Laboratory Exercise 4.1 – Advanced Port Scanning

1. Overview

In this lab, students will learn how Metasploit and Nmap can be combined to streamline the scanning process. Students will learn how to find open ports, how to find the services running on those ports, how to further enumerate discovered ports, and how to save the results for reporting. Students will use the latest Cyber Range: Kali Linux with Metasploitable Environment for this lab to perform port scanning and enumeration.

2. Resources Required

This exercise requires the latest Kali Linux with Metasploitable3 Environment running in the Cyber Range.

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Environment: Kali Linux with Metasploitable3, then click "start" to start your environment and "join" to get to your Linux desktop login. Log in using these credentials:

Username: **student**
Password: **student**

4. Tasks [Knowledge of Nmap and Networking protocols is essential]

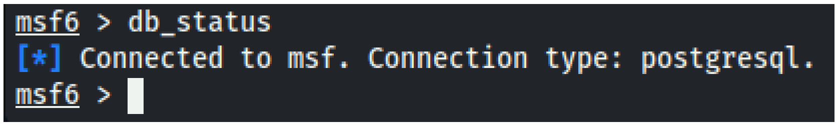
Task 1: Advanced command line scanning with Nmap and Metasploit

Review and refer to the following Nmap cheat sheets during this lab:

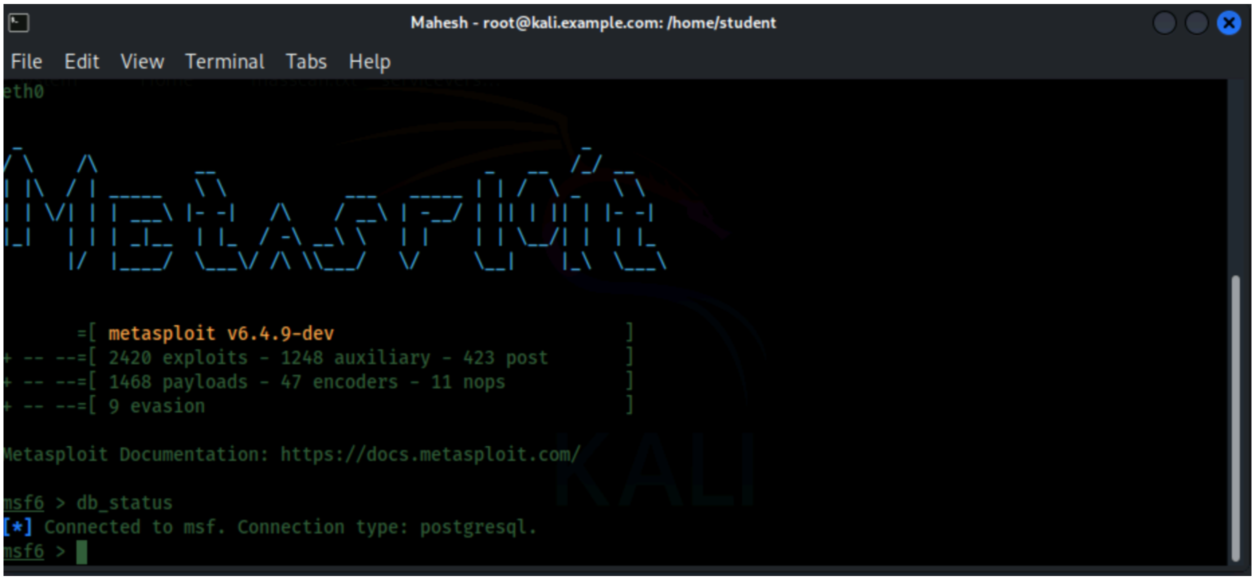
- cheatsheet from SANS
- StationX

Complete the following:

1. Open a terminal window.
2. Type **`sudo su`** to become root.
3. Type **`service postgresql start`** since Metasploit uses the PostgreSQL database.
4. Type **`msfdb init`** to initialize the Metasploit database.
5. Type **`msfconsole`** to start the Metasploit framework.
6. Type **`db_status`** to verify that the database has connectivity. You should see the "[*] postgresql connected to msf" message as displayed in the image below.



```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > 
```



Mahesh - root@kali.example.com: /home/student
File Edit View Terminal Tabs Help

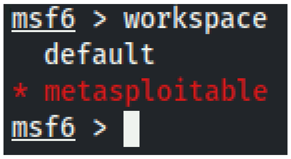
```
eth0

       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > 
```

If the database does not have connectivity or you accidentally started the framework before starting the database, exit out of the terminal and repeat steps 1, 2, 5, and 6. This should do the trick. If for some reason it does not, exit out of the terminal and complete steps 1-6 again.

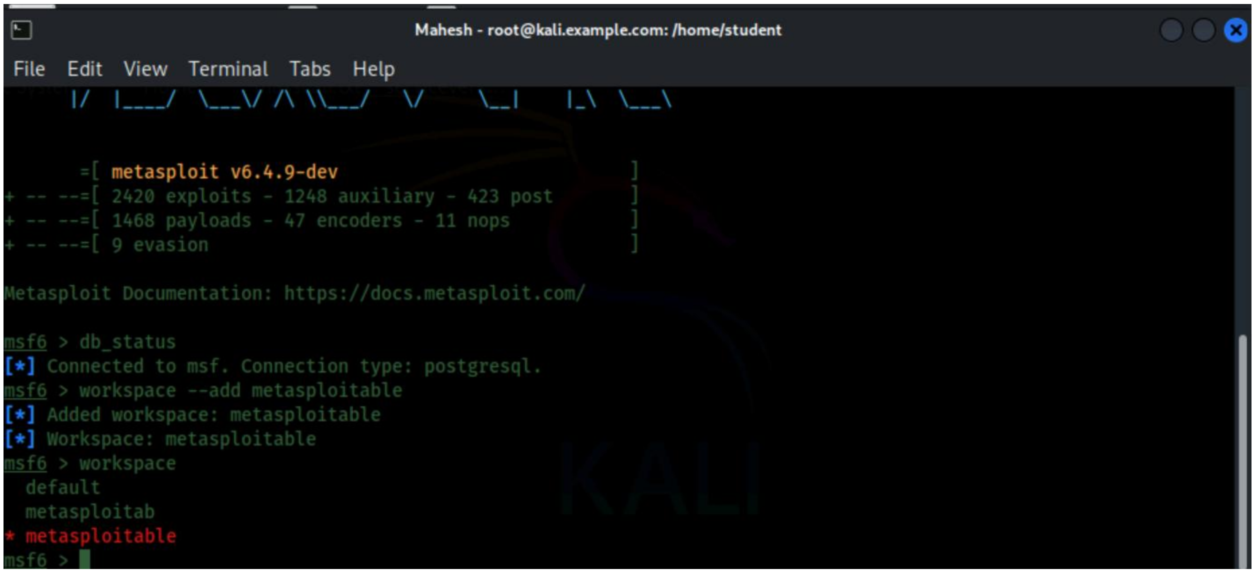
Before we start scanning, we want to create a workspace for our scans. This will make it easier to find the scans at a later time when we complete our reports. It will also prevent the issue of polluting the database when we need to work on more than one project.

