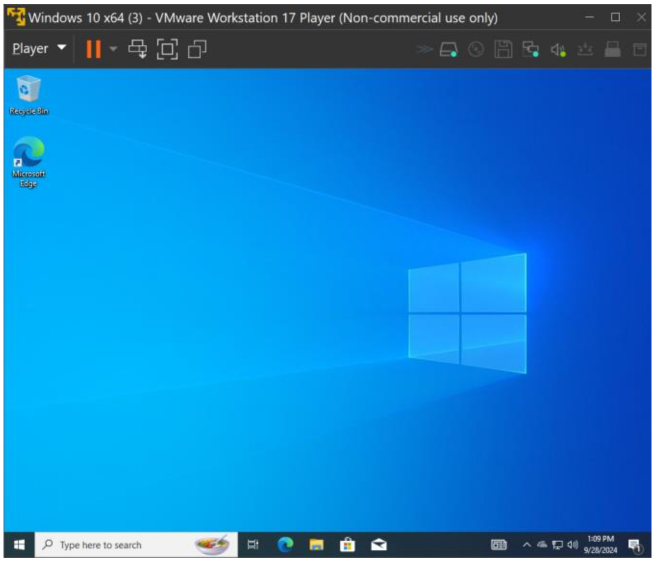
Lab 1: Using Zenmap to Perform Basic Reconnaissance, Performing a Vulnerability Assessment (100 Points)

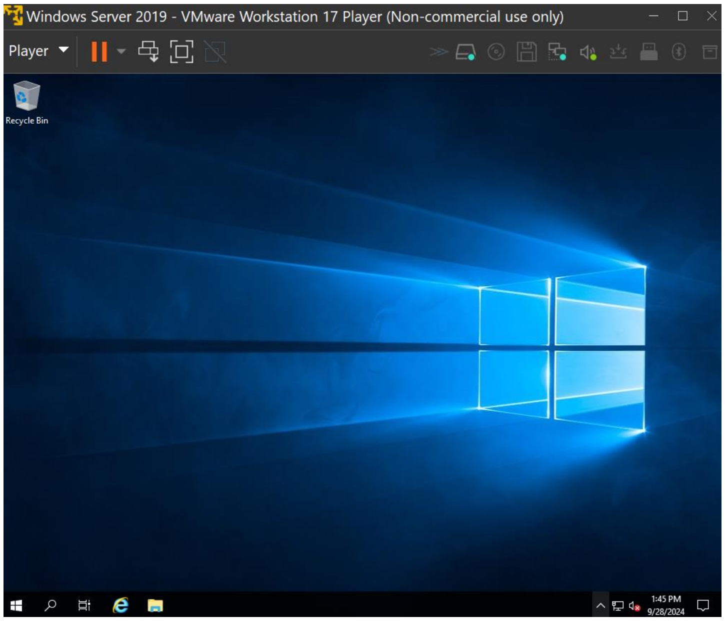
(IMP NOTE: This Assignment will be graded on Tasks Performed by Student (installation of Various Virtual OS, Installing configuringapplications) Take Screenshots whenever complete the task or even you are getting error or any other issues. It is highly recommended to complete tasks. If for some reason Student is not able to complete the complete the tasks partial grades will be awarded.)

Deliverables (Screenshots of Completed Tasks)

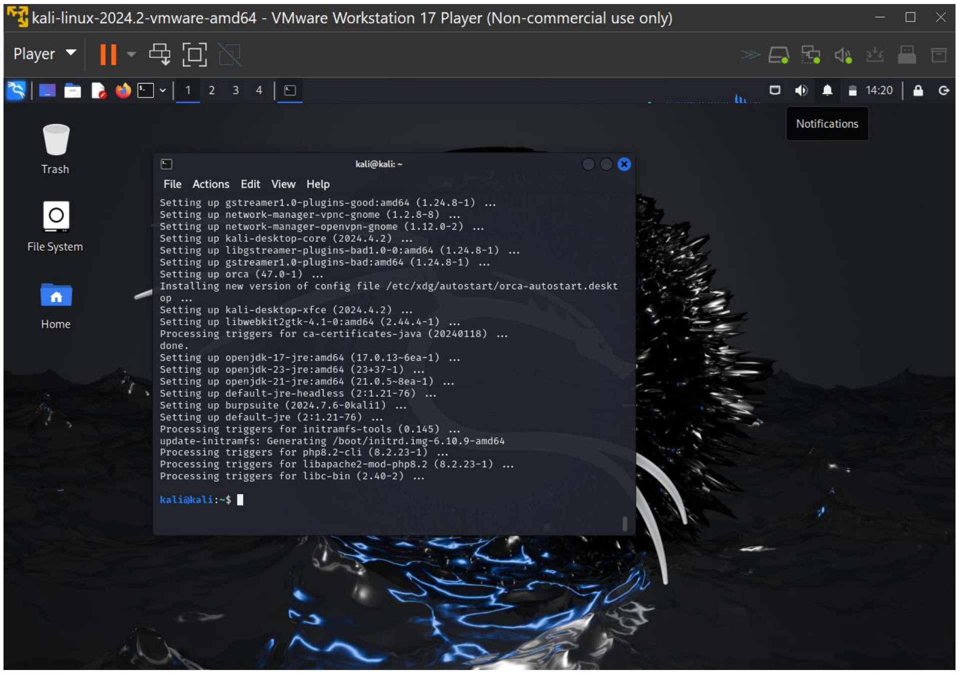
Task 1. Install and Configure Windows 10/11 Virtual Machine. (5 Points)


Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Microsoft Edge
Type here to search
1:09 PM
9/28/2024

Task 2. Install and Configure Windows Server 2016/2019/2022 Virtual Machine. (5 Points)


Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
1:45 PM
9/28/2024

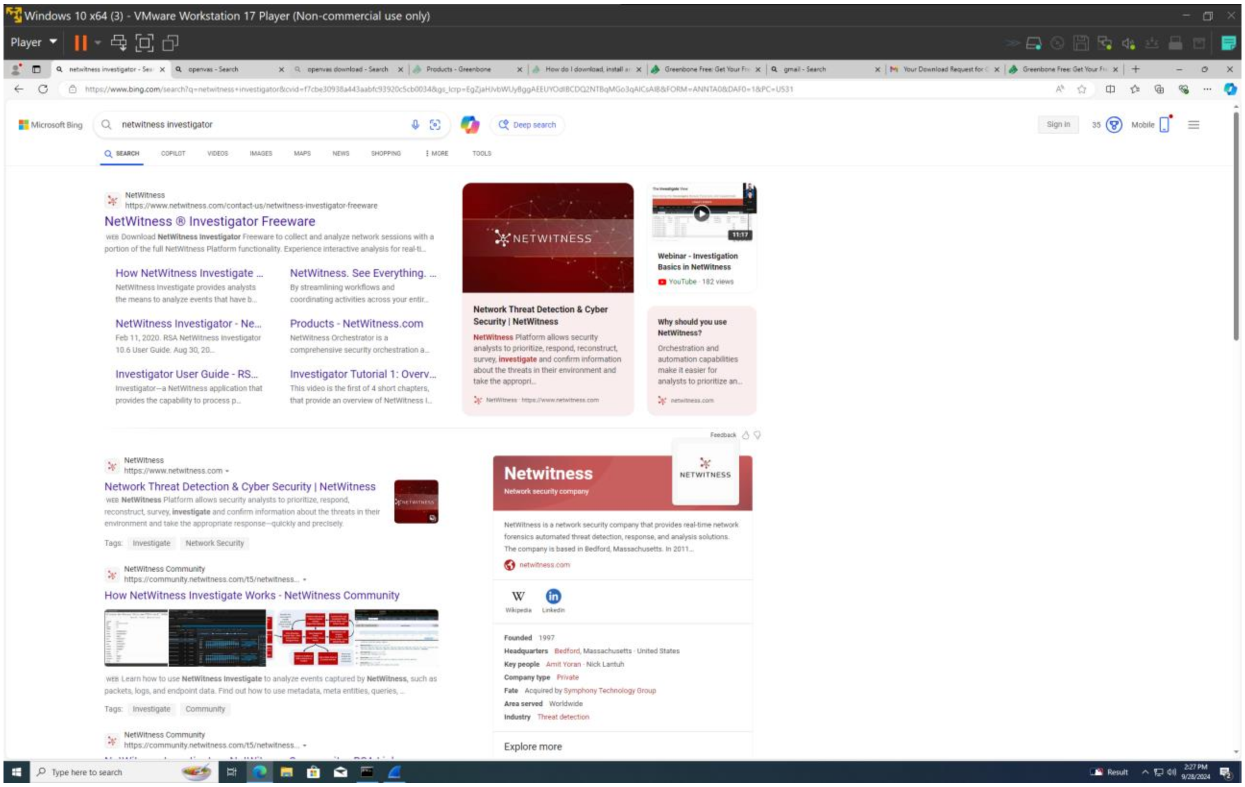
Task 3. Install and Configure Kali Linux Virtual Machine (5 Points)


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
14:20
Notifications
Trash
File System
Home
kali@kali: ~
File
Actions
Edit
View
Help

```
Setting up gstreamer1.0-plugins-good:amd64 (1.24.8-1) ...
Setting up network-manager-vpnc-gnome (1.2.8-8) ...
Setting up network-manager-openvpn-gnome (1.12.0-2) ...
Setting up kali-desktop-core (2024.4.2) ...
Setting up libgstreamer-plugins-bad1.0-0:amd64 (1.24.8-1) ...
Setting up gstreamer1.0-plugins-bad:amd64 (1.24.8-1) ...
Setting up orca (47.0-1) ...
Installing new version of config file /etc/xdg/autostart/orca-autostart.deskt
op ...
Setting up kali-desktop-xfce (2024.4.2) ...
Setting up libwebkit2gtk-4.1-0:amd64 (2.44.4-1) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
Setting up openjdk-17-jre:amd64 (17.0.13~6ea-1) ...
Setting up openjdk-23-jre:amd64 (23+37-1) ...
Setting up openjdk-21-jre:amd64 (21.0.5~8ea-1) ...
Setting up default-jre-headless (2:1.21-76) ...
Setting up burpsuite (2024.7.6-0kali1) ...
Setting up default-jre (2:1.21-76) ...
Processing triggers for initramfs-tools (0.145) ...
update-initramfs: Generating /boot/initrd.img-6.10.9-amd64
Processing triggers for php8.2-cli (8.2.23-1) ...
Processing triggers for libapache2-mod-php8.2 (8.2.23-1) ...
Processing triggers for libc-bin (2.40-2) ...

kali@kali:~$ 
```

Task 4. Tools and Software The following software and/or utilities are required to complete this lab.

- **FileZilla, NetWitness Investigator, OpenVAS, PuTTY, Tftpd64, Wireshark, Zenmap**


Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
netwitness investigator - Sea
openvas - Search
openvas download - Search
Products - Greenbone
How do I download, install a
Greenbone Free: Get Your Fr
gmail - Search
Your Download Request for
Greenbone Free: Get Your Fr
https://www.bing.com/search?q=netwitness+investigator&cvid=f7cbe30938a443aabfc93920c5cb0034&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDQ2NTBqMGo3qAICsAIB&FORM=ANNTA0&DAF0=1&PC=U531
Microsoft Bing
netwitness investigator
Deep search
Sign in
35
Mobile
SEARCH
COPILOT
VIDEOS
IMAGES
MAPS
NEWS
SHOPPING
MORE
TOOLS
NETWITNESS
11:17
Feedback
Type here to search
Result
2:27 PM
9/28/2024

NetWitness
https://www.netwitness.com/contact-us/netwitness-investigator-freeware

NetWitness ® Investigator Freeware

WEB Download **NetWitness Investigator** Freeware to collect and analyze network sessions with a portion of the full NetWitness Platform functionality. Experience interactive analysis for real-ti...

How NetWitness Investigate ...
NetWitness Investigate provides analysts the means to analyze events that have b...

NetWitness. See Everything. ...
By streamlining workflows and coordinating activities across your entir...

NetWitness Investigator - Ne...
Feb 11, 2020. RSA NetWitness Investigator 10.6 User Guide. Aug 30, 20...

Products - NetWitness.com
NetWitness Orchestrator is a comprehensive security orchestration a...

Investigator User Guide - RS...
Investigator—a NetWitness application that provides the capability to process p...

Investigator Tutorial 1: Overv...
This video is the first of 4 short chapters, that provide an overview of NetWitness I...

Network Threat Detection & Cyber Security | NetWitness
NetWitness Platform allows security analysts to prioritize, respond, reconstruct, survey, investigate and confirm information about the threats in their environment and take the appropri...
NetWitness · https://www.netwitness.com

Webinar - Investigation Basics in NetWitness
YouTube · 182 views

Why should you use NetWitness?
Orchestration and automation capabilities make it easier for analysts to prioritize an...
netwitness.com

NetWitness
https://www.netwitness.com

Network Threat Detection & Cyber Security | NetWitness

WEB **NetWitness** Platform allows security analysts to prioritize, respond, reconstruct, survey, **investigate** and confirm information about the threats in their environment and take the appropriate response—quickly and precisely.

Tags: Investigate Network Security

NetWitness Community
https://community.netwitness.com/t5/netwitness...

How NetWitness Investigate Works - NetWitness Community

WEB Learn how to use **NetWitness Investigate** to analyze events captured by **NetWitness**, such as packets, logs, and endpoint data. Find out how to use metadata, meta entities, queries, ...

Tags: Investigate Community

NetWitness Community
https://community.netwitness.com/t5/netwitness...

