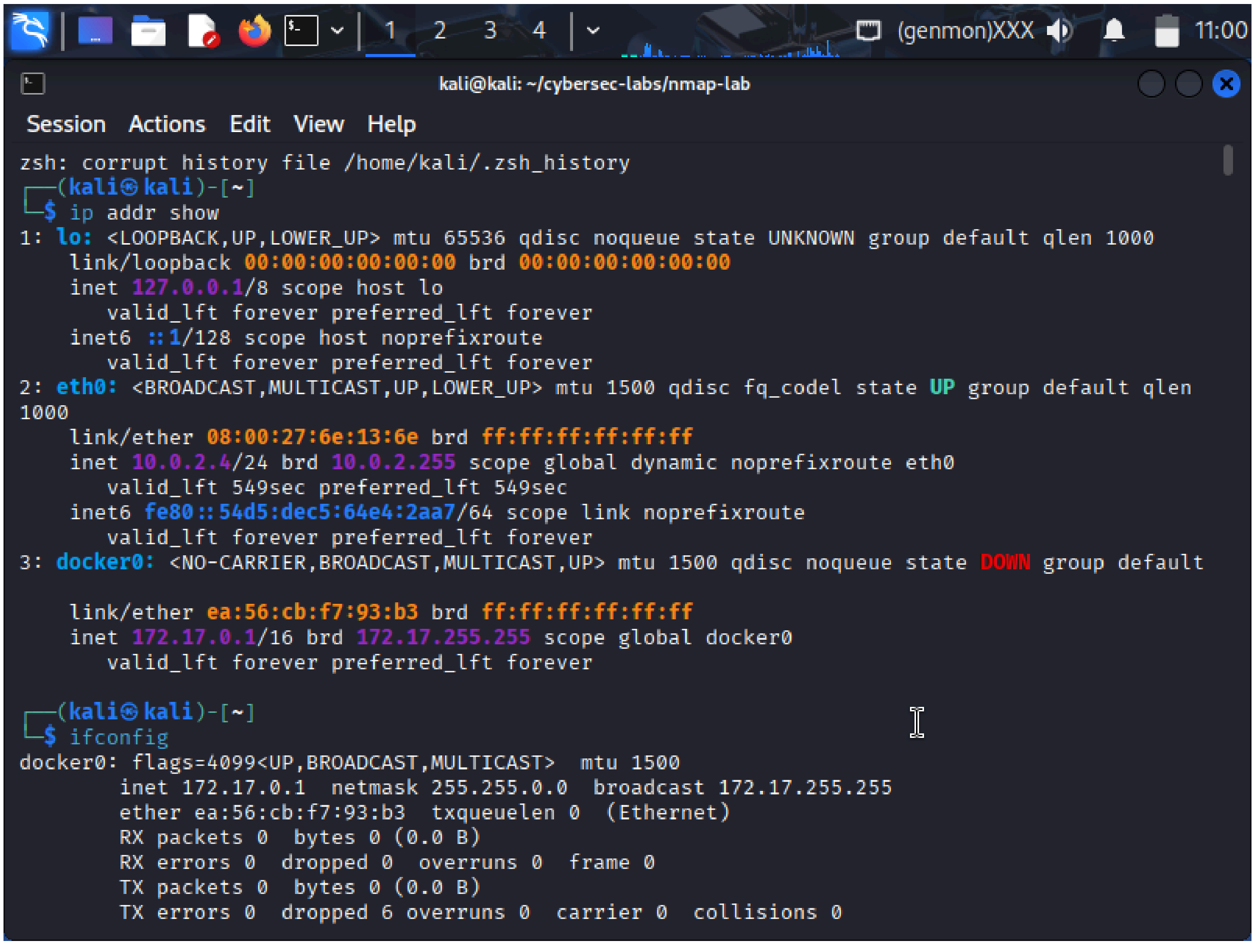
Lab 8: Network Scanning & Enumeration with Nmap

Matthew Cox - COMP 325

Introduction:

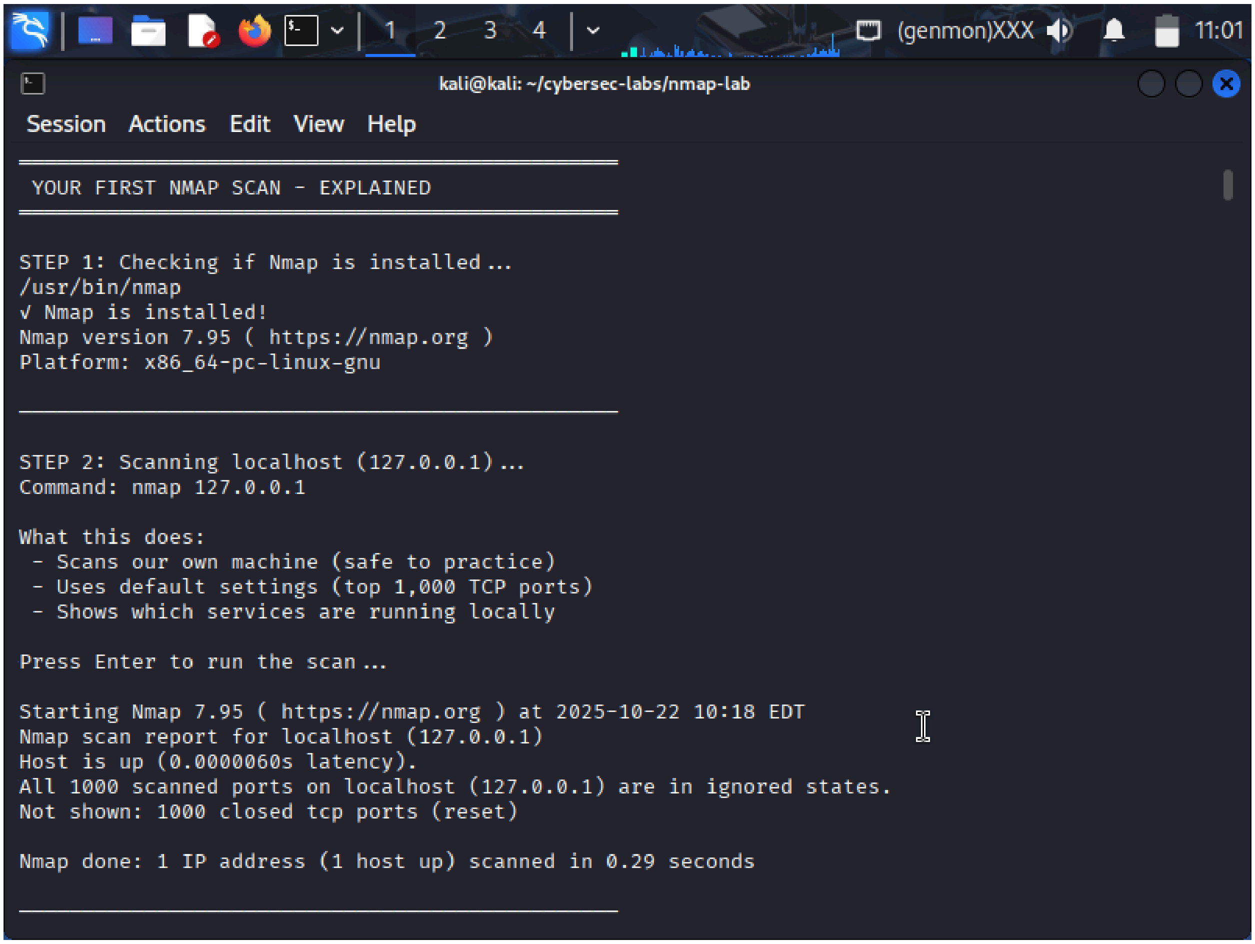
Network scanning and enumeration are foundational steps in penetration testing and security assessments. This lab uses Nmap for network discovery and security auditing to teach practical techniques for uncovering live hosts, open ports, and running services, and for identifying service versions and operating systems. Through a series of hands-on exercises against Linux (Metasploitable) and Windows (Metasploitable3) targets, I will move from basic host discovery to advanced service enumeration and vulnerability detection using the Nmap Scripting Engine (NSE). Along the way, I will learn to interpret scan results, identify potential attack vectors, and choose appropriate scanning techniques.

Body:



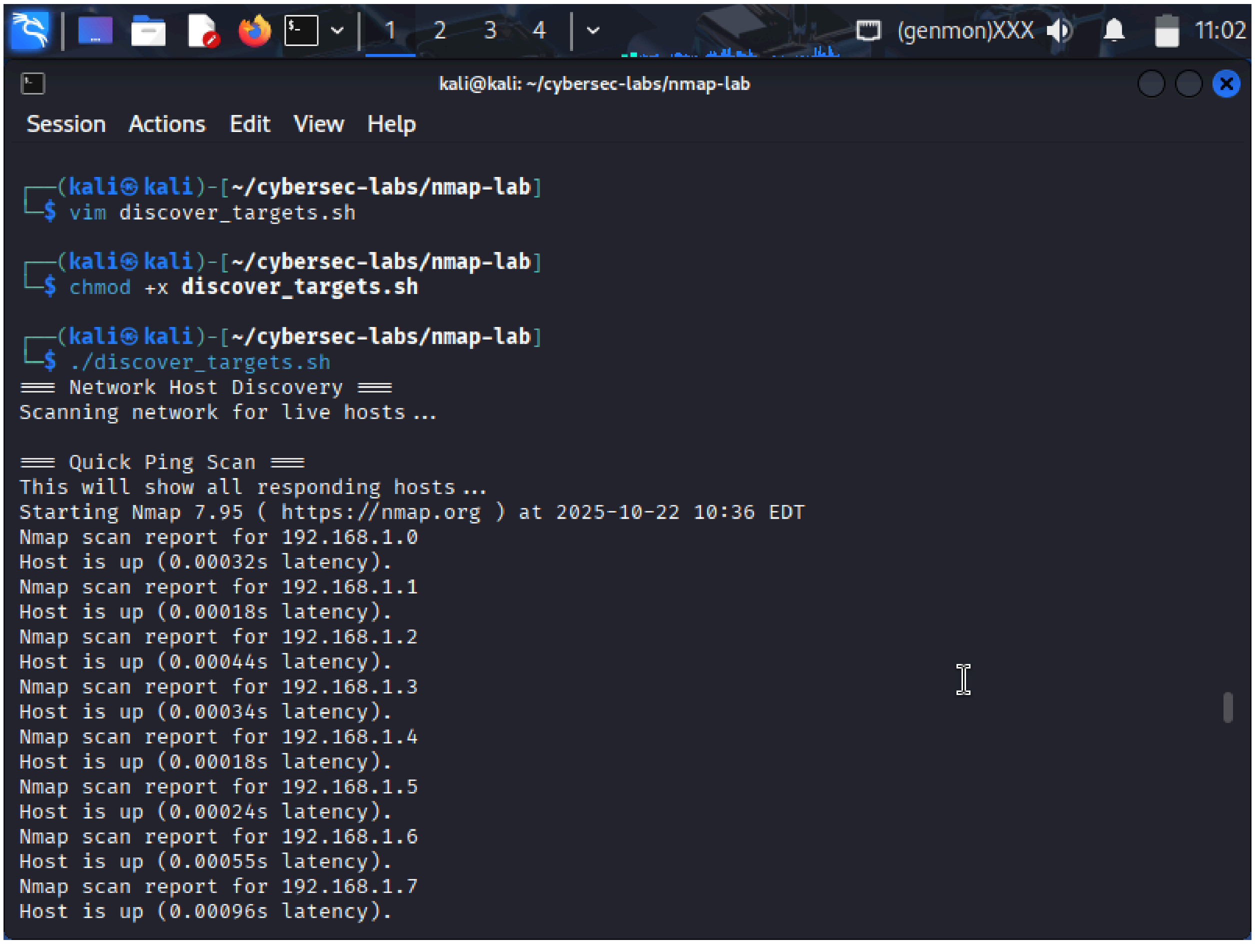
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 549sec preferred_lft 549sec
    inet6 fe80::54d5:dec5:64e4:2aa7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default

