

Laboratory Exercise C1 – Advanced Port Scanning

Due Date: 09/14/2022

Points Possible: Number of points out of total course points or recommended percent of the course grade.

1. Overview

In this lab, students will learn how Metasploit and Nmap can be used in combination 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. For this lab, students will use the Cyber Range: Environment: Kali Linux with Metasploitable (2020.09) environment to perform port scanning and enumeration.

2. Resources Required

This exercise requires a Kali Linux VM running in the Cyber Range.

[Note to instructors: This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Environment: Kali Linux with Metasploitable (2020.09), 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

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 on the below image.

Term: (Fall, Spring, Summer, Winter) 20XX

```
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```

```
Nathaly Flores - student...  
Nathaly Flores - student@kali: ~  
  
File Edit View Terminal Tabs Help  
student@kali:~$ sudo su  
root@kali:/home/student# service postgresql  
Usage: /etc/init.d/postgresql {start|stop|restart|reload|force-reload|status} [version ..]  
root@kali:/home/student# msfdb init  
[+] Starting database  
[+] Creating database user 'msf'  
[+] Creating databases 'msf'  
[+] Creating databases 'msf_test'  
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'  
[+] Creating initial database schema  
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:98: warning: method call without arguments, it always returns nil  
root@kali:/home/student# msfconsole
```

A large, faint watermark logo of Kali Linux is visible across the terminal window.

```
.~+P~~~~~-0+:.  
.+oooyssyyssydyddh++os-----  
+++++++sydhoyso/:.````....-///:+ohhyosyysy+/om++:ooo//o  
++++/////~~/+++++oooysoyosso+++++/////oossosy  
--.'-.---:///+++++////////~////////+++++/  
.....`..-///..  
.:~+P~~~~~-0+:.  
hmMMMMMMMMNNddd\...\M\\...\hddddmMMMMMN  
:Nm-/NNNNNNNNNNNN$$$NMmm6&MMMMMMMMMMMMMMY  
.sm/'-ymMMMMMMMMNN$$$MMMMNN6&MMMMMMMMMMMh`  
-Nd` :MMMMMMMMNN$$$MMMMNN6&MMMMMMMMMMMh`  
-Nh` .ymMMMMMMMMNN$$$MMMMNN6&MMMMMMMMMMm/  
.sNd :MMMMMMMMNN$$$MMMMNN6&MMMMMMMMMMm/  
-mh` :MMMMMMMMNN$$$MMMMNN6&MMMMMMMMMMd  
.`-o++++oooo+:/oooooooo+:o++++oooo++/  
`::`-ooso--/yddh//s+/ossssso:--syN//os:  
/MMMMMMMMMMMMMMMMMd./+++-yy/.osydd/-oo:-`o//...oyodh+  
-hMMmssddd+:dMMmMMH.`.-=mmk.^/^\\^\\^++:^O://^^^\\`:  
.SMmo.-dMd-mN/^||--X--|| ||--X--||  
...../yddh/+...hmo-...hdd:.....\\=v=//.....\\=v=//.....  
=====+=====  
=====+ Session one died of dysentery. +=====  
=====+=====
```

Term: (Fall, Spring, Summer, Winter) 20XX

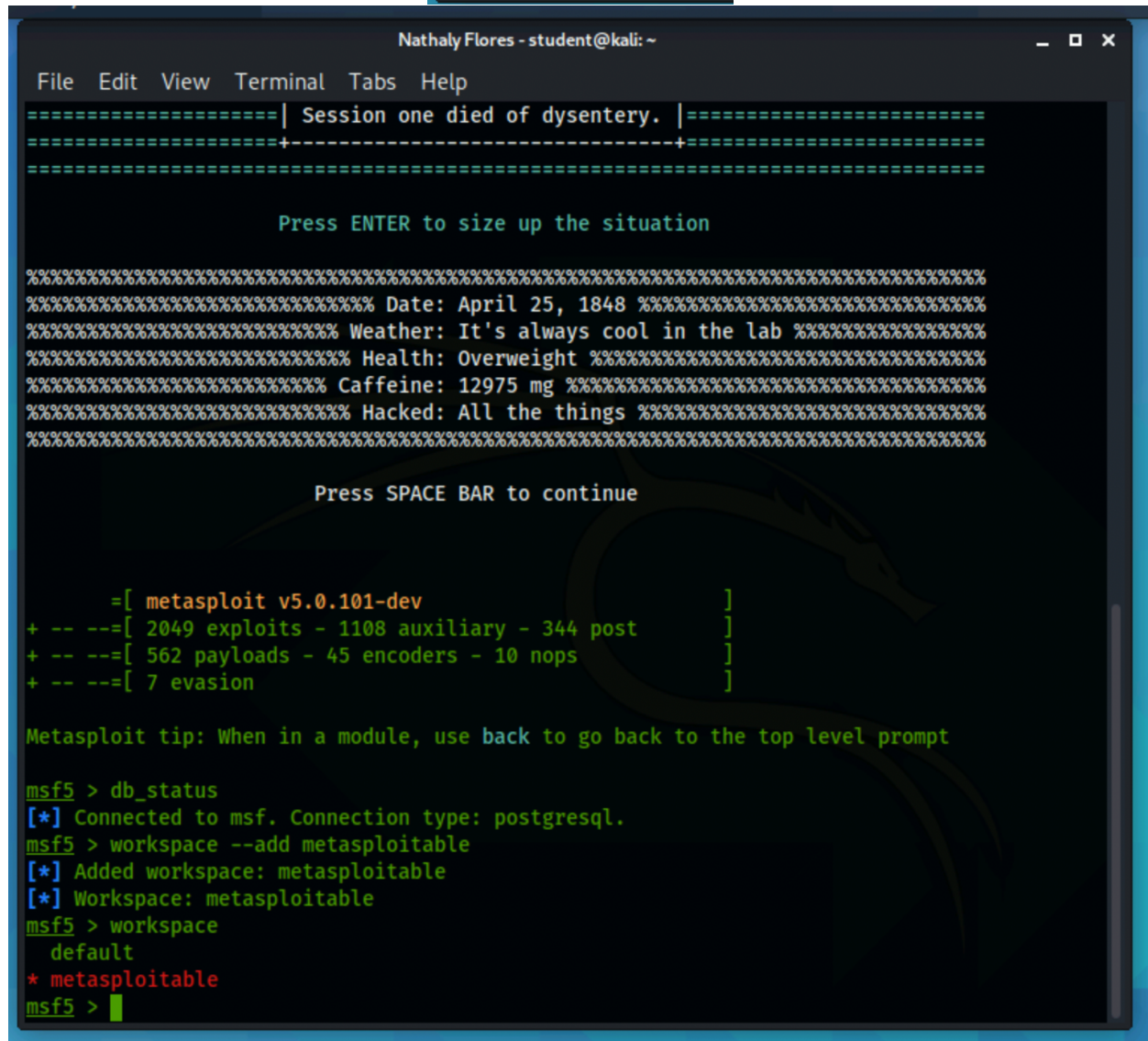
MR
KISER

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
msf5 > workspace
default
* metasploitable
msf5 > █
```



