Laboratory Exercise 3 – Advanced Port Scanning

Instructions for answering lab questions (applies to all future labs):

1. Unless the question only asks you to submit a screenshot, you must verbally answer the question, and attach screenshot to support your answer.
2. You will be graded based on your answer but not the screenshot, and you will not get points if your answer is incorrect (the screenshot contains all information including the correct answer, but you must know and specifically point it out).
3. Your screenshot must be zoom to the proper level that includes necessary information only. You can annotate on the screenshot if you'd like. You screenshot should be legit and readable when being displayed on a regular sized monitor. Do not screenshot the whole monitor display and paste in the document.

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: Kali Linux with Metasploitable (2018)*** environment to perform port scanning and Enumeration.

2. Resources Required

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

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable (2018) environment, 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`**

Task 1: Advanced command line scanning with Nmap and Metasploit

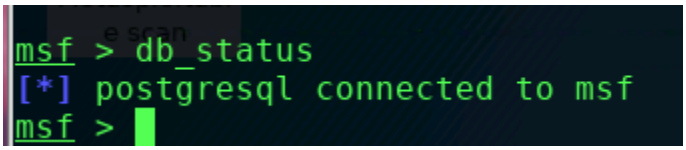
Review and refer to the following Nmap cheat sheets during this lab:

- 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 Postgre SQL 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.

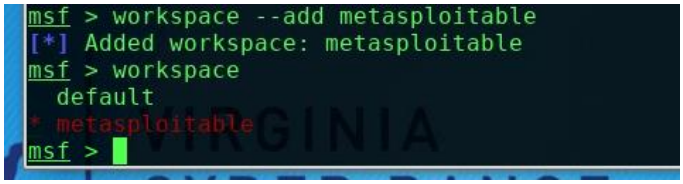


If the database does not have connectivity or you accidently started the framework before starting the database, exit out of the terminal and repeat step 1, 2, 5, and 6. This should do the trick. If for some reason it does not, exit out of the terminal and complete steps 1-6 again.

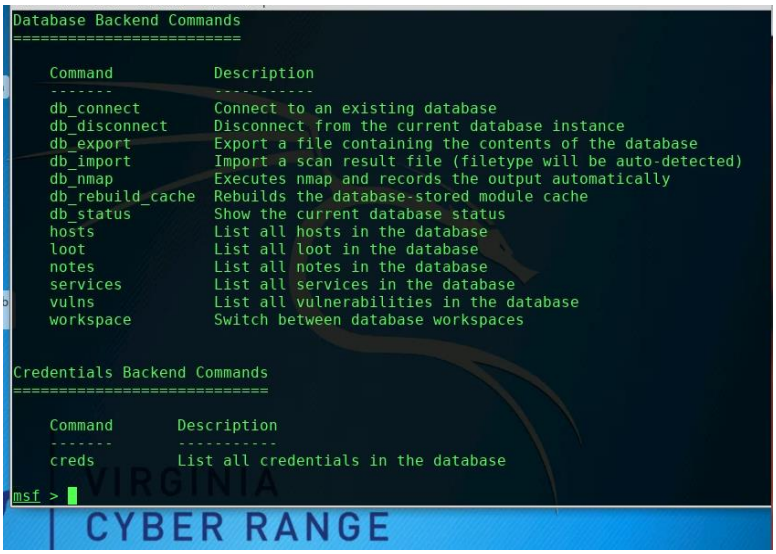
Before we start scanning, we want to create a workspace for our scans. This will make it easier to find the scans at a later time when we complete our reports. It will also prevent the issue of polluting the database when we need to work on more than one project.

Complete the following:

1. Type `workspace --add metasploitable`
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.



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`.