    link/ether ea:56:cb:f7:93:b3 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether ea:56:cb:f7:93:b3  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0
```

This image just shows that I am verifying my connectivity after getting Vagrant Metasploitable3 installed. I ran into multiple obstacles, but this shows that everything is running perfectly.

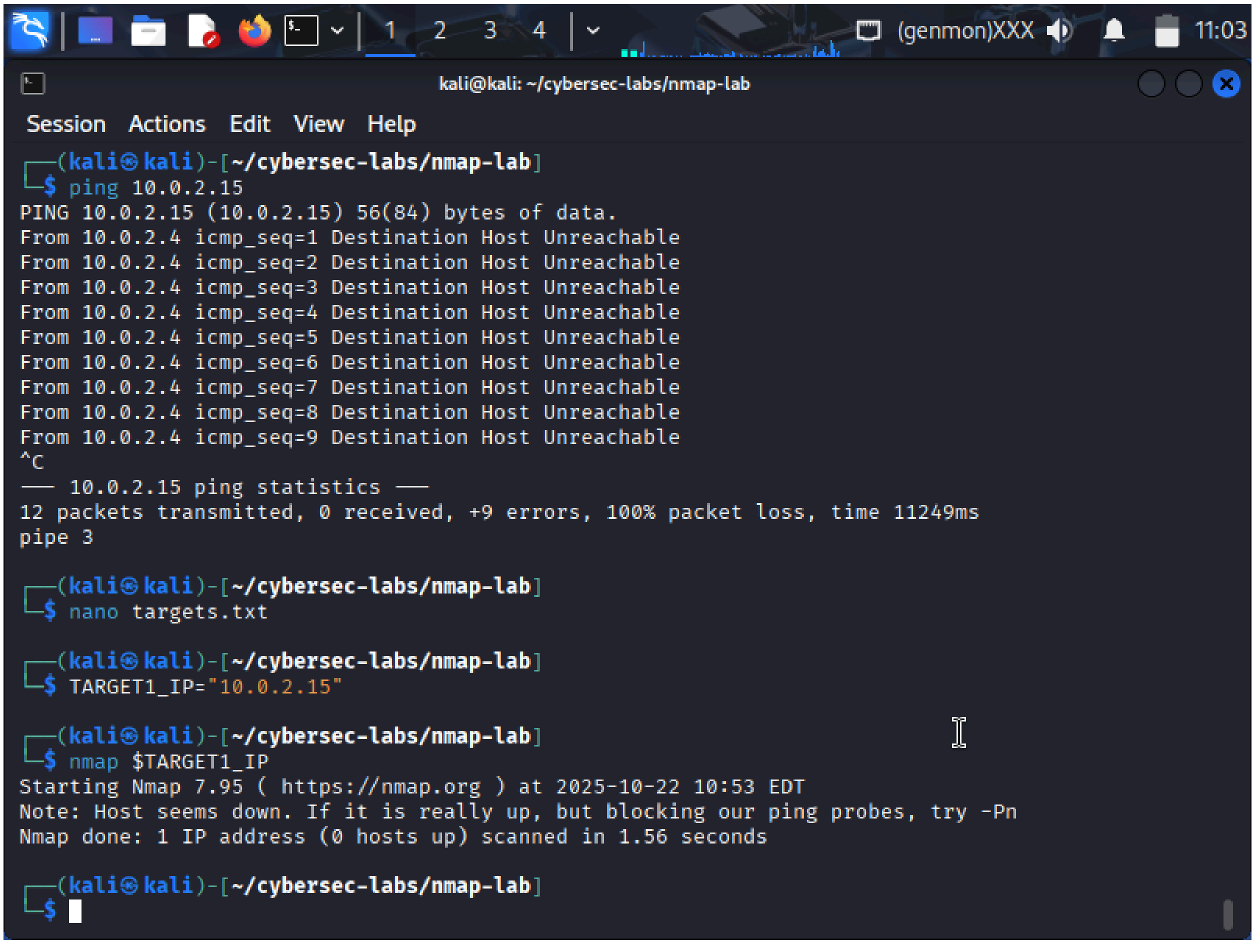


```
═══════════════════════════════════════════════
 YOUR FIRST NMAP SCAN - EXPLAINED
═══════════════════════════════════════════════

STEP 1: Checking if Nmap is installed...
/usr/bin/nmap
√ Nmap is installed!
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu

───────────────────────────────────────────────

STEP 2: Scanning localhost (127.0.0.1)...
Command: nmap 127.0.0.1

What this does:
 - Scans our own machine (safe to practice)
 - Uses default settings (top 1,000 TCP ports)
 - Shows which services are running locally

Press Enter to run the scan...

