Colby Heilner

Professor Torres

3/1

IT 145

Lab 5

Part A:

- Log onto Netlabve1-->Cisco CCNA Cyber Ops v1 Lab 12.1.1.7 Snort and Firewall Rules
- This environment is not properly configured. You can scan the internal network - directly from the external kali box. This is what I want you to do.
-

Log onto the kali box (root/cyberops)

- Scan **ALL** the boxes on the network. For **ALL** the ports that you find:
  - Try to enumerate every port.
  - Schedule your lab accordingly, this lab will take a while
  - use google and/or chatgpt for your research
  - The goal of this lab is to develop your attack surface.
  - screenshot 1-2 scans that you feel are most relevant
  - screenshot your enumeration techniques
  - if you see a front door- try to open it (**do not exploit or brute-force**)

    I can scan all subnets in the environment and then see my attack surface.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Host is up (0.00041s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 192.168.0.10
Host is up (0.00039s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.0.11
Host is up (0.00071s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 50.01 second
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT 209.165.200.224

Starting Nmap 7.40 ( https://nmap.org ) at 2025-03-01 18:43 EST
Note: Host seems down. If it is really up, but blocking our ping
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
root@kali:~# nmap -sT 209.165.200.235

Starting Nmap 7.40 ( https://nmap.org ) at 2025-03-01 18:43 EST
```

- ******ALL I WANT IS YOUR ATTACK SURFACE WITH SOME SCREENSHOTS******

  Let's say I wanted to go into the door, I pick port 80 because I am more familiar with websites then anything.

  Because I am not going to exploit I will just do very light digging. First version and Operating system.

```
root@kali:~# nmap -sT 192.168.0.11 -O -sV -p 80

Starting Nmap 7.40 ( https://nmap.org ) at 2025-03-01 18:46 EST
Nmap scan report for 192.168.0.11
Host is up (0.00050s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.12.0
Warning: OSScan results may be unreliable because we could not find at least
pen and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.6 (97%), Linux 3.16 (95%), ASUS RT-N56U
 (Linux 3.4) (95%), Linux 3.10 - 4.2 (94%), Linux 3.13 (94%), Linux 3.13 - 3
(94%), Android 5.0 - 5.1 (93%), Linux 3.2 - 3.10 (93%), Linux 3.2 - 3.16 (93
Linux 3.4 - 3.10 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

This is super good info, but it may not always be this easy. I can also use things like curl and burp to get a little more manual information. Now that I see nginx 1.12.0 I have got the info I need if I wanted to try and find exploits.

```
root@kali:~# curl http://192.168.0.11
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@kali:~#
```

Works for other ports as well,

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
Warning: OSScan results may be unreliable because w
Aggressive OS guesses: Linux 3.2 - 4.6 (97%), Linux
 4.2 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94
```

Part B:

- Research how to run the below commands, and run them against all of the hosts in NDG Ethical Hacking NetLab 01. Screenshot your results. Use the Metasploit framework ONLY -on Kali -for your scans:
    - Use the Metasploit Unleased website below, (Metasploit fundamentals > Databases > Using the Database) and run the nmap scans according to the website to try to fill up your host area.
    - Search for and run arp_sweep, udp_sweep, syn, tcp, ack, and xmas scans against the hosts on this network.
    - Enumerate the boxes that you see with **ONLY Metasploit** (Auxiliary is your friend)

      Arp sweep did not work for me, here is UDP sweep

```
msf auxiliary(udp_sweep) > run

[*] Sending 13 probes to 192.168.0.0->192.168.0.255 (256 hosts)
[*] Discovered DNS on 192.168.0.254:53 (cf5481050000000000000000)
[*] Discovered NTP on 192.168.0.254:123 (240c04ea0000000000000007f0000
000000000c54f234b71b152f3eb6e20b840dd1431eb6e20b84100c819)
[*] Scanned 256 of 256 hosts (100% complete)
```

      Massive tip is to just set your host for all commands using setg

```
msf auxiliary(xmas) > setg RHOSTS 192.168.0.0/24
RHOSTS => 192.168.0.0/24
msf auxiliary(xmas) >
```

Xmas is horrible.