Netwitness
Network security company

NetWitness is a network security company that provides real-time network forensics automated threat detection, response, and analysis solutions. The company is based in Bedford, Massachusetts. In 2011...
netwitness.com

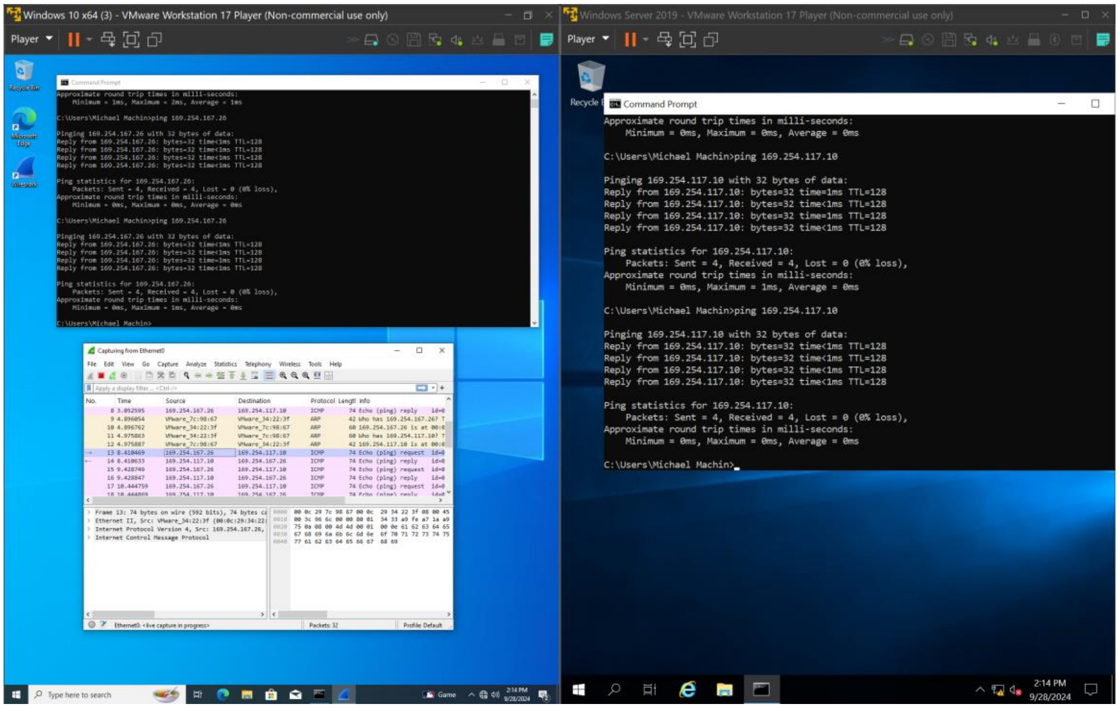
Wikipedia
LinkedIn

Founded 1997
Headquarters Bedford, Massachusetts · United States
Key people Amit Yoran · Nick Lantuh
Company type Private
Fate Acquired by Symphony Technology Group
Area served Worldwide
Industry Threat detection

Explore more

Task 5. (10 Points)

1. Make a screen capture showing the Wireshark traffic that you captured and paste it into your Lab Report file.



Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
Command Prompt

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Michael Machin>ping 169.254.167.26

Pinging 169.254.167.26 with 32 bytes of data:
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.167.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Machin>ping 169.254.167.26

Pinging 169.254.167.26 with 32 bytes of data:
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128
Reply from 169.254.167.26: bytes=32 time=1ms TTL=128
Reply from 169.254.167.26: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.167.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Michael Machin>
```

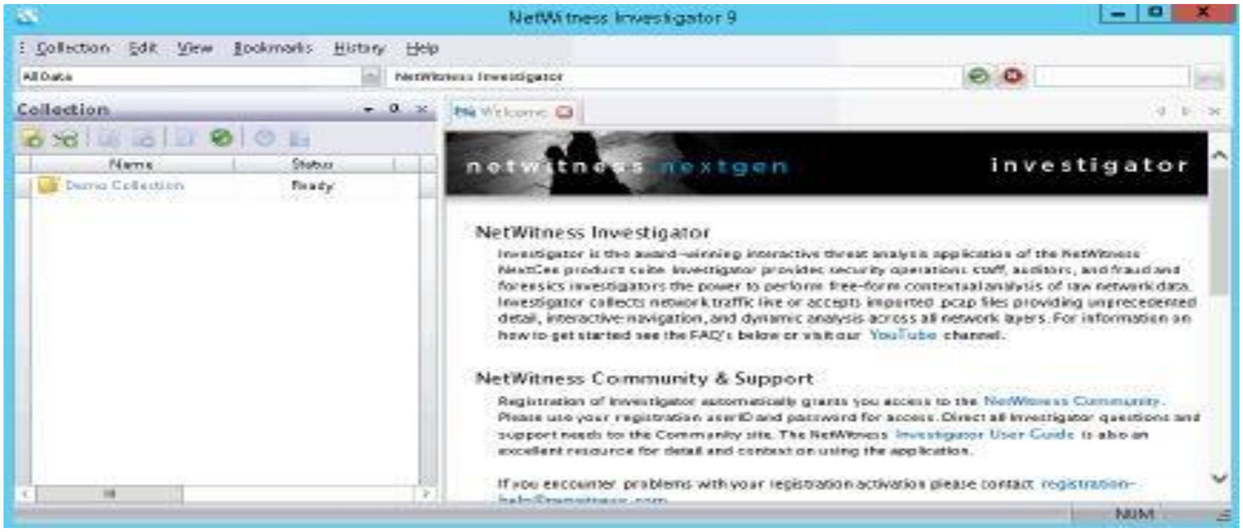
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time         Source             Destination        Protocol Length Info
    8 3.052595     169.254.167.26     169.254.117.10     ICMP       74 Echo (ping) reply    id=0
    9 4.896054     VMware_7c:98:67    VMware_34:22:3f    ARP        42 Who has 169.254.167.26? T
   10 4.896762     VMware_34:22:3f    VMware_7c:98:67    ARP        60 169.254.167.26 is at 00:0
   11 4.975863     VMware_34:22:3f    VMware_7c:98:67    ARP        60 Who has 169.254.117.10? T
   12 4.975887     VMware_7c:98:67    VMware_34:22:3f    ARP        42 169.254.117.10 is at 00:0
   13 8.410469     169.254.167.26     169.254.117.10     ICMP       74 Echo (ping) request  id=0
   14 8.410633     169.254.117.10     169.254.167.26     ICMP       74 Echo (ping) reply    id=0
   15 9.428740     169.254.167.26     169.254.117.10     ICMP       74 Echo (ping) request  id=0
   16 9.428847     169.254.117.10     169.254.167.26     ICMP       74 Echo (ping) reply    id=0
   17 10.444759    169.254.167.26     169.254.117.10     ICMP       74 Echo (ping) request  id=0
   18 10.444869    169.254.117.10     169.254.167.26     ICMP       74 Echo (ping) reply    id=0

> Frame 13: 74 bytes on wire (592 bits), 74 bytes ca
> Ethernet II, Src: VMware_34:22:3f (00:0c:29:34:22:
> Internet Protocol Version 4, Src: 169.254.167.26,
> Internet Control Message Protocol

0000  00 0c 29 7c 98 67 00 0c  29 34 22 3f 08 00 45
0010  00 3c 96 6c 00 00 80 01  34 33 a9 fe a7 1a a9
0020  75 0a 08 00 4d 4d 00 01  00 0e 61 62 63 64 65
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75
0040  77 61 62 63 64 65 66 67  68 69

Ethernet0: <live capture in progress>    Packets: 32    Profile: Default
```

Type here to search
Game
2:14 PM
9/28/2024
Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Command Prompt

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Machin>ping 169.254.117.10

Pinging 169.254.117.10 with 32 bytes of data:
Reply from 169.254.117.10: bytes=32 time=1ms TTL=128
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128
Reply from 169.254.117.10: bytes=32 time=1ms TTL=128
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.117.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Michael Machin>ping 169.254.117.10

Pinging 169.254.117.10 with 32 bytes of data:
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128
Reply from 169.254.117.10: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.117.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Machin>_
```

2. NetWitness Investigator allows analysts to view and analyze packets collected by applications like Wireshark. While Wireshark offers a deep-dive into individual packets, NetWitness offers a high-level view that can be stored and compared with newer packet captures to help identify any new threats or problems.



NetWitness Investigator

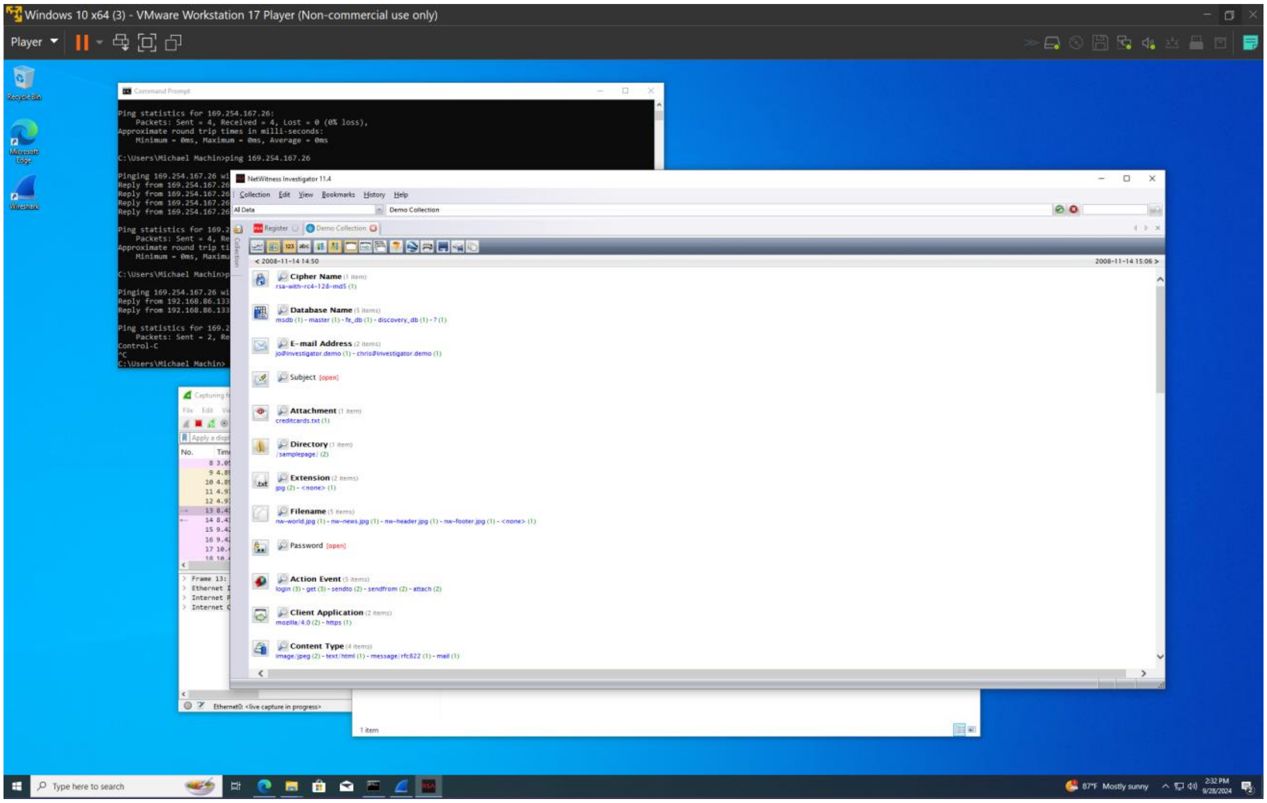
Investigator is the award-winning interactive threat analysis application of the NetWitness NextGen product suite. Investigator provides security operations staff, auditors, and fraud and forensics investigators the power to perform free-form contextual analysis of raw network data. Investigator collects network traffic live or accepts imported .pcap files providing unprecedented detail, interactive navigation, and dynamic analysis across all network layers. For information on how to get started see the FAQ's below or visit our YouTube channel.

NetWitness Community & Support

Registration of Investigator automatically grants you access to the NetWitness Community. Please use your registration userID and password for access. Direct all Investigator questions and support needs to the Community site. The NetWitness Investigator User Guide is also an excellent resource for detail and context on using the application.

If you encounter problems with your registration activation please contact registration-help@netwitness.com

1. Double-click the Demo Collection to see how NetWitness Investigator collects and presents traffic types and security events.



```
Ping statistics for 169.254.167.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Machin>ping 169.254.167.26

Pinging 169.254.167.26 wi
Reply from 169.254.167.26
Reply from 169.254.167.26
Reply from 169.254.167.26
Reply from 169.254.167.26

Ping statistics for 169.2
    Packets: Sent = 4, Re
Approximate round trip ti
    Minimum = 0ms, Maximu