Complete the following:

1. Type **`workspace --add metasploitable`** and press enter.
2. Type **`workspace`** to verify you are working in the metasploitable workspace. There will be an asterisk followed by the word “metasploitable” in red font as you see in the below image.

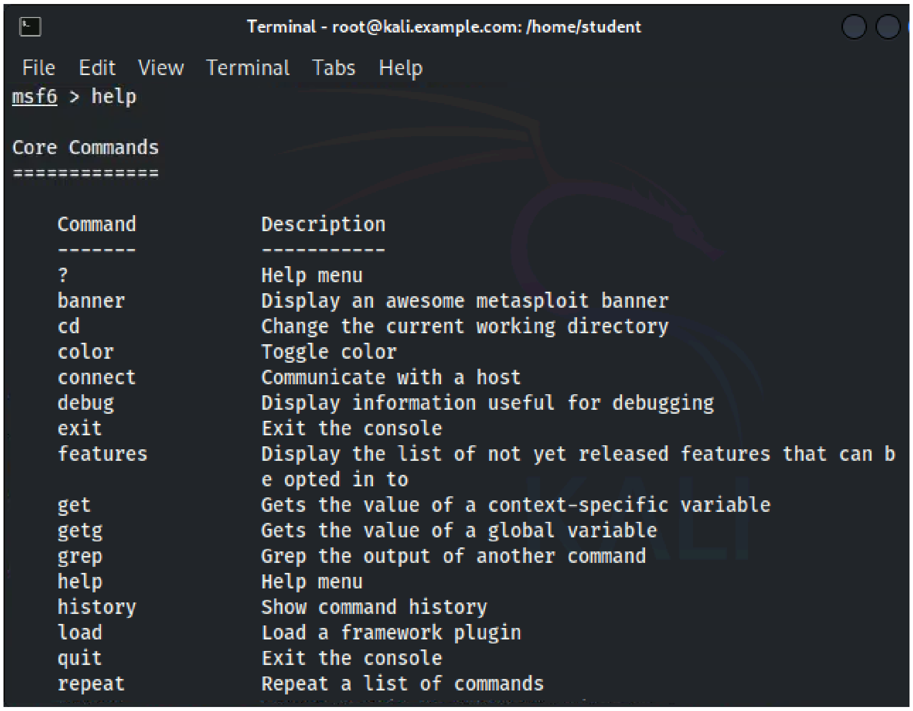


```
msf6 > workspace
  default
* metasploitable
msf6 > 
```

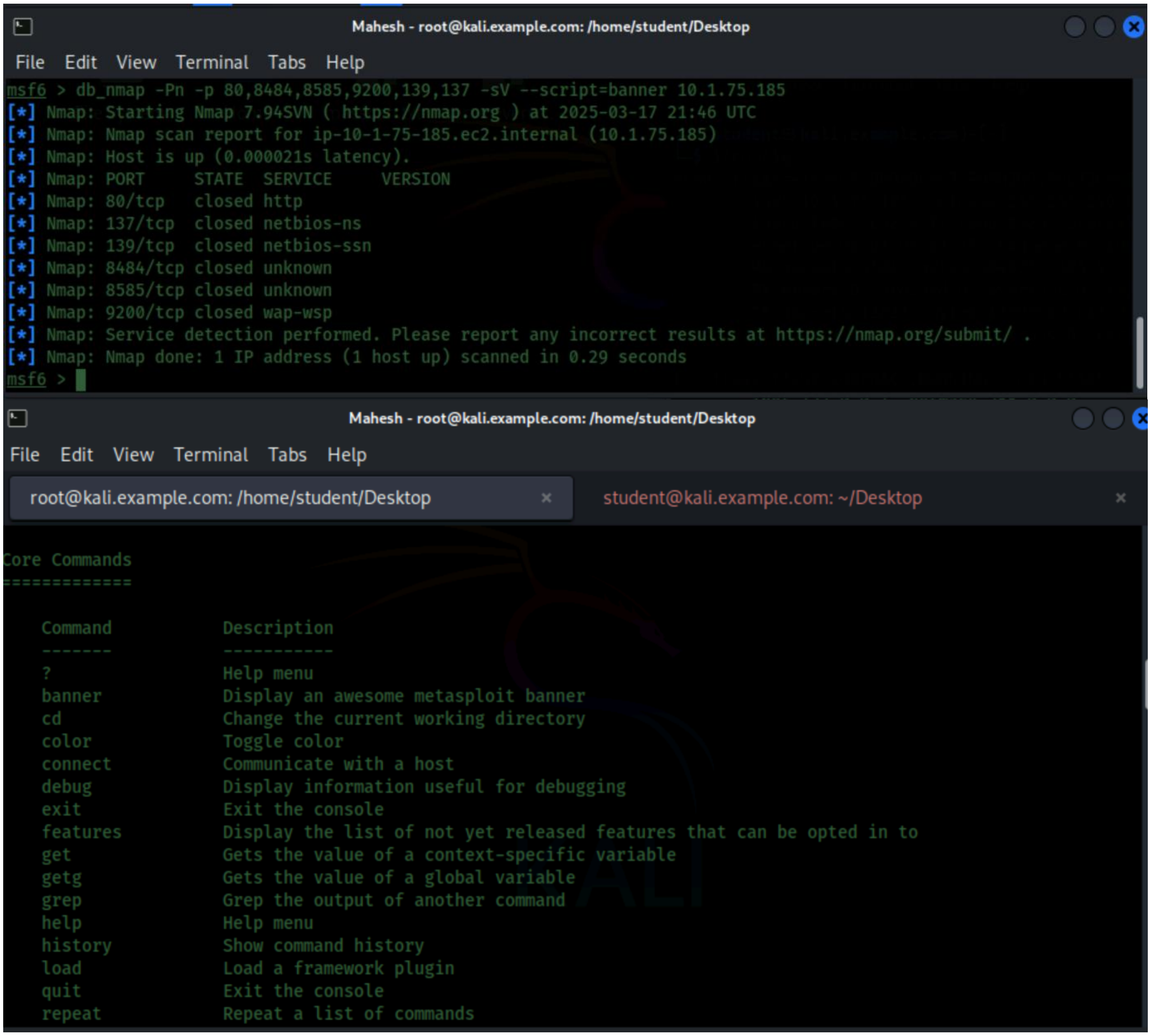

Mahesh - root@kali.example.com: /home/student
File Edit View Terminal Tabs Help

```
   |/  |___/  \___\/ /\ \\___/   \/    \__|   |_\  \___\


       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace --add metasploitable
[*] Added workspace: metasploitable
[*] Workspace: metasploitable
msf6 > workspace
  default
  metasploitab
* metasploitable
msf6 > 
```

We have now created our very own workspace. Our scans will be saved automatically in the workspace. To check the Database Backend Commands, type **help**.