```
msf auxiliary(xmas) > set threads 4
threads => 4
msf auxiliary(xmas) > run

[*]  TCP OPEN|FILTERED 192.168.0.0:1
[*]  TCP OPEN|FILTERED 192.168.0.1:1
[*]  TCP OPEN|FILTERED 192.168.0.2:1
[*]  TCP OPEN|FILTERED 192.168.0.3:1
[*]  TCP OPEN|FILTERED 192.168.0.4:1
[*]  TCP OPEN|FILTERED 192.168.0.5:1
[*]  TCP OPEN|FILTERED 192.168.0.6:1
[*]  TCP OPEN|FILTERED 192.168.0.7:1
[*]  TCP OPEN|FILTERED 192.168.0.8:1
[*]  TCP OPEN|FILTERED 192.168.0.9:1
[*]  TCP OPEN|FILTERED 192.168.0.10:1
[*]  TCP OPEN|FILTERED 192.168.0.11:1
[*]  TCP OPEN|FILTERED 192.168.0.12:1
[*]  TCP OPEN|FILTERED 192.168.0.13:1
[*]  TCP OPEN|FILTERED 192.168.0.14:1
```

Ack scans never got anything.

```
msf auxiliary(ack) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ack) > set ports 21-800
ports => 21-800
msf auxiliary(ack) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ack) >
```

Finally regular tcp got some results.

```
msf auxiliary(syn) > setg threads 10
threads => 10
msf auxiliary(syn) > setg timeout 300
timeout => 300
msf auxiliary(syn) > set ports 1-4000
ports => 1-4000
msf auxiliary(syn) > run

[*]  TCP OPEN 192.168.0.100:22
[*]  TCP OPEN 192.168.0.100:443
[*]  TCP OPEN 192.168.0.100:444
[*]  TCP OPEN 192.168.0.100:514
```

I enjoy using msf but mainly more for its payloads in actual exploitation.

- ******ALL I WANT IS YOUR ATTACK SURFACE WITH SOME SCREENSHOTS******

https://www.offensive-security.com/metasploit-unleashed/using-databases/ (Links to an external site.)

Part C:

- Capture a screenshot of the results of each major command. Research what the below commands do, run them against all of the systems that you find in NISGTC-Ethical Hacking- Lab 1. Remember to run either Tcpdump or Wireshark during your scans.
    - Run dnsrecon, dnsenum, smbclient, nbtscan, snmpenum, nmap, nmblookup, snmpcheck enum4linux, etc.
    - Research additional Enumeration techniques and attempt to **Enumerate ALL** of the ports from all of the host in this lab.
    - If the front door is open, please enter (**do not run exploits or attempt to brute-force**)
    - ******ALL I WANT IS YOUR ATTACK SURFACE WITH SOME SCREENSHOTS******

      I looked at some alternative port scanning methods, enumeration tools etc.. Here is what I found and my results.

A way to find alive hosts,

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address      Count  Len   MAC Vendor
-----------------------------------------------------------------------------
216.5.1.200     00:50:56:98:00:1a    01    060   VMWare, Inc.
```

