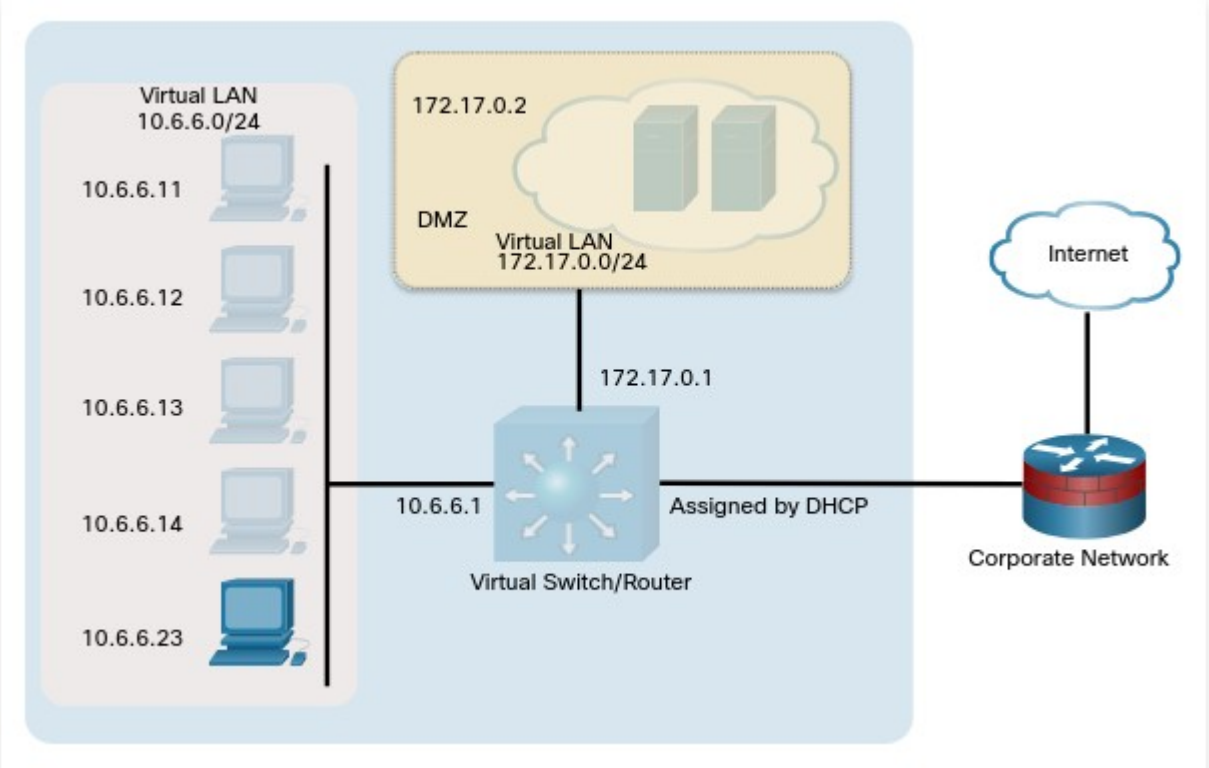
Lab - Enumeration with Nmap
Topology



Objectives
Nmap is a powerful open-source tool for network mapping and discovery. In this lab, you will use Nmap as part of your active reconnaissance strategy.

- Investigate Nmap
- Perform Basic Nmap Scans

Background / Scenario

A Wireshark capture shows unusual activity on a machine on the 10.6.6.0 DMZ network. You've been asked to do some active recon on the machine to determine what services it may be offering and if there are vulnerable applications that could present security issues. The IP address of the suspicious computer is 10.6.6.23. You have access to a Kali Linux system on the 10.6.6.0 network.