C:\Users\Michael Machin>p

Pinging 169.254.167.26 wi
Reply from 192.168.86.133
Reply from 192.168.86.133

Ping statistics for 169.2
    Packets: Sent = 2, Re
Control-C
^C
C:\Users\Michael Machin>
```

NetWitness Investigator 11.4

All Data | Demo Collection

< 2008-11-14 14:50 | 2008-11-14 15:06 >

Cipher Name (1 item)
rsa-with-rc4-128-md5 (1)

Database Name (5 items)
msdb (1) - master (1) - fe_db (1) - discovery_db (1) - ? (1)

E-mail Address (2 items)
jo@investigator.demo (1) - chris@investigator.demo (1)

Subject [open]

Attachment (1 item)
creditcards.txt (1)

Directory (1 item)
/samplepage/ (2)

Extension (2 items)
jpg (2) - <none> (1)

Filename (5 items)
nw-world.jpg (1) - nw-news.jpg (1) - nw-header.jpg (1) - nw-footer.jpg (1) - <none> (1)

Password [open]

Action Event (5 items)
login (3) - get (3) - sendto (2) - sendfrom (2) - attach (2)

Client Application (2 items)
mozilla/4.0 (2) - https (1)

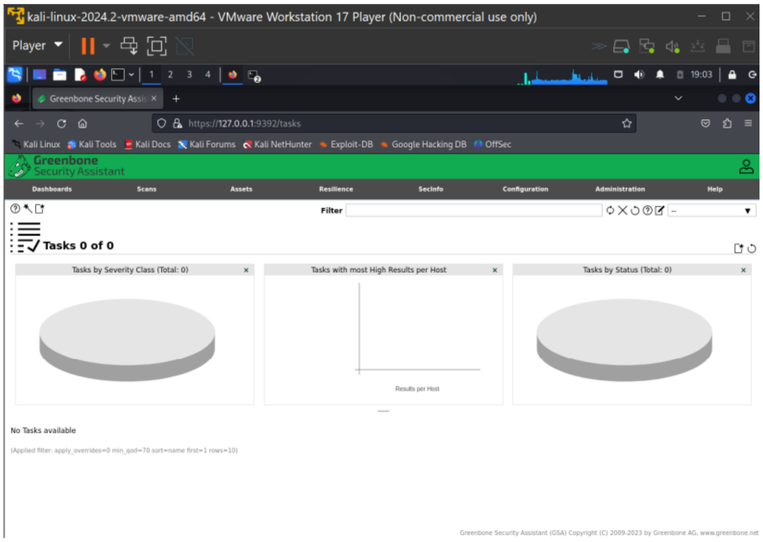
Content Type (4 items)
image/jpeg (2) - text/html (1) - message/rfc822 (1) - mail (1)

Ethernet0: <live capture in progress>

1 item

Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
Command Prompt
Collection Edit View Bookmarks History Help
Register
Demo Collection
Type here to search
87°F Mostly sunny
2:32 PM
9/28/2024

9. Double-click the OpenVAS icon on the vWorkstation desktop to open the application.



Tasks 0 of 0

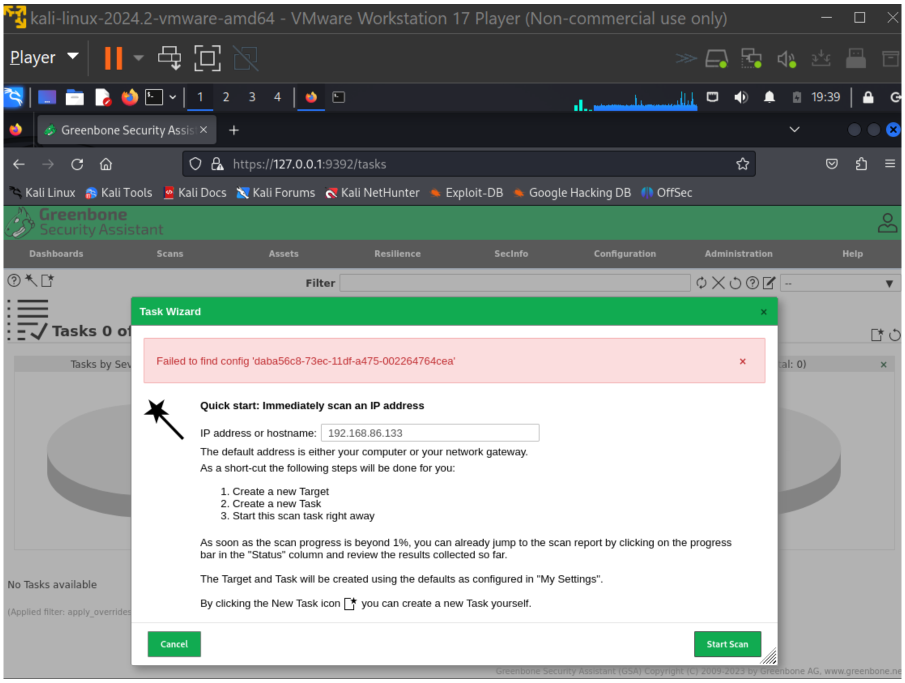
No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:03
Greenbone Security Assis
https://127.0.0.1:9392/tasks
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Tasks by Status (Total: 0)
Results per Host
Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Note: OpenVAS performs remote scans and audits of Unix, Windows, and network infrastructures and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices. It will take five minutes before OpenVAS is ready to use.

10. In the IP address or hostname box at the right of the window, type ***IP address*** of windows machine and click Start Scan to run a basic security scan.


Task Wizard

Failed to find config 'daba56c8-73ec-11df-a475-002264764cea'

Quick start: Immediately scan an IP address

IP address or hostname: 192.168.86.133

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

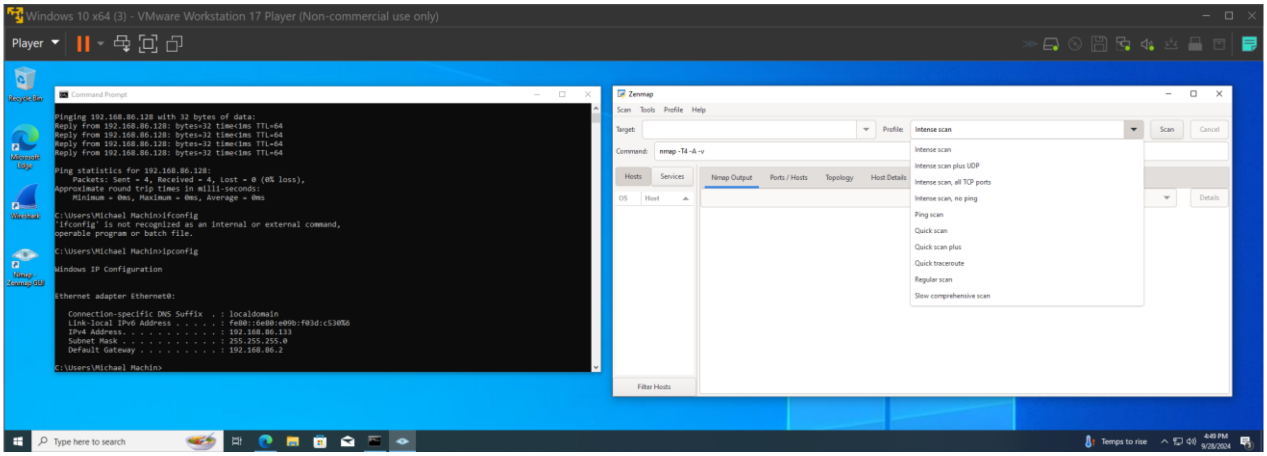
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Greenbone Security Assistant
https://127.0.0.1:9392/tasks
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Cancel
Start Scan

https://greenbone.github.io/docs/latest/22.4/source-build/troubleshooting.html#failed-to-find-scan-configuration

- **HERE IS THE REMEDIATION TO THE ERROR BUT IT DOESN'T FIX IT ON MY MACHINE**

Task 6: Using Zenmap to Perform Basic Reconnaissance

1. Double-click the Nmap-Zenmap GUI icon on the vWorkstation desktop to open the application.

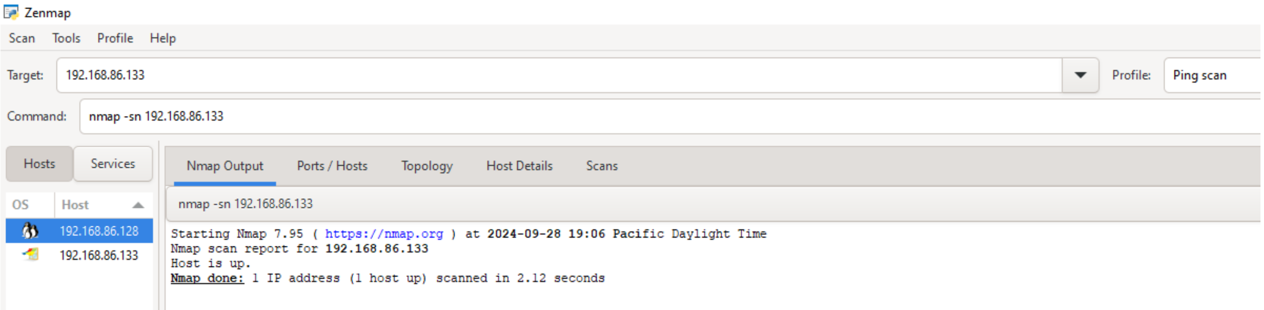

```
Pinging 192.168.86.128 with 32 bytes of data:
Reply from 192.168.86.128: bytes=32 time<1ms TTL=64
Reply from 192.168.86.128: bytes=32 time<1ms TTL=64
Reply from 192.168.86.128: bytes=32 time<1ms TTL=64
Reply from 192.168.86.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.86.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Michael Machin>ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Michael Machin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::6e80:e09b:f03d:c530%6
   IPv4 Address. . . . . . . . . . . : 192.168.86.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.86.2

C:\Users\Michael Machin>
```

Profile: Intense scan

Command: nmap -T4 -A -v

2. From the Target drop-down menu, select IP address of windows machine, the subnet address for this lab.

3. From the Profile drop-down menu, select Ping scan and click Scan. The Command box displays the syntax for the Nmap command. These commands also can be typed manually. The results of the scan will start filling the Nmap Output tab. This scan returns basic information about host availability and the MAC address. You will need this data to complete the deliverables for this lab. The scan is completed when the final line of the output reads Nmap done.



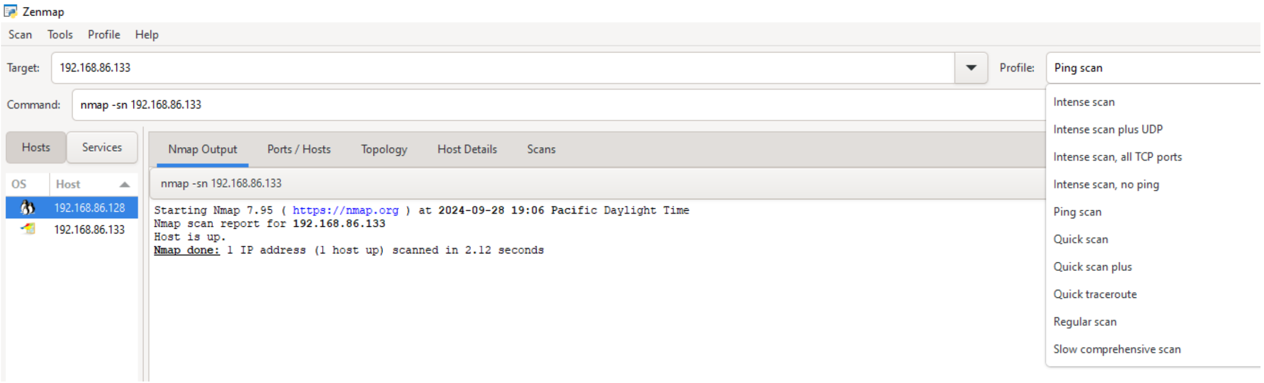
Target: 192.168.86.133

Profile: Ping scan

Command: nmap -sn 192.168.86.133

```
nmap -sn 192.168.86.133
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 19:06 Pacific Daylight Time
Nmap scan report for 192.168.86.133
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

4. **Expand** the **Profile drown-down menu** to see the complete list of scans that Zenmap can perform.



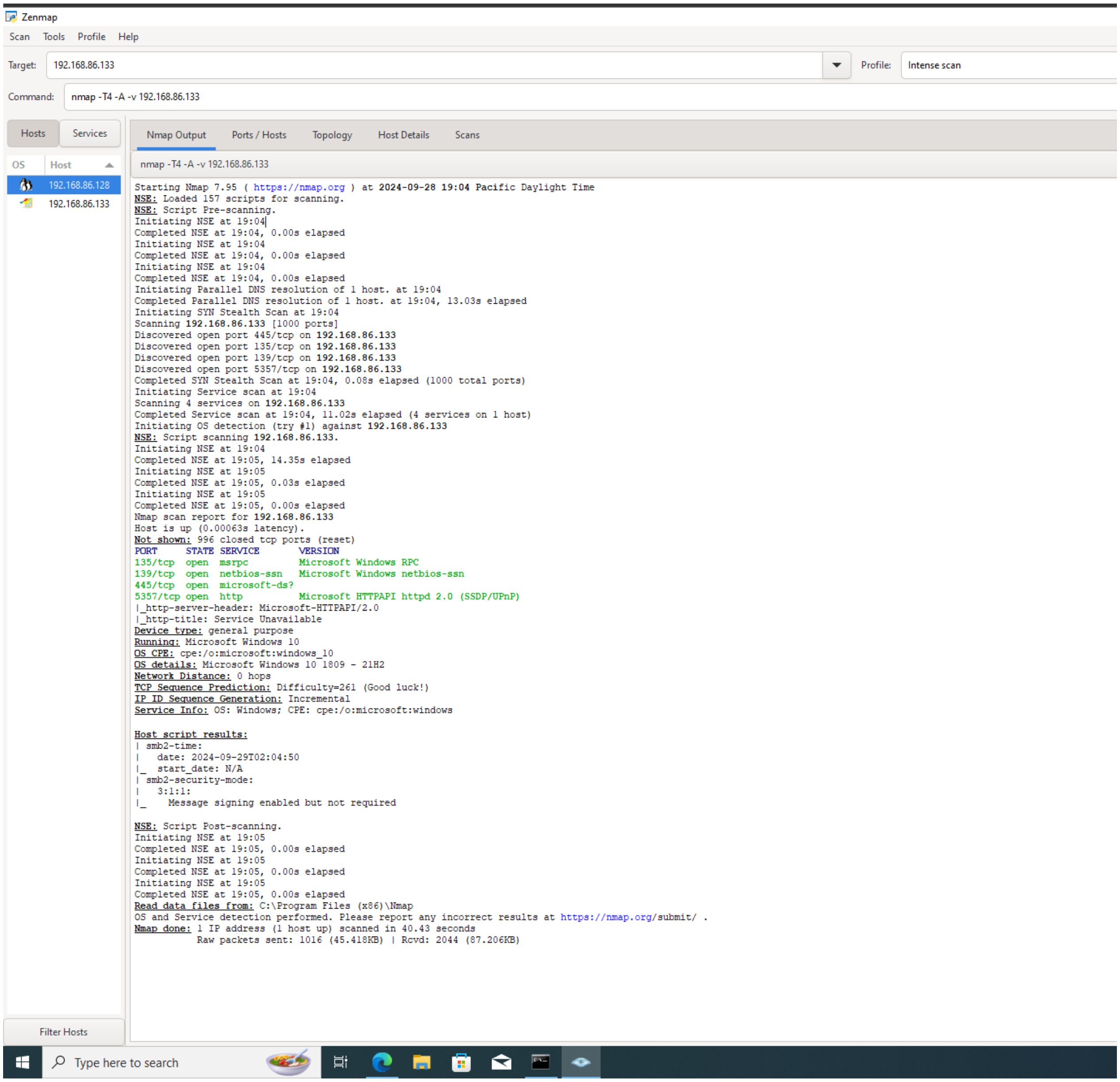
Target: 192.168.86.133

Profile: Ping scan

Command: nmap -sn 192.168.86.133

```
nmap -sn 192.168.86.133
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 19:06 Pacific Daylight Time
Nmap scan report for 192.168.86.133
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

5. To gather more detailed data, **select Intense Scan** from the Profile drop-down menu and **click Scan**.

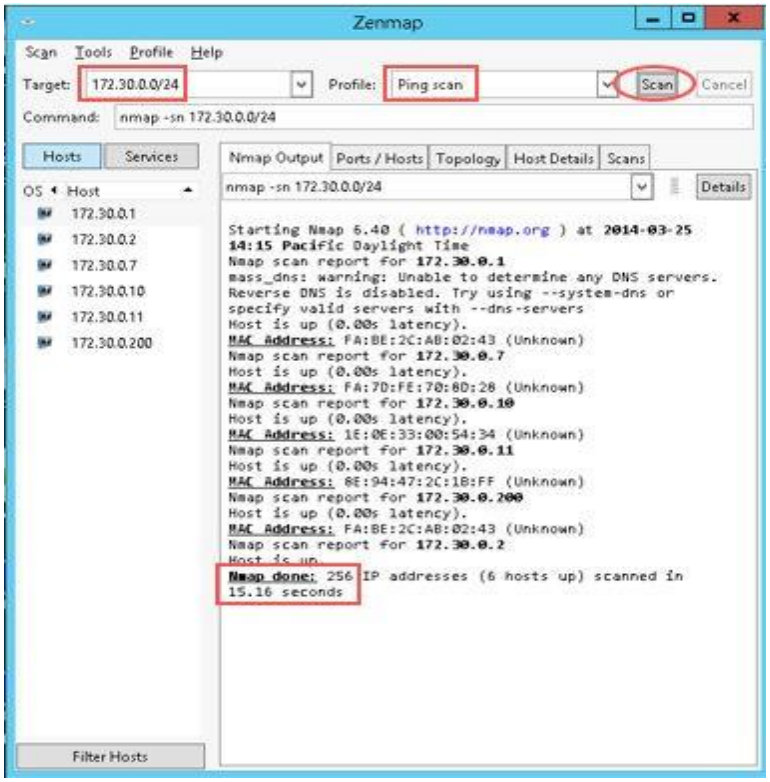


Target: 192.168.86.133

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.86.133

