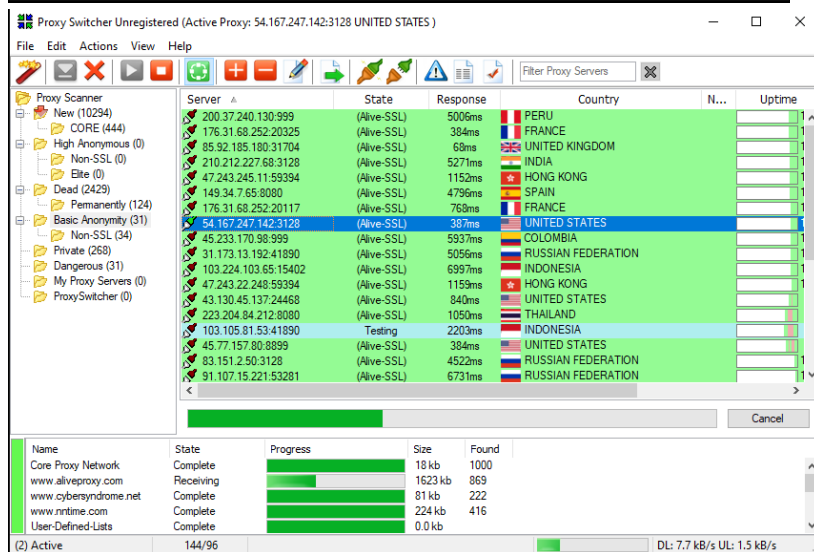
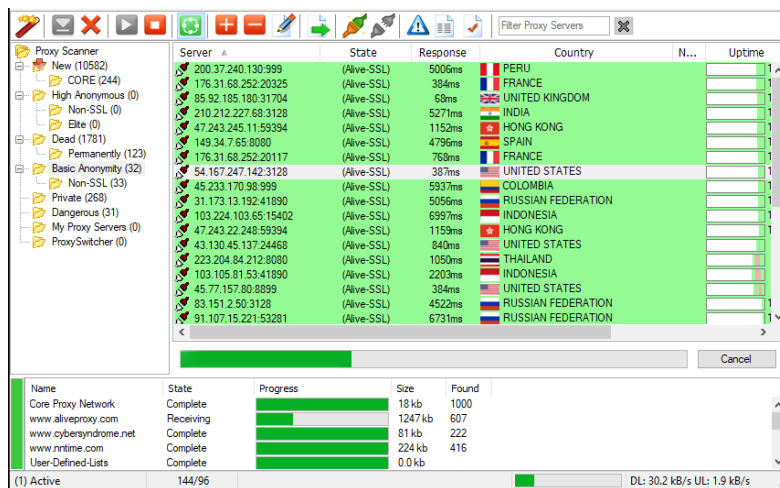
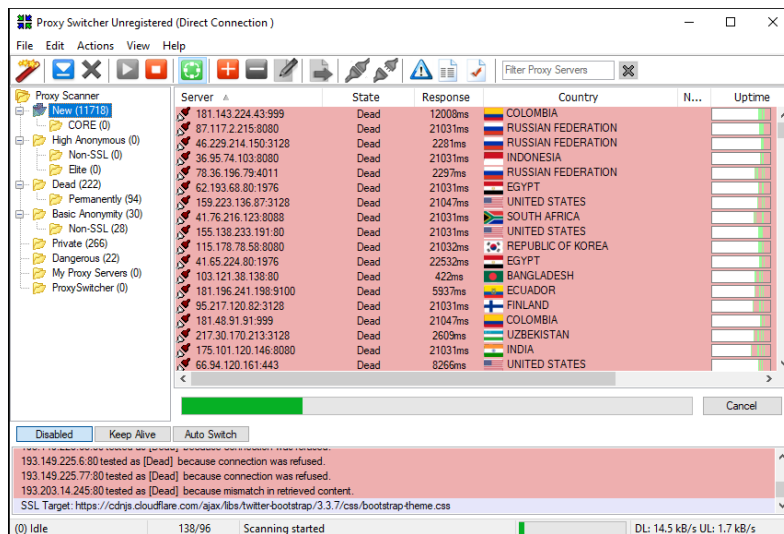
5. Use Proxy Switcher:

- List the available Proxies: Use Common Tasks wizard to find new servers.



- Select any one of the servers from the basic anonymity list and connect to the server. In this example, the connect was made using an available

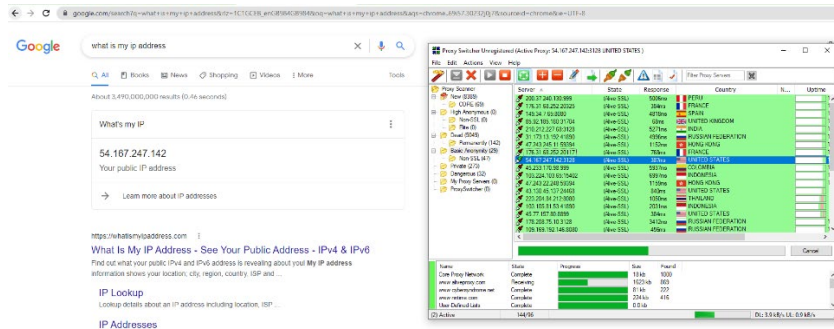
US Server. Make sure you select any available server in Alive-SSL State.



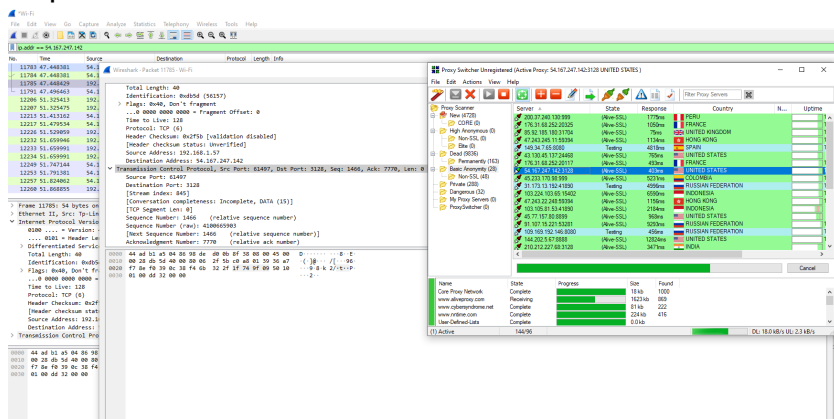
- c. Make sure you are connected: Use Proxy Switcher to check your connection.



d. Check your IP Address.

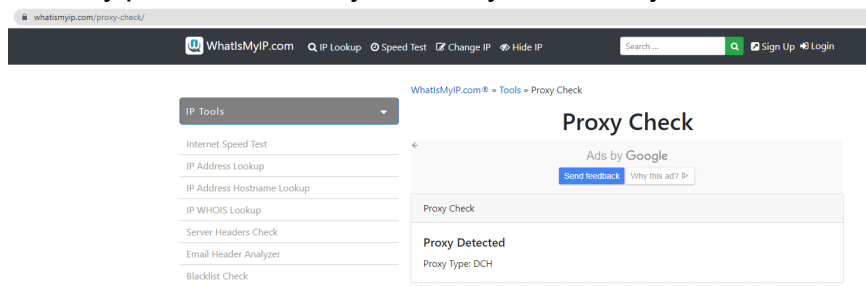


e. Capture Traffic and Check.



6. Use other tools, that you have used so far during information-gathering phase to further analyse. What did you get? Did you manage to identify your proxy server or type?

7. Use Whatismyip.com to check your Proxy. What do you see?



8. Based on your usage of this tool, and the analysis done, write your understanding on using Proxy tools like this. Referring to the above screenshot, what is the Proxy type DCH?

Part 2

1. Use HPING Version 3 to send ICMP/TCP/UDP Packets and analyse the target replies.

- + Target Machine: Windows 10/ Windows Server 2022/ Linux / Bee-Box
- + Attacker Machine: Kali Linux
- + Use Wireshark in the Target Machines to capture the packets and observe

Using HPING3 (Commands):

1. Install HPING3

Install HPING3 and use HELP command to know about the available commands. Try those commands and analyse the outcomes.

```
hping3 --help
```

2. ICMP Scanning

```
hping3 -1 "Target"
```

#in my case it is 192.168.0.20

What is the other method to send an ICMP packet?

3. Sending SYN Packet

```
hping3 -S "Target"
```

Try other commands like TCP Acknowledgement (-L), Fin Flag (-F), RST Flag (-R), etc

Find out other flag commands and test in your network:

PUSH

URG

XMAS

YMAS

4. ACK Scanning on port 80

```
hping3 -A "Target" -p 80
```

5. Sending Fin Packet

```
hping3 -F "Target"
```

6. Sending Syn Packet to a port

```
hping3 -S "Target" -p 80
```

7. Scanning entire subnet

```
hping3 -1 192.168.0.x --rand-dest -I eth0
```

Try to send a limited Syn packet

Try to send Raw IP

Try to send Ack flag without using -A to scan ports from 1500-3000 on a specific target.

Based on the above topology (using a Win Client, Server and Linux Machine), come up with different scenarios to scan and get further information about the target network.

Try yourself(Commands):

1. Send 5 packets to the target and receive response.
2. Send a SYN flag targeting ports 1 to 5000
3. Send UDP Packets by crafting them with data size 600 on the Target

By sending this UDP packet, what did you observe at the Target machine?

Launch Wireshark in the Target Machine

4. Send a TCP SYN Scan request to the Target through port 80 with 3 counts of packet (*Refer to the above commands to execute this task*)

Observe the TCP Packets in the Target using Wireshark. Could you locate the TCP Packets?

Start a new Wireshark capture in the Target Machine

5. Flood the Target with TCP packets

Observe the flooding TCP Packets in the Target machine using Wireshark. Could you look at the information of TCP packets transmitted to and from attacker machine?

