**Laboratory Exercise – Scanning and Enumeration**

Name: Afeefah Manzoor

**1. Overview**

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2018) environment to perform Banner Grabbing with several different scanning tools. Students will also use Netstat to discover what ports are being listened on.

**2. Resources Required**

This exercise requires a Kali Linux with Metasploitable (2018) 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**

**4. Tasks**

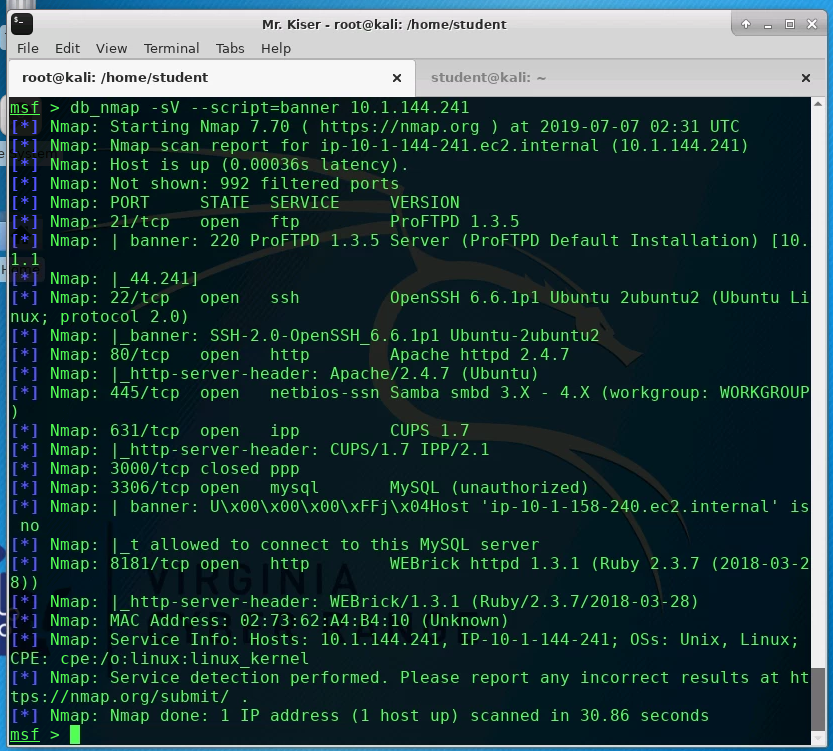
**Task 1: Banner Grabbing with Nmap**

Remember that in order to run Metasploit you have to be root. The target that we are attacking is still the Metasploitable machine (from the last lab exercise) as this is the only target that is in scope. The Metasploit IP will be denoted as <target IP>. **Please do not attack other IPs** as AWS will have several IPs that are out of scope but can be enumerated. Note that banner grabbing can work on several ports and services 80 (http), 21(FTP), 22 (SSH), 25 (SMTP), 23 (Telnet), 8080 (HTTP), and more. It will take practice to know when to use banner grabbing.

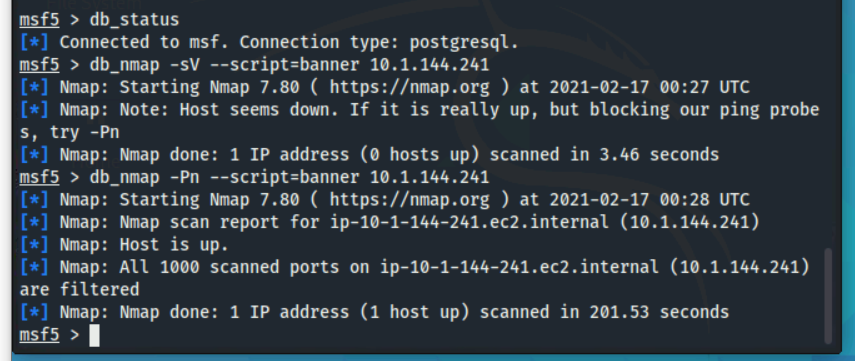
Open a terminal and complete the following commands:

1. Type service postgresql start and hit enter.

2. Type msfconsole and hit enter.

3. Type db\_nmap -sV --script=banner <target IP> and hit enter.

Take a screenshot of the results and name it 4nmapbanner1. Save the scan in the scanning folder that you created for the previous lesson.