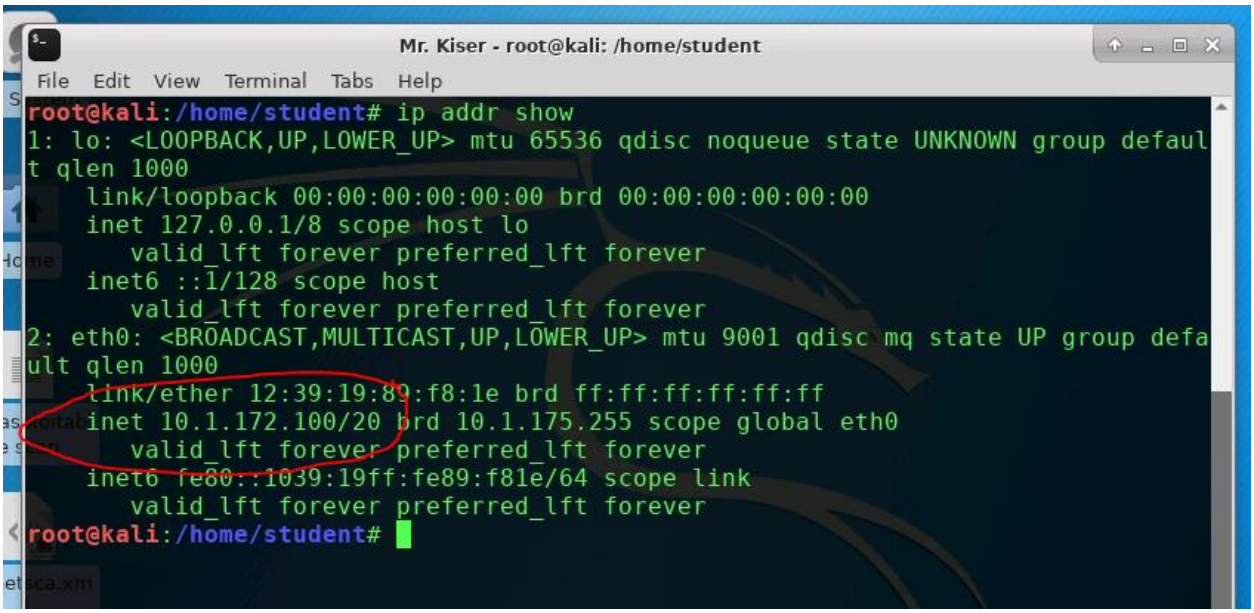


Take notice of the **hosts**, **services**, and **notes**. We will be calling on these when we write reports or when we pick up where we left off. This way we do not have to complete the scans again. They are all saved in the workspace database.

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 (no need to submit):

1. Type `ip addr show` to discover your current network configurations.
2. Write down in space provided or take note of your IP: _____.



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.

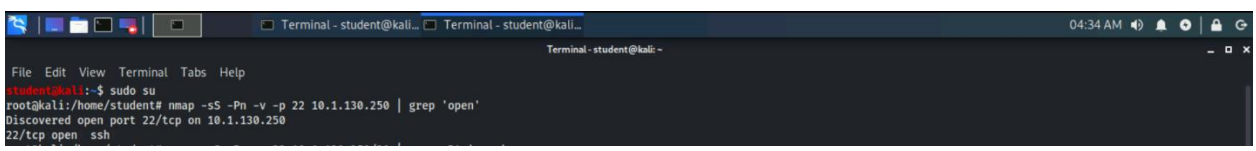
The following commands will help you find the target Metasploitable machine. Open a new terminal window and become root. Type the following:

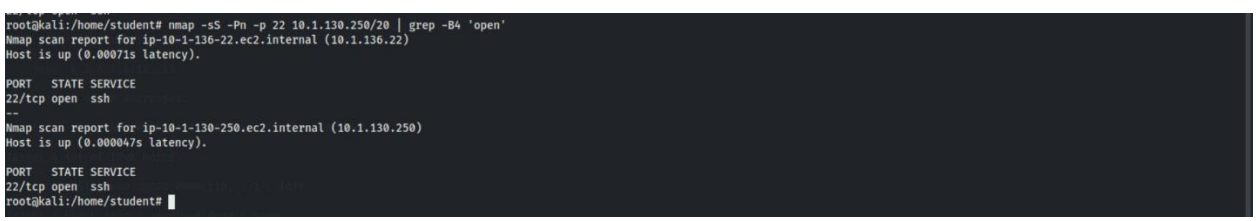
1. `nmap -sS -Pn -v -p 22 <your IP/20> | grep 'open'`
2. `nmap -sS -Pn -p 22 <your IP/20> | grep -B4 'open'`
3. Write down the IP address or copy and paste it into your notes

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 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 searching for "open. " 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)?**
   10.1.136.22
2. **Take two screenshots of the results running above two nmap commands and attach in your submission.**





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

Return to the terminal window with the Metasploit Framework running, at the msf> prompt complete the following:
[NOTE: 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.
2. Type `db_nmap -F -sS -n -v --open --reason 10.1.163.125` and press enter.