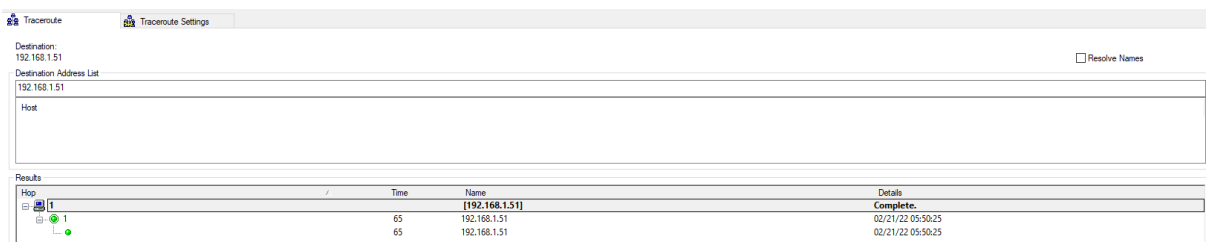
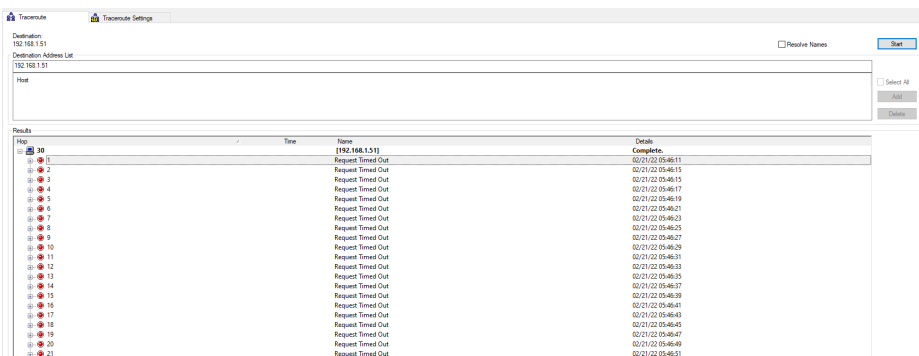
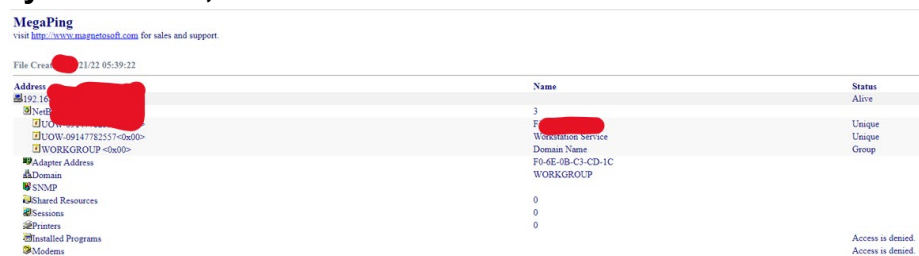
List/demonstrate other tools which could be used for doing similar attacks. Compare and Contrast with HPING3 to further enhance your understanding.

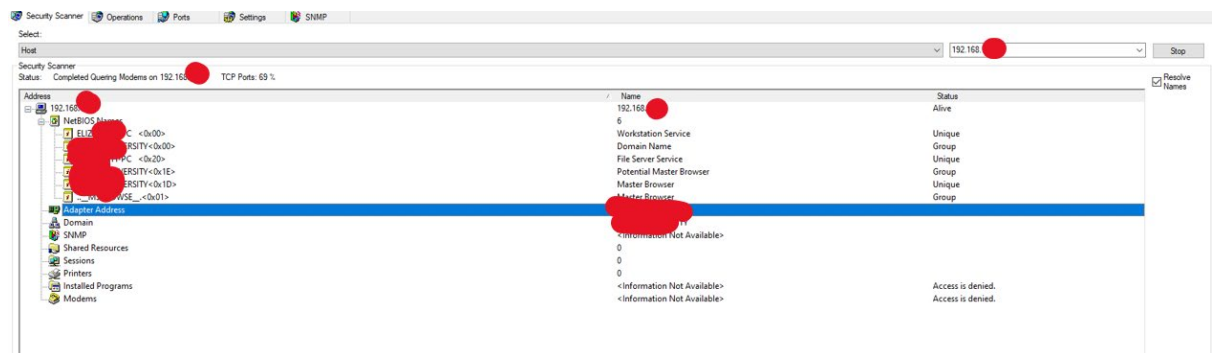
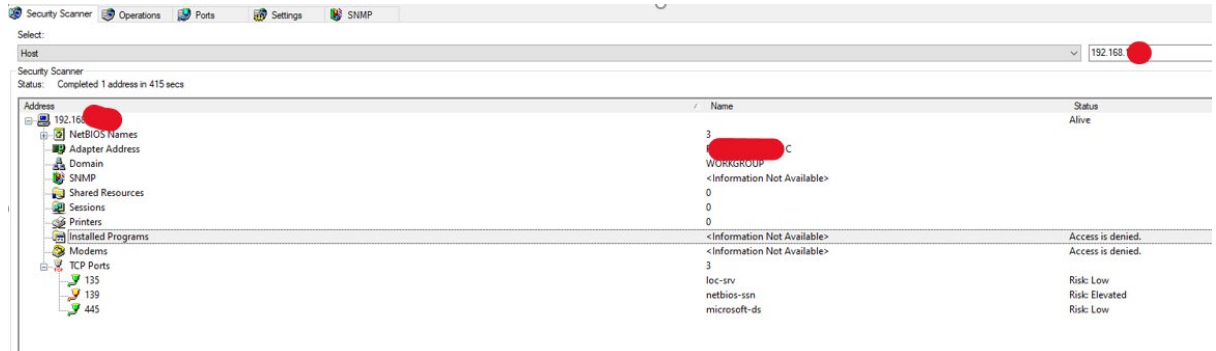
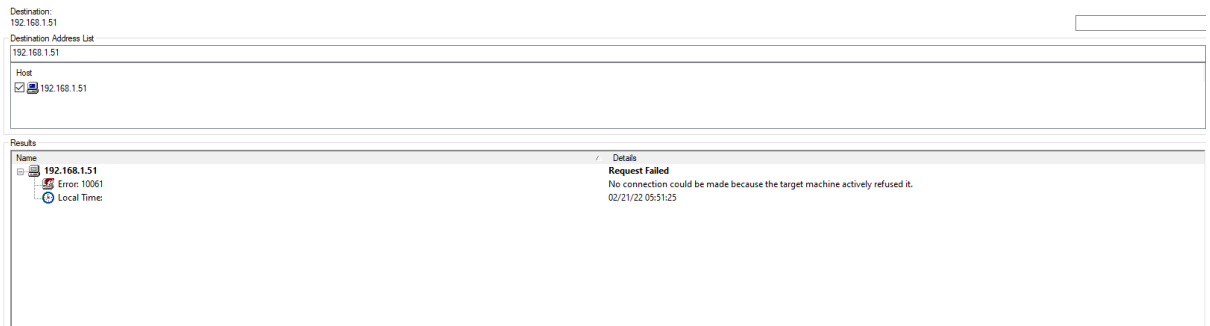
This Page is
intentionally left blank

2. Use MegaPing to identify live hosts and open ports of the Target.

- + Machine: Windows Servers 2022, Windows Client, Linux, Bee Box
- + Use Wireshark in the Target Machines to capture the packets and observe

1. Download MegaPing.
2. Do an Internet Search about MegaPing. What is this tool for? Which website did you download MegaPing? Why?
3. Install MegaPing in Windows Server 2022.
4. Scan your Lab Network. (Look for Information like Active Host Machines, Ports, System info, DNS list host, DNS Lookup name, Network Time Synchronizer, Resources etc.





5. Based on your research earlier at Step 2, you might have known that MegaPing tool could look for potential vulnerabilities within your network. Did you manage to discover any vulnerabilities in your network?

6. Report

MegaPing

visit <http://www.magnetosoft.com> for sales and support.

File Created: 02/21/22 05:56:17

Address	Name	Status
192.168.1.51	192.168.1.51	Alive
NetBIOS Names		
<0x00>	Workstation Service	Unique
<0x00>	Domain Name	Group
<0x20>	File Server Service	Unique
<0x1E>	Potential Master Browser	Group
<0x1D>	Master Browser	Unique
<0x01>	Master Browser	Group
Adapter Address	A4-17-31-37-3E-D5	
Domain	BOTHOUNIVERSITY	
SNMP		0
Shared Resources		0
Sessions		0
Printers		0
Installed Programs		
Modems		Access is denied.
		Access is denied.

This Page is
intentionally left blank

3. Use NetScanTools Pro to initiate various Scans (not limited to ARP Ping Scan, DHCP Server Discovery, Ping Scan, Port Scan etc).

- + Note: NetScanTools Pro is one of the handy tools which could be used for various scanning and enumeration process.
- + Machine: Windows Servers 2022, Windows Client 10, Linux, Bee-Box
- + Use Wireshark in the Target Machines to capture the packets and observe

1. Download NetScanTools Pro.

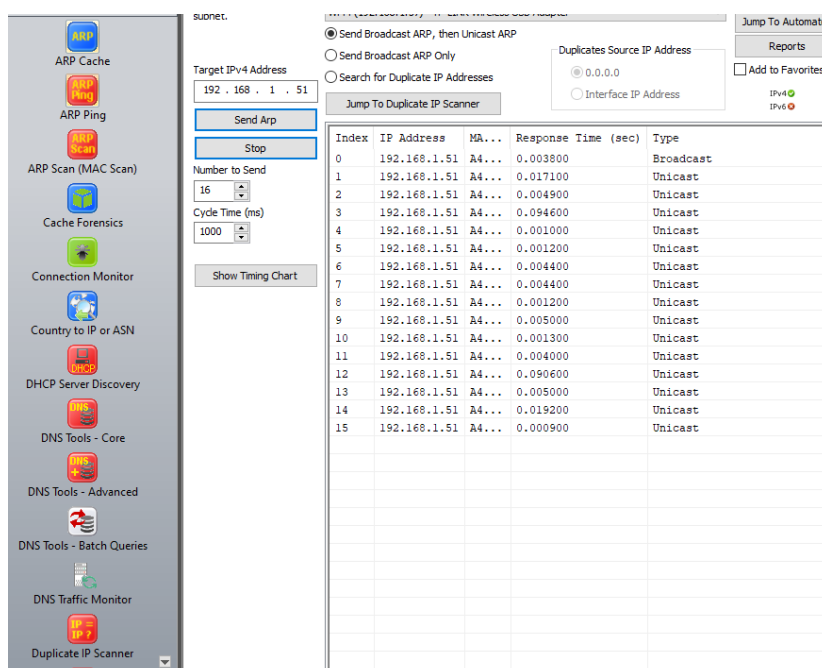
2. Based on our Lectures, (I have discussed about various scans and enumeration methods for which NetScanTools Pro could be used) could you list out the various functions of this tool?