Terminal - root@kali.example.com: /home/student
File Edit View Terminal Tabs Help

```
msf6 > help

Core Commands
=============

    Command           Description
    -------           -----------
    ?                 Help menu
    banner            Display an awesome metasploit banner
    cd                Change the current working directory
    color             Toggle color
    connect           Communicate with a host
    debug             Display information useful for debugging
    exit              Exit the console
    features          Display the list of not yet released features that can b
                      e opted in to
    get               Gets the value of a context-specific variable
    getg              Gets the value of a global variable
    grep              Grep the output of another command
    help              Help menu
    history           Show command history
    load              Load a framework plugin
    quit              Exit the console
    repeat            Repeat a list of commands
```


Mahesh - root@kali.example.com: /home/student/Desktop
File Edit View Terminal Tabs Help

```
msf6 > db_nmap -Pn -p 80,8484,8585,9200,139,137 -sV --script=banner 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 21:46 UTC
[*] Nmap: Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
[*] Nmap: Host is up (0.000021s latency).
[*] Nmap: PORT     STATE  SERVICE     VERSION
[*] Nmap: 80/tcp   closed http
[*] Nmap: 137/tcp  closed netbios-ns
[*] Nmap: 139/tcp  closed netbios-ssn
[*] Nmap: 8484/tcp closed unknown
[*] Nmap: 8585/tcp closed unknown
[*] Nmap: 9200/tcp closed wap-wsp
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
msf6 >
```

Mahesh - root@kali.example.com: /home/student/Desktop
File Edit View Terminal Tabs Help
root@kali.example.com: /home/student/Desktop
student@kali.example.com: ~/Desktop

```
Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    features      Display the list of not yet released features that can be opted in to
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
```

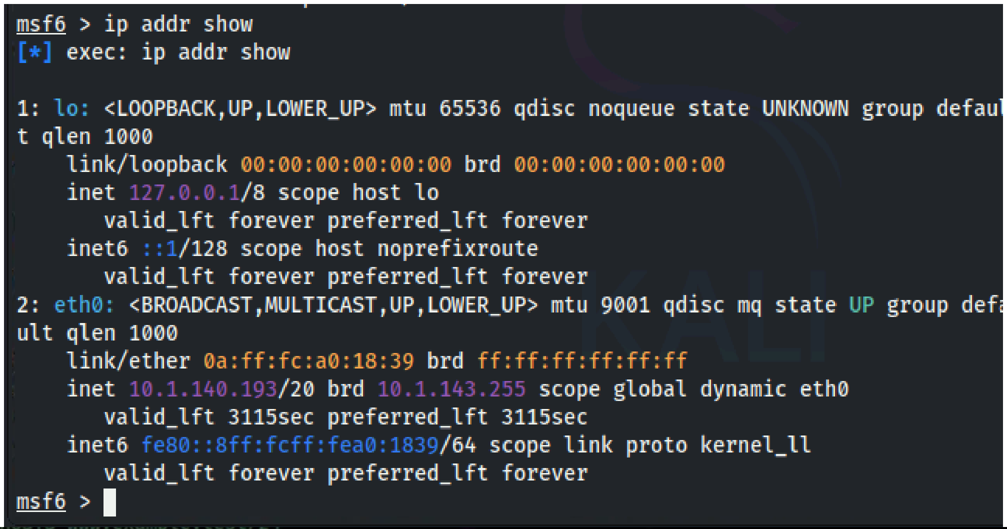
Take notice of the **hosts**, **services**, and **notes**. We will be calling on these when we write reports or when we pick up where we left off. This way we do not have to complete the scans again. They are all saved in the workspace database.

Now we are ready to start scanning the system. There are several ways to discover hosts. Different tactics are used if ports are filtered. We are trying to find a specific target holding the Metasploitable 3 content. Below are several ways to complete the task. Try them all if time permits. We will start with a few simple commands and scans first as a brief refresher.

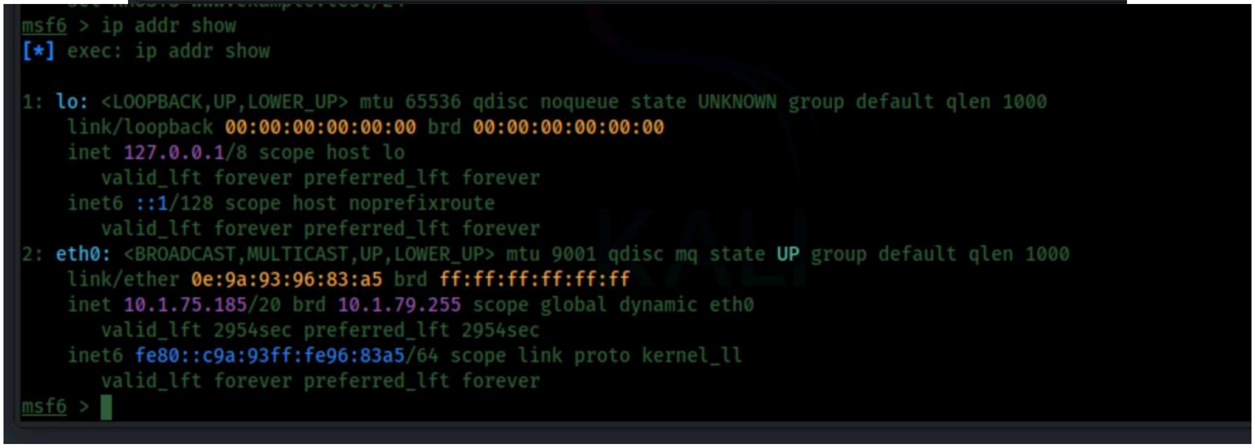
Complete the following:

1. Type **`ip addr show`** to discover your current network configurations.

2. Write down in the space provided or take note of your IP: ______________________________.



```
msf6 > ip addr show
[*] exec: ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group defa
ult qlen 1000
    link/ether 0a:ff:fc:a0:18:39 brd ff:ff:ff:ff:ff:ff
    inet 10.1.140.193/20 brd 10.1.143.255 scope global dynamic eth0
       valid_lft 3115sec preferred_lft 3115sec
    inet6 fe80::8ff:fcff:fea0:1839/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
msf6 >
```