```
nmap -T4 -A -v 192.168.86.133

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 19:04 Pacific Daylight Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:04
Completed NSE at 19:04, 0.00s elapsed
Initiating NSE at 19:04
Completed NSE at 19:04, 0.00s elapsed
Initiating NSE at 19:04
Completed NSE at 19:04, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 19:04
Completed Parallel DNS resolution of 1 host. at 19:04, 13.03s elapsed
Initiating SYN Stealth Scan at 19:04
Scanning 192.168.86.133 [1000 ports]
Discovered open port 445/tcp on 192.168.86.133
Discovered open port 135/tcp on 192.168.86.133
Discovered open port 139/tcp on 192.168.86.133
Discovered open port 5357/tcp on 192.168.86.133
Completed SYN Stealth Scan at 19:04, 0.08s elapsed (1000 total ports)
Initiating Service scan at 19:04
Scanning 4 services on 192.168.86.133
Completed Service scan at 19:04, 11.02s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.86.133
NSE: Script scanning 192.168.86.133.
Initiating NSE at 19:04
Completed NSE at 19:05, 14.35s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.03s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Nmap scan report for 192.168.86.133
Host is up (0.00063s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-09-29T02:04:50
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.43 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2044 (87.206KB)
```



Target: 172.30.0.0/24

Profile: Ping scan

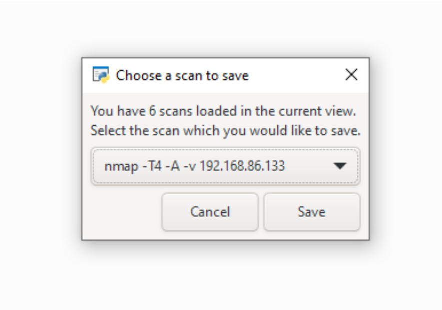
Scan

Command: nmap -sn 172.30.0.0/24

```
172.30.0.1
172.30.0.2
172.30.0.7
172.30.0.10
172.30.0.11
172.30.0.200
```

```
nmap -sn 172.30.0.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-25
14:15 Pacific Daylight Time
Nmap scan report for 172.30.0.1
mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Host is up (0.00s latency).
MAC Address: FA:BE:2C:AB:02:43 (Unknown)
Nmap scan report for 172.30.0.7
Host is up (0.00s latency).
MAC Address: FA:7D:FE:70:8D:28 (Unknown)
Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
MAC Address: 1E:0E:33:00:54:34 (Unknown)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
MAC Address: 8E:94:47:2C:1B:FF (Unknown)
Nmap scan report for 172.30.0.200
Host is up (0.00s latency).
MAC Address: FA:BE:2C:AB:02:43 (Unknown)
Nmap scan report for 172.30.0.2
Host is up
Nmap done: 256 IP addresses (6 hosts up) scanned in
15.16 seconds
```

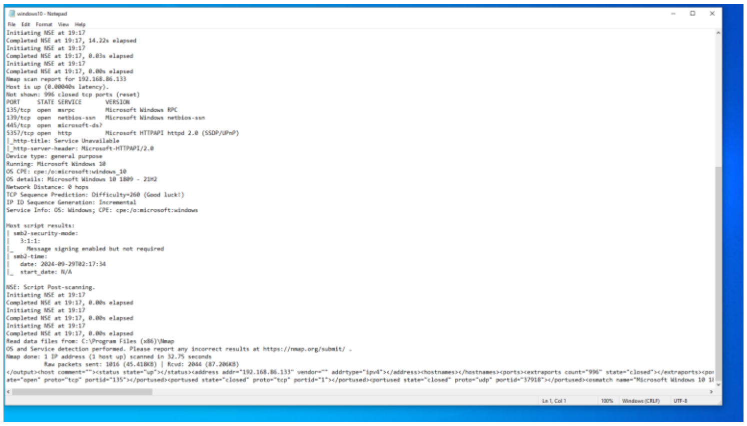
6. **Click Scan > Save Scan** on the Zenmap menu to save the scan results.



Choose a scan to save

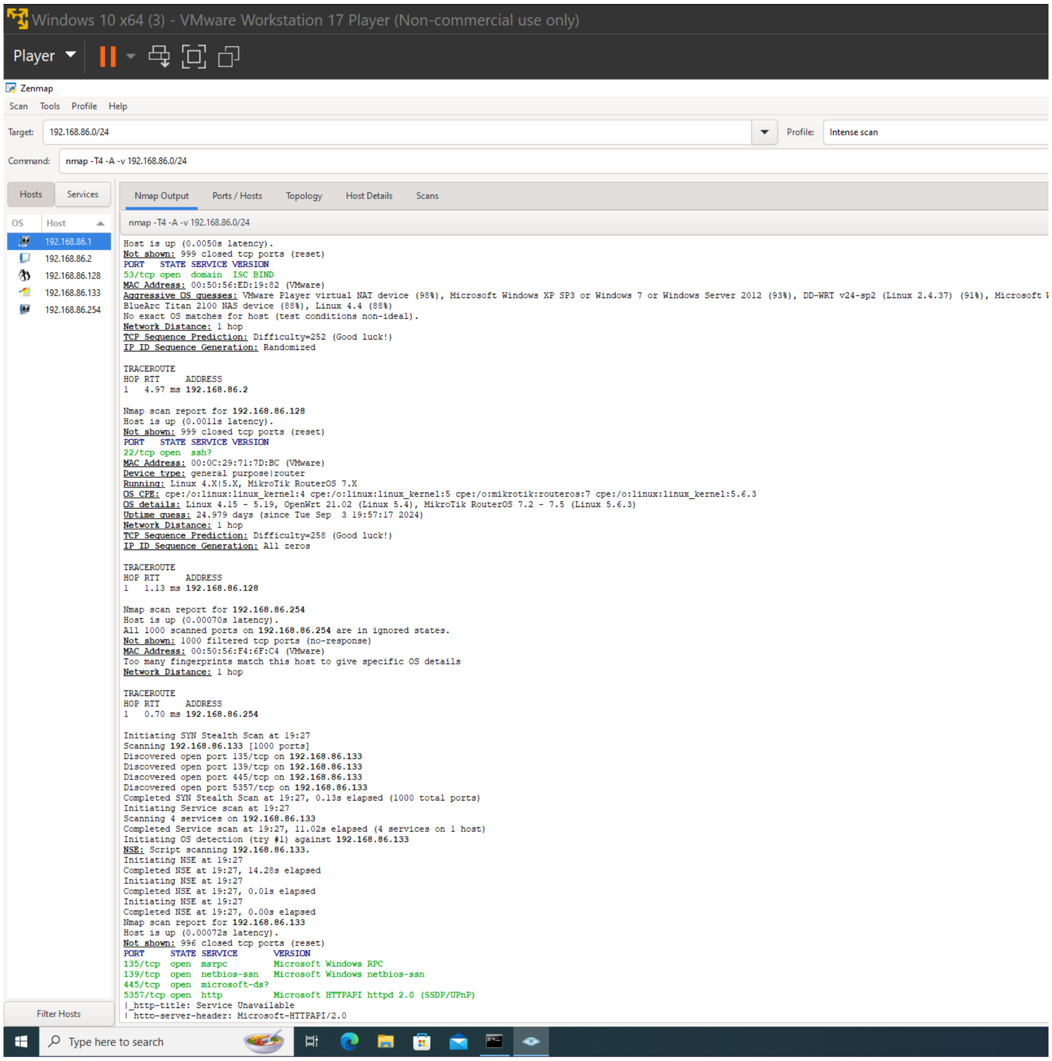
You have 6 scans loaded in the current view. Select the scan which you would like to save.

nmap -T4 -A -v 192.168.86.133



```
Initiating NSE at 19:17
Completed NSE at 19:17, 14.22s elapsed
Initiating NSE at 19:17
Completed NSE at 19:17, 0.03s elapsed
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Nmap scan report for 192.168.86.133
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-09-29T02:17:34
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.75 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2044 (87.206KB)
</output><host comment=""><status state="up"></status><address addr="192.168.86.133" vendor="" addrtype="ipv4"></address><hostnames></hostnames><ports><extraports count="996" state="closed"></extraports><por
ate="open" proto="tcp" portid="135"></portused><portused state="closed" proto="tcp" portid="1"></portused><portused state="closed" proto="udp" portid="37918"></portused><osmatch name="Microsoft Windows 10 18
```

7. In the Choose a scan to save dialog box, **select nmap –T4 –A –v 172.30.0.0/24 (Subnet of target machine)** (the command line for the intense scan) from the drop-down menu and **click Save**.



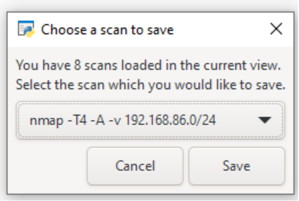
Target: 192.168.86.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.86.0/24

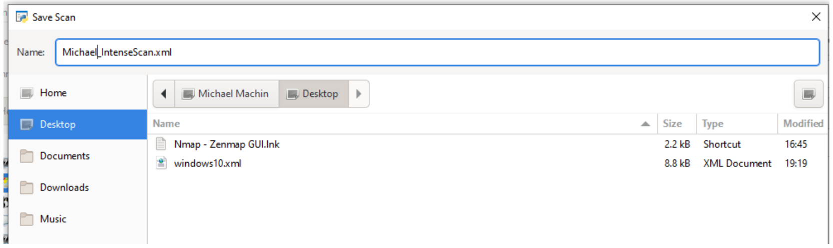
```
nmap -T4 -A -v 192.168.86.0/24

Host is up (0.0050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND
MAC Address: 00:50:56:ED:19:82 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft W
BlueArc Titan 2100 NAS device (88%), Linux 4.4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE
HOP RTT     ADDRESS
1   4.97 ms 192.168.86.2

Nmap scan report for 192.168.86.128
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh?
MAC Address: 00:0C:29:71:7D:BC (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 24.979 days (since Tue Sep  3 19:57:17 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.86.128

Nmap scan report for 192.168.86.254
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.86.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:6F:C4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.86.254

Initiating SYN Stealth Scan at 19:27
Scanning 192.168.86.133 [1000 ports]
Discovered open port 135/tcp on 192.168.86.133
Discovered open port 139/tcp on 192.168.86.133
Discovered open port 445/tcp on 192.168.86.133
Discovered open port 5357/tcp on 192.168.86.133
Completed SYN Stealth Scan at 19:27, 0.13s elapsed (1000 total ports)
Initiating Service scan at 19:27
Scanning 4 services on 192.168.86.133
Completed Service scan at 19:27, 11.02s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.86.133
NSE: Script scanning 192.168.86.133.
Initiating NSE at 19:27
Completed NSE at 19:27, 14.28s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.01s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
Nmap scan report for 192.168.86.133
Host is up (0.00072s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
```

8. In the Save Scan dialog box, navigate to the **Saving folder**. In the Name box, **highlight** the existing text (**.xml**), **type *yourname*_IntenseScan** in the Name box, replacing *yourname* with your own name, and **click Save**.



You have 8 scans loaded in the current view. Select the scan which you would like to save.

nmap -T4 -A -v 192.168.86.0/24

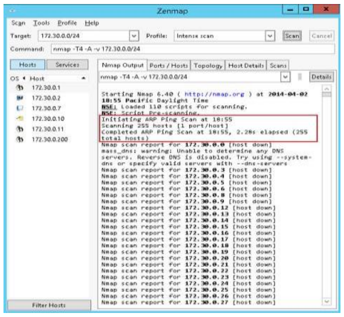


Name: Michael_IntenseScan.xml

Name	Size	Type	Modified
Nmap - Zenmap GUI.lnk	2.2 kB	Shortcut	16:45
windows10.xml	8.8 kB	XML Document	19:19

9. **Use the scrollbar** to review the results of the scan.

The Intense scan is actually a collection of several individual tests. The Nmap Output tab shows the raw output, including the name of each scan and its results (for example, the first scan in the report, the ARP Ping Scan, found 255 hosts on the subnet.) Review the output to identify each test performed by Zenmap.



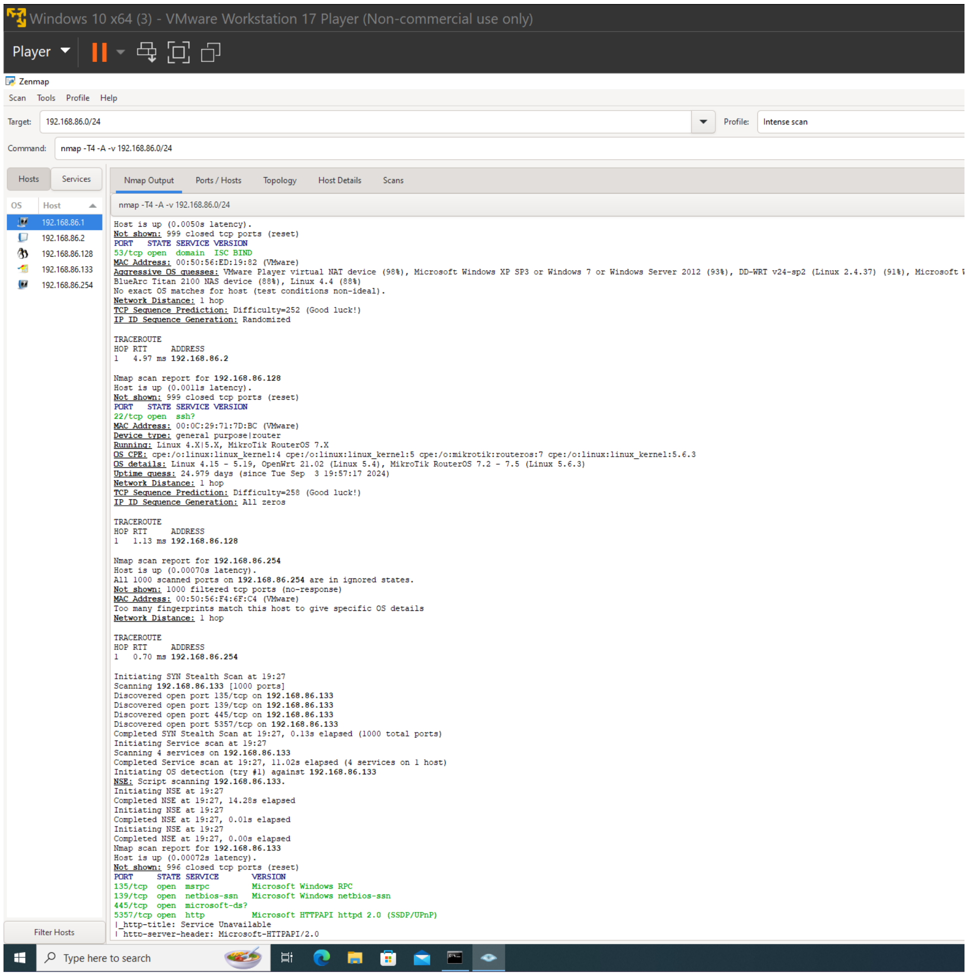
Target: 172.30.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.0/24