Required Resources

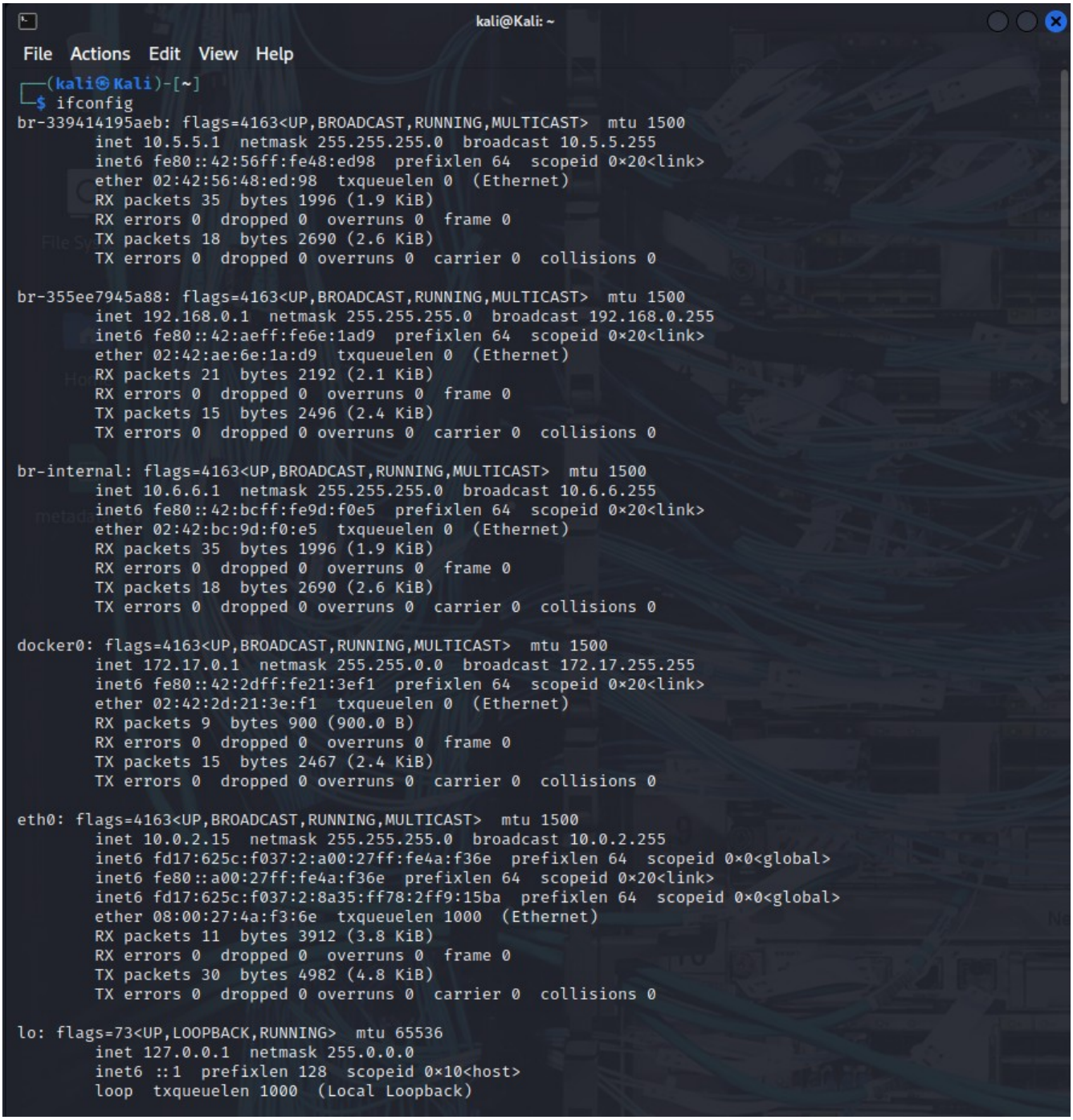
- Kali VM customized for Ethical Hacker course

Instructions

Part 1: Investigate Nmap

Step 1: Log into Kali Linux and verify the environment.

a. Log into the Kali system with the username **kali** and the password **kali**. You are presented with the Kali desktop.
b. Open a terminal window.
c. Verify that Kali has an interface in the 10.6.6.0/24 network using the **ifconfig** command.