3. Install NetScanTools Pro in Windows Server 2022.

Note that, using this tool, you can do an Active operation by sending packets to the target to receive responses. **USE ONLY IN LAB ENVIRONMENT**

4. Scan your Lab Network. (Use Manual Tools to scan range of ports, Hostnames, IP Addresses, MAC Addresses, DHCP Servers etc).

- a. Use utilities like ARP Ping Tool: ARP ping will send ARP packets to the target to find the response time. As discussed in the lecture, using response time, we could gather more information.
- b. Use utilities like ARP Scan Tool: ARP scan will send ARP packets to the range of IPs to rapidly sweep the subnet for devices that are connected.
- c. Similarly, use many utilities available in the tool and discover information about your network.



Use this tool to find all active IPv4 devices on your subnet.

Network Interface: Wi-Fi (192.168.1.57) - TP-LINK Wireless USB Adapter

Starting IPv4 Address: 192.168.1.1 Ending IPv4 Address: 192.168.1.60

Do ARP Scan

Stop

Scan Delay Time (ms): 10

Packets sent per IP: 3

☒ Resolve IPs

☒ Include Local I/F Info

Defaults

Jump To Dupe IP Scan

ARP Scanner Response Summary

1: Response, 6

2: +Other Local I/F, 1

3: No Response, 54

IPv4 Address	MAC Ad...	I/F Manufacturer	Hos...	Notes or Comments
192.168.1.1	44-AD-...		ttr...	
192.168.1.2	B8-5F-...		?	
192.168.1.3	10-7B-...	AS...	?	
192.168.1.4	D4-63-...	ility ...	?	
192.168.1.5	F0-6E-...	Micro...		
192.168.1.6	A4-17-...	ion ...	Eli...	
192.168.1.7	98-DE-...		hos...	

Target Hostname or IPv4 Address: 192.168.1.1

Network Interface: Wi-Fi (192.168.1.57) - TP-LINK Wireless USB Adapter

Completed.

Analyze Target

Stop

Settings

Start Time: Mon, 21 Feb 2022 06:21:09

Target: 192.168.1.1 [192.168.1.1]

Hops: 1

TargetReached? Yes

Possible Operating System(s):

Windows 7 - 32 or 64 bit

5. Based on your usage of this tool, and earlier tools within your lab network, what are the additional details you gathered after using this tool?

6. Report

NetScanTools Pro v11.11

Reports Created with DEMO v11.11

Report created with NetScanTools Pro v11.11 DEMO

Test Results Report

Report Print Date and Time: 02/21/22 06:35:29

Results Database: demo

Analyst: TITR

Organization:

Target: Multiple targets

All tools in the database for the above target are shown.

Test: ARP Scan

Input: 192.168.1.1

Reference: 1043421

Results:

Index	IP Address	MAC Address	Response Time (sec)	Type
0	192.168.1.1	A4-17-...	0.003800	Broadcast
1	192.168.1.2	A4-17-...	0.017100	Unicast
2	192.168.1.3	A4-17-...	0.004900	Unicast
3	192.168.1.4	A4-17-...	0.094600	Unicast
4	192.168.1.5	A4-17-...	0.001000	Unicast
5	192.168.1.6	A4-17-...	0.001200	Unicast
6	192.168.1.7	A4-17-...	0.004400	Unicast
7	192.168.1.8	A4-17-...	0.004400	Unicast
8	192.168.1.9	A4-17-...	0.001200	Unicast
9	192.168.1.10	A4-17-...	0.005600	Unicast
10	192.168.1.11	A4-17-...	0.001300	Unicast
11	192.168.1.12	A4-17-...	0.004000	Unicast
12	192.168.1.13	A4-17-...	0.090900	Unicast

This Page is
intentionally left blank

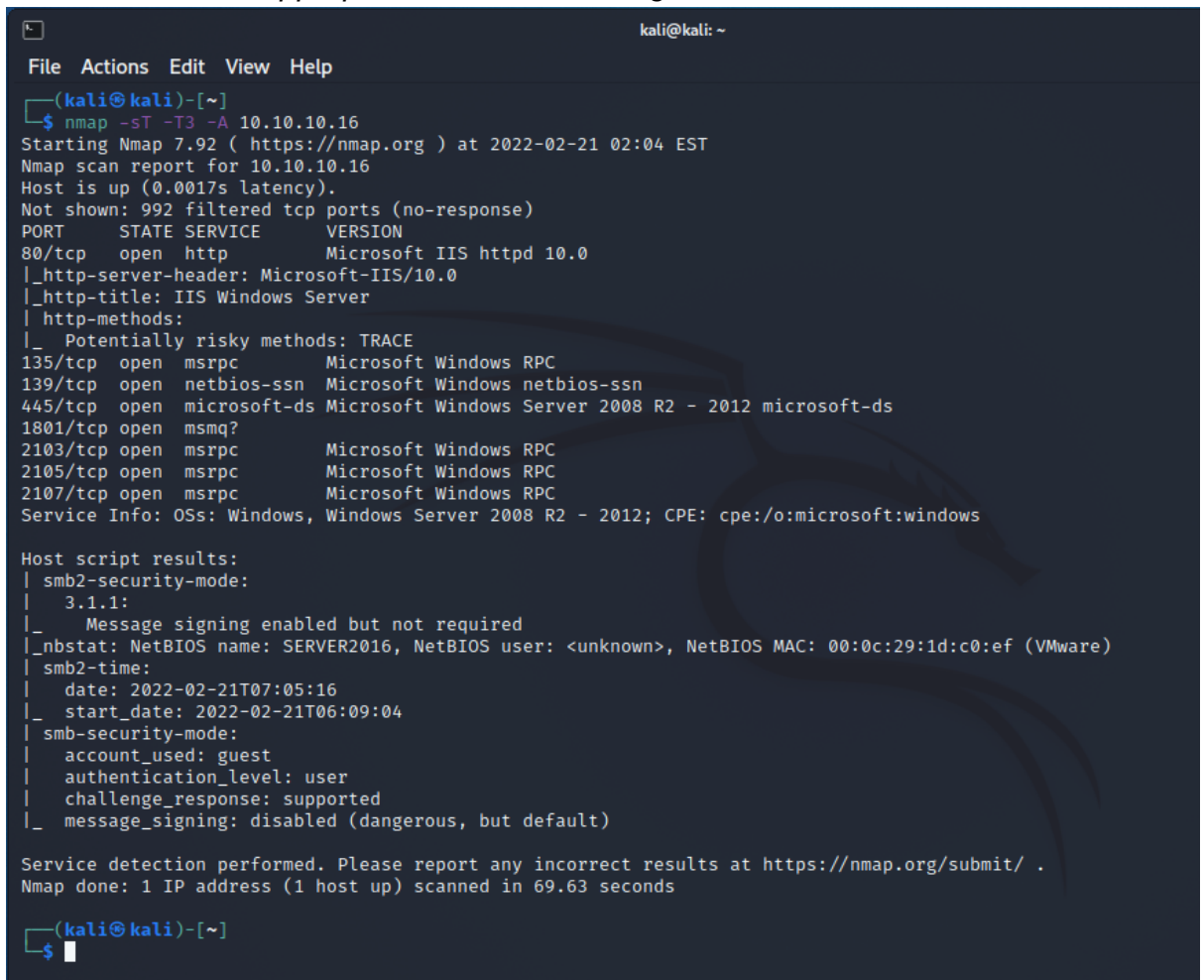
4. Explore various network scanning Techniques

- + Machine: Windows Servers 2022, Linux
- + Use Wireshark to capture the packets in the target machines and observe the changes

Use Nmap to do a TCP Connect scan, Xmas Scan, ACK Flag scan, UDP Scan and IDLE Scan.

Task

1. Login to Win Server 2022, Client, Linux Machines
2. Perform a TCP Connect Scan on Win Server 2022. (Refer to TCP Connect Scan during our Lecture) – IP Address ranges vary from your network to this screenshot – Use appropriate IP Address/ range



```
(kali@kali)-[~]
└─$ nmap -sT -T3 -A 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:04 EST
Nmap scan report for 10.10.10.16
Host is up (0.0017s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
|_http-methods:
|_ Potentially risky methods: TRACE
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
1801/tcp  open  msmq?
2103/tcp  open  msrpc          Microsoft Windows RPC
2105/tcp  open  msrpc          Microsoft Windows RPC
2107/tcp  open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   3.1.1:
|   |_ Message signing enabled but not required
|_ nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:1d:c0:ef (VMware)
|_ smb2-time:
|   date: 2022-02-21T07:05:16
|   start_date: 2022-02-21T06:09:04
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.63 seconds

(kali@kali)-[~]
└─$
```

From the above screenshot, you might notice that the result gives you all open ports, OS Fingerprinting results, nbstat, smb details etc.

3. Perform a Xmas Scan on Win Server 2022. (Refer to Xmas Scan during our Lecture). Note that we are sending a TCP Frame to the target with PSH, URG & FIN flags set.

```

# nmap -sA -v -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:18 EST
Initiating ARP Ping Scan at 02:18
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 02:18, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:18
Completed Parallel DNS resolution of 1 host. at 02:18, 0.02s elapsed
Initiating ACK Scan at 02:18
Scanning 10.10.10.16 [1000 ports]
Completed ACK Scan at 02:18, 2.56s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00048s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
Raw packets sent: 1148 (45.908KB) | Rcvd: 1001 (40.028KB)

```

We are initiating ACK Scan to display the port. Could you observe that the ports are in ignored states.

- ✓ Why?
- ✓ Is it because of Firewall? Is our Firewall Off or On? Try the viceversa.