```
nmap -T4 -A -v 172.30.0.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-02
18:55 Pacific Daylight Time
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:55
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 18:55, 2.28s elapsed (255
total hosts)
Nmap scan report for 172.30.0.0 [host down]
mass_dns: warning: Unable to determine any DNS
servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 172.30.0.3 [host down]
Nmap scan report for 172.30.0.4 [host down]
Nmap scan report for 172.30.0.5 [host down]
Nmap scan report for 172.30.0.6 [host down]
Nmap scan report for 172.30.0.8 [host down]
Nmap scan report for 172.30.0.9 [host down]
Nmap scan report for 172.30.0.12 [host down]
Nmap scan report for 172.30.0.13 [host down]
Nmap scan report for 172.30.0.14 [host down]
Nmap scan report for 172.30.0.15 [host down]
Nmap scan report for 172.30.0.16 [host down]
Nmap scan report for 172.30.0.17 [host down]
Nmap scan report for 172.30.0.18 [host down]
Nmap scan report for 172.30.0.19 [host down]
Nmap scan report for 172.30.0.20 [host down]
Nmap scan report for 172.30.0.21 [host down]
Nmap scan report for 172.30.0.22 [host down]
Nmap scan report for 172.30.0.23 [host down]
Nmap scan report for 172.30.0.24 [host down]
Nmap scan report for 172.30.0.25 [host down]
Nmap scan report for 172.30.0.26 [host down]
Nmap scan report for 172.30.0.27 [host down]
```

10. **Click** the **Ports/Hosts tab** and review the data, being sure to look for the information described in the following table. Make note of the results; you will use this data to complete the deliverables for this lab.



Target: 192.168.86.0/24

Profile: Intense scan

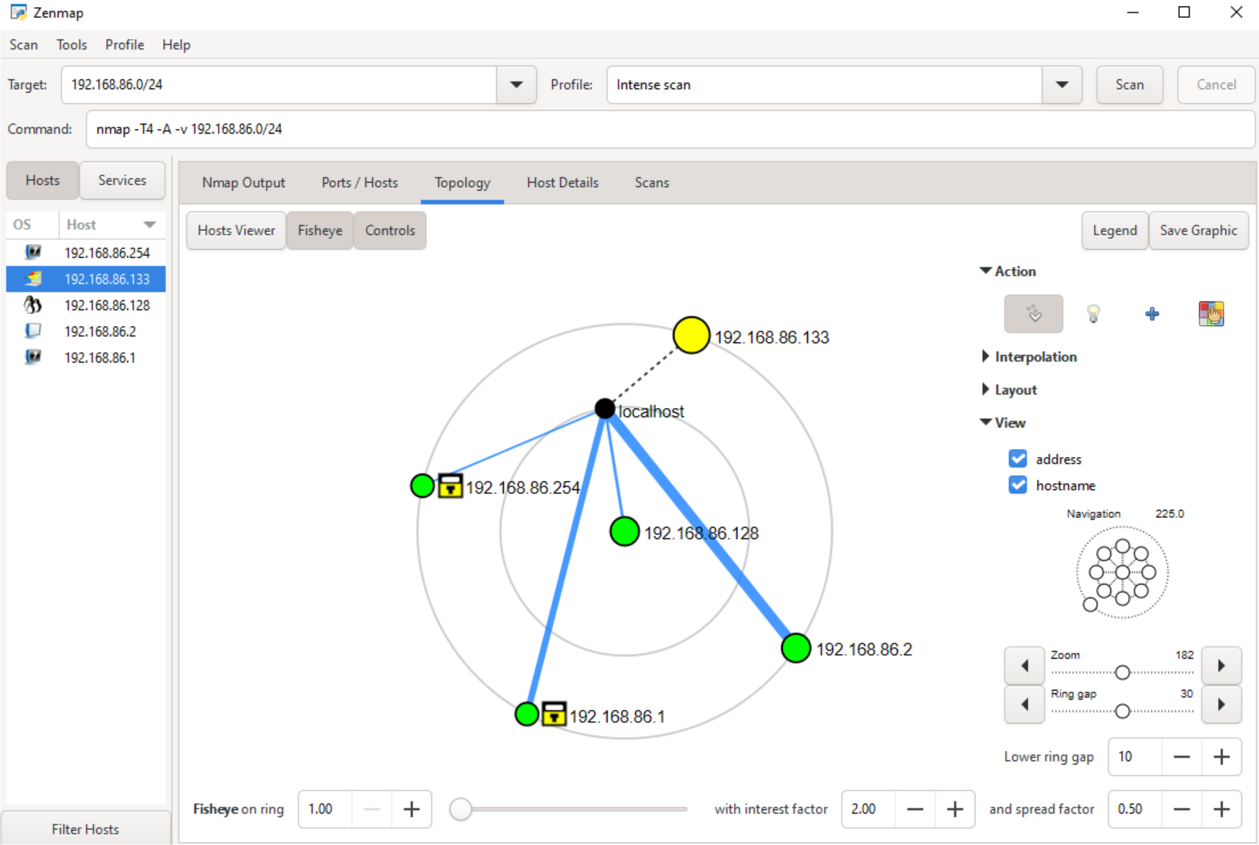
Command: nmap -T4 -A -v 192.168.86.0/24

```
nmap -T4 -A -v 192.168.86.0/24
Host is up (0.0050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND
MAC Address: 00:50:56:ED:19:82 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft W
BlueArc Titan 2100 NAS device (88%), Linux 4.4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE
HOP RTT     ADDRESS
1   4.97 ms 192.168.86.2

Nmap scan report for 192.168.86.128
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh?
MAC Address: 00:0C:29:71:7D:BC (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 24.979 days (since Tue Sep  3 19:57:17 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.86.128

Nmap scan report for 192.168.86.254
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.86.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:6F:C4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms 192.168.86.254

Initiating SYN Stealth Scan at 19:27
Scanning 192.168.86.133 [1000 ports]
Discovered open port 135/tcp on 192.168.86.133
Discovered open port 139/tcp on 192.168.86.133
Discovered open port 445/tcp on 192.168.86.133
Discovered open port 5357/tcp on 192.168.86.133
Completed SYN Stealth Scan at 19:27, 0.13s elapsed (1000 total ports)
Initiating Service scan at 19:27
Scanning 4 services on 192.168.86.133
Completed Service scan at 19:27, 11.02s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.86.133
NSE: Script scanning 192.168.86.133.
Initiating NSE at 19:27
Completed NSE at 19:27, 14.28s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.01s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
Nmap scan report for 192.168.86.133
Host is up (0.00072s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
| http-server-header: Microsoft-HTTPAPI/2.0
```

Note:

11. **Click** the **Topology tab**.

This tab displays a bubble chart of all the IP hosts discovered during the scan. In this report, the bubble chart shows the relative size and connection type of all discovered hosts.



Target: 192.168.86.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.86.0/24

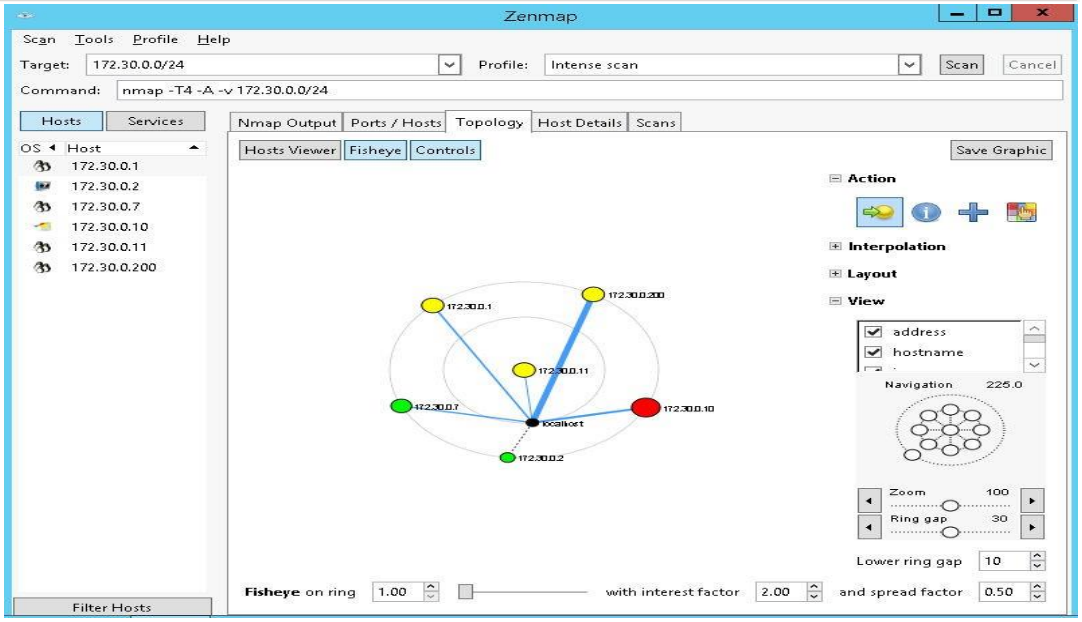
OS	Host
	192.168.86.254
	192.168.86.133
	192.168.86.128
	192.168.86.2
	192.168.86.1

Zoom 182

Ring gap 30

Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50



Target: 172.30.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.0/24

OS	Host
	172.30.0.1
	172.30.0.2
	172.30.0.7
	172.30.0.10
	172.30.0.11
	172.30.0.200

Zoom 100

Ring gap 30

Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Lab Assessment Questions & Answers (32 Points)

1. What is promiscuous mode?

Promiscuous mode is a network interface configuration where the network card captures all packets on the network segment it is connected to, regardless of their destination address. This allows network analysis tools, like Wireshark, to intercept and log traffic for monitoring and analysis purposes, even if the packets are not intended for the device in question.

2. How does Wireshark differ from NetWitness Investigator?

Wireshark is an open-source packet analyzer primarily used for network troubleshooting, analysis, and development. It captures and displays packets in real-time, focusing on packet-level details. In contrast, NetWitness Investigator is a more comprehensive security analytics tool that provides deeper insights into network traffic, including advanced threat detection and forensic analysis.

3. What is the command line syntax for running an Intense Scan with Zenmap on a target subnet of 172.30.0.0/24?