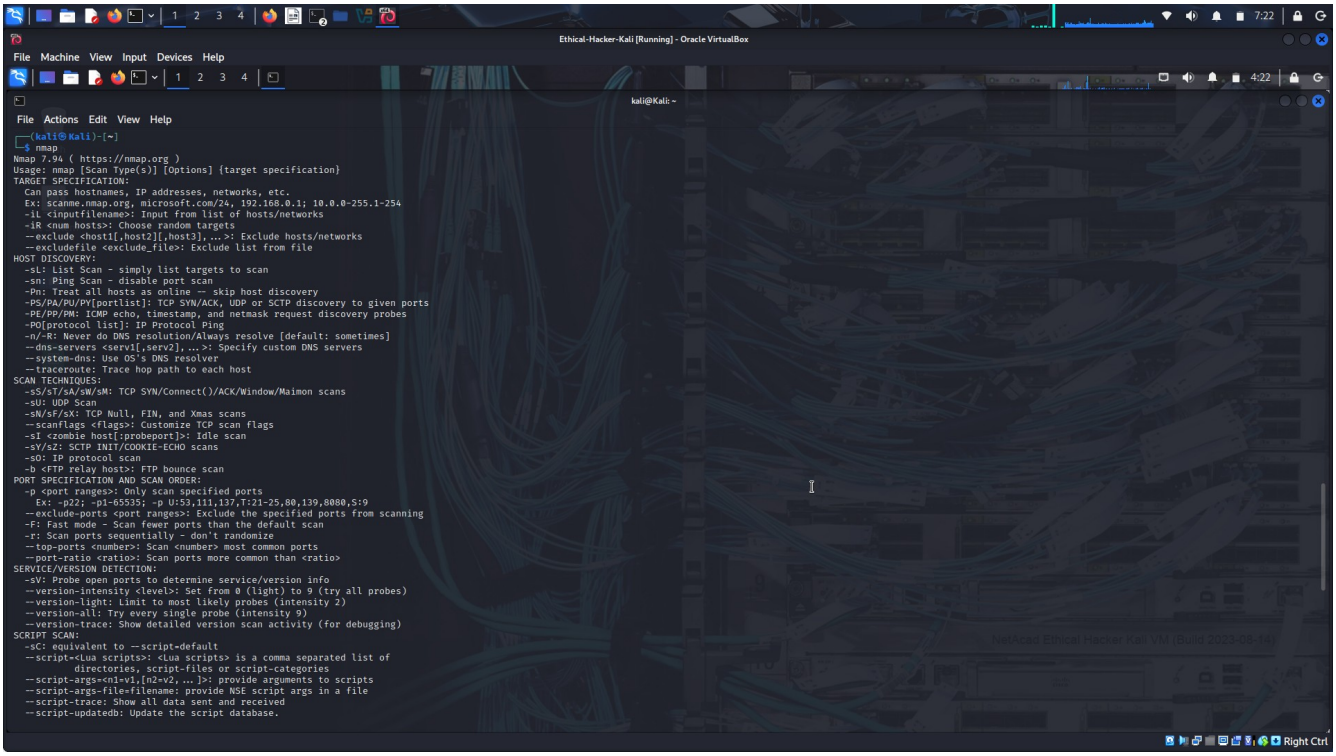


d. Use the **nmap -V** command to verify that Nmap is installed and to display the Nmap version. The output will be similar to what is shown below.