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 10:18 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

───────────────────────────────────────────────
```

This was my first nmap scan.

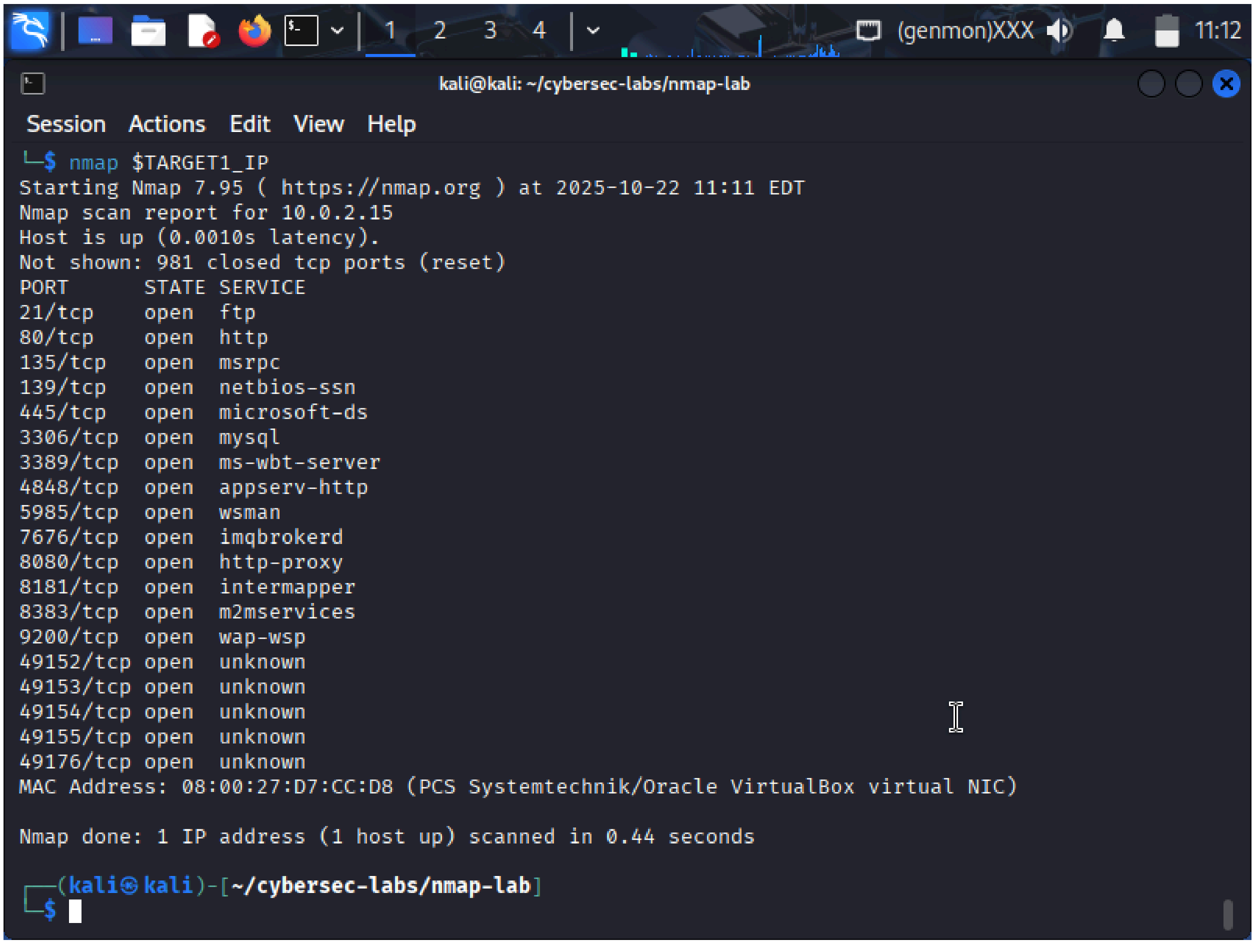


```
┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ vim discover_targets.sh

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ chmod +x discover_targets.sh

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ ./discover_targets.sh
=== Network Host Discovery ===
Scanning network for live hosts...

=== Quick Ping Scan ===
This will show all responding hosts...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 10:36 EDT
Nmap scan report for 192.168.1.0
Host is up (0.00032s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00018s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00044s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00034s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00018s latency).
Nmap scan report for 192.168.1.5
Host is up (0.00024s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00055s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00096s latency).
```



```
┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
From 10.0.2.4 icmp_seq=1 Destination Host Unreachable
From 10.0.2.4 icmp_seq=2 Destination Host Unreachable
From 10.0.2.4 icmp_seq=3 Destination Host Unreachable
From 10.0.2.4 icmp_seq=4 Destination Host Unreachable
From 10.0.2.4 icmp_seq=5 Destination Host Unreachable
From 10.0.2.4 icmp_seq=6 Destination Host Unreachable
From 10.0.2.4 icmp_seq=7 Destination Host Unreachable
From 10.0.2.4 icmp_seq=8 Destination Host Unreachable
From 10.0.2.4 icmp_seq=9 Destination Host Unreachable
^C
--- 10.0.2.15 ping statistics ---
12 packets transmitted, 0 received, +9 errors, 100% packet loss, time 11249ms
pipe 3

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ nano targets.txt

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ TARGET1_IP="10.0.2.15"

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ nmap $TARGET1_IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 10:53 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.56 seconds

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ 
```

In this image, you can tell I ran into an issue. I couldn't ping my Metasploitable3. Later, I found out that I was running my Metasploitable3 on the correct network.