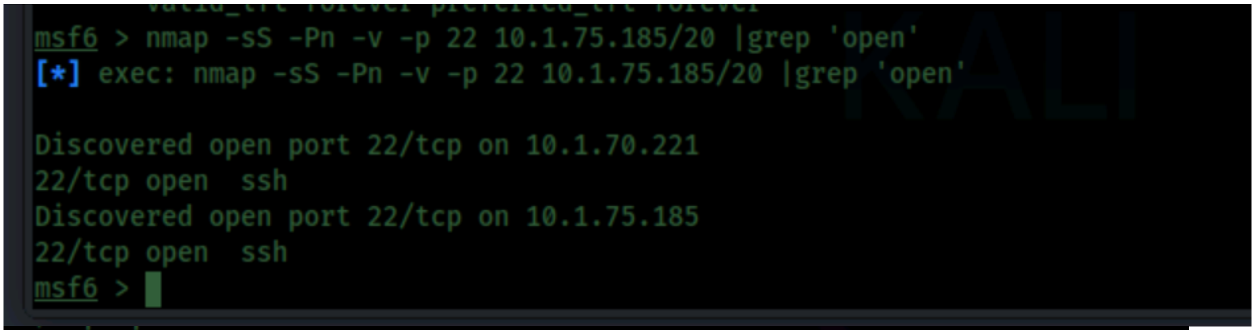
```
msf6 > ip addr show
[*] exec: ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0e:9a:93:96:83:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.1.75.185/20 brd 10.1.79.255 scope global dynamic eth0
       valid_lft 2954sec preferred_lft 2954sec
    inet6 fe80::c9a:93ff:fe96:83a5/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
msf6 >
```

-

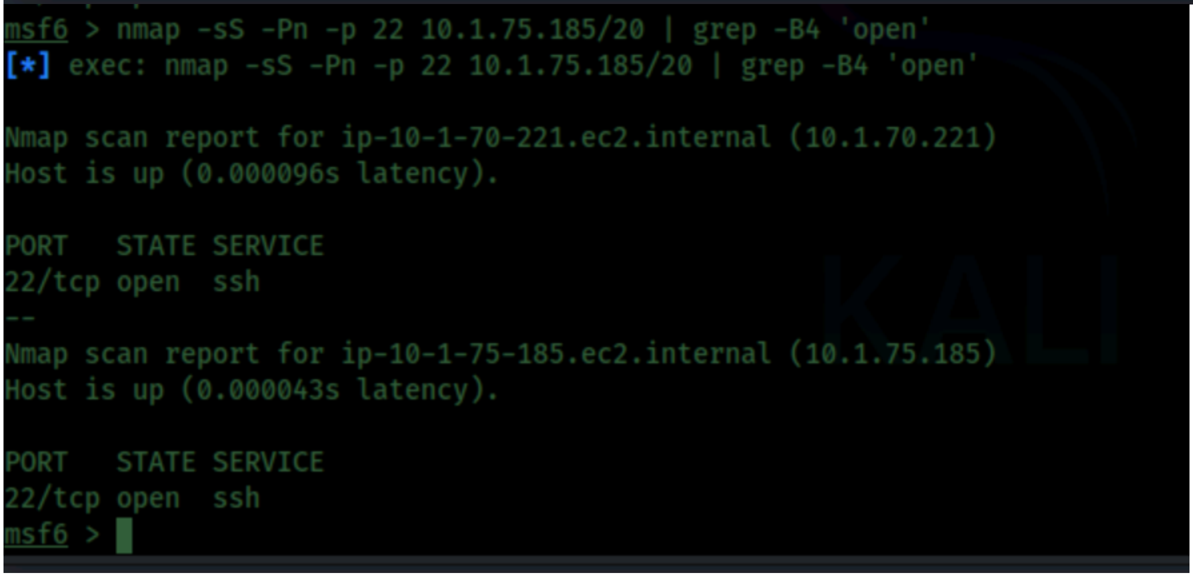
This is our machine, but we have also discovered the subnet with this tactic. In future scans, we don't want to scan ourselves. We can exclude this machine with **--exclude <ip address>** in our scans. It is a good idea to remember this as in many situations your host will have many ports and services that can be found. Thus, polluting the results. Take a screenshot and name it *1ipaddrshow*. Save it in a folder named scanning.

The following commands will help you find the target Metasploitable machine. Open a new terminal window and become root. Type the following:

```
nmap -sS -Pn -v -p 22 10.1.75.185/20 | grep 'open'

nmap -sS -Pn -p 22 10.1.75.185/20 | grep -B4 'open'
```



```
    valid_lft forever preferred_lft forever
msf6 > nmap -sS -Pn -v -p 22 10.1.75.185/20 |grep 'open'
[*] exec: nmap -sS -Pn -v -p 22 10.1.75.185/20 |grep 'open'

Discovered open port 22/tcp on 10.1.70.221
22/tcp open  ssh
Discovered open port 22/tcp on 10.1.75.185
22/tcp open  ssh
msf6 >
```



```
msf6 > nmap -sS -Pn -p 22 10.1.75.185/20 | grep -B4 'open'
[*] exec: nmap -sS -Pn -p 22 10.1.75.185/20 | grep -B4 'open'

Nmap scan report for ip-10-1-70-221.ec2.internal (10.1.70.221)
Host is up (0.000096s latency).

PORT   STATE SERVICE
22/tcp open  ssh
--
Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
Host is up (0.000043s latency).

PORT   STATE SERVICE
22/tcp open  ssh
msf6 >
```

Write down the IP address or copy and paste it into your notes

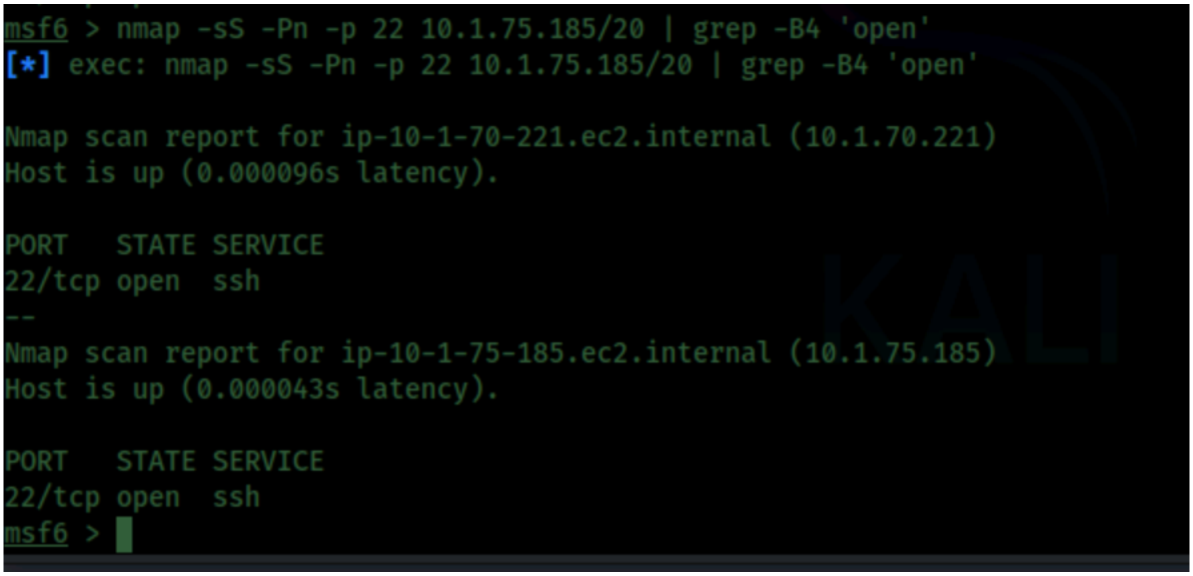
The reason this works is because we disable ping, and know that port 22 is open only on a few machines. The /20 scans the subnet but it is much faster if we only scan port 22. The first command shows verbosity (the amount that is printed to the display while the command is running) pipes that into grep, and searches for "open " ones. The second command drops verbose and adds -B4 which shows the 4 lines before the regex match. Scanning the entire subnet with -p- will take about 20 minutes. Whereas, the other scans take about 10 seconds. You can streamline your pen-testing processes by knowing more about powerful Linux tools like grep and Nmap.