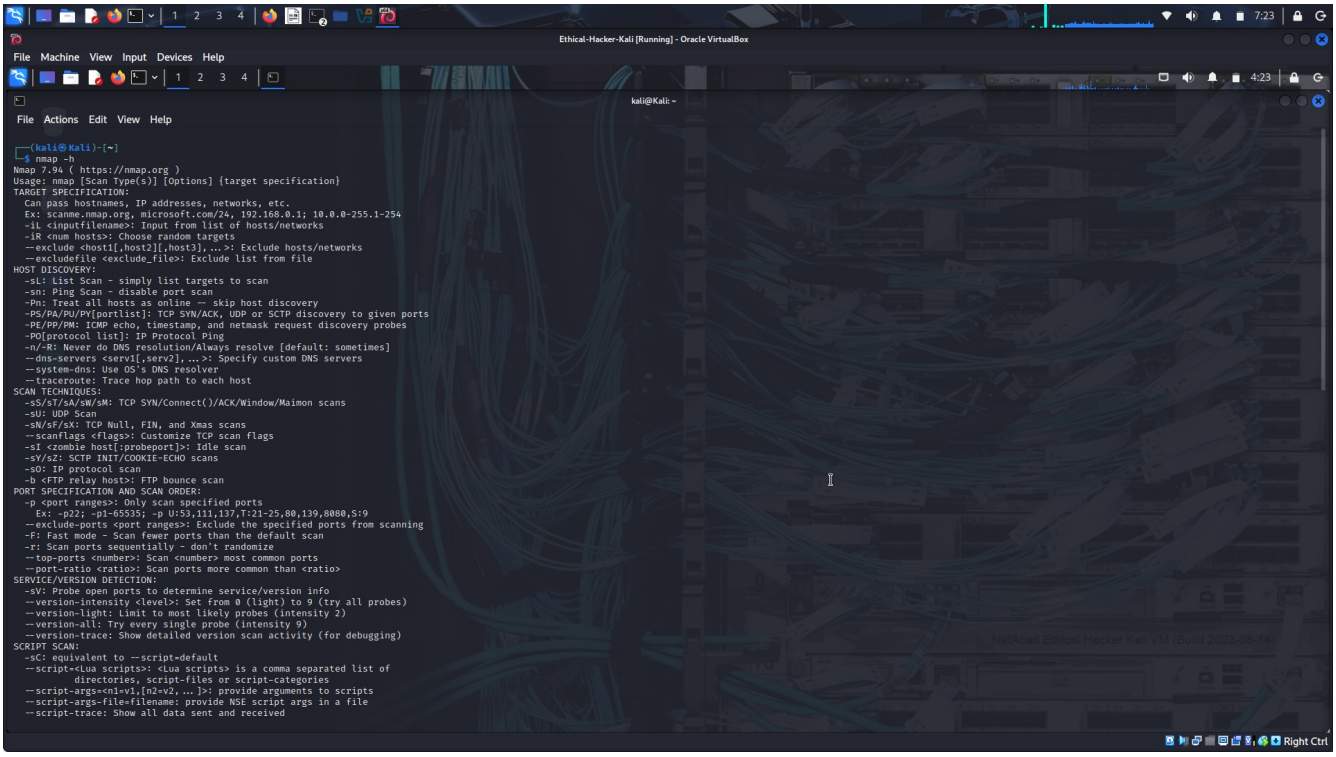
```
┌──(kali㉿Kali)-[~]
└─$ nmap -V
Nmap version 7.94 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.4 openssl-3.0.9 libssh2-1.10.0 libz-1.2.13 libpcre-8.39 libpcap-1.10.4 nmap-libdn
et-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿Kali)-[~]
└─$
```

Step 2: Investigate Nmap Options and Features

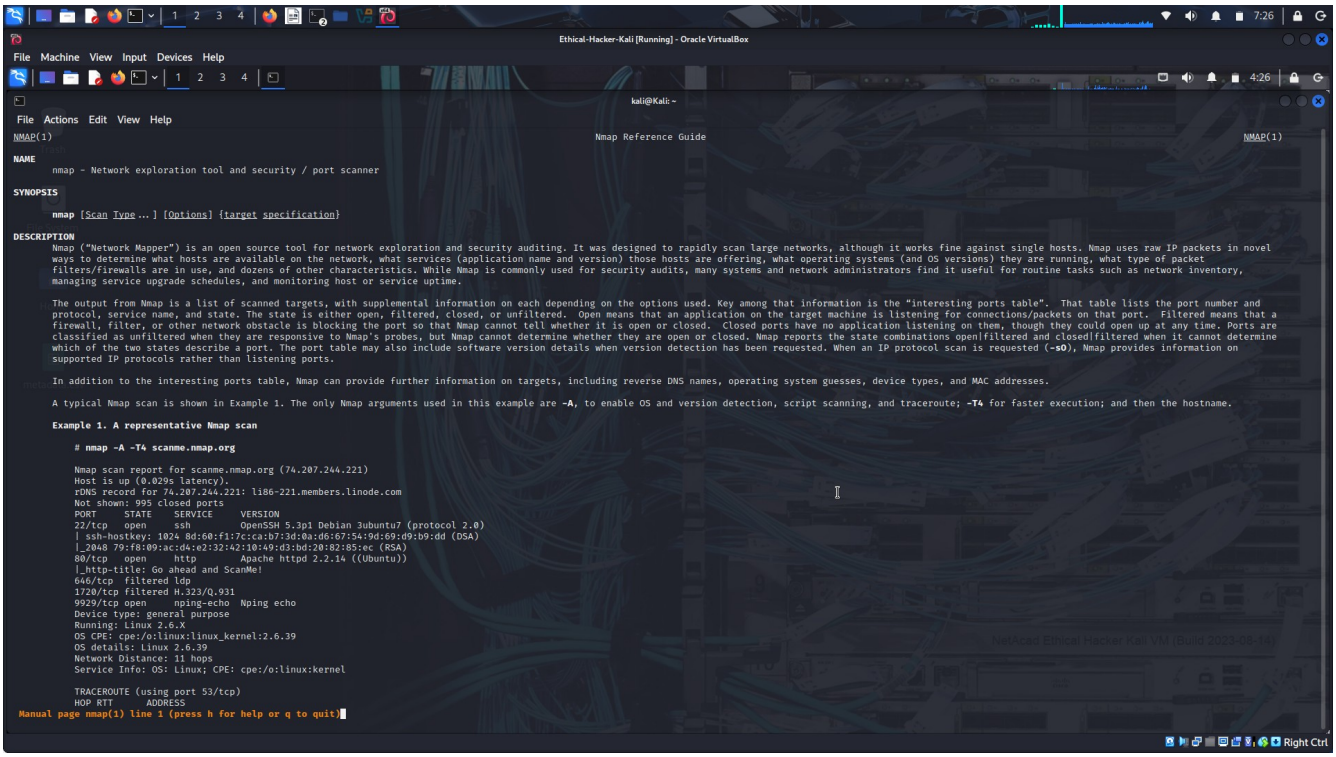
a. Using the command **nmap** without specifying any options or targets returns a list of commonly used Nmap options.