The screenshot shows a Kali Linux terminal window titled "Nathaly Flores - student@kali: ~". The terminal displays the Metasploit framework interface. At the top, a message reads "Session one died of dysentery." followed by a separator line. Below this, a prompt says "Press ENTER to size up the situation". A large ASCII art dragon is visible in the background. The terminal then shows the following commands and output:

```
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > workspace --add metasploitable
[*] Added workspace: metasploitable
[*] Workspace: metasploitable
msf5 > workspace
default
* metasploitable
msf5 > █
```

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`.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
msf5 > 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
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
route        Route traffic through a session
save         Saves the active datastores
sessions     Dump session listings and display information about sessions
set          Sets a context-specific variable to a value
setg         Sets a global variable to a value
sleep        Do nothing for the specified number of seconds
spool        Write console output into a file as well the screen
threads      View and manipulate background threads
tips         Show a list of useful productivity tips
unload       Unload a framework plugin
unset        Unsets one or more context-specific variables
```

```
Nathaly Flores - student@kali: ~
File Edit View Terminal Tabs Help

msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > workspace --add metasploitable
[*] Added workspace: metasploitable
[*] Workspace: metasploitable
msf5 > workspace
default
* metasploitable
msf5 > 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
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
route        Route traffic through a session
save         Saves the active datastores
sessions     Dump session listings and display information about sessions
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

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 that is holding the Metasploitable 3 content. Below are several ways to complete the task. I encourage you to 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 space provided or take note of your IP: 10.1.93.157/20.

```
root@kali:/home/student# 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
        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 12:39:19:89:f8:1e brd ff:ff:ff:ff:ff:ff
    inet 10.1.172.100/20 brd 10.1.175.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::1039:19ff:fe89:f81e/64 scope link
        valid_lft forever preferred_lft forever
root@kali:/home/student#
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~
File Edit View Terminal Tabs Help

Stop some extra running jobs:

    jobs -k 2-6,7,8,11..15

Check a set of IP addresses:

    check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255

Target a set of IPv6 hosts:

    set RHOSTS fe80::3990:0000/110, ::1-::f0f0

Target a block from a resolved domain name:

    set RHOSTS www.example.test/24
msf5 > ip addr
[*] exec: ip addr

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
        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 12:11:a1:da:cb:33 brd ff:ff:ff:ff:ff:ff
    inet 10.1.93.157/20 brd 10.1.95.255 scope global dynamic eth0
        valid_lft 2886sec preferred_lft 2886sec
    inet6 fe80::1011:a1ff:feda:cb33/64 scope link
        valid_lft forever preferred_lft forever
msf5 > 
```

This is our machine, but we have also discovered the subnet with this tactic. In future scans we don't really 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:

1. `nmap -sS -Pn -v -p 22 <your IP/20> | grep 'open'`
-discovered open ports 1. 22/tcp on 10.1.84.151 and 22/tcp on 10.1.93.157 ssh
2. `nmap -sS -Pn -p 22 <your IP/20> | grep -B4 'open'`
ip-10-1-93-157.ec2.internal (10.1.93.157).
3. Write down the IP address or copy and paste it into your notes