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`.
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 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:

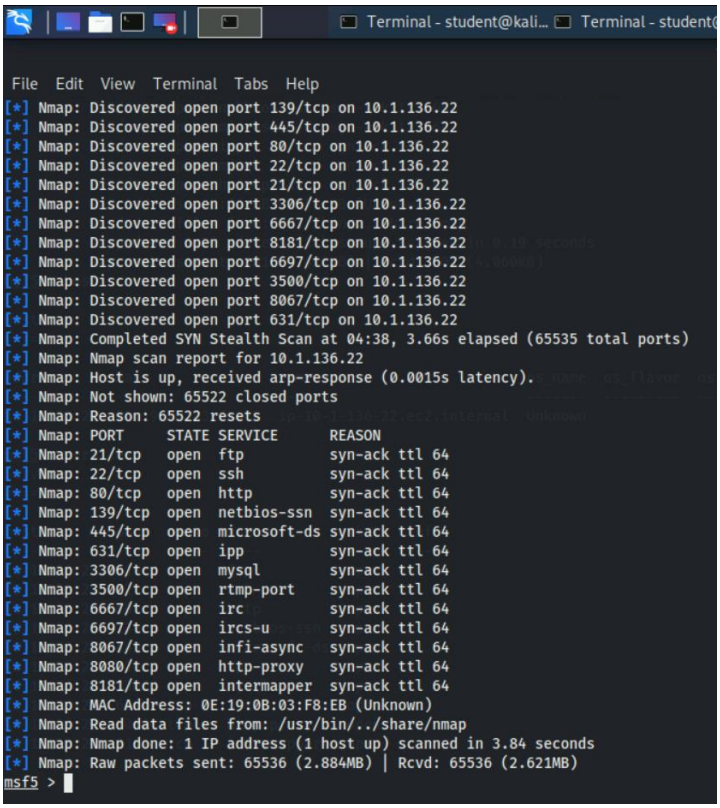
1. Type `sudo su` and press enter.
2. Type `msfconsole` and press enter.
3. Type `workspace metasploitable` and press enter.
4. Type `db_nmap -p- -sS -n -v --open –max-rtt-timeout 100ms --reason <target IP>` and press enter. The target IP should be the host other than your own machine, which you have identified from the previous step. (notice the dash (-) after the parameter p is necessary, it is not a typo)

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

Answer the following questions:

1. **What services were running, and on what ports and protocols? List all of them as you find from the scanning. Take a screenshot of the results and attach to your assignment.**
   Notice: the --max-rtt-timeout option is added so the scan won't take too long. Still, the scanning may take 5 - 10 minutes to finish, be prepared.
   A Syn Stealth scan at 04:38 on ports 8080, 193, 445, 80, 22, 21, 3306, 6667, 8181, 6697, 3500, 8067, and 631. Services like ftp ran on port 21, ssh on 22, http on 80, netbios-ssn on 139, Microsoft-ds on 445, ipp on 631,

mysql on 3306, rtmp-port on 3500, irc on 6667m ircs-u on 6697, infi-async on 8067, http-proxy on 8080, and intermapper on 8181.



Task 3: 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.

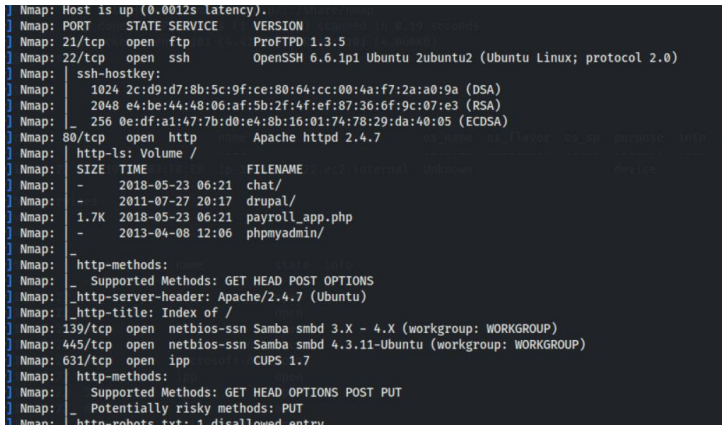
Complete the following:

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`
3. You should run this command against the Metaesploitable host that you have discovered in the previous step, and scan for all the opening ports on that host.