```
└─$ nmap $TARGET1_IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 11:11 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0010s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49176/tcp open  unknown
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$
```

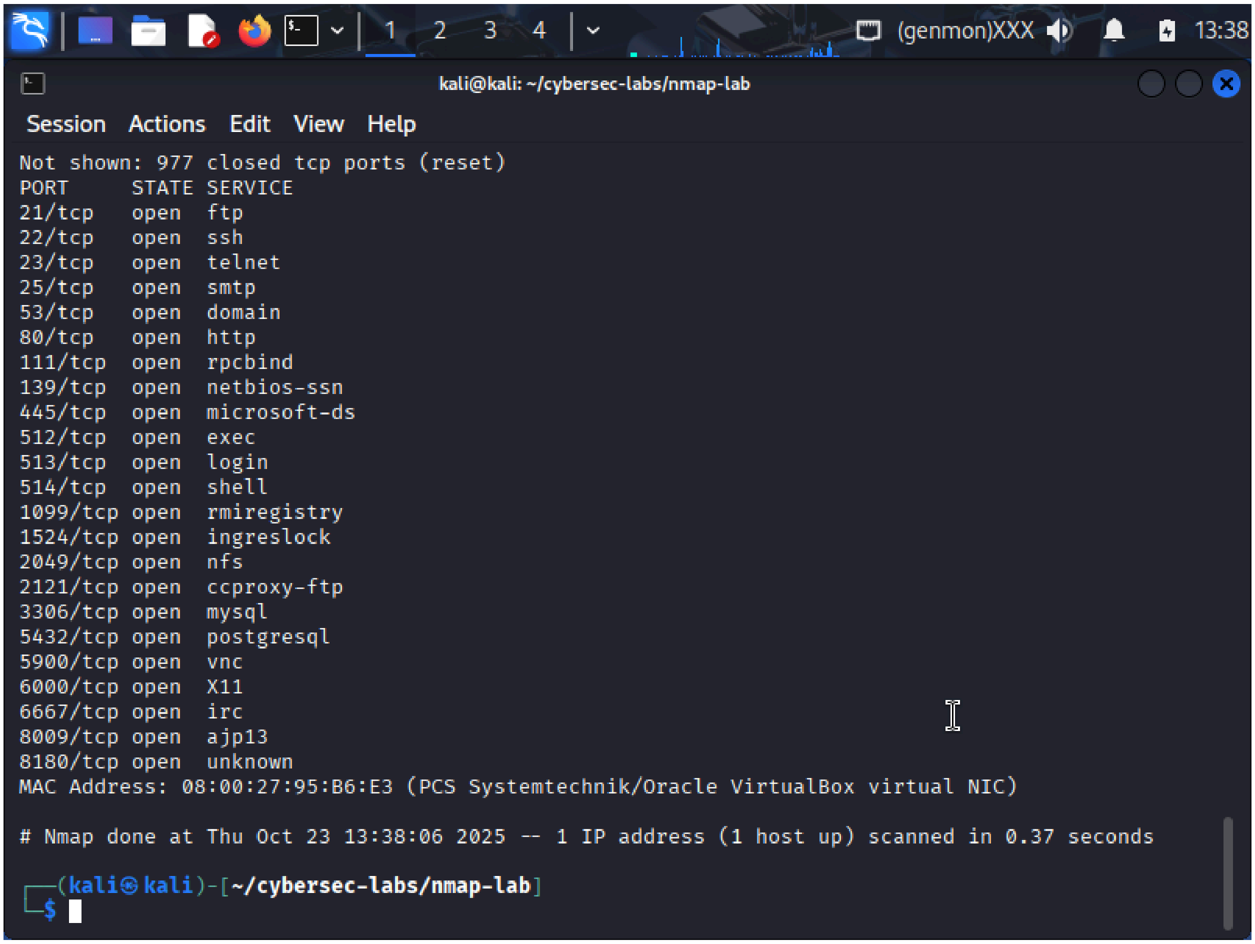
Here is the corrected ping for Metasploitable3 when I made sure everything was on the correct network. Now it is reachable.

Checkpoint questions:

Do you understand why we use -sn for host discovery? Using -sn with nmap performs host discovery to quickly identify which hosts on a network are active and which are offline.

Can you explain the difference between -sn and a regular port scan? -sn purpose is to find which IP addresses are online. While a regular port scan's purpose is to find which ports are open and the service running on them.

Did you successfully identify your two target VMs? Yes.


1 2 3 4
(genmon)XXX
13:38
kali@kali: ~/cybersec-labs/nmap-lab
Session Actions Edit View Help

```
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:95:B6:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