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
student@kali:~/Desktop$ nmap -sS -Pn -v -p 22 <10.1.93.157/20> | grep 'open'
bash: syntax error near unexpected token `|'
student@kali:~/Desktop$ nmap -sS -Pn -v -p 22 10.1.93.157/20 | grep 'open'
You requested a scan type which requires root privileges.
QUITTING!
student@kali:~/Desktop$ sudo su
root@kali:/home/student/Desktop# nmap -sS -Pn -v -p 22 10.1.93.157/20 | grep 'open'
Discovered open port 22/tcp on 10.1.84.151
22/tcp open  ssh
Discovered open port 22/tcp on 10.1.93.157
22/tcp open  ssh
root@kali:/home/student/Desktop# nmap -sS -Pn -p 22 10.1.93.157/20 | grep -B4 'open'
Nmap scan report for ip-10-1-84-151.ec2.internal (10.1.84.151)
Host is up (0.00020s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
--
Nmap scan report for ip-10-1-93-157.ec2.internal (10.1.93.157)
Host is up (0.000044s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
root@kali:/home/student/Desktop#
```

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 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) and 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. Where the other scans take about 10 seconds. You can streamline your pentesting processes by knowing more about powerful Linux tools like grep and Nmap.

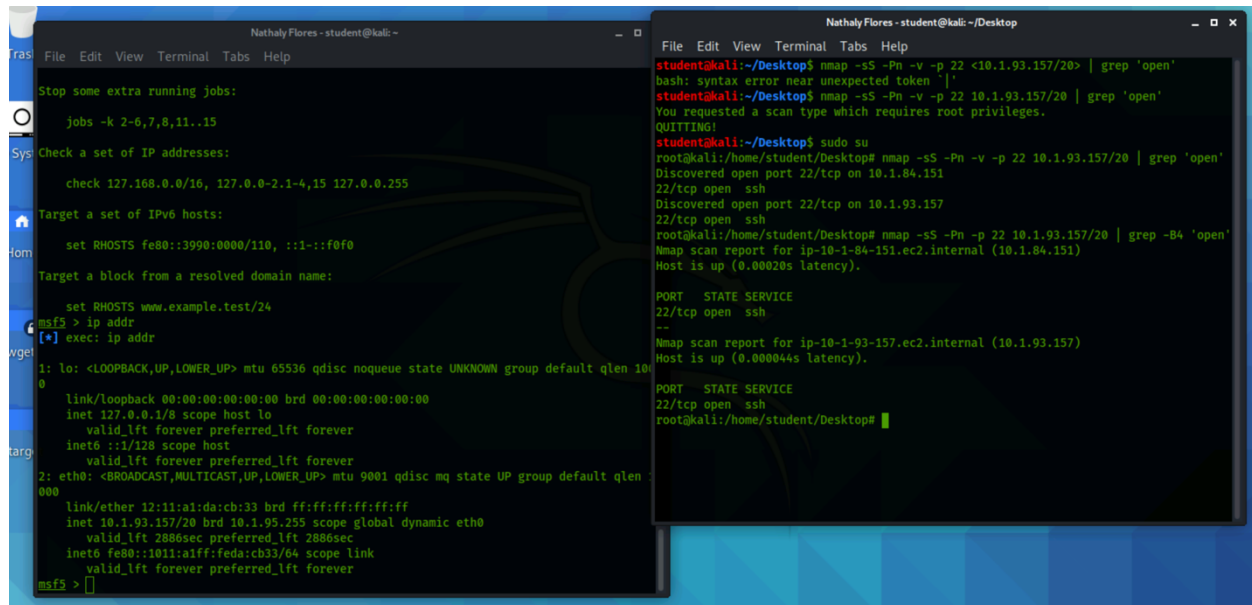
Answer the following questions:

1. What is the host IP on the Metasploitable machine (every student will have a different IP)?
10.1.84.151
2. Take a screenshot of the results name it *2target* and save it in the scanning folder.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX



The image shows two terminal windows. The left window is a Metasploit (msf5) session where the user sets RHOSTS to 10.1.163.125 and runs 'ip addr' to show network interfaces. The right window is a Kali Linux terminal where the user runs 'nmap -sS -p 22 10.1.163.125' and 'nmap -sS -p 22 10.1.163.125 | grep open' to discover open ports and services.

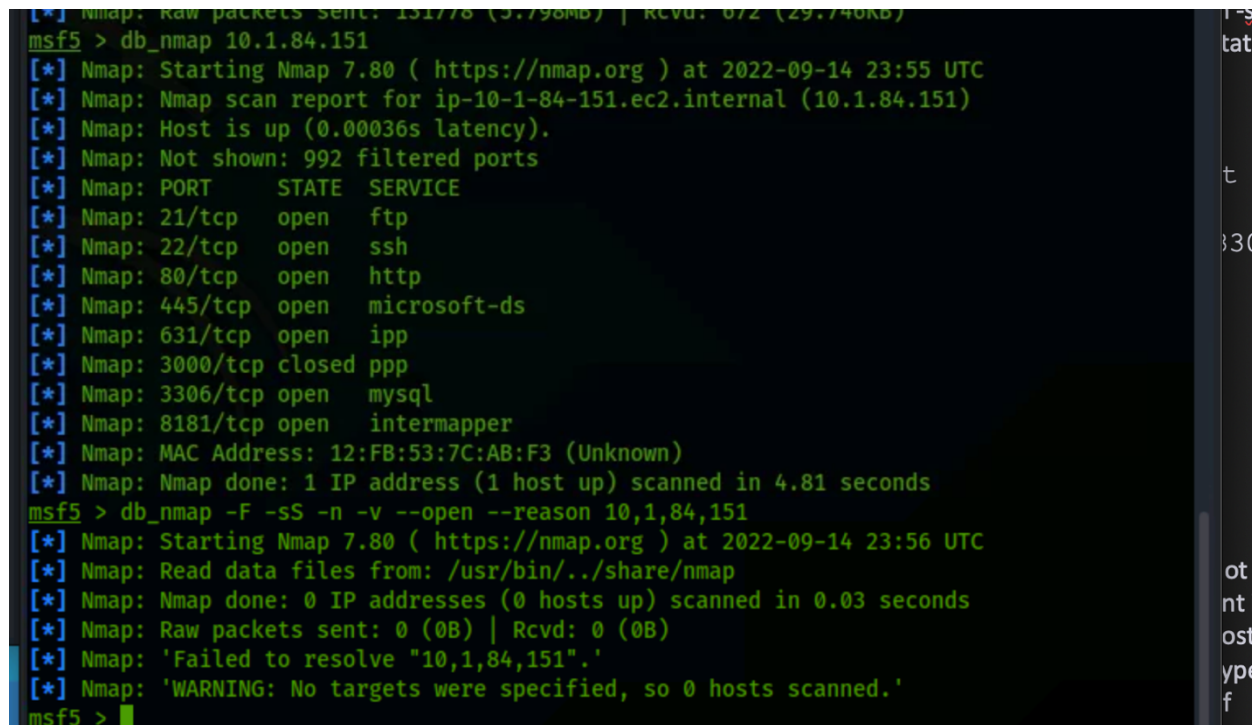
```
Nathaly Flores - student@kali: ~  
File Edit View Terminal Tabs Help  
Stop some extra running jobs:  
jobs -k 2-6,7,8,11..15  
Sys: Check a set of IP addresses:  
check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255  
Target a set of IPv6 hosts:  
set RHOSTS fe80::3990:0000:110, ::1:::f0f0  
Target a block from a resolved domain name:  
set RHOSTS www.example.test/24  
msf5 > ip addr  
[*] exec: ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10  
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  
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 12:11:a1:da:cb:33 brd ff:ff:ff:ff:ff:ff  
inet 10.1.93.157/20 brd 10.1.95.255 scope global dynamic eth0  
valid_lft 2886sec preferred_lft 2886sec  
inet6 fe80::1011:a1ff:feda:cb33/64 scope link  
valid_lft forever preferred_lft forever  
msf5 >   
Nathaly Flores - student@kali: ~/Desktop  
File Edit View Terminal Tabs Help  
student@kali:~/Desktop$ nmap -sS -p 22 <10.1.93.157/20> | grep 'open'  
bash: syntax error near unexpected token '<'  
student@kali:~/Desktop$ nmap -sS -p 22 10.1.93.157/20 | grep 'open'  
You requested a scan type which requires root privileges.  
QUITTING!  
student@kali:~/Desktop$ sudo su  
root@kali:/home/student/Desktop# nmap -sS -p 22 10.1.93.157/20 | grep 'open'  
Discovered open port 22/tcp on 10.1.84.151  
22/tcp open ssh  
Discovered open port 22/tcp on 10.1.93.157  
22/tcp open ssh  
root@kali:/home/student/Desktop# nmap -sS -p 22 10.1.93.157/20 | grep -B4 'open'  
Nmap scan report for ip-10-1-84-151.ec2.internal (10.1.84.151)  
Host is up (0.00020s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
--  
Nmap scan report for ip-10-1-93-157.ec2.internal (10.1.93.157)  
Host is up (0.00044s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
root@kali:/home/student/Desktop#
```

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

Return to the terminal window with the Metasploit Framework running, at the msf5> prompt complete the following:

[IMPORTANT: My Metasploitable IP is 10.1.163.125; everywhere you see this replace it with your Metasploitable IP.]

1. Type db_nmap 10.1.163.125 and press enter.



The image shows a terminal window with the output of the 'db_nmap' command. It displays the results of an Nmap scan for IP 10.1.84.151, including open ports (21/tcp, 22/tcp, 80/tcp, 445/tcp, 631/tcp, 3000/tcp, 3306/tcp, 8181/tcp) and services (ftp, ssh, http, microsoft-ds, ipp, ppp, mysql, intermapper). It also shows the MAC address and the time taken to scan the host.