Answer the following questions:

1. What is the host IP on the Metasploitable machine (every student will have a different IP)?

10.1.75.185

2. Take a screenshot of the results name it *2target* and save it in the scanning folder.



```
msf6 > nmap -sS -Pn -p 22 10.1.75.185/20 | grep -B4 'open'
[*] exec: nmap -sS -Pn -p 22 10.1.75.185/20 | grep -B4 'open'

Nmap scan report for ip-10-1-70-221.ec2.internal (10.1.70.221)
Host is up (0.000096s latency).

PORT   STATE SERVICE
22/tcp open  ssh
--
Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
Host is up (0.000043s latency).

PORT   STATE SERVICE
22/tcp open  ssh
msf6 >
```

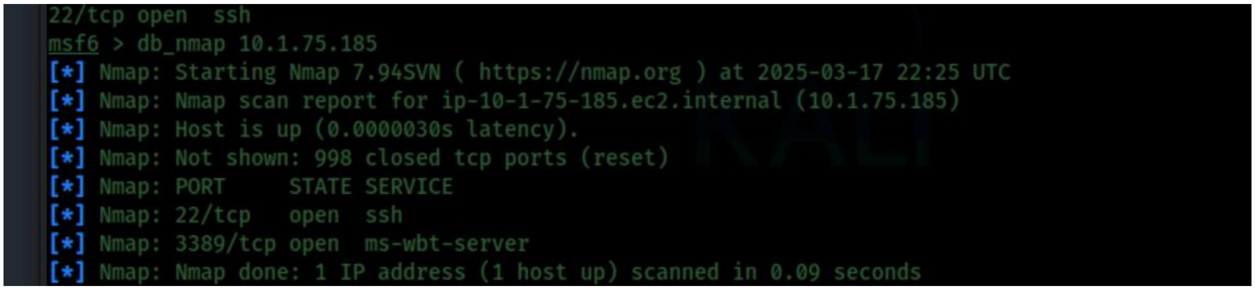
Task 2: Discovering open ports and services with Metasploit and Nmap

Return to the terminal window with the Metasploit Framework running, at the msf6> prompt complete the following:

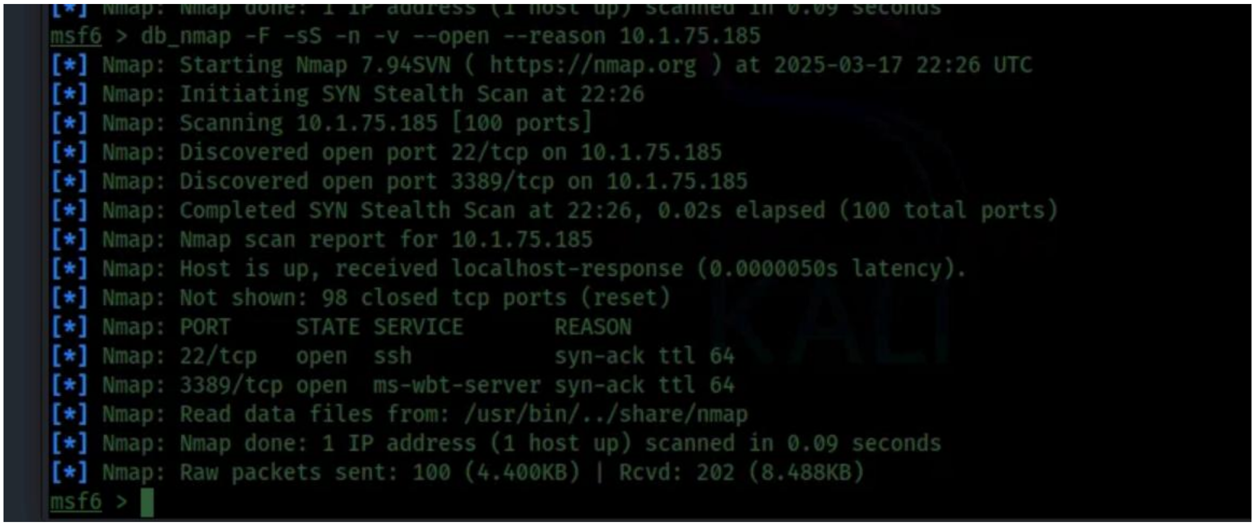
[IMPORTANT: This VM's Metasploitable IP is 10.1.130.245; everywhere you see this replace it with your Metasploitable IP.]

1. Type **`db_nmap`** `10.1.75.185` and press enter.

2. Type **`db_nmap -F -sS -n -v --open --reason`** `10.1.75.185` and press enter.



```
22/tcp open  ssh
msf6 > db_nmap 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:25 UTC
[*] Nmap: Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
[*] Nmap: Host is up (0.0000030s latency).
[*] Nmap: Not shown: 998 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 3389/tcp open  ms-wbt-server
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```