# Nmap done at Thu Oct 23 13:38:06 2025 -- 1 IP address (1 host up) scanned in 0.37 seconds

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ 
```

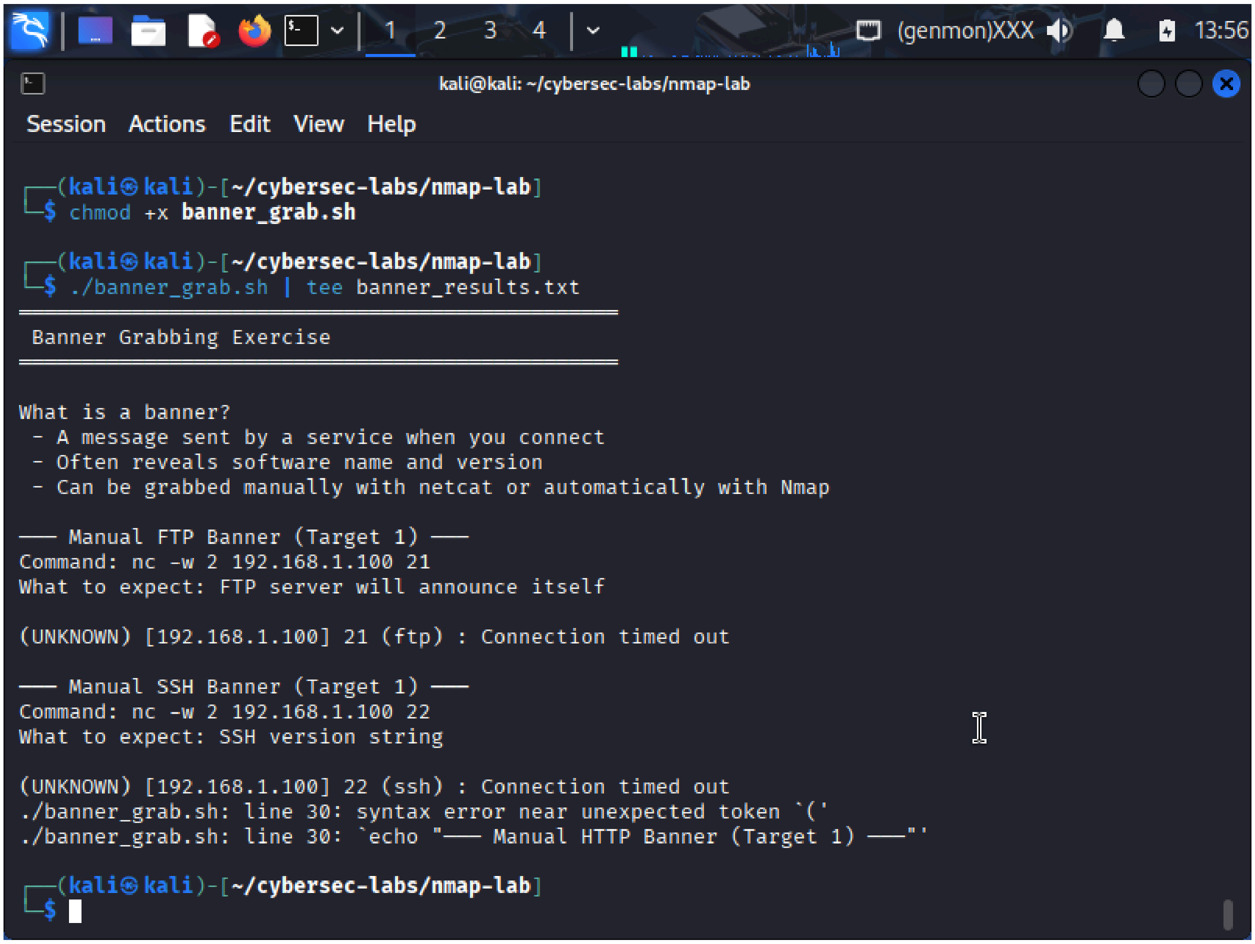
In this image, we are doing the same thing as earlier, but this is the basic Metasploitable rather than the Vagrant Metasploitable3.

Checkpoint Questions:

Can you explain the difference between an "open" and "filtered" port? An open port means a network service is actively listening on that port and accepting connections. A filtered port means nmap was unable to determine if the port is open or closed.

Why might we want to scan all 65,535 ports instead of just the top 1,000? A full scan of all 65,535 ports is used when you need a comprehensive assessment of a system's security, rather than just a quick overview. While Nmap's default scan of the top 1,000 ports is much faster

What does the -p flag do? It is used to specify the ports you want to scan, overriding the default behavior of scanning the 1,000 most common ports.



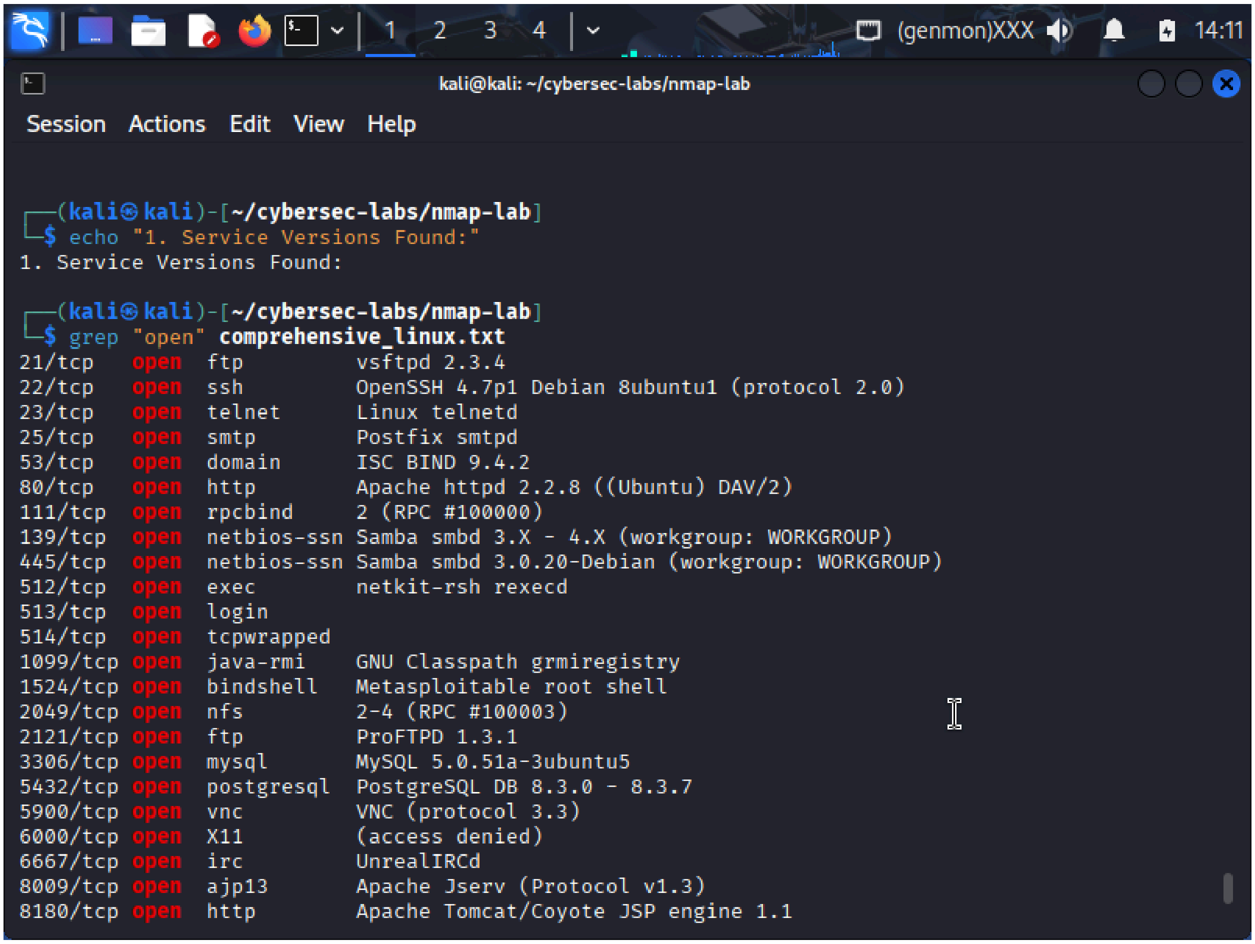
```
┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ chmod +x banner_grab.sh