```
msf5 > db_nmap 10.1.84.151  
[*] Nmap: Raw packets sent: 131778 (3.798MB) | Rcvd: 872 (29.74KB)  
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-14 23:55 UTC  
[*] Nmap: Nmap scan report for ip-10-1-84-151.ec2.internal (10.1.84.151)  
[*] Nmap: Host is up (0.00036s latency).  
[*] Nmap: Not shown: 992 filtered ports  
[*] Nmap: PORT      STATE SERVICE  
[*] Nmap: 21/tcp    open  ftp  
[*] Nmap: 22/tcp    open  ssh  
[*] Nmap: 80/tcp    open  http  
[*] Nmap: 445/tcp   open  microsoft-ds  
[*] Nmap: 631/tcp   open  ipp  
[*] Nmap: 3000/tcp  closed ppp  
[*] Nmap: 3306/tcp  open  mysql  
[*] Nmap: 8181/tcp  open  intermapper  
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)  
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds  
msf5 > db_nmap -F -sS -n -v --open --reason 10,1,84,151  
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-14 23:56 UTC  
[*] Nmap: Read data files from: /usr/bin/./share/nmap  
[*] Nmap: Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds  
[*] Nmap: Raw packets sent: 0 (0B) | Rcvd: 0 (0B)  
[*] Nmap: 'Failed to resolve "10,1,84,151".'  
[*] Nmap: 'WARNING: No targets were specified, so 0 hosts scanned.'  
msf5 >
```

2. Type db_nmap -F -sS -n -v --open --reason 10.1.163.125 and press enter.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
msf5 > db_nmap -F -sS -n -v --open --reason 10.1.84.151
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-15 00:21 UTC
[*] Nmap: Initiating ARP Ping Scan at 00:21
[*] Nmap: Scanning 10.1.84.151 [1 port]
[*] Nmap: Completed ARP Ping Scan at 00:21, 0.03s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 00:21
[*] Nmap: Scanning 10.1.84.151 [100 ports]
[*] Nmap: Discovered open port 21/tcp on 10.1.84.151
[*] Nmap: Discovered open port 3306/tcp on 10.1.84.151
[*] Nmap: Discovered open port 80/tcp on 10.1.84.151
[*] Nmap: Discovered open port 22/tcp on 10.1.84.151
[*] Nmap: Discovered open port 445/tcp on 10.1.84.151
[*] Nmap: Discovered open port 631/tcp on 10.1.84.151
[*] Nmap: Completed SYN Stealth Scan at 00:21, 1.67s elapsed (100 total ports)
[*] Nmap: Nmap scan report for 10.1.84.151
[*] Nmap: Host is up, received arp-response (0.00043s latency).
[*] Nmap: Not shown: 93 filtered ports, 1 closed port
[*] Nmap: Reason: 93 no-responses and 1 reset
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE      REASON
[*] Nmap: 21/tcp    open  ftp          syn-ack ttl 64
[*] Nmap: 22/tcp    open  ssh          syn-ack ttl 64
[*] Nmap: 80/tcp     open  http         syn-ack ttl 64
[*] Nmap: 445/tcp   open  microsoft-ds syn-ack ttl 64
[*] Nmap: 631/tcp   open  ipp          syn-ack ttl 64
[*] Nmap: 3306/tcp  open  mysql        syn-ack ttl 64
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
[*] Nmap: Raw packets sent: 194 (8.520KB) | Rcvd: 8 (332B)
```