To access the Nmap help system use the command **nmap -h**. The help output is divided into sections based on the type of detection that the option supports.



b. The man page for Nmap provides additional information. To access the man page, enter the command **man nmap**. To exit the man pages, press **q** to quit and return to the terminal prompt.



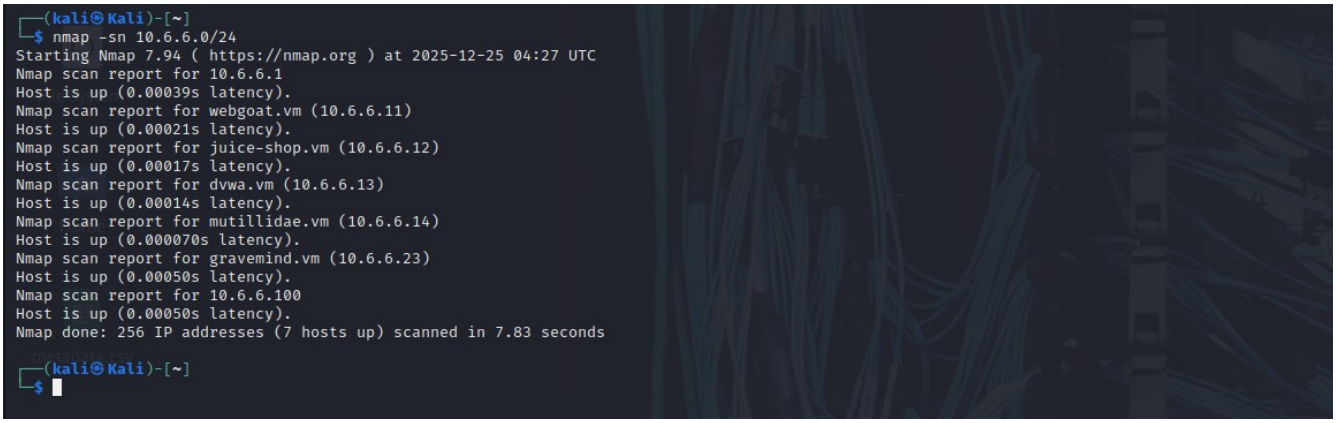
Use the man page for Nmap to complete the table.