```
nmap -T4 -A -v 172.30.0.0/24
```

4. Name at least five different scans that may be performed with Zenmap.

1. Intense Scan
2. Quick Scan
3. Ping Scan
4. TCP Connect Scan
5. Stealth Scan (SYN Scan)

5. How many different tests (i.e., scripts) did your Intense Scan perform?

1. ARP ping scan
2. Parallel DNS Resolution
3. SYN stealth scan
4. Service scan
5. OS detection
6. Traceroute
7. (Among others within the NSE) NSE = nmap scripting engine

6. Based on your interpretation of the Intense Scan, describe the purpose/results of each test's script performed during the report.

During the Intense Scan, a comprehensive assessment of the target system was conducted using multiple Nmap techniques. The SYN Stealth Scan identified open ports, while service version detection revealed the specific software and versions running on those ports. Additionally, the operating system detection provided insights into the underlying OS, which is critical for vulnerability assessment. The use of Nmap's Scripting Engine (NSE) allowed for targeted scripts to check for known vulnerabilities, authentication issues, and gather further details about network services.

7. How many total IP hosts did Zenmap find on the network?

Nmap done: 256 IP addresses (5 hosts up) scanned in 177.68 seconds

8.Review the ZeNmap GUI (Nmap) network discovery and vulnerability assessment scan report and identify the following:

- What was the date and time stamp of the Nmap host scan?

The Nmap host scan was initiated on September 27, 2024, at 19:25.

- How many total tests or scripts ran during the scan?

A total of 34 scripts were run during the scan.

- A SYN stealth scan discovers all open ports on the targeted host. How many ports are open on the targeted host?

There are 4 ports open on 192.168.86.133

- What services/applications are on the targeted host?

•	PORT	STATE	SERVICE	VERSION
•	135/tcp	open	msrpc	Microsoft Windows RPC
•	139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
•	445/tcp	open	microsoft-ds?	
•	5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

What is the MAC layer address of the targeted host?

MAC Address: 00:50:56:F4:6F:C4

- What OS is loaded on the targeted host?

OS details: Microsoft Windows 10 1809 - 21H2

- How many router hops away is the targeted host?

TRACEROUTE

HOP RTT   ADDRESS

1   0.70 ms 192.168.86.254

- Does the ZeNmap GUI (Nmap) scan report provide any information regarding to risk, threats, or vulnerabilities found?

  Yes, the ZeNmap GUI (Nmap) scan highlighted open ports, and services running on those ports. With all the information given we can look for common vulnerabilities based on the service types, OS and open ports

- What must you do to confirm or verify if the identified OS, software, application has the latest release and/or software updates and patches?

  You can check the official vendors website to see if there is an update available. Security advisories and community forums are also places you can check to see if a certain service version is exploitable.

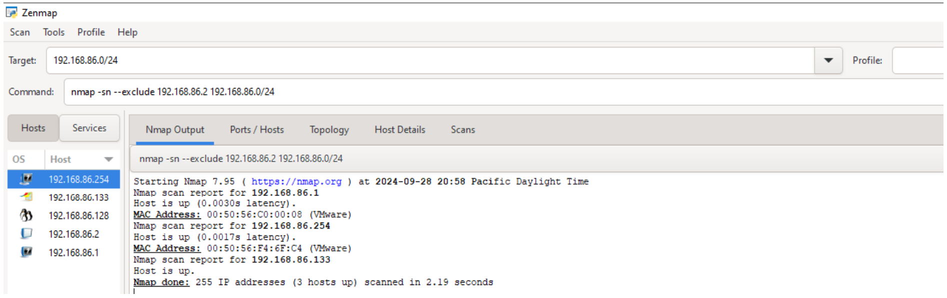
Task 7: Performing a Vulnerability Assessment (10 Points)

Upon completing this Task, you will be able to:
⍰ Identify risks, threats, and vulnerabilities in an IP network infrastructure using Zenmap to perform an IP host, port, and services scan
⍰ Perform a vulnerability assessment scan on a targeted IP subnetwork using OpenVAS
⍰ Compare the results of the Zenmap scan with a OpenVAS vulnerability assessment scan
⍰ Assess the findings of the vulnerability assessment scan and identify critical vulnerabilities
⍰ Make recommendations for mitigating the identified risks, threats, and vulnerabilities as described on the CVE database listing

Scanning a Network with Zenmap

1. In the Command box, of Zenmap (search and type nmap command with option) to scan the or exclude IP address.

Sample command type nmap –sn --exclude 172.30.0.2 172.30.0.0/24 *and* ***press Enter***.



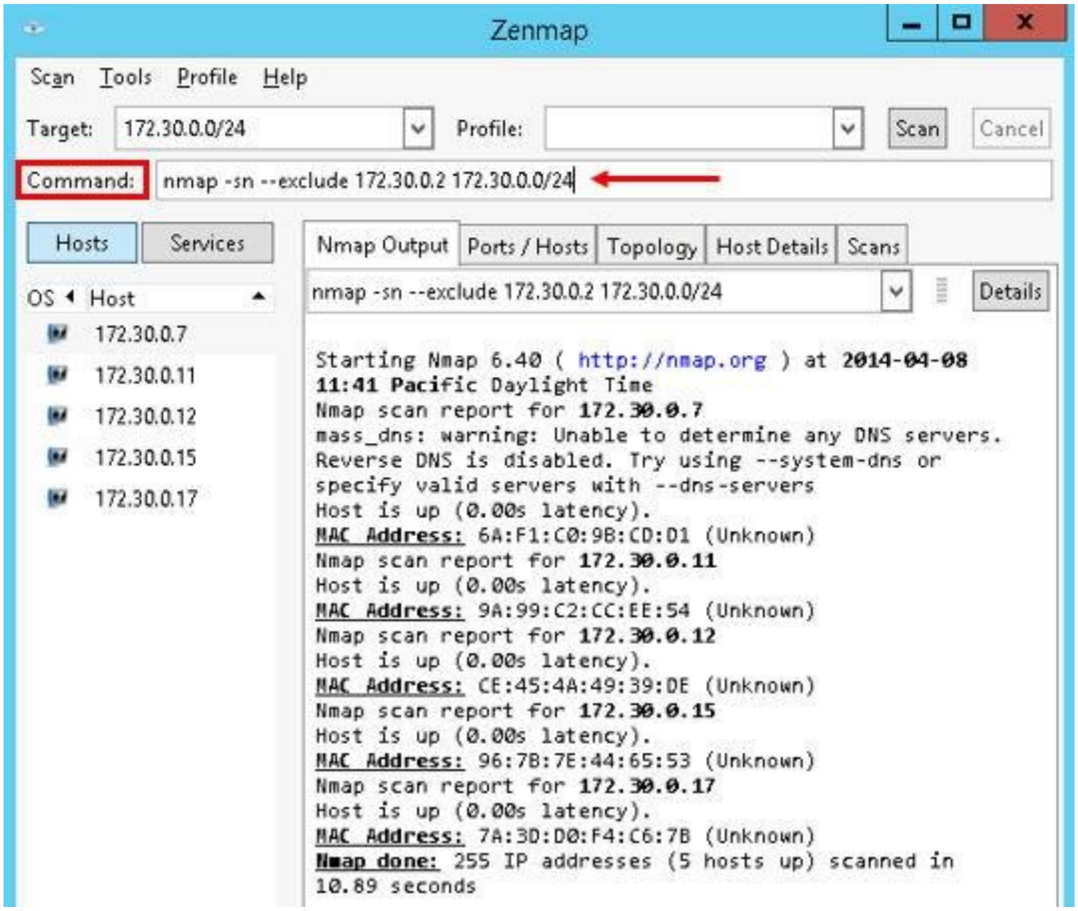
Target: 192.168.86.0/24

Command: nmap -sn --exclude 192.168.86.2 192.168.86.0/24

192.168.86.254
192.168.86.133
192.168.86.128
192.168.86.2
192.168.86.1

```
nmap -sn --exclude 192.168.86.2 192.168.86.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 20:58 Pacific Daylight Time
Nmap scan report for 192.168.86.1
Host is up (0.0030s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.86.254
Host is up (0.0017s latency).
MAC Address: 00:50:56:F4:6F:C4 (VMware)
Nmap scan report for 192.168.86.133
Host is up.
Nmap done: 255 IP addresses (3 hosts up) scanned in 2.19 seconds
```

This command will manually execute a Ping scan (-sn) on all hosts on the 172.30.0.0/24 subnet except the vWorkstation (172.30.0.2). The scan found five hosts on the 172.30.0.0/24 subnet.



Target: 172.30.0.0/24

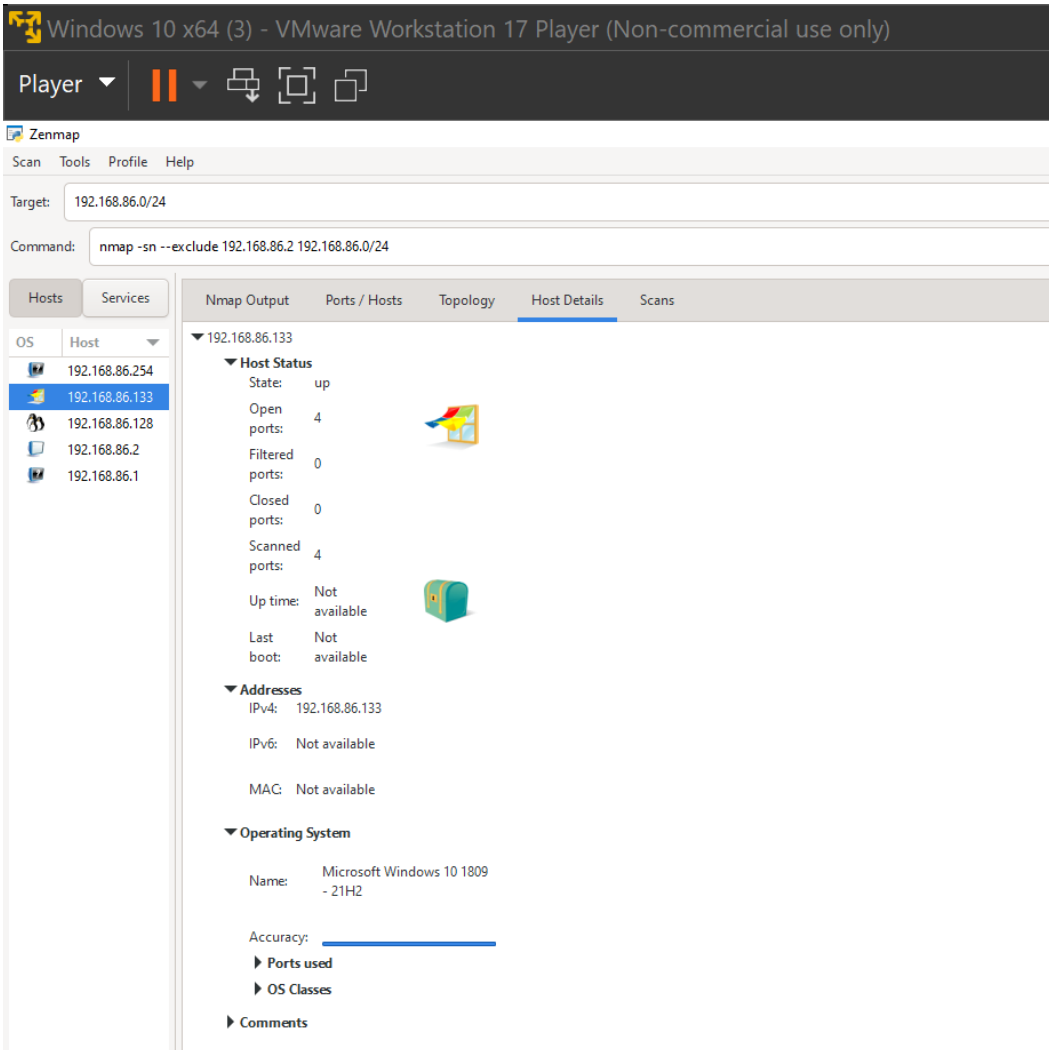
Command: nmap -sn --exclude 172.30.0.2 172.30.0.0/24

```
172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17
```

```
nmap -sn --exclude 172.30.0.2 172.30.0.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-08
11:41 Pacific Daylight Time
Nmap scan report for 172.30.0.7
mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Host is up (0.00s latency).
MAC Address: 6A:F1:C0:9B:CD:D1 (Unknown)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
MAC Address: 9A:99:C2:CC:EE:54 (Unknown)
Nmap scan report for 172.30.0.12
Host is up (0.00s latency).
MAC Address: CE:45:4A:49:39:DE (Unknown)
Nmap scan report for 172.30.0.15
Host is up (0.00s latency).
MAC Address: 96:7B:7E:44:65:53 (Unknown)
Nmap scan report for 172.30.0.17
Host is up (0.00s latency).
MAC Address: 7A:3D:D0:F4:C6:7B (Unknown)
Nmap done: 255 IP addresses (5 hosts up) scanned in
10.89 seconds
```

2. **Click** the **Host Details tab**.

The Ping scan confirms that the machine is available, but can't identify ports, operating systems, or services. The host icon in the Host Details tab matches the one in the OS column of the left pane. These icons indicate that the scan was unable to determine the operating system (OS) of the host.



Target: 192.168.86.0/24

Command: nmap -sn --exclude 192.168.86.2 192.168.86.0/24

OS	Host
	192.168.86.254
	192.168.86.133
	192.168.86.128
	192.168.86.2
	192.168.86.1

192.168.86.133

Host Status

State:	up
Open ports:	4
Filtered ports:	0
Closed ports:	0
Scanned ports:	4
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	192.168.86.133
IPv6:	Not available
MAC:	Not available

Operating System

Name: Microsoft Windows 10 1809 - 21H2

Accuracy:

Ports used

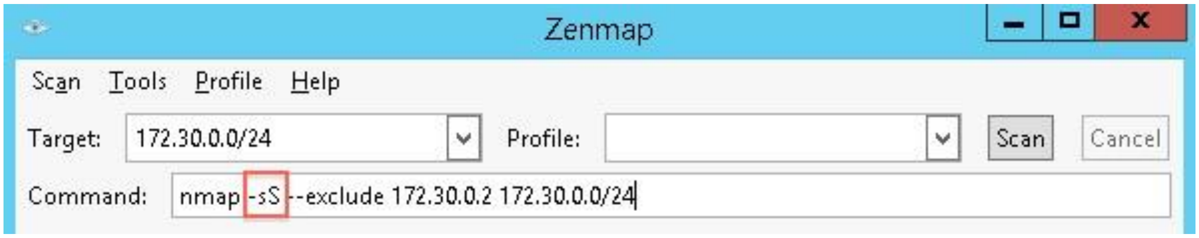
OS Classes

Comments

3. **Click** the **Nmap Output tab** to return to the complete scan results.

4. In the Command box, **highlight –sn**, **type –sS** and **press Enter** to overwrite the existing command and begin a SYN scan of the subnet.

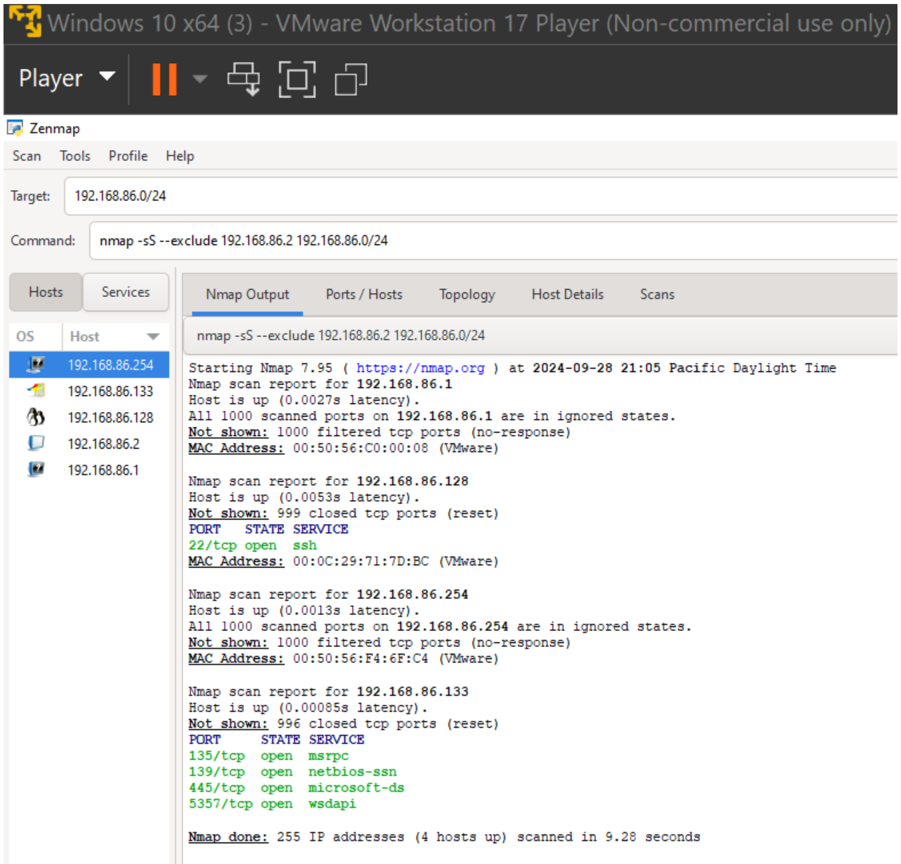
The SYN scan is a form of TCP scanning that is less intrusive on the target host. The scanner, Zenmap, can identify open ports without completing a TCP handshake, which might be noticed by network administrators.



Target: 172.30.0.0/24

Profile:

Command: nmap -sS --exclude 172.30.0.2 172.30.0.0/24

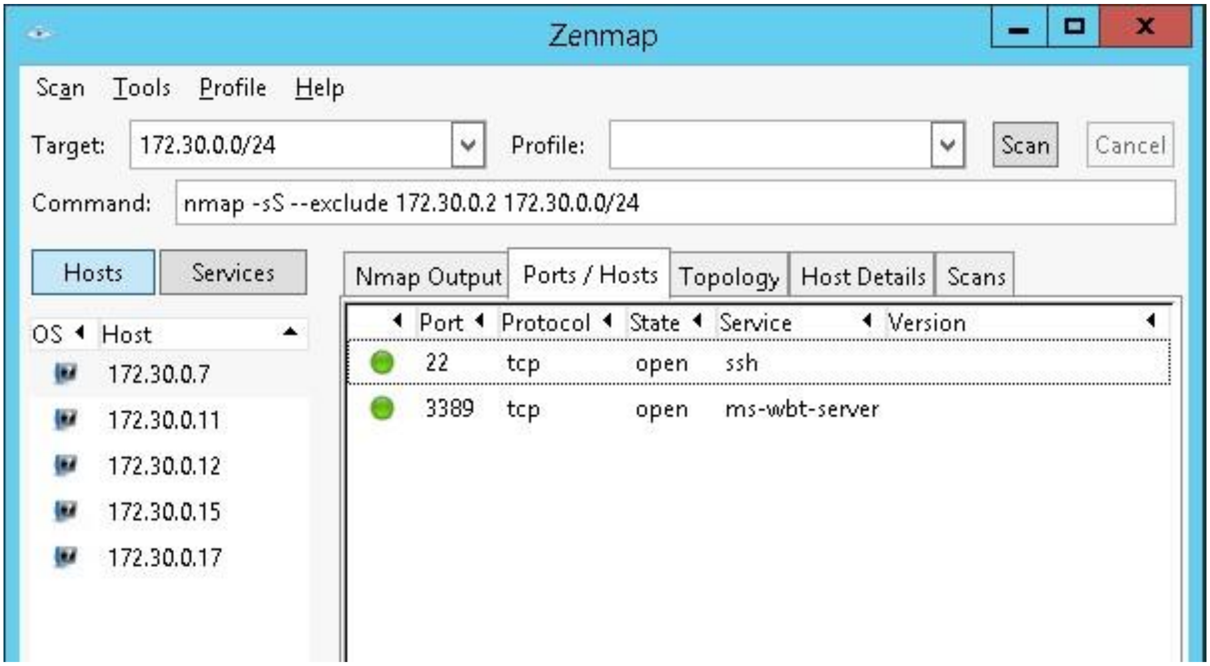


Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