Command breakdown:

- F is a fast scan of 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 its current state
- open this will show only open ports

To view current host results stored in your workspace type `hosts`.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help

-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-m set memory debugging flag (trace|record|usage)
-N changes the number of dots allowed before root lookup is done
-p specifies the port on the server to query
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-U enables UDP mode
-v enables verbose output
-V print version number and exit
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
msf5 > hosts

Hosts
=====

address      mac          name          os_name  os_flavor  os_
sp purpose   info  comments
-----
--
10.1.84.151  12:FB:53:7C:AB:F3  ip-10-1-84-151.ec2.internal  Unknown
device
```

To view the current services stored in your workspace type `services`.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
[*] Nmap: 22/tcp open ssh syn-ack ttl 64
[*] Nmap: 80/tcp open http syn-ack ttl 64
[*] Nmap: 445/tcp open microsoft-ds syn-ack ttl 64
[*] Nmap: 631/tcp open ipp syn-ack ttl 64
[*] Nmap: 3306/tcp open mysql syn-ack ttl 64
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
[*] Nmap: Raw packets sent: 194 (8.520KB) | Rcvd: 8 (332B)
msf5 > service
[*] exec: service

Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]
msf5 > services
Services
=====

host      port  proto  name      state  info
----
10.1.84.151 21    tcp    ftp       open
10.1.84.151 22    tcp    ssh       open
10.1.84.151 80    tcp    http      open
10.1.84.151 445   tcp    microsoft-ds open
10.1.84.151 631   tcp    ipp       open
10.1.84.151 3000  tcp    ppp       closed
10.1.84.151 3306  tcp    mysql     open
10.1.84.151 8181  tcp    intermapper open
msf5 > |
```

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 is taking 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.

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

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
+ -- ==[ 562 payloads - 45 encoders - 10 nops      ]
+ -- ==[ 7 evasion                                ]