Maybe, Yes!!! Initially, we might have turned the Firewall Off. Turn them On and execute Xmas scan with aggressive timing. Here the timing is -T4. Again, Turn them Off and execute the same.

```

(kali@kali)-[~]
$ nmap -sX -T4 10.10.10.16
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sX -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:11 EST
Nmap scan report for 10.10.10.16
Host is up (0.00034s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

(root@kali)-[/home/kali]
# nmap -sX -T4 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:12 EST
Nmap scan report for 10.10.10.16
Host is up (0.00049s latency).
All 1000 scanned ports on 10.10.10.16 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.66 seconds

```

Can you identify the difference between firewall status? With reference to our lecture, ACK probe could be sent with random sequence number on the target. If there is an response saying unfiltered, then it means the port is closed. If there is no response, then the port is filtered.

In all my scans, the ports are in ignored states. Could you able to find out a way to identify the status of the ports? Do some research.

4. Perform UDP Scan on Win Server 2022. (Refer to UDP Scan during our Lecture).

Lets find out the UDP ports on the target. I used -T5 to send packets quicker which waits only for 0.3 seconds for the response.

```
(root@kali)~[/home/kali]
# nmap -sU -T5 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:21 EST
Warning: 10.10.10.16 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.16
Host is up (0.00046s latency).
Not shown: 988 open|filtered udp ports (no-response)
PORT      STATE SERVICE
19/udp     closed chargen
137/udp    open  netbios-ns
161/udp    open  snmp
3389/udp   closed ms-wbt-server
18543/udp  closed unknown
19315/udp  closed keyshadow
21902/udp  closed unknown
26407/udp  closed unknown
38498/udp  closed unknown
41058/udp  closed unknown
41896/udp  closed unknown
49503/udp  closed unknown
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
```

Lets now do a Zombie scan. Two choices for us to test. One make Win Server 2022 as Zombie and target Windows 10 and other vice versa.

```
(root@kali)~[/home/kali]
# nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:22 EST
Idle scan using zombie 10.10.10.16 (10.10.10.16:80); Class: Incremental
Even though your Zombie (10.10.10.16; 10.10.10.16) appears to be vulnerable to IP ID sequence prediction (class: Incremental), our attempts have failed. This generally means that either the Zombie uses a separate IP ID base for each host (like Solaris), or because you cannot spoof IP packets (perhaps your ISP has enabled egress filtering to prevent IP spoofing), or may be the target network recognizes the packet source as bogus and drops them
QUITTING!
```

```
(root@kali)~[/home/kali]
# nmap -Pn -p 80 -sI 10.10.10.10 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:23 EST
Idle scan using zombie 10.10.10.10 (10.10.10.10:80); Class: Incremental
Nmap scan report for 10.10.10.16
Host is up (0.0068s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

Observe the output. Why is the difference?

5. Perform Ping sweep Scan on Target Network. (Refer to Ping Sweep Scan during our Lecture).