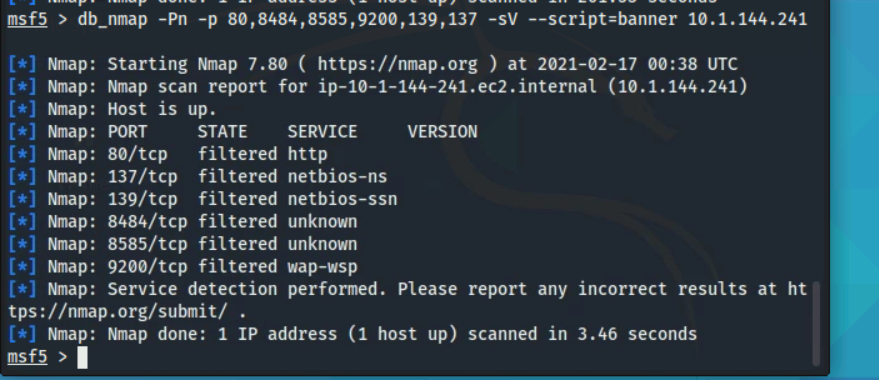
Type the following command:

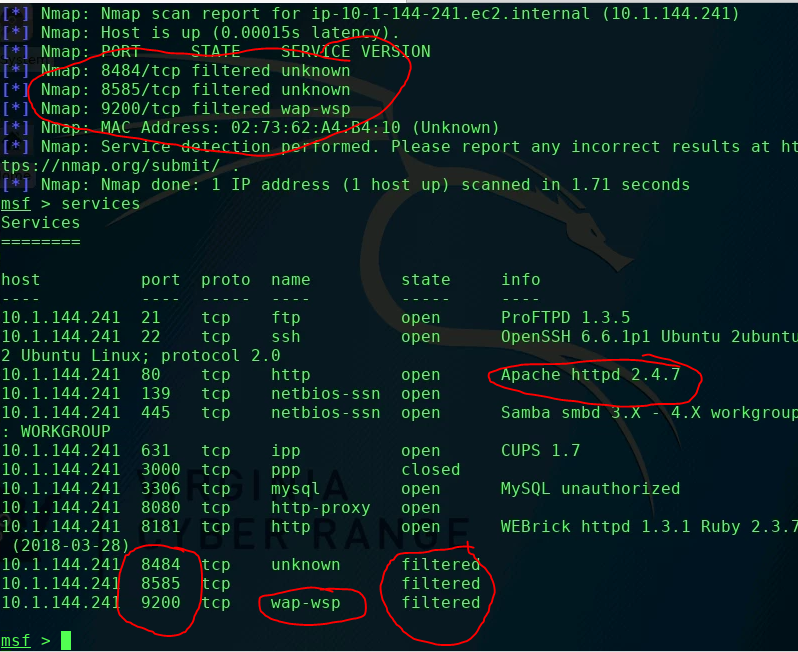
db\_nmap -Pn -p 80,8484,8585,9200,139,137 -sV --script=banner <target IP>

and hit enter.

As you can see, this scan specifies a few ports that we knew were on the target machine (recall from the previous lesson) but are not discovered with other scans.

Take a screenshot of the results and name it 5nmapbanner2. Save the scan in the scanning folder. Paste a copy of your screenshot here.