Metasploit tip: Open an interactive Ruby terminal with irb

msf5 > metasploitable
[-] Unknown command: metasploitable.
msf5 > metasploitable
[-] Unknown command: metasploitable.
msf5 > metasploitable
[-] Unknown command: metasploitable.
msf5 > db_nmap -T4 -p- -sS -n -v --open --reason 10.1.84.151
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-16 18:52 UTC
[*] Nmap: Initiating ARP Ping Scan at 18:52
[*] Nmap: Scanning 10.1.84.151 [1 port]
[*] Nmap: Completed ARP Ping Scan at 18:52, 0.04s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 18:52
[*] Nmap: Scanning 10.1.84.151 [65535 ports]
[*] Nmap: Discovered open port 22/tcp on 10.1.84.151
[*] Nmap: Discovered open port 21/tcp on 10.1.84.151
[*] Nmap: Discovered open port 80/tcp on 10.1.84.151
[*] Nmap: Discovered open port 3306/tcp on 10.1.84.151
[*] Nmap: Discovered open port 445/tcp on 10.1.84.151
```

Answer the following questions:

1. What services did you find and what ports were running? See the screenshot. Below it shows the services and ports that are running.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
[*] Nmap: Scanning 10.1.84.151 [65535 ports]
[*] Nmap: Discovered open port 22/tcp on 10.1.84.151
[*] Nmap: Discovered open port 21/tcp on 10.1.84.151
[*] Nmap: Discovered open port 80/tcp on 10.1.84.151
[*] Nmap: Discovered open port 3306/tcp on 10.1.84.151
[*] Nmap: Discovered open port 445/tcp on 10.1.84.151
[*] Nmap: Discovered open port 631/tcp on 10.1.84.151
[*] Nmap: SYN Stealth Scan Timing: About 23.37% done; ETC: 18:54 (0:01:42 remaining)
[*] Nmap: Increasing send delay for 10.1.84.151 from 0 to 5 due to 27 out of 67 dropped probes since last increase.
[*] Nmap: SYN Stealth Scan Timing: About 40.91% done; ETC: 18:55 (0:01:58 remaining)
[*] Nmap: Increasing send delay for 10.1.84.151 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
[*] Nmap: SYN Stealth Scan Timing: About 41.12% done; ETC: 18:56 (0:02:40 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 42.71% done; ETC: 18:57 (0:03:10 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 44.95% done; ETC: 18:58 (0:03:31 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 48.08% done; ETC: 18:59 (0:03:51 remaining)
[*] Nmap: Discovered open port 3500/tcp on 10.1.84.151
[*] Nmap: SYN Stealth Scan Timing: About 65.31% done; ETC: 19:03 (0:03:56 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 73.36% done; ETC: 19:04 (0:03:21 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 79.63% done; ETC: 19:05 (0:02:43 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 85.45% done; ETC: 19:06 (0:02:02 remaining)
[*] Nmap: Discovered open port 6697/tcp on 10.1.84.151
[*] Nmap: SYN Stealth Scan Timing: About 90.82% done; ETC: 19:06 (0:01:20 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 95.96% done; ETC: 19:07 (0:00:36 remaining)
[*] Nmap: Completed SYN Stealth Scan at 19:07, 910.00s elapsed (65535 total ports)
[*] Nmap: Nmap scan report for 10.1.84.151
[*] Nmap: Host is up, received arp-response (0.00040s latency).
[*] Nmap: Not shown: 65526 filtered ports, 1 closed port
[*] Nmap: Reason: 65526 no-responses and 1 reset
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE      REASON
[*] Nmap: 21/tcp    open  ftp          syn-ack ttl 64
[*] Nmap: 22/tcp    open  ssh          syn-ack ttl 64
[*] Nmap: 80/tcp     open  http         syn-ack ttl 64
[*] Nmap: 445/tcp   open  microsoft-ds syn-ack ttl 64
[*] Nmap: 631/tcp   open  ipp          syn-ack ttl 64
[*] Nmap: 3306/tcp  open  mysql        syn-ack ttl 64
[*] Nmap: 3500/tcp  open  rtmp-port    syn-ack ttl 64
[*] Nmap: 6697/tcp open  ircs-u       syn-ack ttl 64
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
```

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

These are the results of the folder 3ServicesPorts below save onto this assignment.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
[*] Nmap: Completed SYN Stealth Scan at 19:07, 910.00s elapsed (65535 total ports)
[*] Nmap: Nmap scan report for 10.1.84.151
[*] Nmap: Host is up, received arp-response (0.00040s latency).
[*] Nmap: Not shown: 65526 filtered ports, 1 closed port
[*] Nmap: Reason: 65526 no-responses and 1 reset
[*] Nmap: Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
[*] Nmap: PORT      STATE SERVICE      REASON
[*] Nmap: 21/tcp    open  ftp          syn-ack ttl 64
[*] Nmap: 22/tcp    open  ssh          syn-ack ttl 64
[*] Nmap: 80/tcp    open  http         syn-ack ttl 64
[*] Nmap: 445/tcp   open  microsoft-ds syn-ack ttl 64
[*] Nmap: 631/tcp   open  ipp          syn-ack ttl 64
[*] Nmap: 3306/tcp  open  mysql        syn-ack ttl 64
[*] Nmap: 3500/tcp  open  rtmp-port    syn-ack ttl 64
[*] Nmap: 6697/tcp  open  ircs-u       syn-ack ttl 64
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 910.16 seconds
[*] Nmap: Raw packets sent: 131780 (5.798MB) | Rcvd: 671 (29.504KB)
msf5 > |
```

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? **ARP Scan, Ping**
2. Take a screenshot of the results name it appropriately. **See the screenshot below**