```
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
msf6 > db_nmap -F -sS -n -v --open --reason 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:26 UTC
[*] Nmap: Initiating SYN Stealth Scan at 22:26
[*] Nmap: Scanning 10.1.75.185 [100 ports]
[*] Nmap: Discovered open port 22/tcp on 10.1.75.185
[*] Nmap: Discovered open port 3389/tcp on 10.1.75.185
[*] Nmap: Completed SYN Stealth Scan at 22:26, 0.02s elapsed (100 total ports)
[*] Nmap: Nmap scan report for 10.1.75.185
[*] Nmap: Host is up, received localhost-response (0.0000050s latency).
[*] Nmap: Not shown: 98 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE       REASON
[*] Nmap: 22/tcp   open  ssh           syn-ack ttl 64
[*] Nmap: 3389/tcp open  ms-wbt-server syn-ack ttl 64
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[*] Nmap: Raw packets sent: 100 (4.400KB) | Rcvd: 202 (8.488KB)
msf6 >
```

,m

Command breakdown:

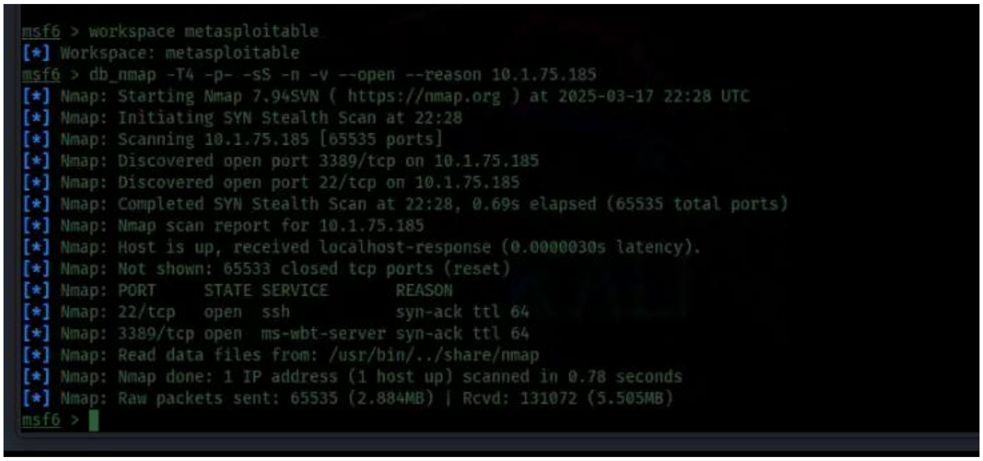
- **-F** is a fast scan of the top 100 ports
- **-sS** is a syn scan or TCP port scan
- **-n** for host discovery; do not resolve DNS
- **-v** This increases the verbosity level (how much is printed to your display) use –vv for greater effect
- **--reason** this will output the reason a port is in its current state
- **--open** this will show only open ports

To view current host results stored in your workspace type **hosts.**
To view the current services stored in your workspace type **services.**

We could scan for all the ports on the host instead of only the top 100 by using a **-p-** instead of **-F**; however, this would take some time. Note that the environment in the Cyber Range is always changing. If this scan takes too long, it can be terminated early with CTRL+c. If this is the case, you may not be able to answer the questions.

Open a new terminal window and complete the following:

1. Type **sudo su** and press enter.
2. Type **msfconsole** and press enter.
3. Type **workspace metasploitable** and press enter.
4. Type **db_nmap -T4 -p- -sS -n -v --open --reason <target IP>** and press enter.



```
msf6 > workspace metasploitable
[*] Workspace: metasploitable
msf6 > db_nmap -T4 -p- -sS -n -v --open --reason 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:28 UTC
[*] Nmap: Initiating SYN Stealth Scan at 22:28
[*] Nmap: Scanning 10.1.75.185 [65535 ports]
[*] Nmap: Discovered open port 3389/tcp on 10.1.75.185
[*] Nmap: Discovered open port 22/tcp on 10.1.75.185
[*] Nmap: Completed SYN Stealth Scan at 22:28, 0.69s elapsed (65535 total ports)
[*] Nmap: Nmap scan report for 10.1.75.185
[*] Nmap: Host is up, received localhost-response (0.0000030s latency).
[*] Nmap: Not shown: 65533 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE       REASON
[*] Nmap: 22/tcp   open  ssh           syn-ack ttl 64
[*] Nmap: 3389/tcp open  ms-wbt-server syn-ack ttl 64
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
[*] Nmap: Raw packets sent: 65535 (2.884MB) | Rcvd: 131072 (5.505MB)
msf6 >
```

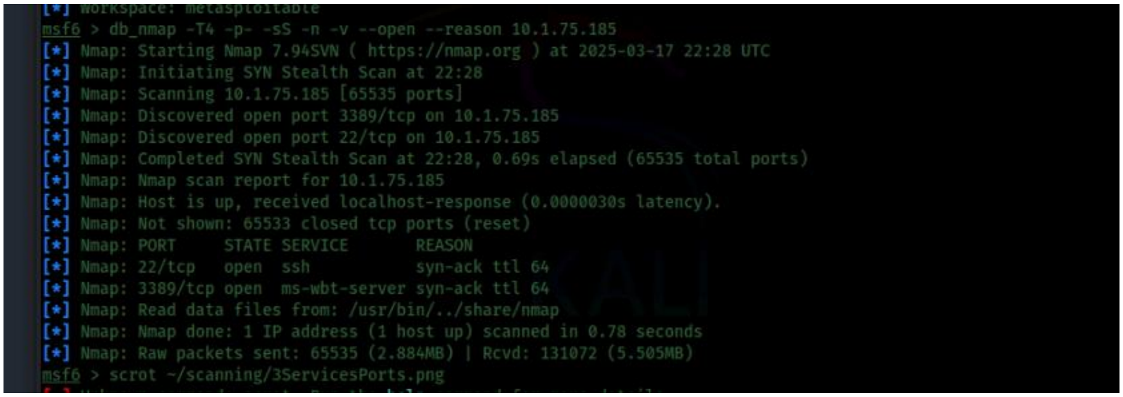
Now we can continue with other scans while this one scans in the background.

Answer the following questions:

1. What services did you find and what ports were running?

   SSH on port 22/tcp
   Microsoft SQL Server (ms-wbt-server) on port 3339/tcp

2. Take a screenshot of the results name it *3ServicesPorts* and save it in the scanning folder.



```
[*] Workspace: metasploitable
msf6 > db_nmap -T4 -p- -sS -n -v --open --reason 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:28 UTC
[*] Nmap: Initiating SYN Stealth Scan at 22:28
[*] Nmap: Scanning 10.1.75.185 [65535 ports]
[*] Nmap: Discovered open port 3389/tcp on 10.1.75.185
[*] Nmap: Discovered open port 22/tcp on 10.1.75.185
[*] Nmap: Completed SYN Stealth Scan at 22:28, 0.69s elapsed (65535 total ports)
[*] Nmap: Nmap scan report for 10.1.75.185
[*] Nmap: Host is up, received localhost-response (0.0000030s latency).
[*] Nmap: Not shown: 65533 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE       REASON
[*] Nmap: 22/tcp   open  ssh           syn-ack ttl 64
[*] Nmap: 3389/tcp open  ms-wbt-server syn-ack ttl 64
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
[*] Nmap: Raw packets sent: 65535 (2.884MB) | Rcvd: 131072 (5.505MB)
msf6 > scrot ~/scanning/3ServicesPorts.png
```

Task 3: Run a UDP scan using Metasploit and Nmap

If there were an SNMP (Simple Network Management Protocol), NetBIOS, or ISAKMP/IKE service running, performing a UDP scan can discover this. The switch -sU is a UDP scan.

Complete the following:

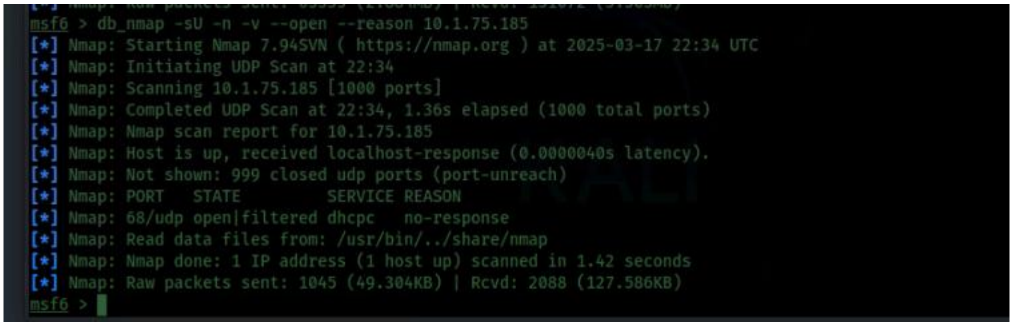
1. Type **`db_nmap -sU -n -v --open --reason <target IP>`** and press enter.

Answer the following questions:

1. What services did you find?

68/udp open|filtered dhcpc. The service associated with this port **is dhcpc** but there is no response from the service,nmap couldn't confirm whether it is truly open or filtered by firewall.

2. Take a screenshot of the results and name it appropriately.