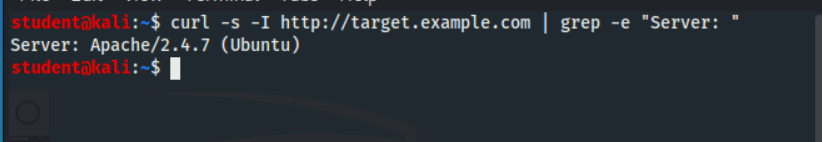


Task 2: Banner Grabbing with cURL

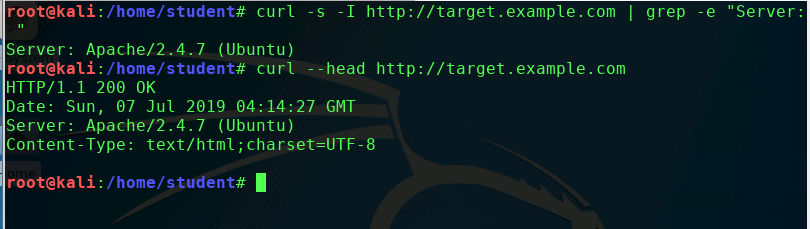
To use cURL we are going to need the domain. In this case that is <http://target.example.com>. cURL will work in the msf console; however, it is best to execute this command in a new terminal, so that it can be easily referred back to.

Open a new terminal tab and complete the following commands:

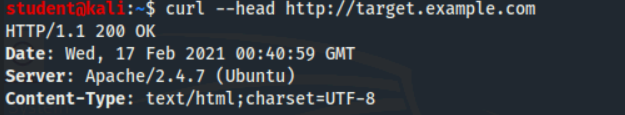
1. Type curl -s -I http://target.example.com | grep -e "Server: “ and hit enter. Take a screenshot of the results and name it 6cURLbanner1 and save it to the scanning folder. These screenshots will be referenced in the report in later modules.



1. Type curl --head http://target.example.com and hit enter.



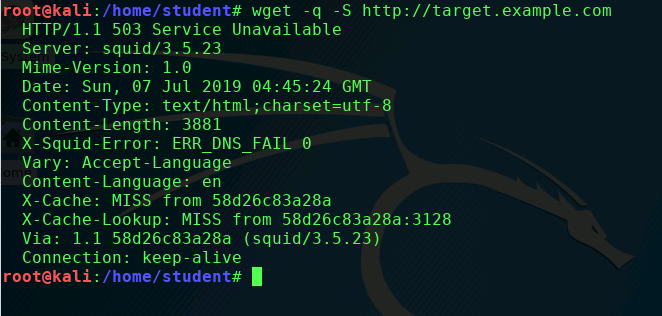
Take a screenshot of the results and name it 7cURLbanner2. Save the scan in the scanning folder.

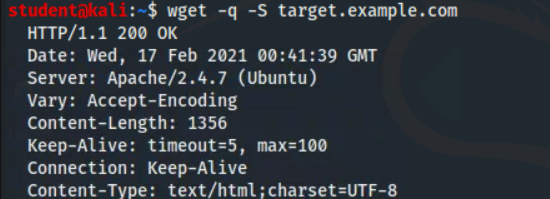


**Task 3: Banner Grabbing with Wget**

Again, it is best to execute this command in a new terminal so it can be easily referred back to later. Take a screenshot of the results and name it 8wgetbanner and save it to the scanning folder.

Type the following command: wget -q -S target.example.com and hit enter.