A hping3 command that FLOODS packets

```
root@bt:~# hping3 -S 216.5.1.200 -p 1-55555 --flood
HPING 216.5.1.200 (eth0 216.5.1.200): S set, 40 headers
hping in flood mode, no replies will be shown
```

```
k 550789737, win 0, length 0
20:22:09.772338 IP 216.6.1.100.25732 > 216.5.1.200.tcpmux: Flags [S], seq 1270
1470, win 512, length 0
20:22:09.772440 IP 216.5.1.200.tcpmux > 216.6.1.100.25732: Flags [R.], seq 0,
k 1270631471, win 0, length 0
20:22:09.772475 IP 216.6.1.100.25733 > 216.5.1.200.tcpmux: Flags [S], seq 4747
357, win 512, length 0
20:22:09.772576 IP 216.5.1.200.tcpmux > 216.6.1.100.25733: Flags [R.], seq 0,
k 474781358, win 0, length 0
20:22:09.772610 IP 216.6.1.100.25734 > 216.5.1.200.tcpmux: Flags [S], seq 5806
451, win 512, length 0
20:22:09.772711 IP 216.5.1.200.tcpmux > 216.6.1.100.25734: Flags [R.], seq 0,
k 580687452, win 0, length 0
20:22:09.772745 IP 216.6.1.100.25735 > 216.5.1.200.tcpmux: Flags [S], seq 7720
692, win 512, length 0
20:22:09.772845 IP 216.5.1.200.tcpmux > 216.6.1.100.25735: Flags [R.], seq 0,
k 772073693, win 0, length 0
20:22:09.772879 IP 216.6.1.100.25736 > 216.5.1.200.tcpmux: Flags [S], seq 7353
487, win 512, length 0
20:22:09.772979 IP 216.5.1.200.tcpmux > 216.6.1.100.25736: Flags [R.], seq 0,
k 735322488, win 0, length 0
20:22:09.773013 IP 216.6.1.100.25737 > 216.5.1.200.tcpmux: Flags [S], seq 2075
7268, win 512, length 0
```

9creen shot does not do it justice. ^

You could also just run curl to see if you get anything. I did.

```
root@bt:~# curl -I 216.5.1.200
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Thu, 27 Dec 2012 02:39:12 GMT
Accept-Ranges: bytes
ETag: "42dec35adbe3cd1:0"
Server: Microsoft-IIS/7.5
Date: Sun, 02 Mar 2025 01:24:26 GMT
```

This is a fairly good idea of enum on ftp. Checking to see if its open and performing a small banner grab, then checking for anon login, **which it has!**

```
root@bt:~# nc -nv 216.5.1.200 21
(UNKNOWN) [216.5.1.200] 21 (ftp) open
220 Microsoft FTP Service

500 '
 ': command not understood.

500 '
 ': command not understood.
help
451 The parameter is incorrect.
-help
451 The parameter is incorrect.
^C
root@bt:~# ftp 216.5.1.200
Connected to 216.5.1.200.
220 Microsoft FTP Service
Name (216.5.1.200:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
```

I could then look through it or perform more commands to learn version and find exploits.

This could also be considered a method of finding open ports I believe.

```
root@bt:~# nc -nv 216.5.1.200 26
(UNKNOWN) [216.5.1.200] 26 (?) : Connection refused
root@bt:~# nc -nv 216.5.1.200 27
(UNKNOWN) [216.5.1.200] 27 (?) : Connection refused
root@bt:~# nc -nv 216.5.1.200 443
(UNKNOWN) [216.5.1.200] 443 (https) : Connection refused
root@bt:~# nc -nv 216.5.1.200 80
(UNKNOWN) [216.5.1.200] 80 (www) open
```

Now if I find out it had smb running I can run some of these commands which were not installed in the netlab.

enum4linux -U 192.168.1.100

enum4linux -S 192.168.1.100

enum4linux -a 192.168.1.100

smbclient -L //192.168.1.100 -U anonymous%""

```
root@bt:~# smbclient -L //216.5.1.200 -U anonymous%""
Anonymous login successful
Domain=[WORKGROUP] OS=[Windows 7 Professional 7600] Server=[Windows 7 Professional 6.1]

        Sharename       Type      Comment
        ---------       ----      -------
Error returning browse list: NT_STATUS_ACCESS_DENIED
session request to 216.5.1.200 failed (Called name not present)
session request to 216 failed (Called name not present)
session request to *SMBSERVER failed (Called name not present)
NetBIOS over TCP disabled -- no workgroup available
root@bt:~#
```