



SCANNING THE NETWORK ON THE LAN

ETHICAL HACKING & Lab # 2

Student Info

Name: SRIJA PABBA

Student ID: 00866719

Email:spabb6@unh.newhaven.edu

Table of Contents

I.	Executive Summary	2
	Highlights	
	Objectives	
II.	Lab Description Details	2
	Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives	
III.	Supporting Evidence.....	15
IV.	Conclusion & Wrap-Up	17
	Summary with observations, Success & Failures, Challenges	

Executive Summary

Highlights

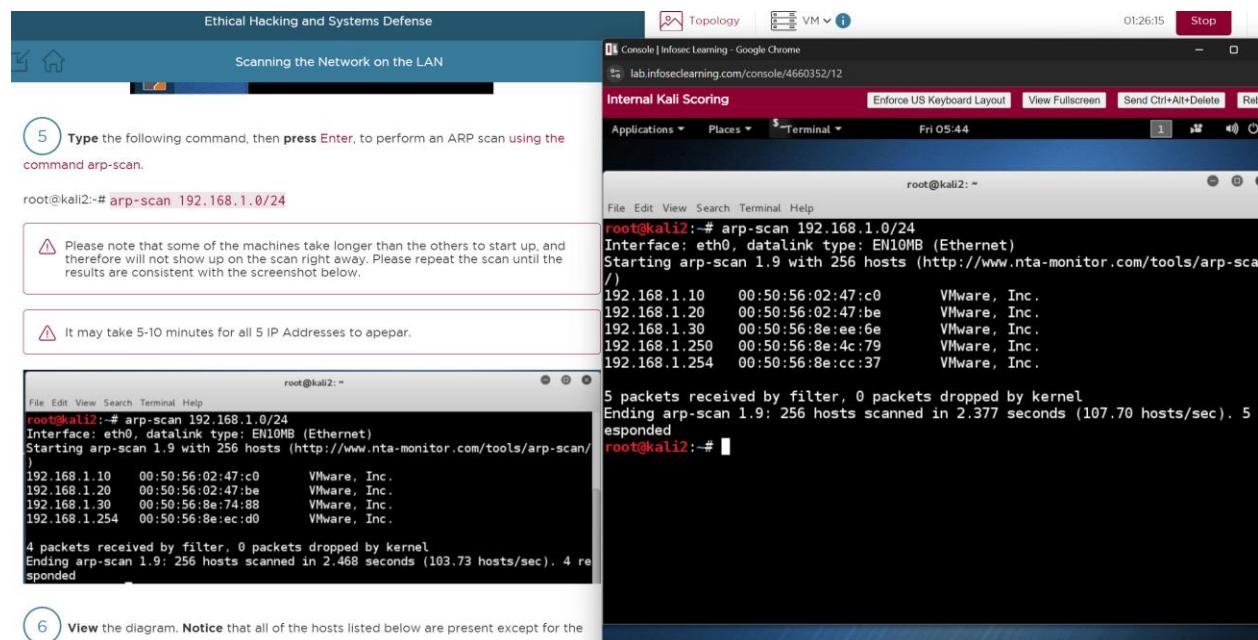
In this lab, I will perform a network scan using Kali Linux to identify hosts and open TCP ports on a local area network (LAN). I'll use nmap/Zenmap for scanning, followed by exploiting vulnerabilities using Metasploit and Armitage.

Objectives

The objective of this lab is for me to scan the LAN for active machines, identify their open ports, and exploit the vulnerabilities found using Metasploit and Armitage to gain control of a target machine.

Lab Description Details

Arp-scan 192.168.1.0/24



Nmap -sT 192.168.1.10

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Internal Kali Scoring". The command entered is "root@kali2:~# nmap -sT 192.168.1.10". The output of the scan is displayed, showing various open ports and services on the target host.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:30 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00017s latency).
Not shown: 971 filtered ports
PORT      STATE SERVICE
7/tcp      open  echo
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
21/tcp     open  ftp
23/tcp     open  telnet
25/tcp     open  smtp
42/tcp     open  nameserver
53/tcp     open  domain
80/tcp     open  http
88/tcp     open  kerberos-sec
110/tcp    open  pop3
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
143/tcp    open  imap
389/tcp    open  ldap
443/tcp    open  https
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
5268/tcp   open  globalcatLDAP
MAC Address: 00:50:56:02:47:CO (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.13 seconds
```

Nmap -sT 192.168.1.20

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Internal Kali Scoring". The command entered is "root@kali2:~# nmap -sT 192.168.1.20". The output of the scan is displayed, showing various open ports and services on the target host.