```
(root@kali)~[/home/kali]
# nmap -sP 10.10.10.*
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 02:23 EST
Nmap scan report for 10.10.10.1
Host is up (0.00088s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 10.10.10.2
Host is up (0.00034s latency).
MAC Address: 00:50:56:F4:76:12 (VMware)
Nmap scan report for 10.10.10.10
Host is up (0.00028s latency).
MAC Address: 00:0C:29:60:3C:DA (VMware)
Nmap scan report for 10.10.10.16
Host is up (0.00034s latency).
MAC Address: 00:0C:29:1D:C0:EF (VMware)
Nmap scan report for 10.10.10.254
Host is up (0.00044s latency).
MAC Address: 00:50:56:E9:75:26 (VMware)
Nmap scan report for 10.10.10.11
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.17 seconds
(root@kali)~[/home/kali]
```

Observe the output.

After using various tools so far, what are the details you have gathered? Document them. My advice would be to document automated reports as evidences for your demonstration.

This Page is
intentionally left blank

5. Identify Target Operating System with TTL

- + Machine: Windows Servers 2022, Windows 10, Linux, Bee-Box.
- + Use Wireshark to capture the packets from the target machine and observe TTL, TCP Window Size to determine the Operating System.

Task

- Before starting this task, you need to know the TTL & TCP Window Size values of different Operating Systems. With reference to our discussion during our lectures,
 - What is TCP Window Size?
 - List out the values below.
- Login to Win Server 2022. Use Packet Capturing tool and start capturing packets.
- Ping Win Server 2022 from Windows 10, Linux and Kali Machines
- Observe the captured packets in Win Server 2022.
 - Select icmp packets from each target machines to the Server and look for the packet details.

The top screenshot shows a Wireshark packet capture on a Windows Server 2022 interface. The packet list shows several ICMP Echo (ping) request and reply packets. The packet details pane for the selected packet shows the following information:

- Ethernet II, Src: VMware_a6:9e:f4 (00:0c:29:a6:9e:f4), Dst: VMware_6a:5c:12b (00:0c:29:6a:5c:12b)
- Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.16
- Internet Control Message Protocol (ICMP), Type: Echo (ping) request, Id: 0xe305, Seq: 8/2048, Ttl: 64 (reply in 92)

The bottom screenshot shows a Wireshark packet capture on a Kali Linux interface. The packet list shows several ICMP Echo (ping) request and reply packets. The packet details pane for the selected packet shows the following information:

- Ethernet II, Src: VMware_a6:9e:f4 (00:0c:29:a6:9e:f4), Dst: VMware_6a:5c:12b (00:0c:29:6a:5c:12b)
- Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.16
- Internet Control Message Protocol (ICMP), Type: Echo (ping) request, Id: 0xe305, Seq: 8/2048, Ttl: 64 (reply in 92)

- From the above output, could you determine what is the Operating System running in host machines?

- c. What details did you gather?**
- d. What assumptions could be made with the gathered information?**
- e. Refer to the Wireshark - .pcapng file (Wireshark Sample Capture) given to you in Moodle. Analyse that and list out the Operating Systems captured.**

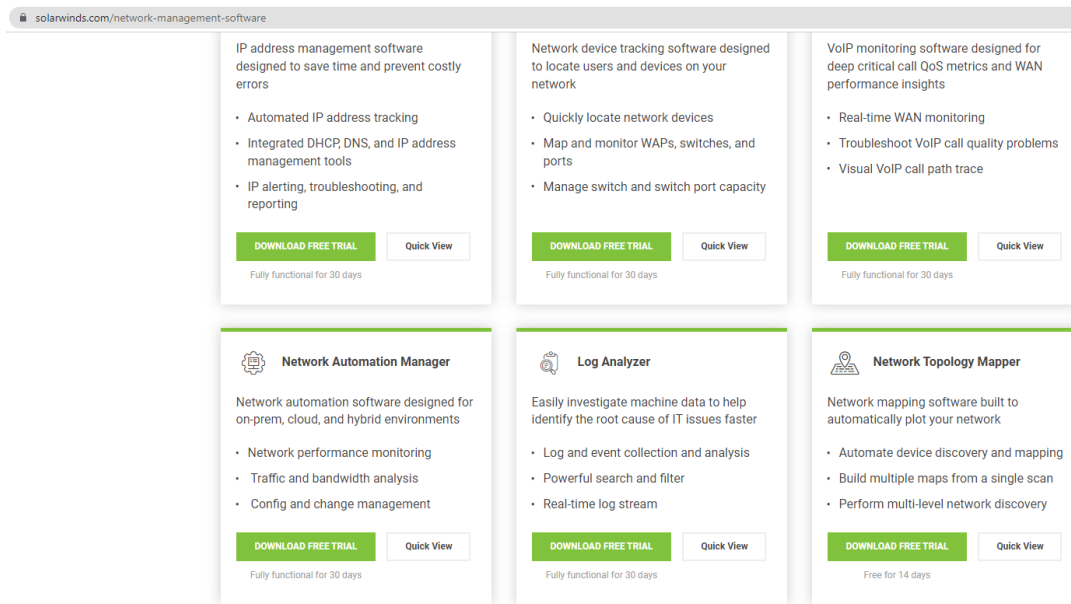
This Page is
intentionally left blank

6. Map your Network

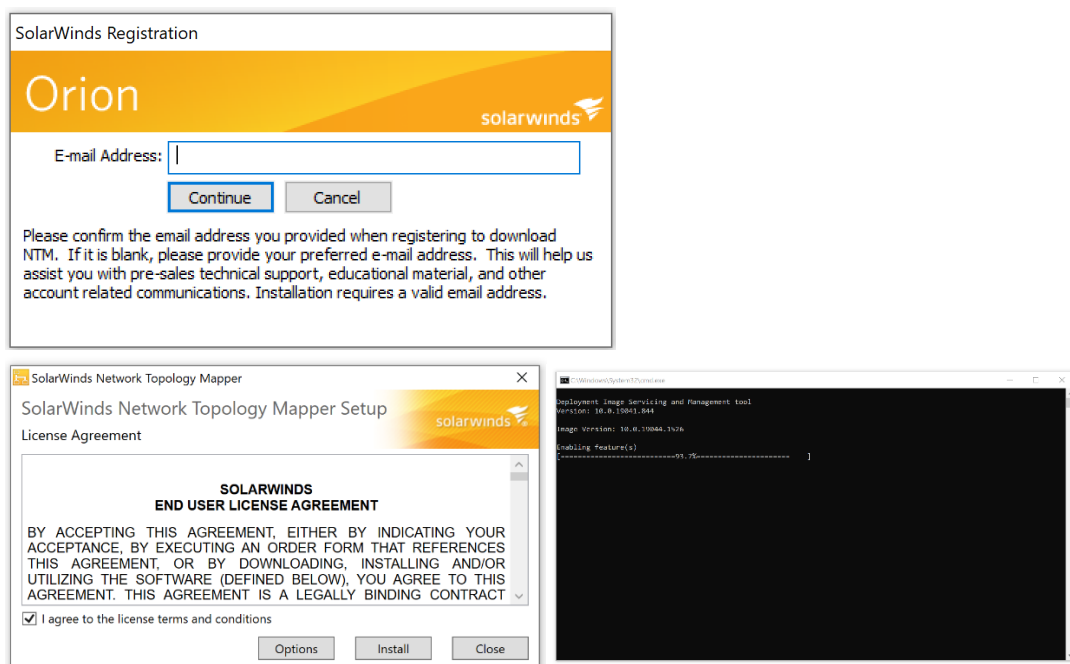
- + Machine: Windows Servers 2022, Windows 10, Linux, Bee-Box.
- + Map your network using Automatic Mapping Tool.

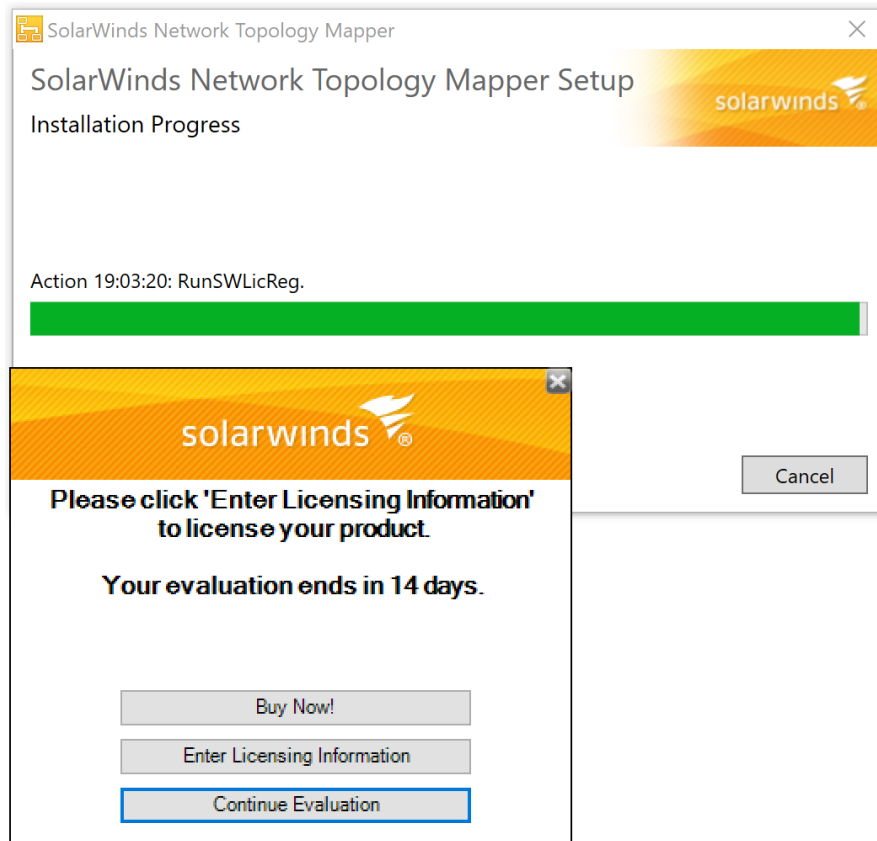
Task

1. Download Network Topology Mapper from Solarwinds. (You may use different tool to accomplish this task)



2. Install the tool in Windows Server 2022.

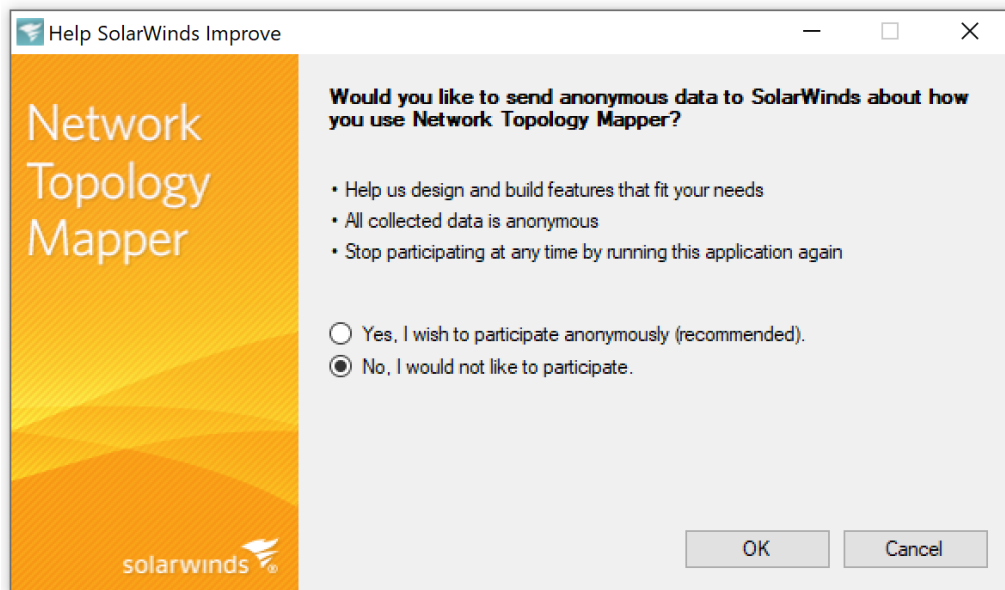




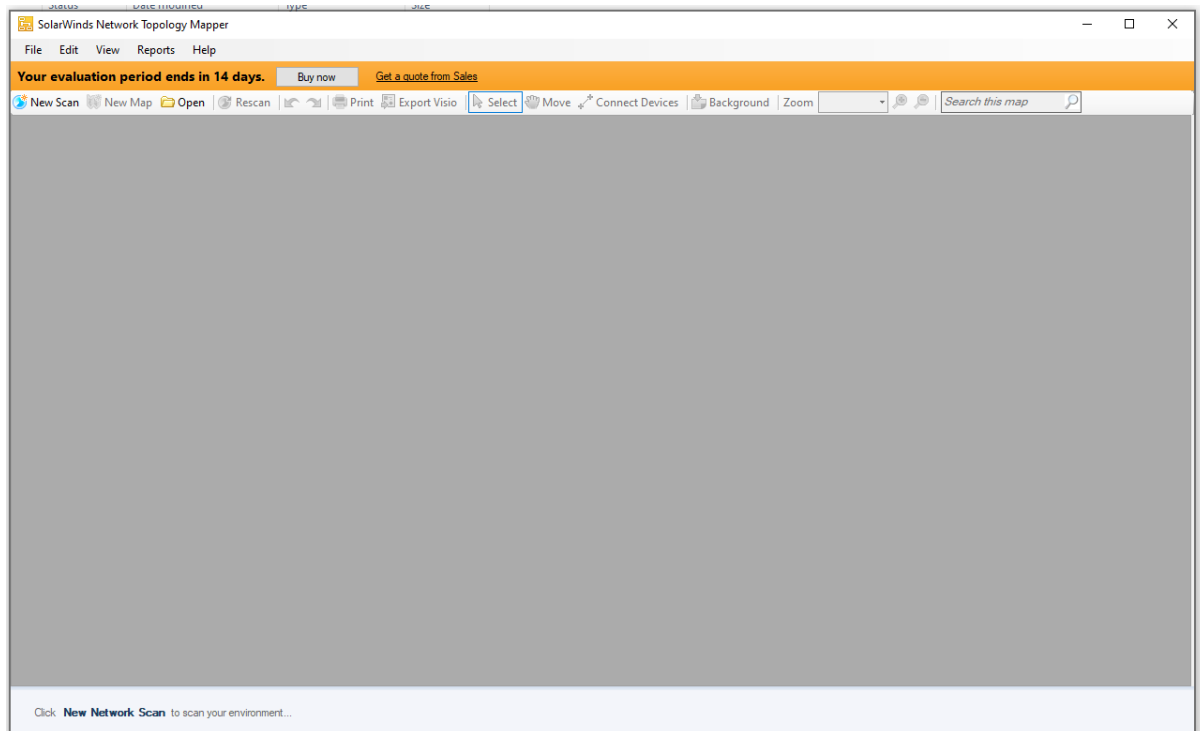
If you are using Network Topology Mapper from Solarwinds,

a) what option did you select on the following “Would you like to send anonymous data to SolarWinds about how you use Network Topology Mapper?”

b) Why did you select the stated option?



3. After Installation, begin a New Scan



4. Select SNMP Credentials and Select the Network.

Network Topology Scan

SNMP Credentials

Pick SNMP credentials used for discovery on your network from list of stored Credentials or add new credential. Credentials are used in the order listed below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Stored Credentials:

☐	Name		
☒	private ✓		
☐	public ✓		

Discovery Credentials:

☐	#	Name		
☒	1	public		
☐	2	private		

New Credential

SNMP must be enabled on your devices before running Network Discovery Scan to get the results on the map.
[» Learn more about SNMP](#)

Next > Cancel

Network Topology Scan

Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Subnets IP Ranges Free-form IPs Do-Not-Scan List

Start Address: 192.168.1.0 **End Address:** 192.168.1.255

Add

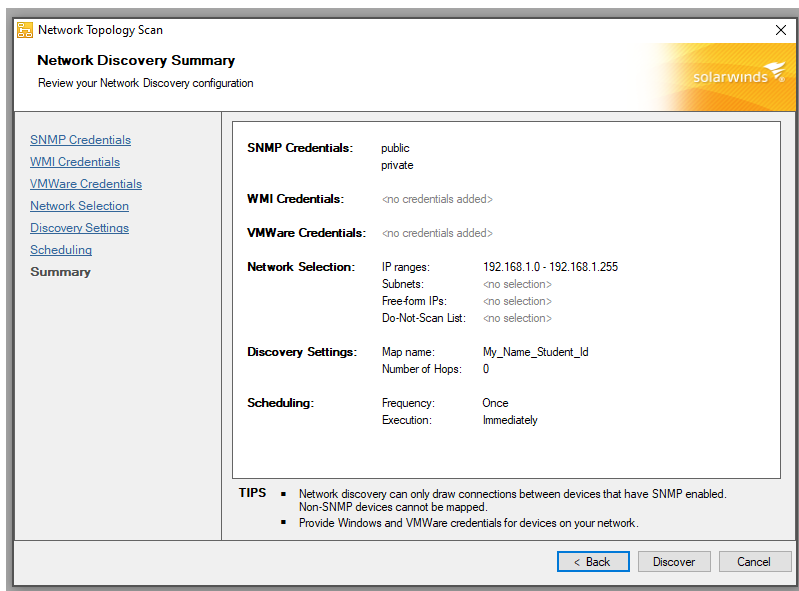
To include IPv6 addresses in the discovery, add them in the Free-form IPs tab.

Network Selection Summary:

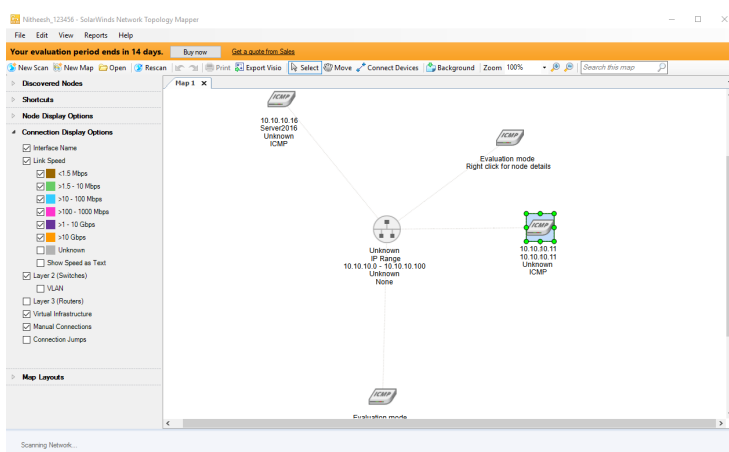
Subnets:	No selection
IP Ranges:	1x
Free-form IP Entries:	No selection
Do-Not-Scan List:	No selection

< Back Next > Cancel

5. Assign your name and Student Id as the Name to Scan and Discover the network.



6. Use the details to map your network. You will now have a network topology. Expand and explore the Node Display Options, Map Layouts to gather more information.



7. Use Integration with Windows Tools to gain access using Remote Desktop, gather more information using ping, traceroute, Telnet etc.

8. Generate Report

Nitheesh_123456 - Inventory report

Export Print Options

IP Address	IP Addresses	Hostname	Primary Role	Roles	Sysname	Machine Type	Vendor	Location	Contact	System Description	Polling Method	MAC Addresses
10.10.10.2	10.10.10.2	10.10.10.2	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.8	10.10.10.8	WIN-4L1UT...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.10	10.10.10.10	DESKTOP-G...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.11	10.10.10.11	10.10.10.11	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.16	10.10.10.16	Server2016	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
		IP Range10...	Network Segm...	Network...		Unknown	Unknown				None	

Part 3

With reference to our lectures, enumeration when you try and connect to the system and do deliberate actions to gather more information. The initial process of enumeration includes finding names of the machines within Target network. Using the gathered names, detailed information on network and its resources could be probed.

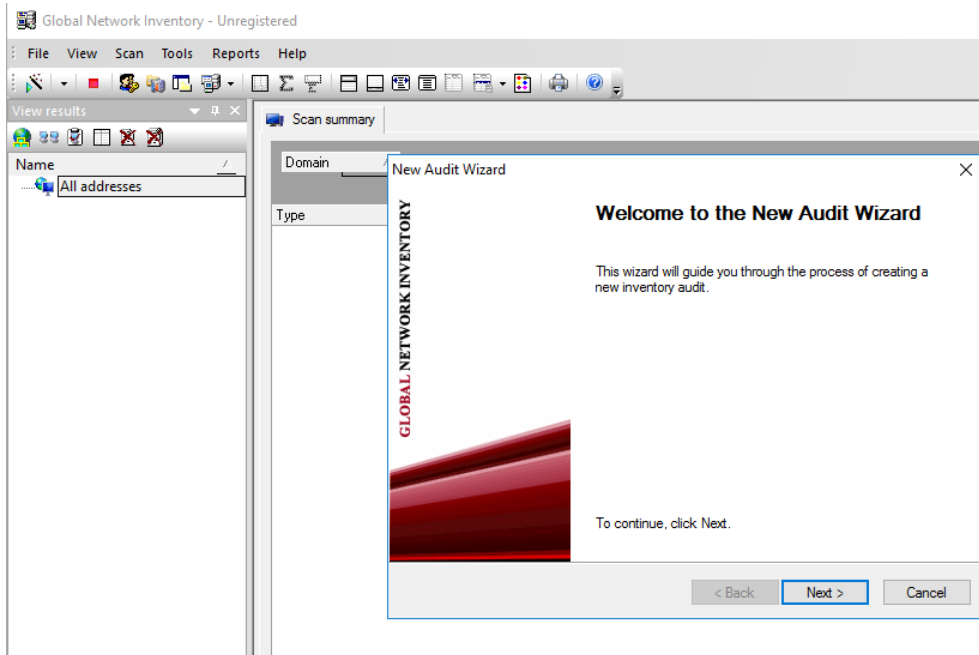
1. Enumerate using Tools

+ Machine: Windows Servers 2022.

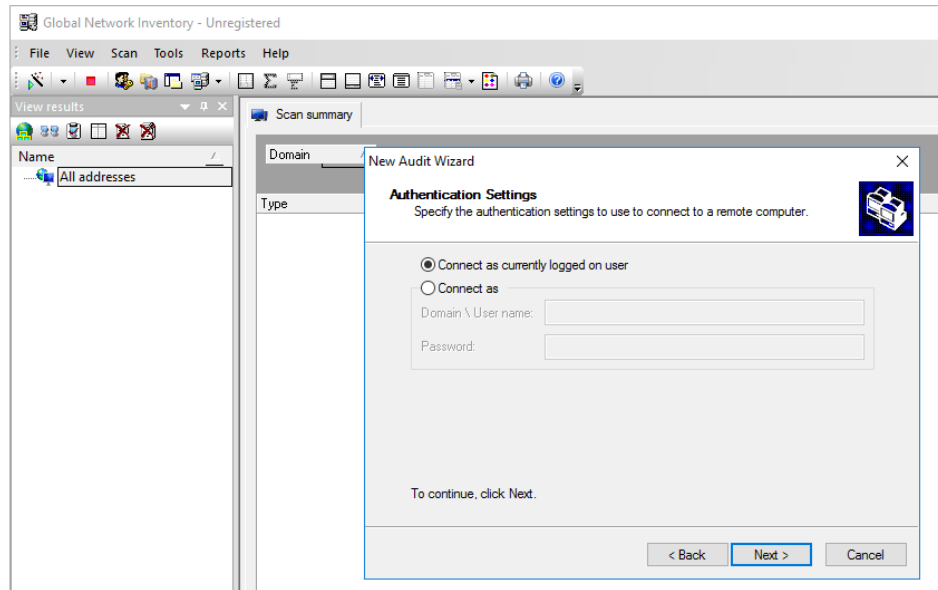
Using tools like Global Network Inventory is used to scan the networks based on IP range, Domain, Host etc.