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ ./banner_grab.sh | tee banner_results.txt
════════════════════════════════════════════════
 Banner Grabbing Exercise
════════════════════════════════════════════════

What is a banner?
 - A message sent by a service when you connect
 - Often reveals software name and version
 - Can be grabbed manually with netcat or automatically with Nmap

── Manual FTP Banner (Target 1) ──
Command: nc -w 2 192.168.1.100 21
What to expect: FTP server will announce itself

(UNKNOWN) [192.168.1.100] 21 (ftp) : Connection timed out

── Manual SSH Banner (Target 1) ──
Command: nc -w 2 192.168.1.100 22
What to expect: SSH version string

(UNKNOWN) [192.168.1.100] 22 (ssh) : Connection timed out
./banner_grab.sh: line 30: syntax error near unexpected token `('
./banner_grab.sh: line 30: `echo "── Manual HTTP Banner (Target 1) ──"'

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ 
```

After various Nmap scans on Metaploitable3, I made a banner-grabbing script. Which is just to show me that when I connect to a service, I'll receive this message identifying itself.

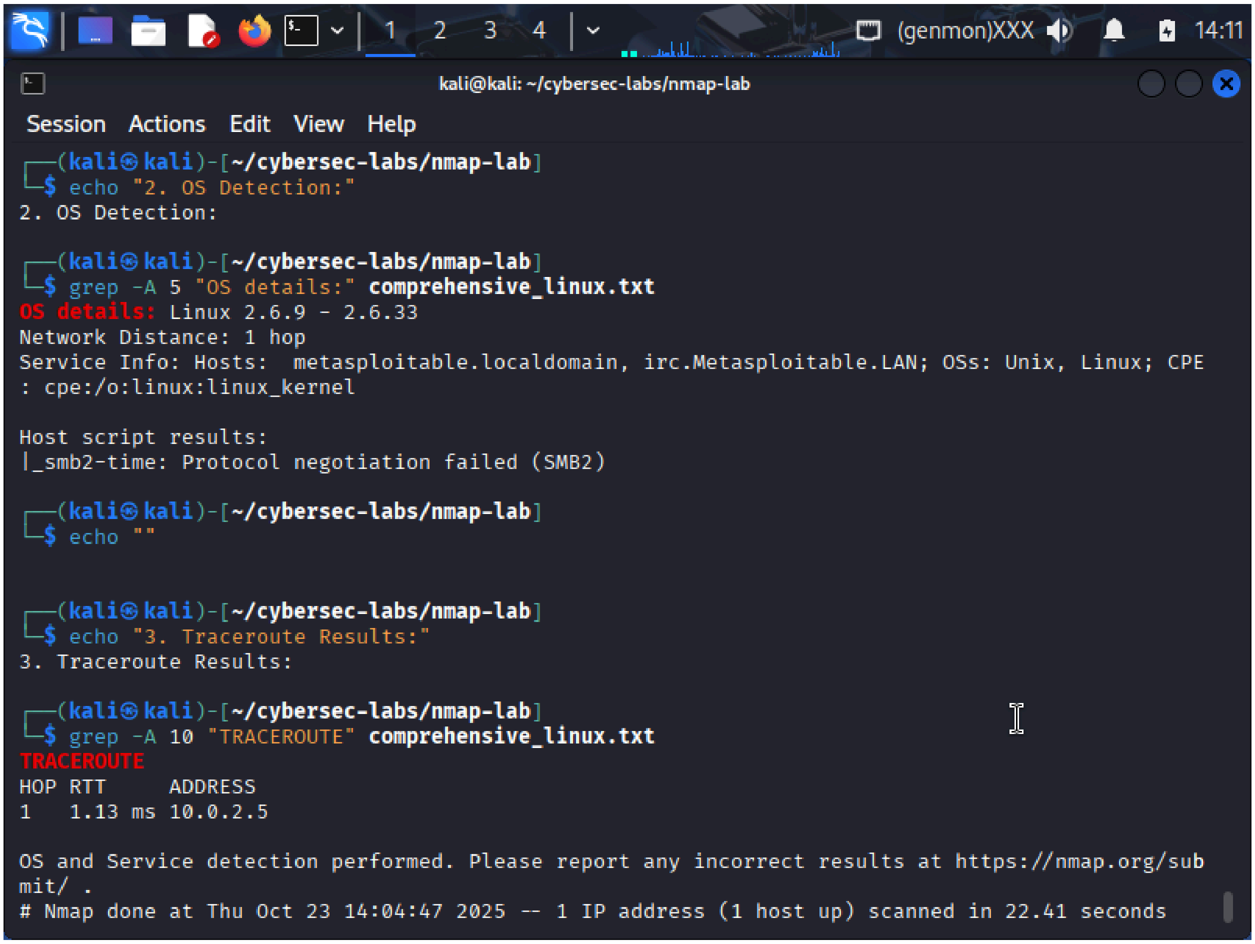
Checkpoint Questions:
Can you explain why knowing "Apache 2.2.8" is more useful than just knowing "http"? It provides a precise, actionable starting point for a security assessment.

What's the difference between --version-intensity 0 and --version-intensity 9? –version-intensity 0 is the fastest version. –version-intensity 9 is the slowest version.

Why might manual banner grabbing sometimes work when Nmap's -sV doesn't? Manual banner grabbing sometimes succeeds where -sV fails because it allows a human operator to perform flexible and creative interactions with a network service.