```
nmap -sS --exclude 192.168.86.2 192.168.86.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 21:05 Pacific Daylight Time
Nmap scan report for 192.168.86.1
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.86.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.86.128
Host is up (0.0053s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:71:7D:BC (VMware)

Nmap scan report for 192.168.86.254
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.86.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:6F:C4 (VMware)

Nmap scan report for 192.168.86.133
Host is up (0.00085s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 255 IP addresses (4 hosts up) scanned in 9.28 seconds
```

5. **Click** the first host IP, **IP address** to select it, and **click** the **Ports/Host tab** to see the services using the TCP protocol.

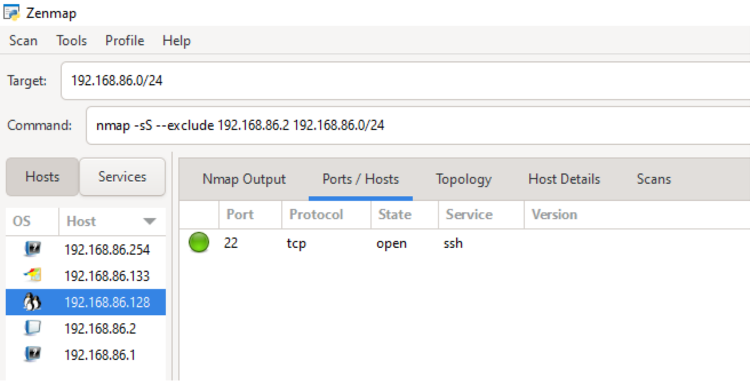


Target: 172.30.0.0/24

Command: nmap -sS --exclude 172.30.0.2 172.30.0.0/24

OS	Host
	172.30.0.7
	172.30.0.11
	172.30.0.12
	172.30.0.15
	172.30.0.17

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	
●	3389	tcp	open	ms-wbt-server	



Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

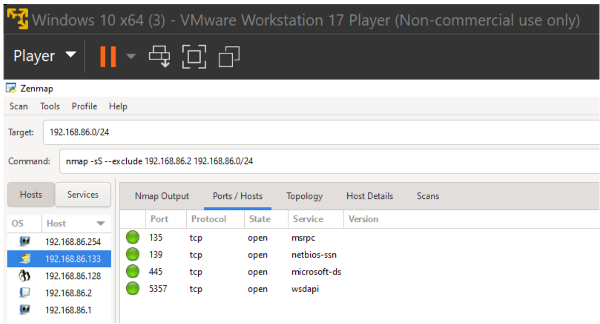
OS	Host
	192.168.86.254
	192.168.86.133
	192.168.86.128
	192.168.86.2
	192.168.86.1

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	

6. **Repeat step 6** for the remaining host IP addresses.

Notice that the SYN scan can identify the services (e.g. SSH, FTP, etc.), but not the versions of these applications. You will discover that information in a later step.

7. **Make a screen capture** showing the details in the **Ports/Hosts tab for IP address** and **paste** it in your Lab Report file. You may need to take multiple screen captures to show the entire display.

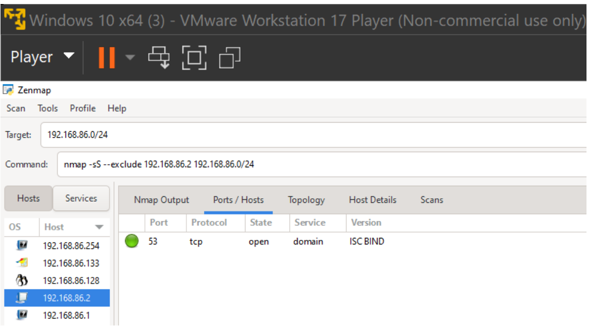


Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

OS	Host
	192.168.86.254
	192.168.86.133
	192.168.86.128
	192.168.86.2
	192.168.86.1

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	microsoft-ds	
●	5357	tcp	open	wsdapi	

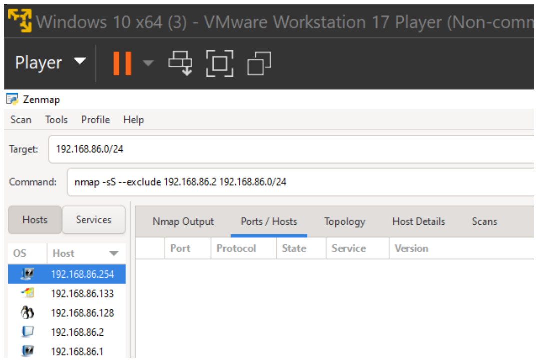


Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

OS	Host
	192.168.86.254
	192.168.86.133
	192.168.86.128
	192.168.86.2
	192.168.86.1

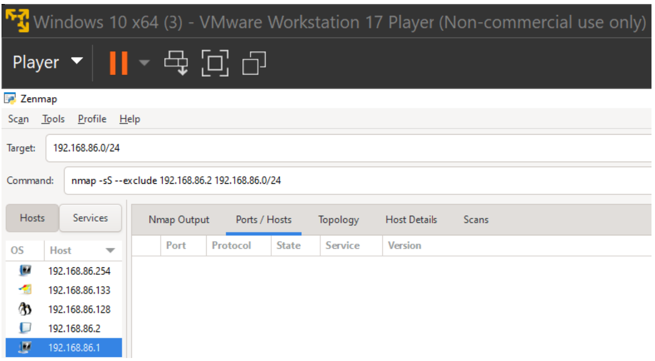
	Port	Protocol	State	Service	Version
●	53	tcp	open	domain	ISC BIND


Windows 10 x64 (3) - VMware Workstation 17 Player (Non-comm
Player
Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
OS Host

Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

192.168.86.254
192.168.86.133
192.168.86.128
192.168.86.2
192.168.86.1


Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
OS Host

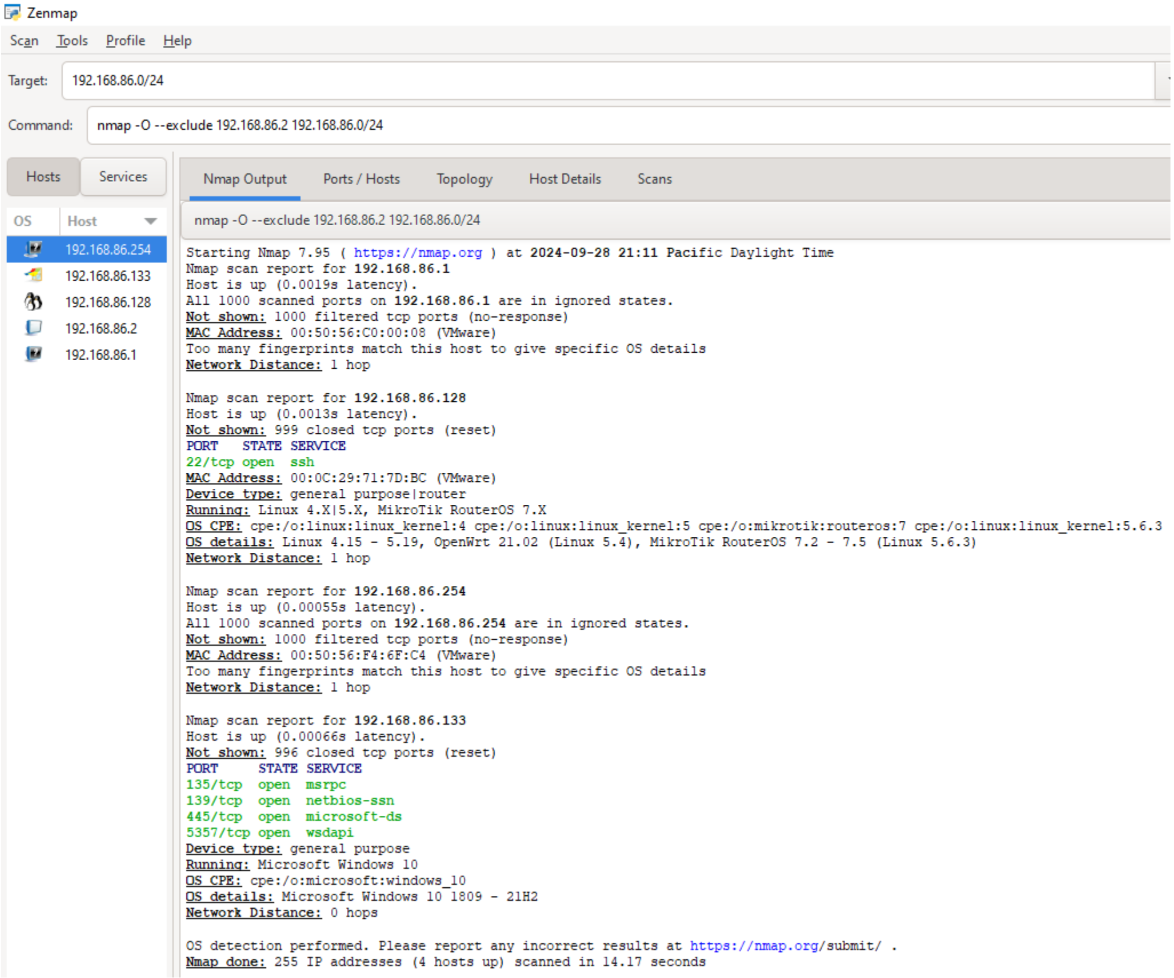
Target: 192.168.86.0/24

Command: nmap -sS --exclude 192.168.86.2 192.168.86.0/24

192.168.86.254
192.168.86.133
192.168.86.128
192.168.86.2
192.168.86.1

8. **Click** the **Nmap Output tab** to return to the complete scan results.

9. In the Command box, **highlight –sS**, **type –O** and **press Enter** to begin the OS fingerprinting scan and determine which operating systems (OS) are running on the network hosts.



Target: 192.168.86.0/24

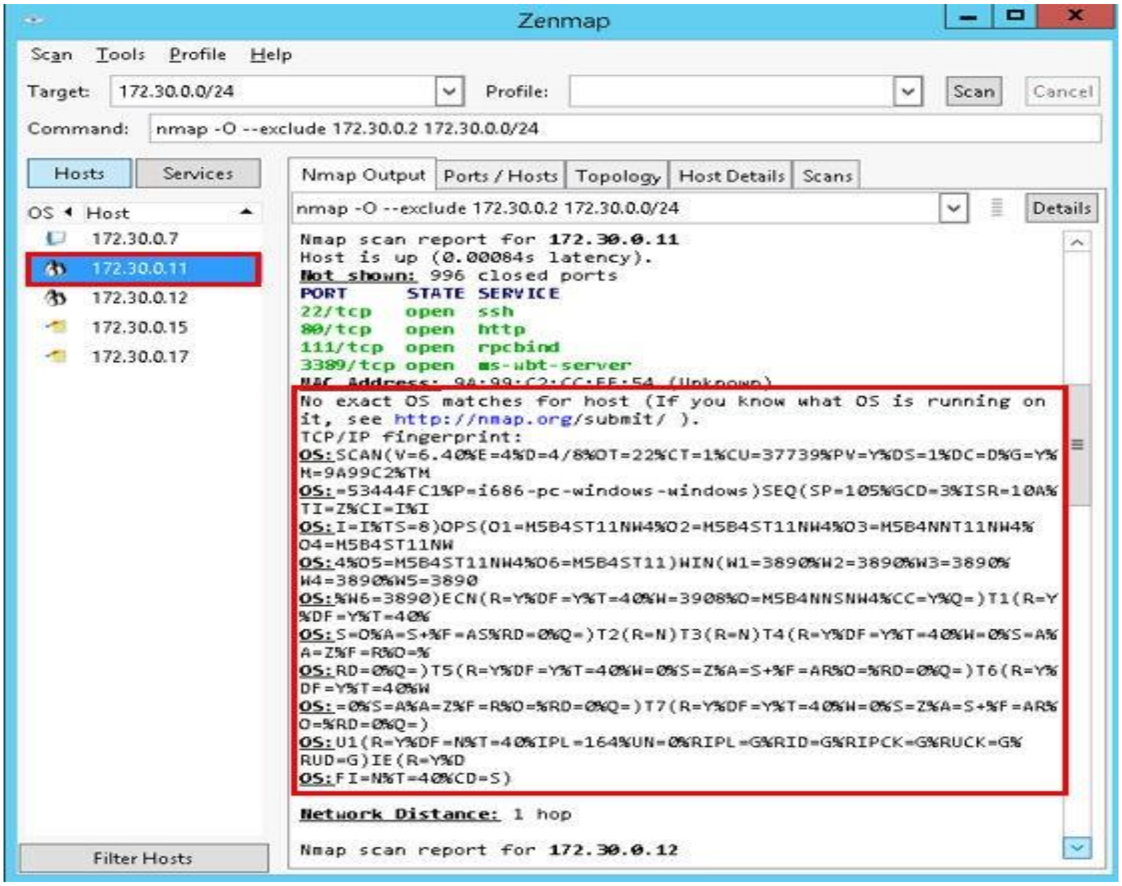
Command: nmap -O --exclude 192.168.86.2 192.168.86.0/24

192.168.86.254
192.168.86.133
192.168.86.128
192.168.86.2
192.168.86.1

nmap -O --exclude 192.168.86.2 192.168.86.0/24

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 21:11 Pacific Daylight Time
Nmap scan report for 192.168.86.1
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.86.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.86.128
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:71:7D:BC (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

Nmap scan report for 192.168.86.254
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.86.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:6F:C4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.86.133
Host is up (0.00066s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 255 IP addresses (4 hosts up) scanned in 14.17 seconds
```