Task

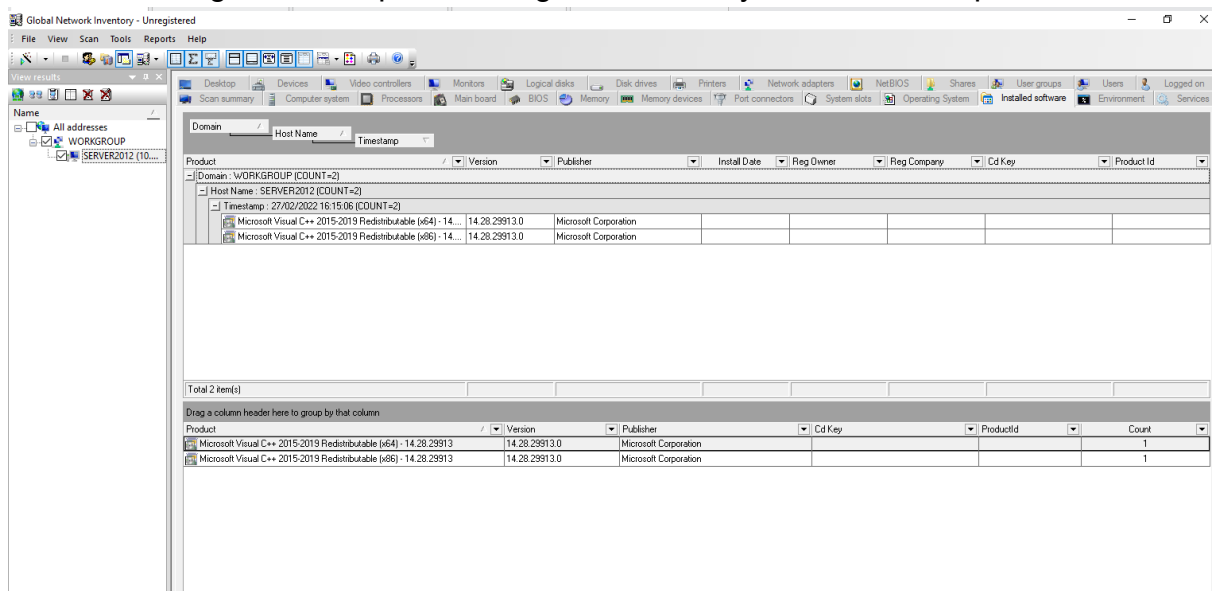
1. Download Global Network Inventory tool. (You may use different tool to accomplish this task)
2. Install GNI tool. Open the New Audit Wizard and initiate the scan. You have two options to proceed further.



- a. Connect as currently logged on user
If you are using this tool in an initial stage where you don't have the user credentials of the target, use this option. However, by using this option you might only get basic information like Physical and Logical addresses.
- b. Connect as
Once you have managed to get the user credentials of the target, use that and connect as the target and gather information.



3. Do scans using both the options and gather as many information as possible.



What is the difference between both the scans?

Using user credentials, did you manage to gather information like Software's Installed, Services Running, NetBIOS information, Users, User Groups, Operating System etc?

Yes!! – What are your gathered information?

No!! – Why? Reason out and do research, troubleshoot and gather the above information.

4. Generate Report

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Services | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Services

Name	Start Type	State	File
Domain: WORKGROUP (COUNT=196)			
Host Name: SERVER0216 (COUNT=196)			
Timestamp: 27/02/2022 16:15:06 (COUNT=196)			
Application Experience	Manual	Stopped	C:\Windows\System32\svchost.exe -k ApplicationExperience
Application Host Helper Service	Automatic	Running	C:\Windows\System32\svchost.exe -k aehdsvc
Application Identity	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Application Information	Manual	Stopped	C:\Windows\System32\svchost.exe -k aehdsvc
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe
Application Management	Manual	Stopped	C:\Windows\System32\svchost.exe -k aehdsvc
Agent Deployment Service (AppXSVC)	Manual	Stopped	C:\Windows\System32\svchost.exe -k wscntfrg
ASP.NET State Service	Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
Background Intelligent Transfer Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Background Transfer Infrastructure Service	Automatic	Running	C:\Windows\System32\svchost.exe -k DcomLaunch
Base Filtering Engine	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetwork
BranchCache	Automatic	Running	C:\Windows\System32\svchost.exe -k PeerDist
CardSpace Propagation	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Client for NFS	Automatic	Running	C:\Windows\System32\svchost.exe
Cloud Key Isolation	Manual	Stopped	C:\Windows\System32\svchost.exe
Color Management	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalService
COM+ System Application	Manual	Running	C:\Windows\System32\svchost.exe -k Process (DCE4B3F1-FD8B-11D1-96D2-0005F57A2328)
Computer Browser	Disabled	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Content Manager	Manual	Stopped	C:\Windows\System32\svchost.exe
Cryptographic Services	Automatic	Running	C:\Windows\System32\svchost.exe -k NetworkService
DCOM Server Process Launcher	Automatic	Running	C:\Windows\System32\svchost.exe -k DcomLaunch
Device Association Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Device Install Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k DcomLaunch
Device Setup Manager	Manual	Stopped	C:\Windows\System32\svchost.exe -k netvcs
Dhcp Client	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Diagnostic Policy Service	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetwork
Diagnostic Service Host	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalService
Diagnostic System Host	Manual	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
DeviceNet User Taskhost Client	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Desktop | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Desktop

Screen Name (Executable)	Screen Size (Width)	Screen Size (Height)	Screen Size (Area)
Host Name: SERVER0216 (COUNT=7)			
Timestamp: 27/02/2022 16:15:06 (COUNT=7)			
Name: DEFAULT (COUNT=1)			
Name: ES_APPPOOL.NET v4.5 (COUNT=1)			0
Name: ES_APPPOOL.NET v4.5 Classic (COUNT=1)			0
Name: NT_AUTHORITY\LOCAL SERVICE (COUNT=1)			0
Name: NT_AUTHORITY\NETWORK SERVICE (COUNT=1)			0
Name: NT_AUTHORITY\SYSTEM (COUNT=1)			0
Name: SERVER0216\administrator (COUNT=1)			0
Total 7 items			0

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali Linux 2021.4e-vmware...

Global Network Inventory Network adapters | February 27, 2022

visit <http://www.maasnetwork.com> for sales and support.

Network adapters

Adapter Name	MAC Address	Adapter IP Address	Adapter IP Subnet	Adapter Default IP Gateway	Manufacturer	Adapter Type	XPnP Enabled
Domain: WORKGROUP (COUNT=1)							
Host Name: SERVER0216 (COUNT=1)							
Timestamp: 27/02/2022 16:15:06 (COUNT=1)							
Microsoft i80274c Gigabit Network Connection	00 0C 29 8C 7C 49	10 10 10 12	255.255.255.0	10 10 10 2	Intel Corporation	Ethernet 802.3	No
Total 1 items							

5. What are the other similar tools did you manage to research? Could you compare those tools with this and discuss the pros and cons?

This Page is
intentionally left blank

2. Enumerate using Nmap and Net Use

+ Machine: Kali, Windows Servers 2022, Win 10, Linux, Bee-Box.

Using this technique, we could gather User names, User groups, List of Computers, OS, Ports, Names, Network resources, Services, Policies and Passwords

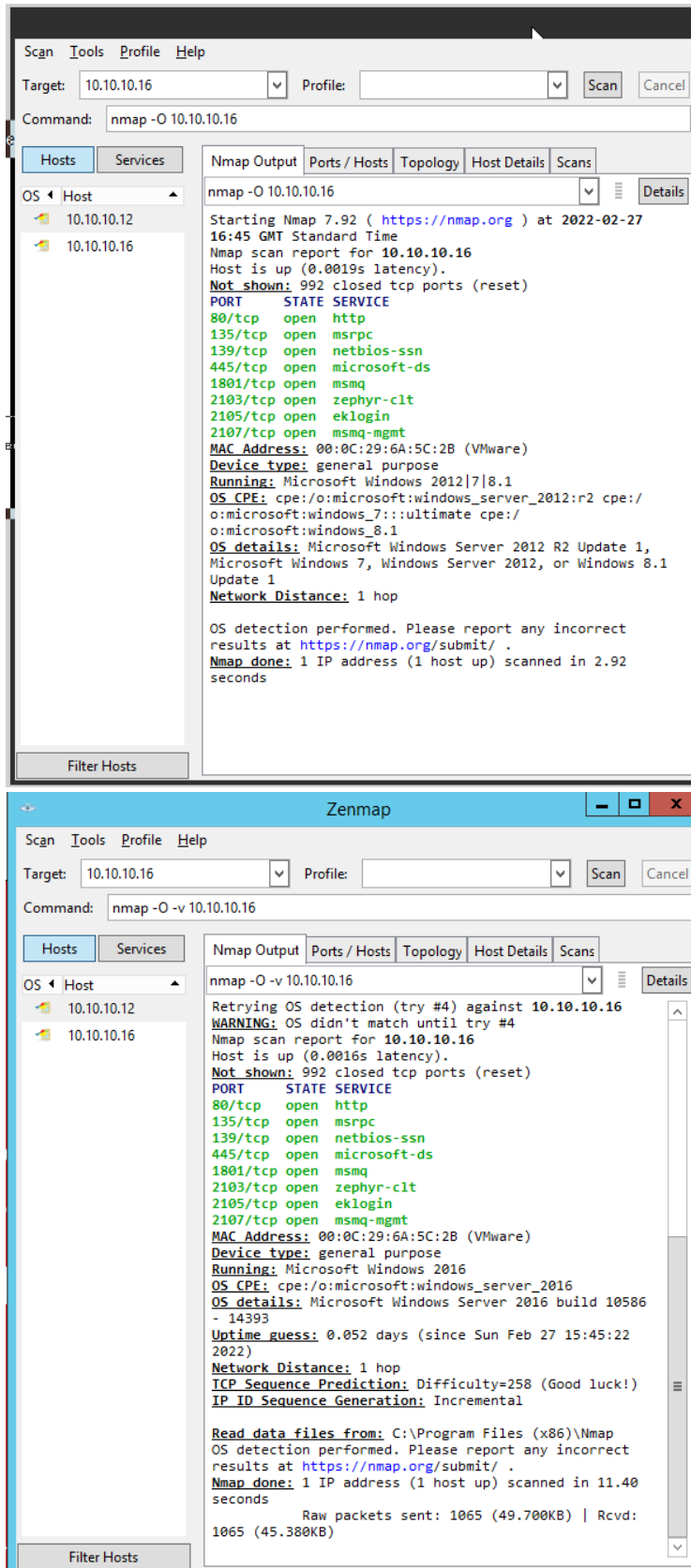
Task

1. Open Nmap in Kali Linux
2. By default, you could see an Intense scan profile present. Do various scans on the target OS. Refer to our lecture sessions to use various nmap commands.
3. Based on the earlier activities, we have managed to find our Users, Host Names, Live Hosts, List of Machines in the Target Network etc. Now, let us focus on gathering ports open, their services and shared resources.
4. Issue the nmap command to find out the operating system. Which command would you use?

Nmap -O <Target> (Used to Fingerprint the OS of a host – Detect Operating System)

Nmap -O -v <Target> (Used to Fingerprint the OS of a host – Detect Operating System)

what is the difference between the above two commands?



- From the above output/ or from your output gathered in Kali Linux (Attacker), what is your finding? Did you notice Ports 80, 135, 139, 445, 1801 etc are open and 139 is using netbios service?

6. Let us use NBTSTAT:

- What is NBTSTAT?
- Which OS does NBTSTAT work?
- How do you find similar information using only Kali Linux?

NBTSTAT command to look at NETBIOS related information. NBTSTAT is a diagnostic tool for NetBIOS over TCP/IP. It's primary objective is to troubleshoot NetBIOS name resolution problems. (Wikipedia)