```
msf6 > db_nmap -sU -n -v --open --reason 10.1.75.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:34 UTC
[*] Nmap: Initiating UDP Scan at 22:34
[*] Nmap: Scanning 10.1.75.185 [1000 ports]
[*] Nmap: Completed UDP Scan at 22:34, 1.36s elapsed (1000 total ports)
[*] Nmap: Nmap scan report for 10.1.75.185
[*] Nmap: Host is up, received localhost-response (0.0000040s latency).
[*] Nmap: Not shown: 999 closed udp ports (port-unreach)
[*] Nmap: PORT   STATE         SERVICE REASON
[*] Nmap: 68/udp open|filtered dhcpc   no-response
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
[*] Nmap: Raw packets sent: 1045 (49.304KB) | Rcvd: 2088 (127.586KB)
msf6 >
```

Task 4: Service Version Scanning

Before we continue, we want to get more information on the services that are running. The switch **-sV** will search for service versions, and the **-sC** will use default scripts (OS detection, service, fragmentation) and is considered invasive. You can view the default scripts here.

Complete the following:

1. Type **`db_nmap -sS -sV -sC -v -n -p <list of ports found> <target IP>`** and press enter.
2. My Example: **`db_nmap -sS -sV -sC -v -n -p 21,22,80,445,631,3000,3306,8181,3389,8484,8585,9200,49153,49202,49203 10.1.163.125`**

Answer the following questions:

1. What new information was discovered?

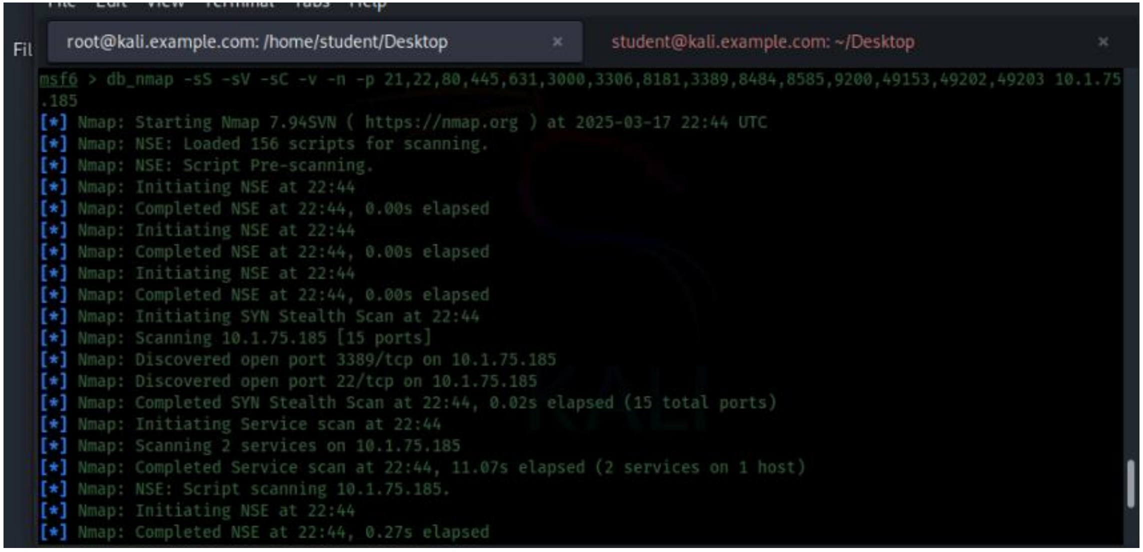
The scan found two open ports on 10.1.75.185:

Port 22/tcp → Open SSH service (OpenSSH 9.7p1 Debian 5, Protocol 2.0)
Port 3389/tcp → Open Remote Desktop Protocol (RDP)

Other ports that were scanned (21, 80, 445, 631, 3000, 3306, 8181, 8484, 8585, 9200, 49153, 49202, 49203) were closed.

The system is running Linux OS (CPE: o:linux:linux_kernel).

2. Take a screenshot of the results and name it appropriately.


Fil
root@kali.example.com: /home/student/Desktop
student@kali.example.com: ~/Desktop

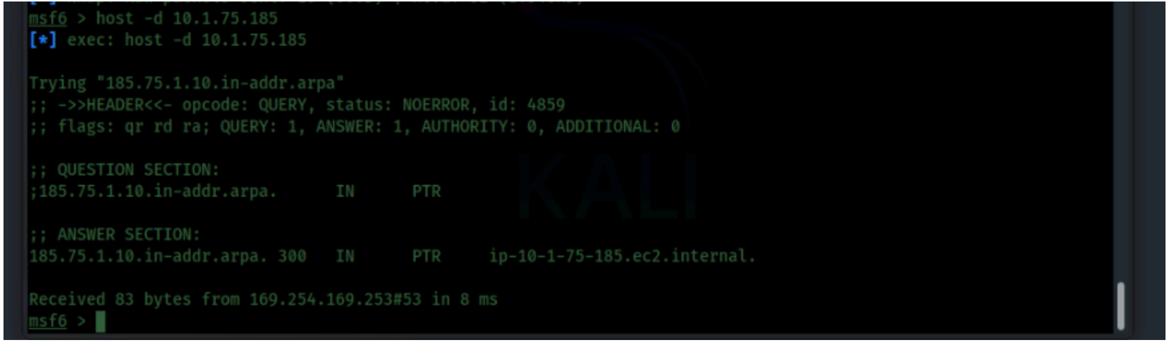
```
msf6 > db_nmap -sS -sV -sC -v -n -p 21,22,80,445,631,3000,3306,8181,3389,8484,8585,9200,49153,49202,49203 10.1.75
.185
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 22:44 UTC
[*] Nmap: NSE: Loaded 156 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 22:44
[*] Nmap: Completed NSE at 22:44, 0.00s elapsed
[*] Nmap: Initiating NSE at 22:44
[*] Nmap: Completed NSE at 22:44, 0.00s elapsed
[*] Nmap: Initiating NSE at 22:44
[*] Nmap: Completed NSE at 22:44, 0.00s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 22:44
[*] Nmap: Scanning 10.1.75.185 [15 ports]
[*] Nmap: Discovered open port 3389/tcp on 10.1.75.185
[*] Nmap: Discovered open port 22/tcp on 10.1.75.185
[*] Nmap: Completed SYN Stealth Scan at 22:44, 0.02s elapsed (15 total ports)
[*] Nmap: Initiating Service scan at 22:44
[*] Nmap: Scanning 2 services on 10.1.75.185
[*] Nmap: Completed Service scan at 22:44, 11.07s elapsed (2 services on 1 host)
[*] Nmap: NSE: Script scanning 10.1.75.185.
[*] Nmap: Initiating NSE at 22:44
[*] Nmap: Completed NSE at 22:44, 0.27s elapsed
```

Task 5: Cleaning up your hosts' list

So, now that we have completed several scans, we may want to clean up our hosts list. If you do not have any extra hosts, this part of the lesson is for information purposes only.

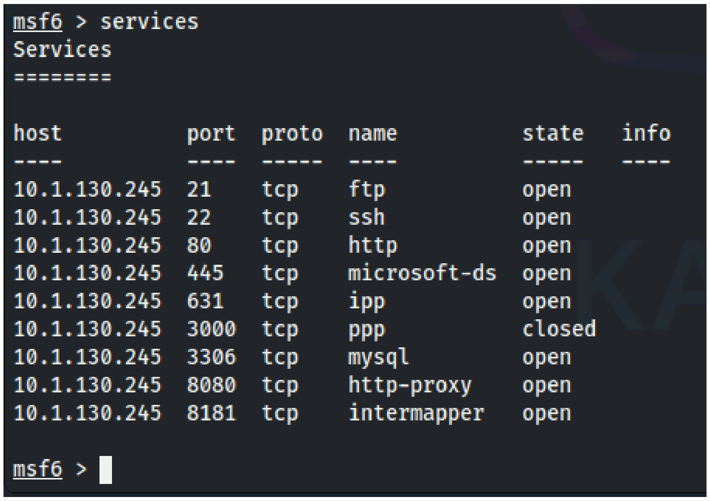
The only host we want on the list is the Metasploitable machine. To do this, we type **`hosts`** in the msfconsole to view our hosts. If we have any hosts other than our Metasploitable target, they need to be deleted.

To do this, we type **`hosts –d <host IP we want deleted>`**. Once we have deleted the hosts that are out of our scope, we should be left with only the Metasploitable host. In my case, that is 10.1.130.245. The last screenshot is of the Metasploit services database found by typing **`services`** and pressing enter in the msfconsole.

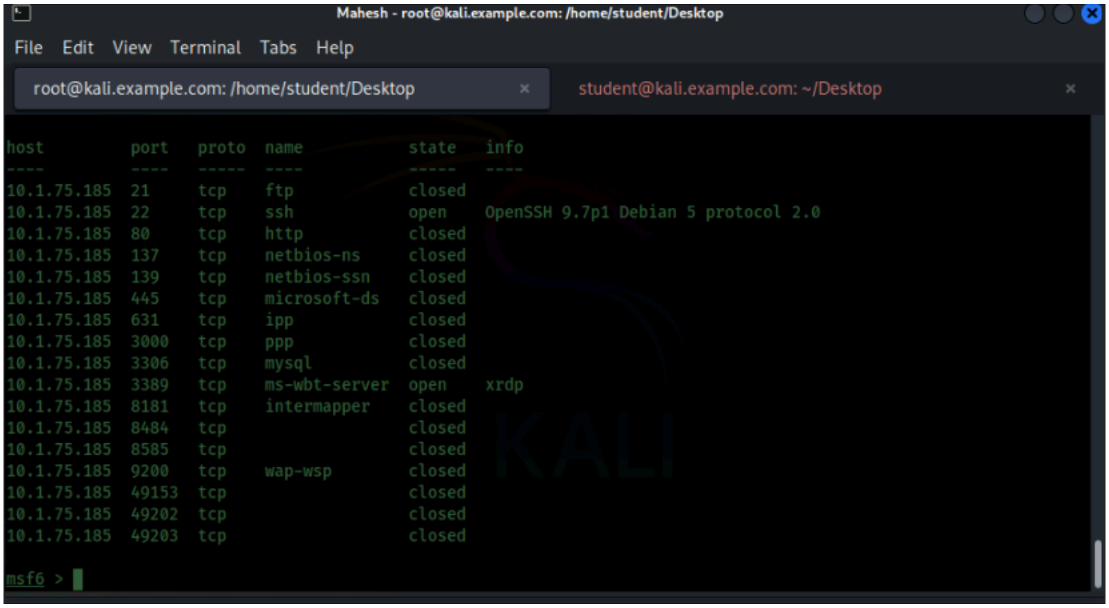