Answer the following questions:

1. **What new information was discovered? Take a screenshot of the results to justify your answer.**

   The new information that was discovered was the Port as well as the State(open or closed), the Service, the version(like ProFTPD 1.3.5), the SIZE(like 1.7k), the TIME(like 2018-05-23-06:21), the and the FILENAME(like chat/).



```
Nmap: Host is up (0.0012s 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 2c:d9:d7:8b:5c:9f:ce:80:64:cc:00:4a:f7:2a:a0:9a (DSA)
Nmap:     2048 e4:be:44:48:06:af:5b:2f:4f:ef:87:36:6f:9c:07:e3 (RSA)
Nmap: |_  256 0e:df:a1:47:7b:d0:e4:8b:16:01:74:78:29:da:40:05 (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: GET HEAD POST OPTIONS
Nmap: |_http-server-header: Apache/2.4.7 (Ubuntu)
Nmap: |_http-title: Index of /
Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Nmap: 445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Nmap: 631/tcp  open  ipp         CUPS 1.7
Nmap: | http-methods:
Nmap:     Supported Methods: GET HEAD OPTIONS POST PUT
Nmap: |_  Potentially risky methods: PUT
```

Task 4: Cleaning up your hosts list

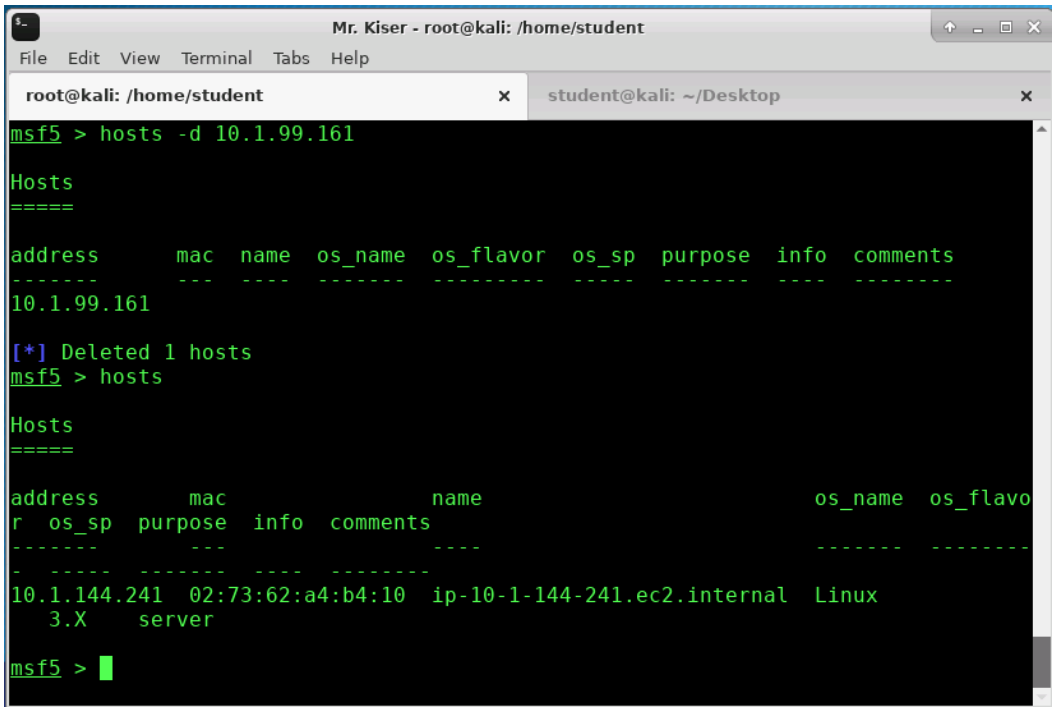
So, now that we have completed several scans, we may want to clean up our hosts list. The only host we want in the list is the Metasploitable machine. To do this, we type `hosts` in the msfconsole to view our hosts. If we have any hosts other than our Metasploitable target, they need to be deleted. To 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` in the msfconsole.