Option	Description
-A	Aggressive scan that enables OS detection, version detection, script scanning and traceroute
-O	Enables OS detection
-p <port ranges>	Allows for specific ports or port ranges to be scanned
-sF	Performs TCP FIN scan
-sn	Performs host discovery scan
-sS	Performs TCP SYN scan
-sT	Performs TCP Connect scan
-sV	Probes open ports to determine service/version info
-T<0-5>	Sets the timing of the scan. Higher numbers produce results faster. Slower scans elude detection better.
-v	Increases the verbosity of the output
--open	Only reports open (or possibly open) ports

Part 2: Perform Basic Nmap Scans

Step 1: Initiate a basic Nmap scan of the target computer.

a. To quickly scan the DMZ for active hosts, you can perform a discovery scan. In a discovery scan, the scanning host sends an ICMP echo request (ping), a TCP SYN to port 443, a TCP ACK to port 80, and an ICMP timestamp request. A response to any of the requests indicates that the host is up and the IP protocol stack on the host is functioning. Enter the following command to scan the DMZ network:

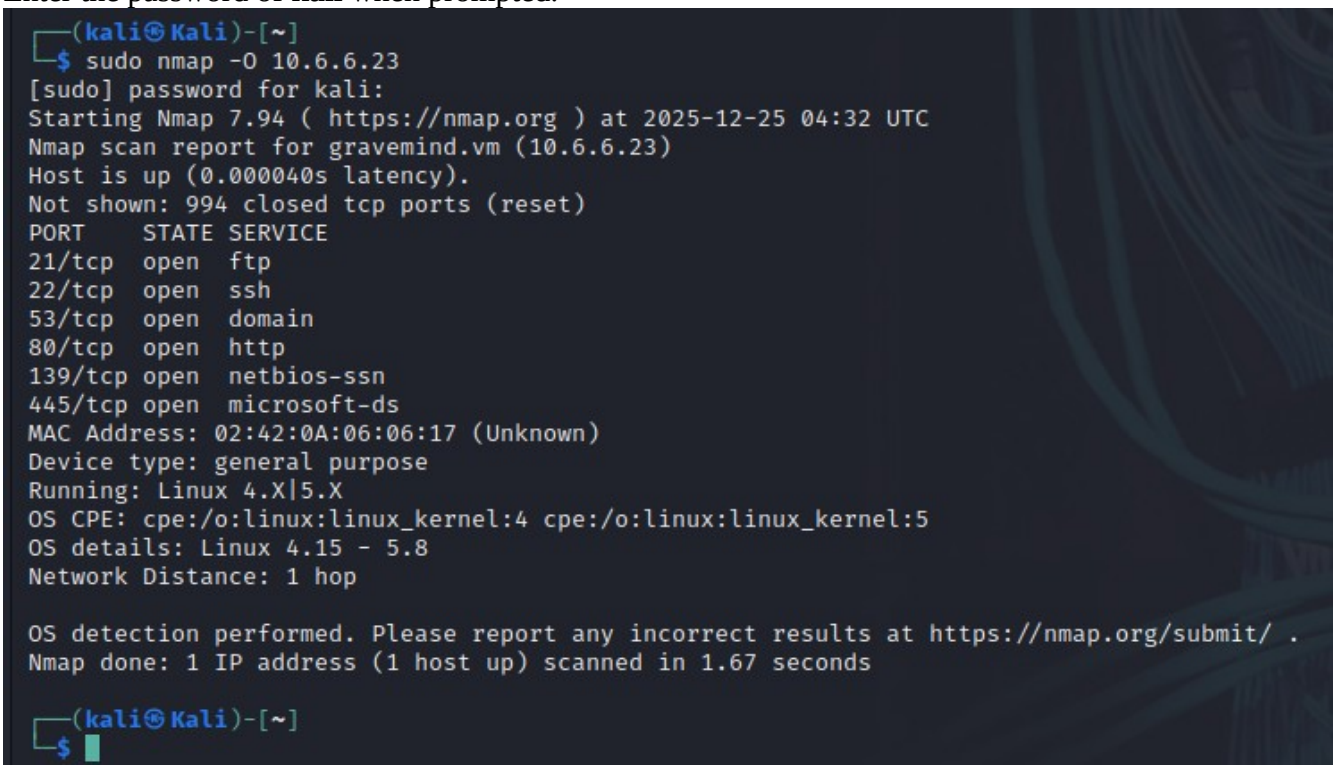


The host 10.6.6.23 was identified as suspicious in a Wireshark capture, and it is necessary to perform additional reconnaissance to discover more about the computer and its services. Use the **nmap** command to execute a default scan on the target host.