```
┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ echo "1. Service Versions Found:"
1. Service Versions Found:

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ grep "open" comprehensive_linux.txt
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```



```
┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ echo "2. OS Detection:"
2. OS Detection:

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ grep -A 5 "OS details:" comprehensive_linux.txt
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ echo ""


┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ echo "3. Traceroute Results:"
3. Traceroute Results:

┌──(kali㉿kali)-[~/cybersec-labs/nmap-lab]
└─$ grep -A 10 "TRACEROUTE" comprehensive_linux.txt
TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 10.0.2.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
# Nmap done at Thu Oct 23 14:04:47 2025 -- 1 IP address (1 host up) scanned in 22.41 seconds
```

These few screenshots show an analysis -A flag result of the combined version and OS detection. This breaks down a detailed flag output.

Checkpoint Questions:

Why does OS detection require root privileges? Because it relies on sending and receiving raw packets.

What's the difference between the -O and -A flags? -A is a shortcut for enabling several aggressive scanning features at once, including the OS detection done by -O.

If you see "Network Distance: 1 hop," what does that tell you? Network Distance: 1 hop tells you that the target device is on the same local network segment as the machine running Nmap.

Why might service banners be more reliable than TCP/IP fingerprinting for OS detection? Banner grabbing can be more reliable than TCP/IP fingerprinting for OS detection.

Checkpoint Questions:

Can you explain the difference between the default, safe, and vuln script categories? Default: Purpose: Scripts that run automatically when you use the -sC or --script=default option. Safe: Scripts that won't harm or disrupt the target system. Vuln: Scripts specifically designed for vulnerability detection.

Why would you use --script=ftp-anon instead of manually checking for anonymous FTP? Because --script=ftp-anon automates, standardizes, and extends the check, making it faster, more reliable, and more useful for scanning many hosts or building repeatable reports.

What does it mean when an NSE script says "VULNERABLE"? It structured result status used by vulnerability-related scripts to clearly indicate that a host or service appears to be affected by a known issue.

How would you find out what a specific NSE script does? Get the built-in help (fast)

Nmap exposes a short help for scripts:

```
nmap --script-help <scriptname>
```

```
# example:
```

```
nmap --script-help ftp-anon
```

This prints the script's short description, categories, arguments, author, and a usage example.

Knowledge Assessment:

Question 1: What Nmap flag is used to perform a ping sweep without port scanning?
b) -sn

Question 2: True or False: A TCP SYN scan (-sS) requires root/administrator privileges
True

Question 3: Which Nmap option enables service version detection?

a) -sV

Question 4: Which flag would you use to save scan results in all output formats simultaneously?
d) -oA

Question 5: Which NSE script category would you use to run safe, commonly used enumeration scripts?
c) --script=default

Question 6: What timing template (-T) is recommended for fast scanning in a lab environment?
d) T4

Question 7: True or False: UDP scanning (-sU) is typically faster than TCP scanning because UDP is connectionless
False

Question 8: Which command would perform OS detection on a target?
b) nmap -O target

Question 9: What does the command nmap --script vuln -p 445 192.168.1.100 do?
b) Checks port 445 for known vulnerabilities

Question 10: Which scan type completes the full TCP three-way handshake?
b) -sT (Connect scan)

Conclusion:

Scanning and enumeration are the foundation of any effective security effort. They’re the first active step in penetration testing and account for roughly 70% of real engagements because the quality of your reconnaissance directly determines the success of later actions. Beyond pen tests, scanning helps security assessments uncover unauthorized services and misconfigurations, supports network management by maintaining asset inventories and finding shadow IT, aids compliance auditing by verifying patches and allowed services, speeds incident response by locating compromised systems or backdoors, and fuels vulnerability management and red-team planning by continuously validating security posture and mapping attack paths. In this lab you practiced host discovery, multiple port-scan types (TCP SYN, connect, UDP, stealth), service version detection, OS fingerprinting, NSE-based checks, evasion/timing controls, and producing professional output the practical skills that feed every subsequent phase (exploitation, escalation, lateral movement). Keep refining enumeration: better intel = safer, faster, and more effective security work.