```
C:\Users\Administrator>nbtstat -A 10.10.10.16
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
SERVER2016	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2016	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6A-5C-2B
```

```
C:\Users\Administrator>nbtstat -A 10.10.10.12
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
SERVER2012	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2012	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6C-7C-49
```

7. Now use net use command to view the created shared folders from your hosts.

```
C:\Users\Administrator>net use
New connections will be remembered.
```

Status	Local	Remote	Network
	Z:	\\vmware-host\Shared Folders	UMware Shared Folders

The command completed successfully.

8. Do research on net use. Know what is the purpose of net use command? Which OS versions is that supported etc.?

This Page is
intentionally left blank

3. Enumerate Services

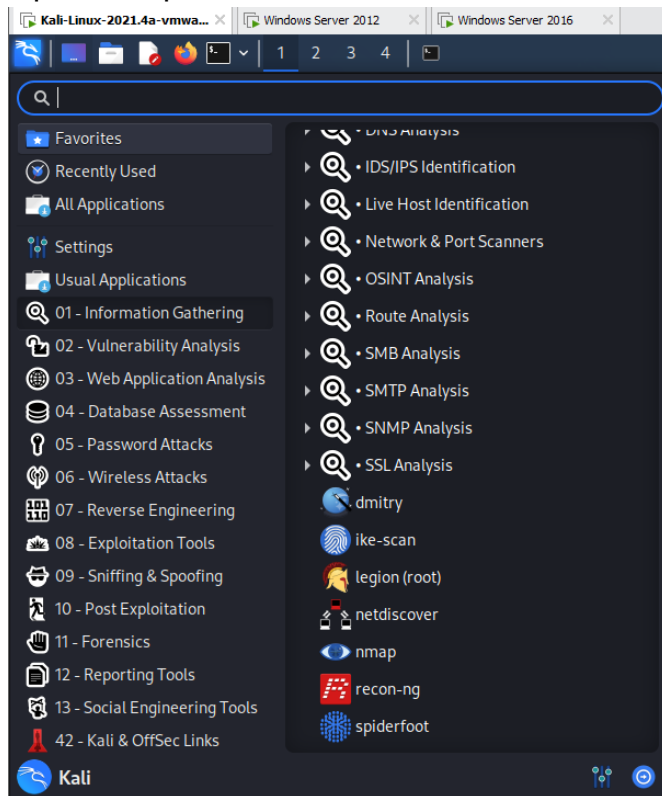
- + Machine: Windows Servers 2022, Windows Client, Linux.

Scan all the machines in the target network, list out the up and running machines, find open ports, find the status of firewall and enumerate the services running on the port along with their versions.

Note: You must target the victim machines here. Windows Servers and Clients are the Victim Machines and you attack using your Kali. IP Addresses ranges mentioned in this lab are based on my (Instructors) lab setup. It might not be the same for you. Make necessary amendments suitable to your network setup.

Task

1. Open Nmap in Kali Linux



2. Execute the commands (not limited to)

- a. **nmap -sP 10.0.0.0/24**