```
msf5 > db_nmap -sU -n -v --open --reason 10.1.84.151
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-16 19:14 UTC
[*] Nmap: Initiating ARP Ping Scan at 19:14
[*] Nmap: Scanning 10.1.84.151 [1 port]
[*] Nmap: Completed ARP Ping Scan at 19:14, 0.04s elapsed (1 total hosts)
[*] Nmap: Initiating UDP Scan at 19:14
[*] Nmap: Scanning 10.1.84.151 [1000 ports]
[*] Nmap: Completed UDP Scan at 19:14, 21.09s elapsed (1000 total ports)
[*] Nmap: Nmap scan report for 10.1.84.151
[*] Nmap: Host is up, received arp-response (0.00011s latency).
[*] Nmap: All 1000 scanned ports on 10.1.84.151 are open|filtered because of 1000 no-responses
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
[*] Nmap: Raw packets sent: 2001 (57.882KB) | Rcvd: 1 (28B)
msf5 > |
```

Task 4: Service Version Scanning

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

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? It is checking all ports that was entered also it give a ping to all of them and time is being completed
2. Take a screenshot of the results and name it appropriately.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
[*] Nmap: Completed ARP Ping Scan at 19:14, 0.04s elapsed (1 total hosts)
[*] Nmap: Initiating UDP Scan at 19:14
[*] Nmap: Scanning 10.1.84.151 [1000 ports]
[*] Nmap: Completed UDP Scan at 19:14, 21.09s elapsed (1000 total ports)
[*] Nmap: Nmap scan report for 10.1.84.151
[*] Nmap: Host is up, received arp-response (0.00011s latency).
[*] Nmap: All 1000 scanned ports on 10.1.84.151 are open|filtered because of 1000 no-responses
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
[*] Nmap: Raw packets sent: 2001 (57.882KB) | Rcvd: 1 (28B)
msf5 > db_nmap -sS -sV -sC -v -n -p 21,22,80,445,631,3306,3500,6697 10.1.84.151
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-16 19:18 UTC
[*] Nmap: NSE: Loaded 151 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 19:18
[*] Nmap: Completed NSE at 19:18, 0.00s elapsed
[*] Nmap: Initiating NSE at 19:18
[*] Nmap: Completed NSE at 19:18, 0.00s elapsed
[*] Nmap: Initiating NSE at 19:18
[*] Nmap: Completed NSE at 19:18, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 19:18
[*] Nmap: Scanning 10.1.84.151 [1 port]
[*] Nmap: Completed ARP Ping Scan at 19:18, 0.03s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 19:18
[*] Nmap: Scanning 10.1.84.151 [8 ports]
[*] Nmap: Discovered open port 21/tcp on 10.1.84.151
[*] Nmap: Discovered open port 22/tcp on 10.1.84.151
[*] Nmap: Discovered open port 3306/tcp on 10.1.84.151
[*] Nmap: Discovered open port 445/tcp on 10.1.84.151
[*] Nmap: Discovered open port 6697/tcp on 10.1.84.151
[*] Nmap: Discovered open port 631/tcp on 10.1.84.151
[*] Nmap: Discovered open port 80/tcp on 10.1.84.151
[*] Nmap: Discovered open port 3500/tcp on 10.1.84.151
[*] Nmap: Completed SYN Stealth Scan at 19:18, 0.04s elapsed (8 total ports)
[*] Nmap: Initiating Service scan at 19:18
[*] Nmap: Scanning 8 services on 10.1.84.151
[*] Nmap: Completed Service scan at 19:18, 6.01s elapsed (8 services on 1 host)
[*] Nmap: NSE: Script scanning 10.1.84.151.
[*] Nmap: Initiating NSE at 19:18
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~
File Edit View Terminal Tabs Help
[*] Nmap: Host is up (0.00038s latency).
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          ProFTPD 1.3.5
[*] Nmap: 22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 24:3b:af:03:c1:03:da:7d:9e:2a:99:d9:78:ff:c4:3d (DSA)
[*] Nmap: |   2048 39:5a:a7:9a:ca:59:40:b9:ee:c3:f9:87:d2:0e:be:5c (RSA)
[*] Nmap: |   256 53:71:b2:76:af:89:d7:a8:43:11:51:9c:e4:0d:f9:fd (ECDSA)
[*] Nmap: 80/tcp    open  http         Apache httpd 2.4.7
[*] Nmap: | http-ls: Volume /
[*] Nmap: |   SIZE  TIME                FILENAME
[*] Nmap: |   -    2018-05-23 06:21   chat/
[*] Nmap: |   -    2011-07-27 20:17   drupal/
[*] Nmap: | 1.7K  2018-05-23 06:21   payroll_app.php
[*] Nmap: |   -    2013-04-08 12:06   phpmyadmin/
[*] Nmap: |_
[*] Nmap: |_ http-methods:
[*] Nmap: |_ Supported Methods: OPTIONS GET HEAD POST
[*] Nmap: |_ http-server-header: Apache/2.4.7 (Ubuntu)
[*] Nmap: |_ http-title: Index of /
[*] Nmap: 445/tcp    open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
[*] Nmap: 3306/tcp    open  mysql       MySQL (unauthorized)
[*] Nmap: 3500/tcp    open  http        WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
[*] Nmap: |_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
[*] Nmap: |_ http-methods:
[*] Nmap: |_ Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_ http-robots.txt: 1 disallowed entry
[*] Nmap: |_ /
[*] Nmap: |_ http-server-header: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
[*] Nmap: |_ http-title: Ruby on Rails: Welcome aboard
[*] Nmap: 6697/tcp    open  irc         UnrealIRCd
[*] Nmap: 8181/tcp    open  http        WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
[*] Nmap: |_ http-methods:
[*] Nmap: |_ Supported Methods: GET HEAD
[*] Nmap: |_ http-server-header: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
[*] Nmap: |_ http-title: Site doesn't have a title (text/html; charset=utf-8).
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Service Info: Hosts: 10.1.84.151, IP-10-1-84-151, irc.TestIRC.net; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
[*] Nmap: users: 1
[*] Nmap: servers: 1
[*] Nmap: lusers: 1
[*] Nmap: lservers: 0
[*] Nmap: _ server: irc.TestIRC.net
[*] Nmap: MAC Address: 12:FB:53:7C:AB:F3 (Unknown)
[*] Nmap: Service Info: Hosts: 10.1.84.151, IP-10-1-84-151, irc.TestIRC.net; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: _clock-skew: mean: 1s, deviation: 2s, median: 0s
[*] Nmap: smb-os-discovery:
[*] Nmap: OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
[*] Nmap: Computer name: ip-10-1-84-151
[*] Nmap: NetBIOS computer name: IP-10-1-84-151\x00
[*] Nmap: Domain name: \x00
[*] Nmap: FQDN: ip-10-1-84-151
[*] Nmap: _ System time: 2022-09-16T19:18:11+00:00
[*] Nmap: smb-security-mode:
[*] Nmap: account_used: guest
[*] Nmap: authentication_level: user
[*] Nmap: challenge_response: supported
[*] Nmap: _ message_signing: disabled (dangerous, but default)
[*] Nmap: smb2-security-mode:
[*] Nmap: 2.02:
[*] Nmap: _ Message signing enabled but not required
[*] Nmap: smb2-time:
[*] Nmap: date: 2022-09-16T19:18:12
[*] Nmap: _ start_date: N/A
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 19:19
[*] Nmap: Completed NSE at 19:19, 0.00s elapsed
[*] Nmap: Initiating NSE at 19:19
[*] Nmap: Completed NSE at 19:19, 0.00s elapsed
[*] Nmap: Initiating NSE at 19:19
[*] Nmap: Completed NSE at 19:19, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 107.17 seconds
[*] Nmap: Raw packets sent: 9 (380B) | Rcvd: 9 (380B)
msf5 > |
```

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 in 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 scope, we should be left with only the Metasploitable host. In my case, that is 10.1.163.125. The below screenshots are examples of how to delete out of scope hosts. For the first two screenshots, the only IP in scope is the Linux Server. The last screenshot is of the Metasploit services database found by typing `services` and pressing enter in the msfconsole.