```
msf6 > host -d 10.1.75.185
[*] exec: host -d 10.1.75.185

Trying "185.75.1.10.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4859
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;185.75.1.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
185.75.1.10.in-addr.arpa. 300   IN      PTR     ip-10-1-75-185.ec2.internal.

Received 83 bytes from 169.254.169.253#53 in 8 ms
msf6 > 
```

services



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

host          port  proto  name           state   info
----          ----  -----  ----           -----   ----
10.1.130.245  21    tcp    ftp            open
10.1.130.245  22    tcp    ssh            open
10.1.130.245  80    tcp    http           open
10.1.130.245  445   tcp    microsoft-ds   open
10.1.130.245  631   tcp    ipp            open
10.1.130.245  3000  tcp    ppp            closed
10.1.130.245  3306  tcp    mysql          open
10.1.130.245  8080  tcp    http-proxy     open
10.1.130.245  8181  tcp    intermapper    open

msf6 >
```



Mahesh - root@kali.example.com: /home/student/Desktop
File Edit View Terminal Tabs Help
root@kali.example.com: /home/student/Desktop
student@kali.example.com: ~/Desktop

```
host          port   proto  name           state   info
----          ----   -----  ----           -----   ----
10.1.75.185   21     tcp    ftp            closed
10.1.75.185   22     tcp    ssh            open    OpenSSH 9.7p1 Debian 5 protocol 2.0
10.1.75.185   80     tcp    http           closed
10.1.75.185   137    tcp    netbios-ns     closed
10.1.75.185   139    tcp    netbios-ssn    closed
10.1.75.185   445    tcp    microsoft-ds   closed
10.1.75.185   631    tcp    ipp            closed
10.1.75.185   3000   tcp    ppp            closed
10.1.75.185   3306   tcp    mysql          closed
10.1.75.185   3389   tcp    ms-wbt-server  open    xrdp
10.1.75.185   8181   tcp    intermapper    closed
10.1.75.185   8484   tcp                   closed
10.1.75.185   8585   tcp                   closed
10.1.75.185   9200   tcp    wap-wsp        closed
10.1.75.185   49153  tcp                   closed
10.1.75.185   49202  tcp                   closed
10.1.75.185   49203  tcp                   closed

msf6 >
```

5. References:

https://www.aelius.com/njh/subnet_sheet.html
https://nmap.org/book/nse-usage.html
https://nmap.org/nsedoc/categories/default.html