Answer the following questions:

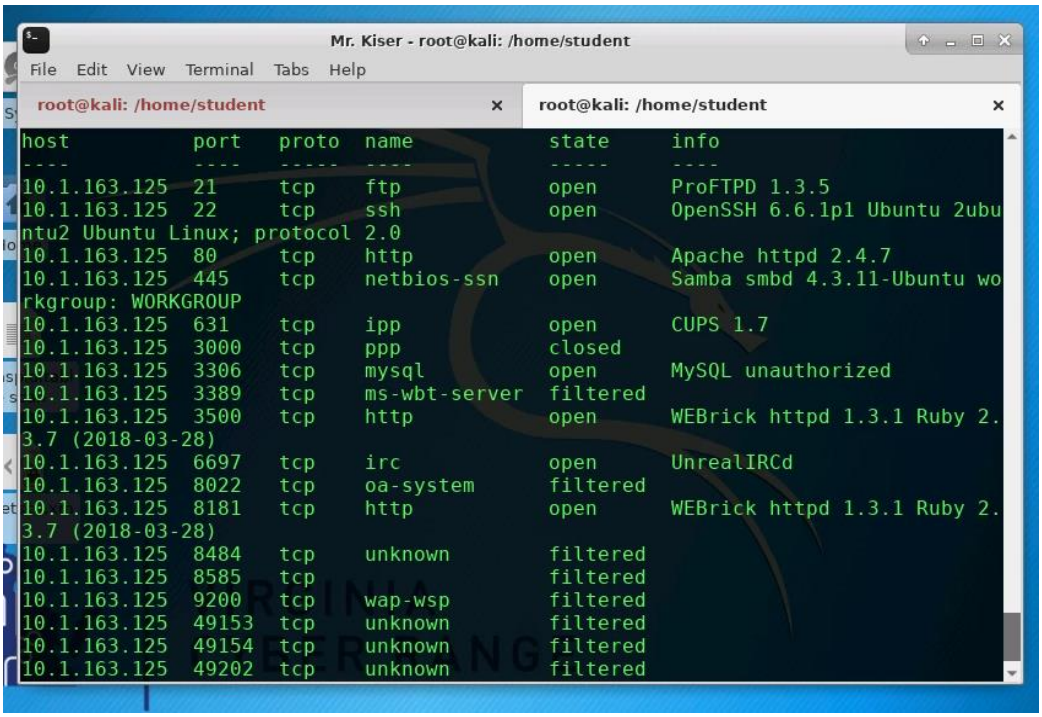
1. **After cleaning up the host list, type the services command in the msfconsole, take a screenshot of the result and submit.**

```
File  Edit  View  Terminal  Tabs  Help
Hosts
=====

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

msf5 > hosts

Hosts
=====

address      mac               name                        os_name  os_flavor  os_sp  purpose  info  comments
-------      ---               ----                        -------  ---------  -----  -------  ----  --------
10.1.136.22  0e:19:0b:03:f8:eb  ip-10-1-136-22.ec2.internal  Unknown                   device

msf5 > services
Services
========

host         port  proto  name         state  info
----         ----  -----  ----         -----  ----
10.1.136.22  21    tcp    ftp          open   ProFTPD 1.3.5
10.1.136.22  22    tcp    ssh          open   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 Ubuntu Linux; protocol 2.0
10.1.136.22  80    tcp    http         open   Apache httpd 2.4.7
10.1.136.22  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.1.136.22  445   tcp    netbios-ssn  open   Samba smbd 4.3.11-Ubuntu workgroup: WORKGROUP
10.1.136.22  631   tcp    ipp          open   CUPS 1.7
10.1.136.22  3306  tcp    mysql        open   MySQL unauthorized
10.1.136.22  3500  tcp    http         open   WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)
10.1.136.22  6667  tcp    irc          open   UnrealIRCd
10.1.136.22  6697  tcp    irc          open   UnrealIRCd
10.1.136.22  8067  tcp    irc          open   UnrealIRCd
10.1.136.22  8080  tcp    http         open   Jetty 8.1.7.v20120910
10.1.136.22  8181  tcp    http         open   WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)

msf5 >
```

```
Mr. Kiser - root@kali: /home/student
File  Edit  View  Terminal  Tabs  Help
root@kali: /home/student        student@kali: ~/Desktop

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 >
```



Services



5. References:

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

[This portion of the lesson plan is provided for instructors that will be using this lesson plan and associated material in their class.]

KSAs Addressed

From (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf)

Knowledge:

- **K0177**:Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- **K0398:** Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).

Skills:

- **S0153:** Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.
- **S0264:** Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).

Abilities:

- **A0160**: Ability to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise

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

Course Title

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

Knowledge Units (KUs) Addressed: (from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf) covered:

(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Basic Cyber Operations (BCO)
- Basic Networking (BNW)