```
(kali㉿kali)-[~]
$ nmap -sP 10.10.10.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:23 EST
Nmap scan report for 10.10.10.2
Host is up (0.00093s latency).
Nmap scan report for 10.10.10.11
Host is up (0.0020s latency).
Nmap scan report for 10.10.10.12
Host is up (0.0039s latency).
Nmap scan report for 10.10.10.16
Host is up (0.0019s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.53 seconds
```

This lab activity has a number of nmap commands. Could you list out all the descriptions of these commands?

For example, the 1st command used here is **nmap -sP 10.10.10.0/24**

What is the purpose of all the commands listed in this part?

b. Nmap -sS 10.10.10.12

```

# nmap -sS 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:29 EST
Nmap scan report for 10.10.10.12
Host is up (0.00049s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa
1030/tcp   open  iad1
1031/tcp   open  iad2
1032/tcp   open  iad3
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt

```

c. nmap -ssV -O 10.10.10.12

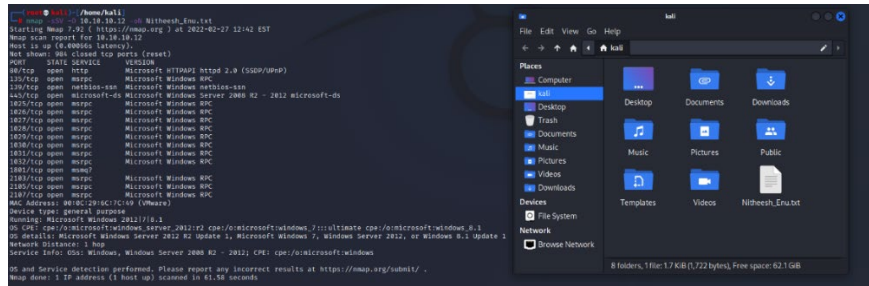
```

(root@kali) - [/home/kali]
# nmap -ssV -O 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:36 EST
Nmap scan report for 10.10.10.12
Host is up (0.00047s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
1025/tcp   open  msrpc        Microsoft Windows RPC
1026/tcp   open  msrpc        Microsoft Windows RPC
1027/tcp   open  msrpc        Microsoft Windows RPC
1028/tcp   open  msrpc        Microsoft Windows RPC
1029/tcp   open  msrpc        Microsoft Windows RPC
1030/tcp   open  msrpc        Microsoft Windows RPC
1031/tcp   open  msrpc        Microsoft Windows RPC
1032/tcp   open  msrpc        Microsoft Windows RPC
1801/tcp   open  msmq?
2103/tcp   open  msrpc        Microsoft Windows RPC
2105/tcp   open  msrpc        Microsoft Windows RPC
2107/tcp   open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:6C:7C:49 (VMware)
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:::
ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, W
indows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

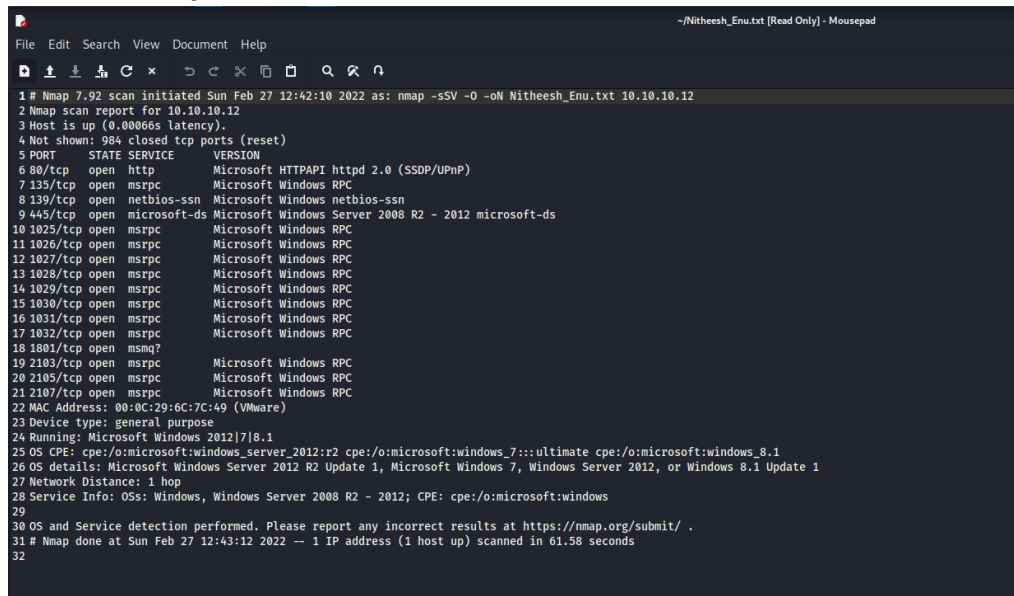
OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.12 seconds

```

d. Save this report to a txt file with your name. What command do you use to save?



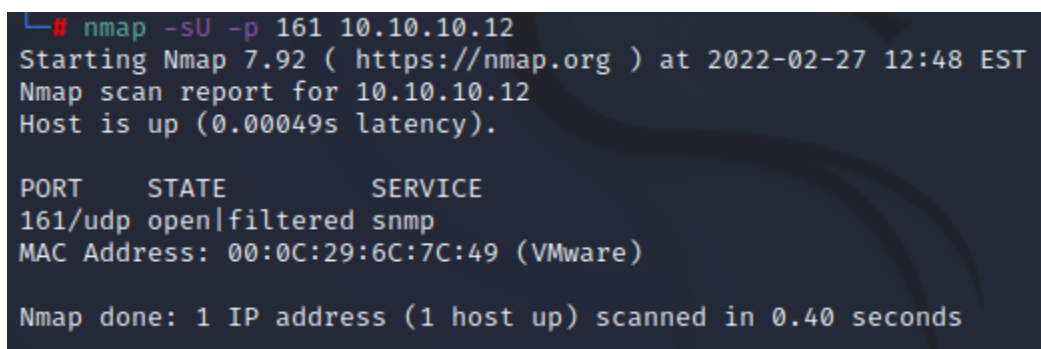
3. Save the Report



4. Now, let us focus on SNMP.

Which is the default port for SNMP?

a. Check the port status.



- b. From the above output, knowing that SNMP Service is running in port 161 and the status is open, execute a script to extract the SNMP Community string from the target machine.

```
(root@kali)~[/home/kali]
# nmap -sU -p 161 --script=snmp-brute 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 13:24 EST
Nmap scan report for 10.10.10.12
Host is up (0.00056s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-brute:
|_ public - Valid credentials
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

100

```
(root@kali)-[/hone/kali]
└─$ msfconsole
```

Know about MSF console. Do not use Linux. Refer to Metasploit.com.

a. Use auxiliary/scanner/snmp/snmp_login. Setg RHOSTS <target>. Exploit.

```
msf6 > use auxiliary/scanner/snmp/snmp_login
msf6 auxiliary(scanner/snmp/snmp_login) > setg RHOSTS 10.10.10.12
RHOSTS => 10.10.10.12
msf6 auxiliary(scanner/snmp/snmp_login) > exploit

[!] No active DB -- Credential data will not be saved!
[+] 10.10.10.12:161 - Login Successful: public (Access level: read-only); Proof (sysDescr.0): Hardware: Intel64
Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Did you notice that the target has a read-only community string? This is the vulnerability via SNMP which could be used to exploit the target. *(If you don't understand SNMP Community String – refer to our lectures and do research)*

b. Use Enumeration to exploit further.

```
msf6 auxiliary(scanner/snmp/snmp_login) > use auxiliary/scanner/snmp/snmp_enum
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit

[+] 10.10.10.12, Connected.

[*] System information:

Host IP           : 10.10.10.12
Hostname          : Server2012.accb.com
Description       : Hardware: Intel64 Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Wi
ndows Version 6.3 (Build 9600 Multiprocessor Free)
Contact          : -
Location         : -
Uptime snmp      : 00:23:23.07
Uptime system    : 00:22:46.53
System date      : 2022-2-27 18:33:18.3

[*] User accounts:

["Guest"]
["krbtgt"]
["Administrator"]

[*] Network information:

IP forwarding enabled : no
Default TTL           : 128
TCP segments received : 9320
TCP segments sent     : 9312
TCP segments retrans  : 8
Input datagrams       : 405
```

After enumerating the target on SNMP, what information did you gather?

In similar method, could you try to enumerate LDAP on an ADDS and modify domain user accounts?

4. Reflect on the above activities

+ Machine: Your virtual Lab Network

- Understanding on all the activities
- Understanding about various tools used
- New/ Similar tools you identified and used
- Compare and Contrast the tutorial tools with your identified tools
- Rate yourself: How confident are you to do footprinting and reconnaissance activity ethically?
- Any other Troubleshooting Steps, you need to share?

Part 1:

- ✓ Using command line to
 - establish the hops between the target
 - establish domain records from Authoritative Server
- ✓ Using tools to
 - extract web pages if available
 - Identify the process running in the target
 - Identify the hosts running in the target network

Part 2:

- ✓ Using commands, scanning tools and Packet Capture Tools to scan the network to
 - Identify the Open Ports and Services
 - Identify the target Operating Systems
 - Identify potential vulnerabilities within the target Network
 - Map the entire network
 - Generate automated reports from various tools used to document as evidence

Part 3:

- ✓ Using tools and Packet Captures to enumerate the network to
 - Gather concrete information
 - Generate automated reports from various tools used to document as evidence

End of Activity 2 *****

This Page is
intentionally left blank