By default, Nmap performs a connect scan of 1000 most common TCP ports. This makes use of the operating system's networking software to establish a full TCP connection. This type of scan creates a lot of networking traffic and increases the probability of detection by intrusion detection services. You can also specify a TCP connect scan using the command option **nmap -sT**.
The output of the connect scan includs the status codes shown below:

Status	Response Received	Interpretation
Open	TCP SYN-ACK	There is a service listening on the identified port.
Closed	TCP RST	There is no service listening on the identified port.
Filtered	No response, or an ICMP destination unreachable message received.	The port is being filtered by a firewall.

The **-O** option can be used to further determine information about the operating system running on the target host. Some Nmap options require additional permissions and must be run as **root** or using the **sudo** command. To find operating system information on the target host, use the **nmap -O** command. Enter the password of **kali** when prompted.



Step 2: Obtain additional information about the host and services.

a. To provide additional information about the target computer, it is possible to combine different options into a single command line. The previous command identified several potentially open ports on the 10.6.6.23 host. You can use **-v**, **-p**, and **-sV** to find additional information about the services running on the open ports. This command provides information about the FTP service running on port 21 on the target in verbose mode, with the timing set to fast (**-T4**):

```
┌──(kali㉿Kali)-[~]
└─$ nmap -v -p21 -sV -T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-25 04:35 UTC
Nmap wishes you a merry Christmas! Specify -sX for Xmas Scan (https://nmap.org/book/man-port-scanning-techniques.html).
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 04:35
Scanning 10.6.6.23 [2 ports]
Completed Ping Scan at 04:35, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 04:35
Scanning gravemind.vm (10.6.6.23) [1 port]
Discovered open port 21/tcp on 10.6.6.23
Completed Connect Scan at 04:35, 0.00s elapsed (1 total ports)
Initiating Service scan at 04:35
Scanning 1 service on gravemind.vm (10.6.6.23)
Completed Service scan at 04:35, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 10.6.6.23.
Initiating NSE at 04:35
Completed NSE at 04:35, 0.00s elapsed
Initiating NSE at 04:35
Completed NSE at 04:35, 0.00s elapsed
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00017s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

┌──(kali㉿Kali)-[~]
└─$
```

The **-A** option executes OS detection, version detection, script scanning, and traceroute. The **-A** scan can be very intrusive and therefore will be detected by many IDS systems, so ensure that you have permission before attempting this scan outside of the lab environment. To gather more information regarding the FTP service, enter the command **nmap -p21 -sV -A 10.6.6.23**.

The sample detailed output of this command is shown below:

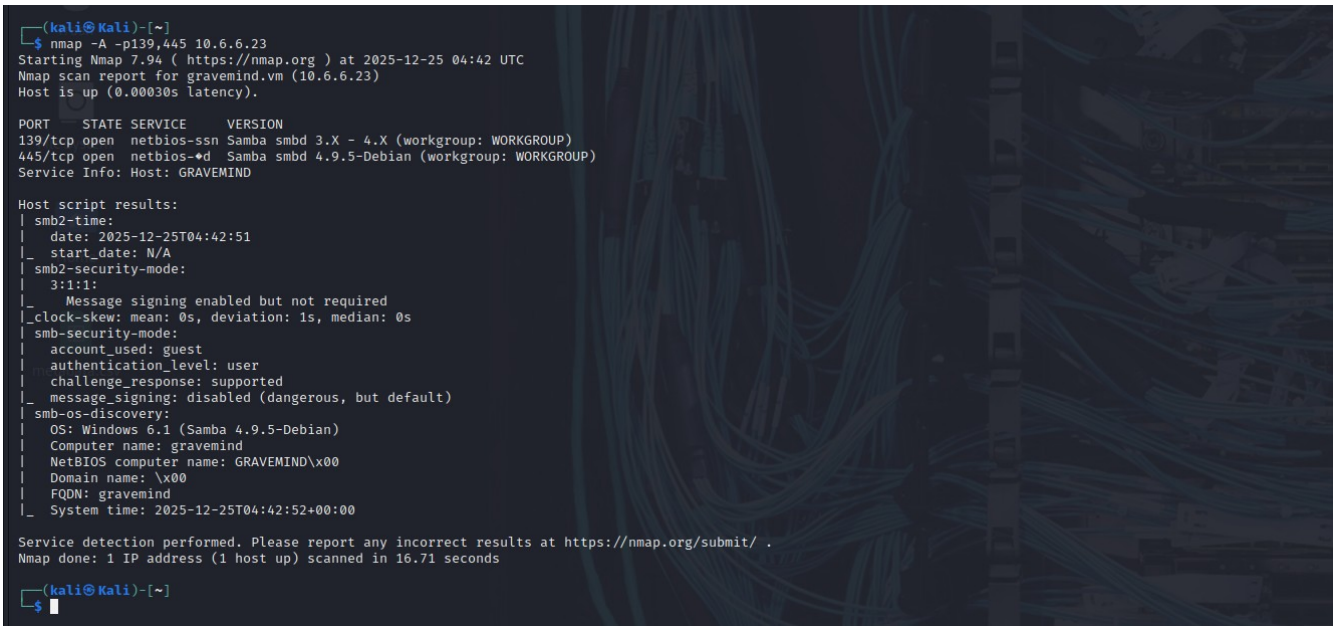
```
┌──(kali㉿Kali)-[~]
└─$ nmap -p21 -sV -A 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-25 04:37 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.6.6.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              16 Aug 13  2021 file1.txt
| -rw-r--r--    1 0        0              16 Aug 13  2021 file2.txt
| -rw-r--r--    1 0        0              29 Aug 13  2021 file3.txt
|_-rw-r--r--    1 0        0              26 Aug 13  2021 supersecretfile.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds

┌──(kali㉿Kali)-[~]
└─$
```