10. **Click IP address** in the left pane.
This scan discovered both open TCP ports (as did the SYN scan) and made a guess at the operating system for each host. The OS icon in the left pane changed as a result of that guess.



Target: 172.30.0.0/24

Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

```
172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17
```

```
nmap -O --exclude 172.30.0.2 172.30.0.0/24
```

```
Nmap scan report for 172.30.0.11
Host is up (0.00084s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
3389/tcp open  ms-wbt-server
MAC Address: 9A:99:C2:CC:EE:54 (Unknown)
No exact OS matches for host (If you know what OS is running on
it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=4/8%OT=22%CT=1%CU=37739%PV=Y%DS=1%DC=D%G=Y%
M=9A99C2%TM
OS:=53444FC1%P=i686-pc-windows-windows)SEQ(SP=105%GCD=3%ISR=10A%
TI=Z%CI=I%I
OS:I=I%TS=8)OPS(O1=M5B4ST11NW4%O2=M5B4ST11NW4%O3=M5B4NNT11NW4%
O4=M5B4ST11NW
OS:4%O5=M5B4ST11NW4%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%
W4=3890%W5=3890
OS:%W6=3890)ECN(R=Y%DF=Y%T=40%W=3908%O=M5B4NNSNW4%CC=Y%Q=)T1(R=Y
%DF=Y%T=40%
OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%
A=Z%F=R%O=%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%
DF=Y%T=40%W
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%
O=%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
RUD=G)IE(R=Y%D
OS:FI=N%T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 172.30.0.12
```

***Lab Assessment Questions & Answers* (18 Points)**

1. What is Zenmap typically used for? How is it related to Nmap? Describe a scenario in which you would use this type of application.

Zenmap is a graphical user interface (GUI) for Nmap, which is a powerful network scanning tool. Zenmap allows users to visualize and interact with Nmap's capabilities more easily, making it accessible for those who may not be comfortable using command-line interfaces.

2. Which application can be used to perform a vulnerability assessment scan in the reconnaissance phase of the ethical hacking process?

Nessus is an application that can be used to perform a vulnerability assessment scan in the reconnaissance phase of the ethical hacking process.

3. What must you obtain before you begin the ethical hacking process or penetration test on a live production network, even before performing the reconnaissance step?

You need a scope of engagement before you start the ethical hacking process or penetration test

4. What is a CVE listing? Who hosts and sponsors the CVE database listing Web site?

A CVE (Common Vulnerabilities and Exposures) listing is a standardized identifier for publicly known vulnerabilities. The CVE database is hosted and maintained by the MITRE Corporation, a not-for-profit organization that manages several federally funded research and development centers. The CVE program is sponsored by the U.S. Department of Homeland Security (DHS).

5. Can Zenmap detect which operating systems are present on IP servers and workstations? Which option includes that scan?

Zenmap can detect which operating systems are present on IP servers and workstations using the -O flag

6. How can you limit the breadth and scope of a vulnerability scan?

You can use the --exclude flag to limit the breadth and scope of a vulnerability scan

7. Once a vulnerability has been identified by OpenVAS, where would you check for more information regarding the identified vulnerability, exploits, and any risk mitigation solution?

You can check the CVE database, the NVD database, other exploit databases, security advisories, threat intelligence platforms like crowdstrike, or other security forums for more information regarding identified vulnerabilities, exploits, and for a risk mitigation solution

8. What is the major difference between Zenmap and OpenVAS?

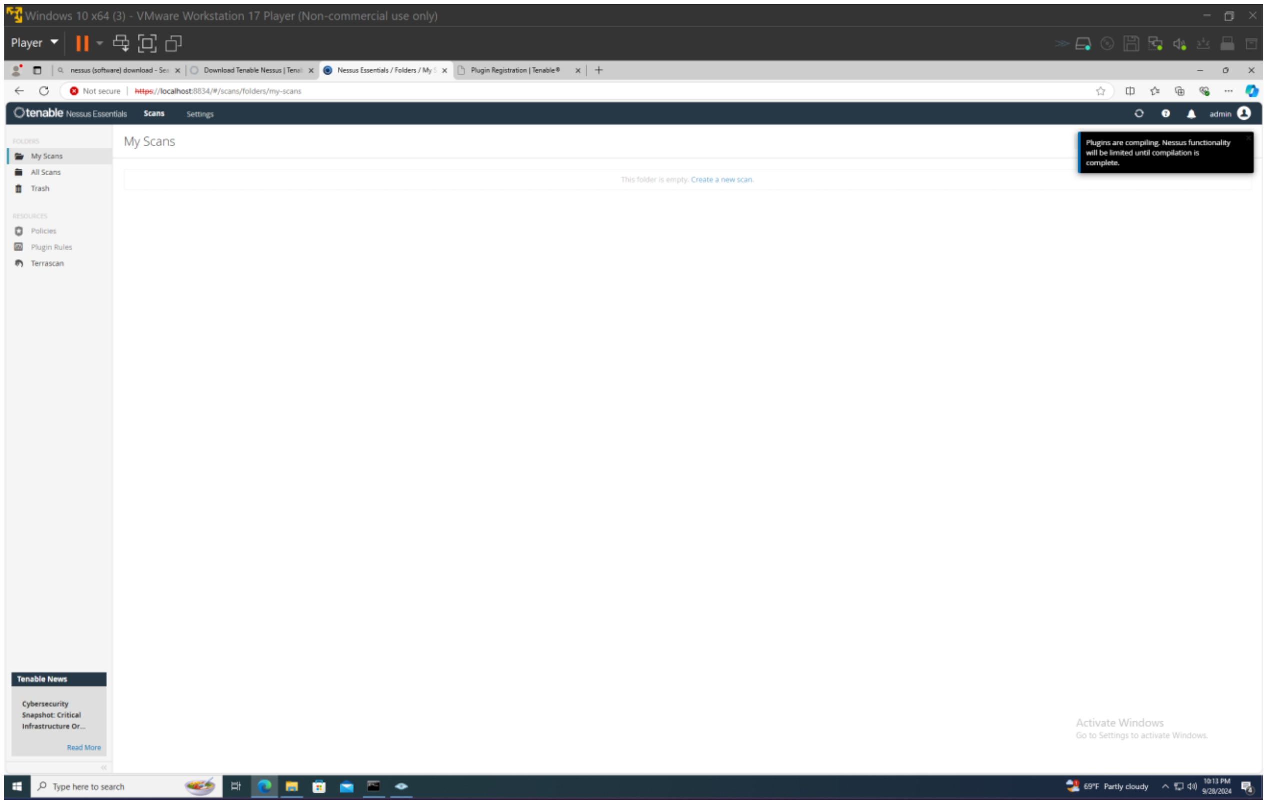
Zenmap is mainly used for reconnaissance and network mapping. You would use Zenmap to create a visual representation of your network and identify live hosts, services, and open ports. OpenVAS is used in the vulnerability assessment phase to identify security weaknesses in systems and applications.

9. Why do you need to run both tools like Zenmap and OpenVAS to complete the reconnaissance phase of the ethical hacking process?

Once you've identified hosts, ports, operating systems and services, you would then use OpenVas to find misconfigurations or vulnerabilities within the information you found using zenmap/nmap.

Challenge Exercise : Install, Configure Nessus® and Perform a Vulnerability Assessment Scan (15 Points)

1. **Install and Load the " Nessus®.**

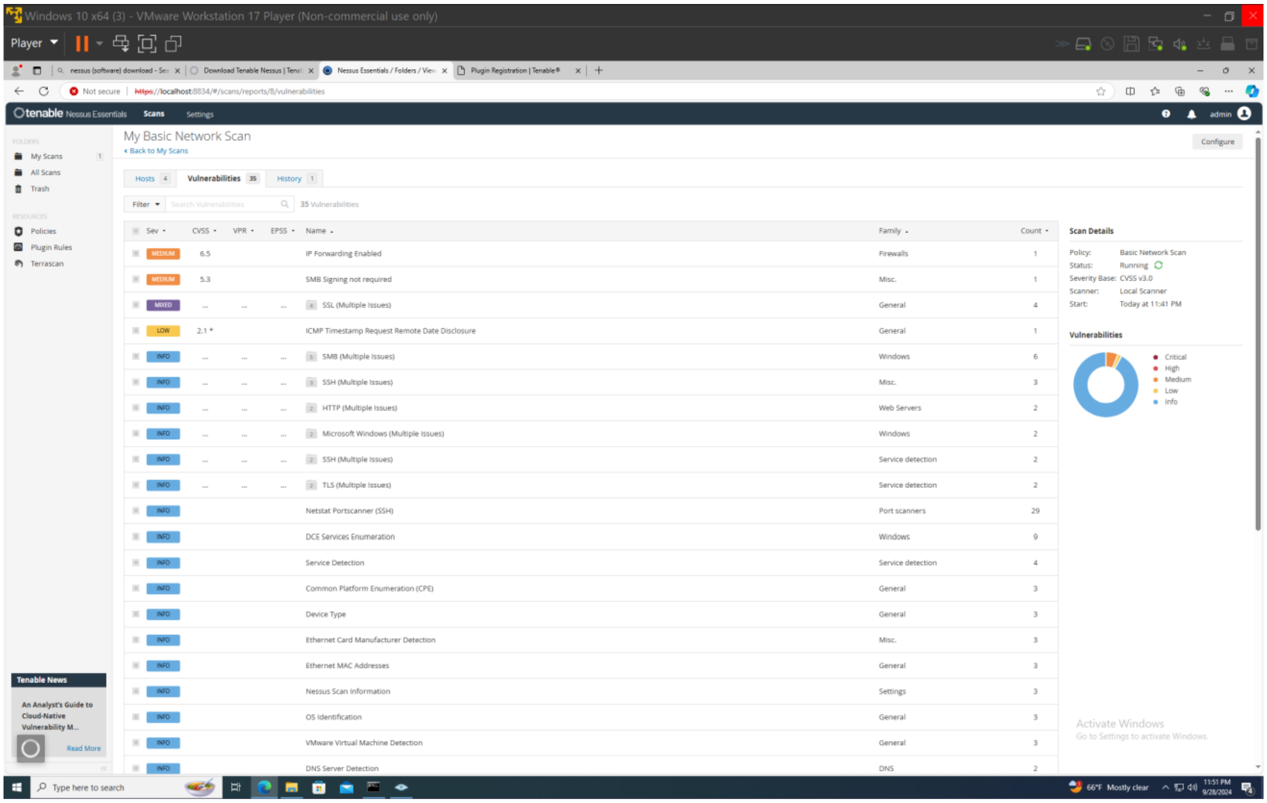

Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
https://localhost:8834/#/scans/folders/my-scans
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Critical Infrastructure Or...
Read More
Activate Windows
Go to Settings to activate Windows.
Type here to search
69°F Partly cloudy
10:13 PM
9/28/2024

My Scans

This folder is empty. Create a new scan.

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

2. Connect to the Nessus®.


Windows 10 x64 (3) - VMware Workstation 17 Player (Non-commercial use only)
Player
https://localhost:8834/#/scans/reports/8/vulnerabilities
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
An Analyst's Guide to Cloud-Native Vulnerability M...
Read More
Configure
Activate Windows
Go to Settings to activate Windows.
Type here to search
66°F Mostly clear
11:51 PM
9/28/2024

My Basic Network Scan

‹ Back to My Scans

Hosts 4 | Vulnerabilities 35 | History 1

Filter ▾ | Search Vulnerabilities | 35 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.5			IP Forwarding Enabled	Firewalls	1
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	4 SSL (Multiple Issues)	General	4
LOW	2.1 *			ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	...	...	3 SSH (Multiple Issues)	Misc.	3
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	2 Microsoft Windows (Multiple Issues)	Windows	2
INFO	...	...	...	2 SSH (Multiple Issues)	Service detection	2
INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	29
INFO				DCE Services Enumeration	Windows	9
INFO				Service Detection	Service detection	4
INFO				Common Platform Enumeration (CPE)	General	3
INFO				Device Type	General	3
INFO				Ethernet Card Manufacturer Detection	Misc.	3
INFO				Ethernet MAC Addresses	General	3
INFO				Nessus Scan Information	Settings	3
INFO				OS Identification	General	3
INFO				VMware Virtual Machine Detection	General	3
INFO				DNS Server Detection	DNS	2

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:41 PM

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

3. **There are five fields to enter the scan target:**

   o Name

   o Type

   o Policy

   o Scan Targets

   o Targets