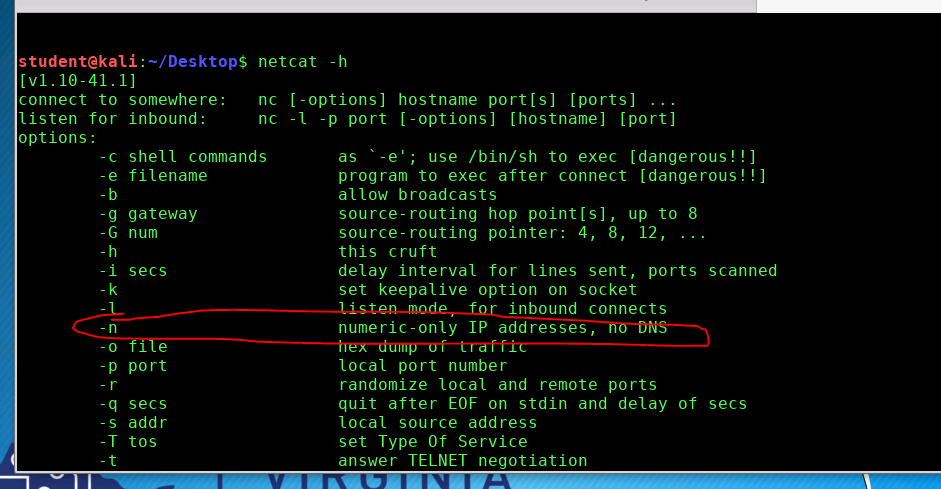


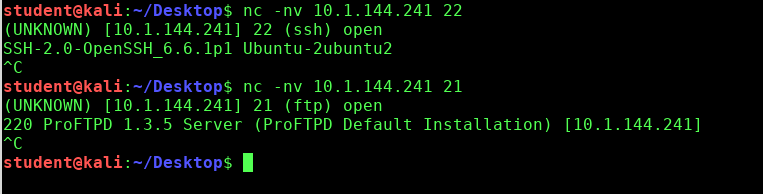
**Task 4: Banner Grabbing with Netcat**

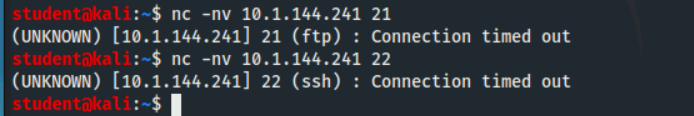
It is best to execute this command in a new terminal so it can be easily referred back to later. Remember to take a screenshot of the results and name it 9netcatbanner and save it to the scanning folder.

Type the following commands:

* nc -h and hit enter. We do not want to resolve DNS, so we need a -n, and we want to print more results to the screen, so we will use -v. Combine them for a -nv.
* nc -nv <target IP> 22 and hit enter.Press ctrl+c as soon as you see the server results.
* nc -nv <target IP> 21 and hit enter.Press ctrl+c as soon as you see the server