Examine the output of the **nmap -A** command. Notice that the output indicates that a connection was made between the Kali Linux system and the target FTP service. How many files on the FTP server are accessible through this connection? **4 text files**
What weakness in the FTP server configuration enabled the Kali Linux system to log into the FTP server? **The FTP server is configured to permit anonymous logins.**

Step 3: Investigate SMB Services with Scripts

The Server Message Block (SMB) protocol is a network file sharing protocol supported on Windows computers and by SAMBA on Linux. SMB enables applications to read and write files or request services over a network. Open public shares or shared devices such as print servers on a network, can be accessed through SMB.

a. The earlier scan of open ports on the target computer indicates that the SMB ports 139 and 445 are open. Find more information on these ports using the **-A** and **-p** command options. The **-A** option executes several functions including running the default scripts. Specify more than one port to scan by listing them separately with a comma between them.



Examine the information returned by the Nmap scan. From this information, it can be determined that the target computer is a member of the default workgroup, named WORKGROUP, and that SMB supported on this host through SAMBA on Linux.

What is the NetBIOS computer name assigned to the target host? **GRAVEMIND\x00**

Nmap contains the powerful Nmap Scripting Engine (NSE), which enables the programming of various Nmap options and conditional actions to be taken as a result of the responses. NSE has built-in scripts that enumerate users, groups, and network shares. One of the more commonly used scripts for SMB discovery is the **smb-enum-users.nse** script. Use the Nmap NSE script with the command:

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-users.nse -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-25 04:46 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00014s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   GRAVEMIND\arbiter (RID: 1001)
|     Full name:
|     Description:
|     Flags:       Password not required, Account disabled, Normal user account
|   GRAVEMIND\masterchief (RID: 1000)
|     Full name:
|     Description:
|_    Flags:       Password not required, Account disabled, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

┌──(kali㉿Kali)-[~]
└─$
```

Did the script uncover any SMB usernames on the target host? If so, how many? **Yes, 2 usernames: arbiter and masterchief.**

A serious security concern is the existence of publicly shared directories (folders). You can enumerate the network shares using another NSE script, **smb-enum-shares.nse.** To discover shared directories on the target computer. Use the Nmap share enumeration script with the command:

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-25 04:48 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.6.6.23\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.5-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\workfiles:
|     Type: STYPE_DISKTREE
|     Comment: Confidential Workfiles
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\spool\samba
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 7.71 seconds

┌──(kali㉿Kali)-[~]
└─$
```

Examine the output created by the **smb-enum-shares** script. In the output, share names that end with a "$" character represent hidden shares that include system and administrative shares. How many hidden shares were discovered on the target host? **2**

What serious security risk is uncovered in this script output? **Anonymous access: READ/WRITE.**

N/B
Nmap scans can be used to identify active devices on a network. The basic scans will uncover open ports and services that may need to be secured. Anonymous access to FTP files or network shares can be detected and corrected or limited. Malicious actors can use these same functions to find computers that may be vulnerable to attack.