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
msf5 > hosts

Hosts
=====

address      mac          name          os_name  os_flavo
r  os_sp  purpose  info  comments
-----  ---  ----  -----  -----
10.1.99.161
10.1.144.241  02:73:62:a4:b4:10  ip-10-1-144-241.ec2.internal  Linux
3.X      server

msf5 > █
```

```
msf5 > hosts -d 10.1.99.161

Hosts
=====

address      mac          name          os_name  os_flavor  os_sp  purpose  info  comments
-----  ---  ----  -----  -----  -----  -----  -----
10.1.99.161

[*] Deleted 1 hosts
msf5 > hosts

Hosts
=====

address      mac          name          os_name  os_flavo
r  os_sp  purpose  info  comments
-----  ---  ----  -----  -----
10.1.144.241  02:73:62:a4:b4:10  ip-10-1-144-241.ec2.internal  Linux
3.X      server

msf5 > █
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

Services

host	port	proto	name	state	info
10.1.163.125	21	tcp	ftp	open	ProFTPD 1.3.5
10.1.163.125	22	tcp	ssh	open	OpenSSH 6.6.1p1 Ubuntu 2ub
ntu2 Ubuntu Linux; protocol	2.0				
10.1.163.125	80	tcp	http	open	Apache httpd 2.4.7
10.1.163.125	445	tcp	netbios-ssn	open	Samba smbd 4.3.11-Ubuntu w
rkgroup: WORKGROUP					
10.1.163.125	631	tcp	ipp	open	CUPS 1.7
10.1.163.125	3000	tcp	ppp	closed	
10.1.163.125	3306	tcp	mysql	open	MySQL unauthorized
10.1.163.125	3389	tcp	ms-wbt-server	filtered	
10.1.163.125	3500	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2
3.7 (2018-03-28)					
10.1.163.125	6697	tcp	irc	open	UnrealIRCd
10.1.163.125	8022	tcp	oa-system	filtered	
10.1.163.125	8181	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2
3.7 (2018-03-28)					
10.1.163.125	8484	tcp	unknown	filtered	
10.1.163.125	8585	tcp		filtered	
10.1.163.125	9200	tcp	wap-wsp	filtered	
10.1.163.125	49153	tcp	unknown	filtered	
10.1.163.125	49154	tcp	unknown	filtered	
10.1.163.125	49202	tcp	unknown	filtered	

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
msf5 > hosts -d 10.1.80.2

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
10.1.80.2     12:b8:c2:75:e6:b4      Unknown              device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.80.99

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
10.1.80.99    12:7b:87:8b:97:93      Unknown              device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.80.252

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
10.1.80.252   12:1b:a3:d8:af:e5      Unknown              device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.81.170

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
10.1.81.170   12:ad:da:63:0e:eb      Unknown              device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.81.62
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
Nathaly Flores - student@kali: ~/Desktop
File Edit View Terminal Tabs Help
msf5 > hosts -d 10.1.95.85

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----      ---              ----  -
10.1.95.85    12:39:f0:aa:fd:23  Unknown  device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.95.198

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----      ---              ----  -
10.1.95.198   12:50:ab:38:68:cb  Unknown  device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.95.199

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----      ---              ----  -
10.1.95.199   12:ce:71:ac:70:b7  Unknown  device

[*] Deleted 1 hosts
msf5 > hosts -d 10.1.95.227

Hosts
=====

address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----      ---              ----  -
10.1.95.227   12:6d:4b:ef:fe:9b  Unknown  device

[*] Deleted 1 hosts
msf5 > 
```

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title

Term: (Fall, Spring, Summer, Winter) 20XX

```
10.1.93.227 12.00.40.E1.7E.9D Unknown device
[*] Deleted 1 hosts
msf5 > services
Services
=====
host      port  proto  name      state  info
-----  -
10.1.84.151 21    tcp    ftp        open   ProFTPD 1.3.5
10.1.84.151 22    tcp    ssh        open   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 Ubuntu Linux; protocol 2.0
10.1.84.151 80    tcp    http       open   Apache httpd 2.4.7
10.1.84.151 445   tcp    netbios-ssn open   Samba smbd 4.3.11-Ubuntu workgroup: WORKGROUP
10.1.84.151 631   tcp    ipp        open   CUPS 1.7
10.1.84.151 3000  tcp    ppp        closed
10.1.84.151 3306  tcp    mysql      open   MySQL unauthorized
10.1.84.151 3500  tcp    http       open   WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)
10.1.84.151 6697  tcp    irc        open   UnrealIRCd
10.1.84.151 8181  tcp    http       open   WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)
msf5 > 
```

5. References:

https://www.aelius.com/njh/subnet_sheet.html

<https://nmap.org/book/nse-usage.html>

<https://nmap.org/nsedoc/categories/default.html>