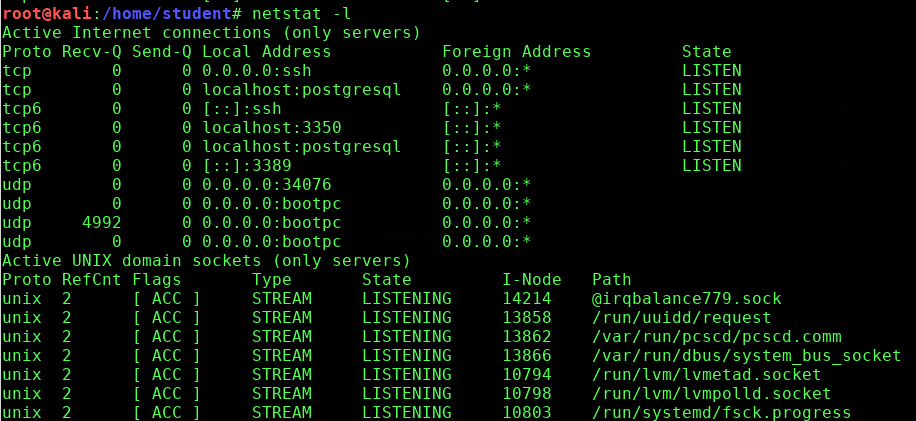


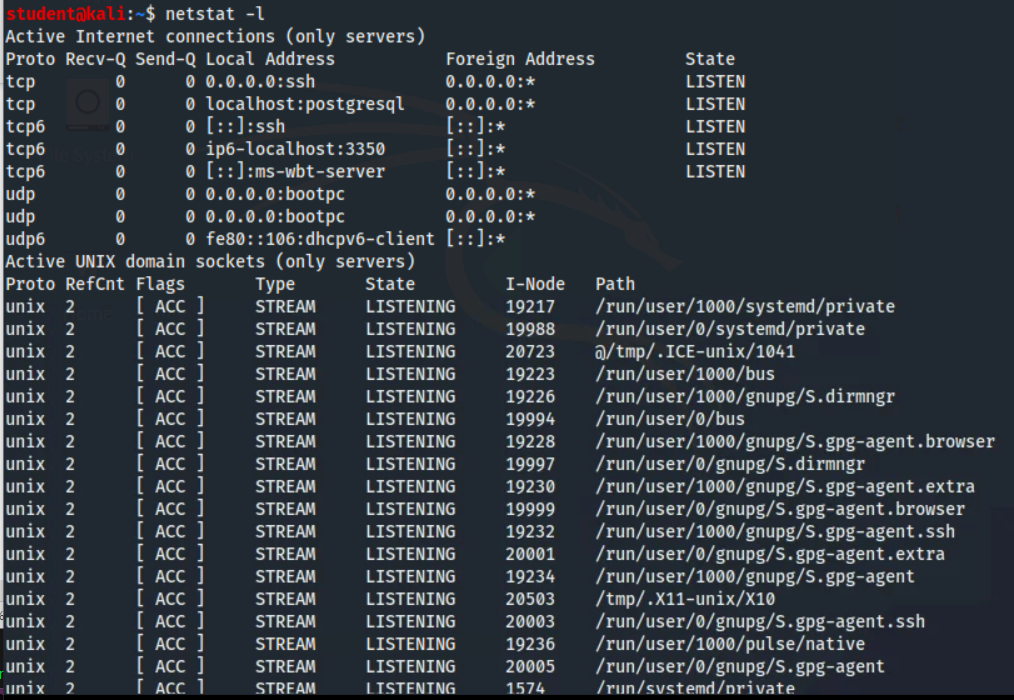


Task 5: Discovering listening ports with Netstat

Remember that Netstat is a utility that will list network connections. Attackers can use this information to gain a better understanding of the network. It is best to execute this command in a new terminal so it can be easily referred back to later.

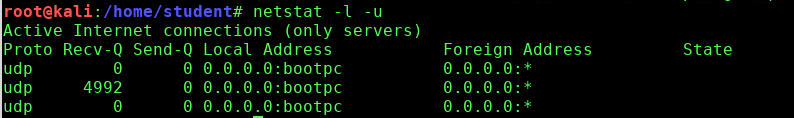
Type the following command: netstat -l and hit enter. This scan will list all listening ports. This is too much information and we need to narrow it down. Ensure you take a screenshot of the results and name it 10netstat1 and save it to the scanning folder.

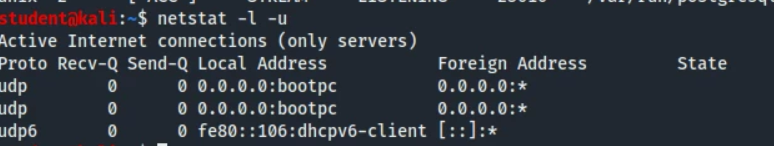




Next we will scan for only UDP ports that are listening. Type the following command:

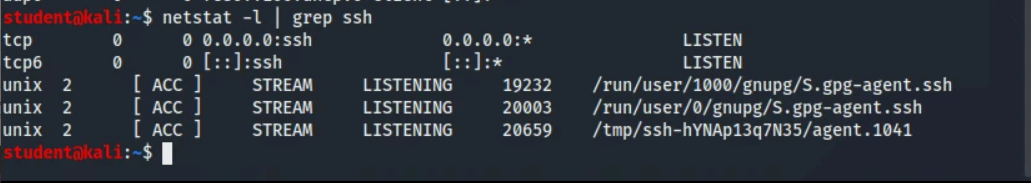
netstat -l -u and hit enter.





You can filter the scan with grep by port or service. Type the following command: netstat -l | grep ssh and hit enter.





Now let’s try a few more way to filter. Type the following commands:

* netstat -l | grep rdp and hit enter.
* netstat -l | grep 21 and hit enter.

What we are attempting to do is gain as much information about the network as possible so that we can find vulnerabilities. Netstat is useful to administrators as a check to see if attackers have opened or connected to listening ports; however, the Netstat tool will also allow an attacker to see all listening ports. This will provide an attacker with a further understanding of the network and what services they may be able to exploit.

Attach the screenshots for the last two netstat commands here and submit your lab worksheet.