```
Host is up (0.0042s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingerlock
2049/tcp   open  nfs
3306/tcp   open  mysql
5432/tcp   open  postgresql
6667/tcp   open  irc
8009/tcp   open  ajp13
8180/tcp   open  unknown
MAC Address: 00:50:56:80:47:EE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

CHALLENGE #3

12 Type the following command, then press Enter, to perform a TCP scan of 192.168.1.254 and determine what ports are open.

```
root@kali2:~#
```

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

Nmap -sT 192.168.1.30

```
root@kali2:~# nmap -sT 192.168.1.30
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-08 01:12 EDT
Nmap scan report for 192.168.1.30
Host is up (0.0042s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:50:56:02:47:E6 (VMware)

root@kali2:~# nmap -sT 192.168.1.30
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:37 EDT
Nmap scan report for 192.168.1.30
Host is up (0.00014s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  flag4:232441
MAC Address: 00:50:56:8E:5D:E7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.92 seconds
root@kali2:~#
```

Nmap -sT 192.168.1.254

```
Ethical Hacking and Systems Defense
Scanning the Network on the LAN
12 Type the following command, then press Enter, to perform a
TCP scan of 192.168.1.254 and determine what ports are open.

root@kali2:~# nmap -sT 192.168.1.254
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-08 01:15 EDT
Nmap scan report for 192.168.1.254
Host is up (0.0011s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:80:E7:B7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.22 seconds
root@kali2:~# nmap -sT 192.168.1.254
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:41 EDT
Nmap scan report for 192.168.1.254
Host is up (0.00017s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:8E:11:DE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
root@kali2:~#
```

Nmap -O 192.168.1.10 | tail

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

13 Type the following command, then press Enter, to perform an OS scan of 192.168.1.10 to determine the operating system of this host.

```
root@kali2:~# nmap -O 192.168.1.10 | tail
```

root@kali2:~# nmap -O 192.168.1.10 | tail

Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-09-20 00:41 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00007s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
MAC Address: 00:50:56:8E:11:DE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
root@kali2:~# nmap -O 192.168.1.10 | tail
MAC Address: 00:50:56:02:47:C0 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/phone
Running: Microsoft Windows 2008[7]Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7:::professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::: cpe:/o:microsoft:windows_vista_sp1:::sp1
OS details: Windows Server 2008 R2, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 44.00 seconds
root@kali2:~#

Nmap -O 192.168.1.20 | tail

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

14 Type the following command, then press Enter, to perform an OS scan of 192.168.1.20 to determine the operating system of this host.

```
root@kali2:~# nmap -O 192.168.1.20 | tail
```

root@kali2:~# nmap -O 192.168.1.20 | tail

Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-09-20 00:41 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00007s latency).
Not shown: 997 filtered ports
OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 41.81 seconds
root@kali2:~# nmap -O 192.168.1.20 | tail
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone/general purpose
Running (JUST GUESSING): Microsoft Windows Phone|2008[7]|Vista|2012 (94%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:microsoft:windows_cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7:::professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::: cpe:/o:microsoft:windows_vista:::sp1 cpe:/o:microsoft:windows_server_2012 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (94%), Windows Server 2008 R2 (93%), Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 SP1 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 SP1 (89%), Microsoft Windows 8 Enterprise (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 26.94 seconds
root@kali2:~#

Nmap -O 192.168.1.30 | tail

Ethical Hacking and Systems Defense
Scanning the Network on the LAN

15 Type the following command, then press Enter, to perform an OS scan of 192.168.1.30 to determine the operating system of this host.

```
root@kali2:~# nmap -O 192.168.1.30 | tail
```

root@kali2:~# nmap -O 192.168.1.30 | tail

16 Type the following command, then press Enter, to perform an OS scan of 192.168.1.254 to determine the operating system of

```
root@kali2:~# nmap -O 192.168.1.30 | tail
```

File Edit View Search Terminal Help

Running (JUST GUESSING): Microsoft Windows Phone[2008|7] Vista[2012 (94%), FreeBSD 6.X (86%) OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7:::professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::: cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012 cpe:/o:freebsd:freebsd:6.2 Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (94%), Windows Server 2008 R2 (93%), Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 SP1 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 SP1 (89%), Microsoft Windows 8 Enterprise (89%) No exact OS matches for host (test conditions non-ideal). Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 26.94 seconds

root@kali2:~# nmap -O 192.168.1.30 | tail

8180/tcp open flag4:232441 MAC Address: 00:0C:29:FA:00:2A (VMware) Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33 Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds

root@kali2:~#

Nmap -O 192.168.1.254 | tail

```
root@kali2:~# nmap -O 192.168.1.254 | tail
```

root@kali2:~# nmap -O 192.168.1.254 | tail

17 Type the following command, then press Enter, to open Zenmap. After Zenmap opens, type 192.168.1.* in the Target box

```
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop
```

OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds

root@kali2:~# nmap -O 192.168.1.254 | tail

MAC Address: 00:50:56:8E:11:DE (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Comau C4G robot control unit (92%)
Aggressive OS guesses: Comau C4G robot control unit (92%), FreeBSD 8.1 (85%), OpenBSD 4.3 (85%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

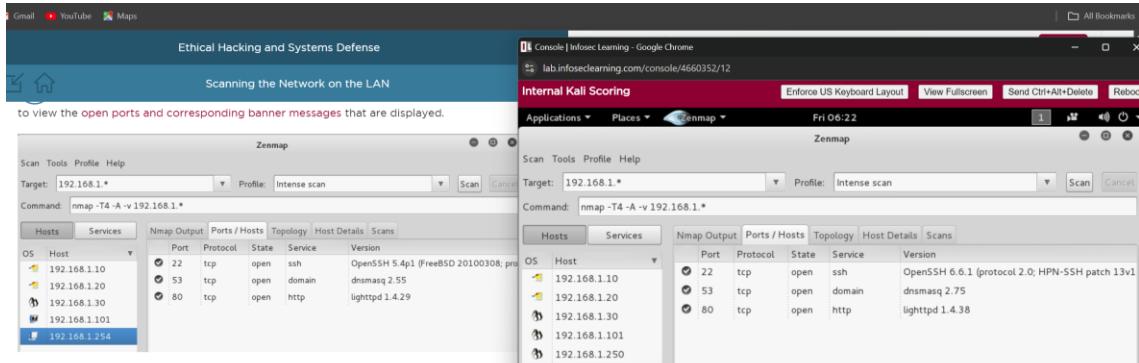
OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 31.64 seconds

```
Device type: specialized  
Running (JUST GUESSING): Comau C4G robot control unit (92%)  
Aggressive OS guesses: Comau C4G robot control unit (92%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop
```

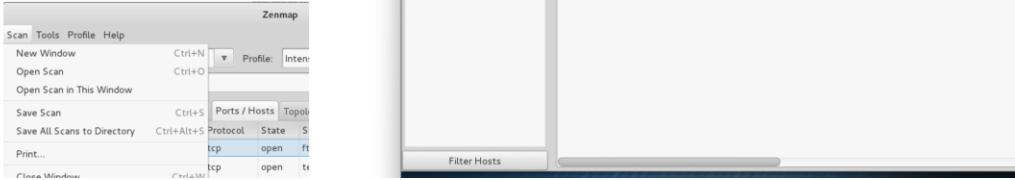
OS detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 37.93 seconds

root@kali2:~#

I had run 192.168.1.* in Zenmap



23 Select Scan from the menu bar and then select Quit to close Zenmap.



18 After the scan is complete, the five hosts will be displayed in the left panel of Zenmap.



19 Click on the first host and click the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed.

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

Filter Hosts 49165 tcp open msrpc Microsoft Windows RPC

20 Click on the second host and click the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed.

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.10	21	tcp	open	ftp	Microsoft ftptd
	192.168.1.20	22	tcp	open	ssh	APC AOS cryptlib sshd (protocol 2.0)
	192.168.1.30	80	tcp	open	http	Microsoft IIS httpd 10.0
	192.168.1.101	135	tcp	open	msrpc	Microsoft Windows RPC
	192.168.1.254	139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
	192.168.1.20	445	tcp	open	microsoft-ds	(primary domain: WORKGROUP)
	192.168.1.20	3389	tcp	open	ms-wbt-server	
	192.168.1.20	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Internal Kali Scoring

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

Fri 06:20

Zenmap

Scan Tools Profile Help

Target: 192.168.1.* Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.1.*

Ports / Hosts Tab (Selected)

Port	Protocol	State	Service	Version
21	tcp	open	ftp	Microsoft ftptd
22	tcp	open	ssh	APC AOS cryptlib sshd (protocol 2.0)
80	tcp	open	http	Microsoft IIS httpd 10.0
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
445	tcp	open	microsoft-ds	(primary domain: WORKGROUP)
3389	tcp	open	ms-wbt-server	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

Filter Hosts 192.168.1.254

21 Click on the third host and click the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed.

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.10	139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
	192.168.1.20	445	tcp	open	microsoft-ds	(primary domain: WORKGROUP)
	192.168.1.30	3389	tcp	open	ms-wbt-server	
	192.168.1.254	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Internal Kali Scoring

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

Fri 06:21

Zenmap

Scan Tools Profile Help

Target: 192.168.1.* Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.1.*

Ports / Hosts Tab (Selected)

Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	
514	tcp	open	shell	Netkit rsh
1099	tcp	open	java-rmi	Java RMI Registry
1524	tcp	open	shell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
6667	tcp	open	irc	Unreal ircd

I had used msfconsole in armitage

Msf > db_nmap 192.168.1.*

lab.infoseclearning.com/console/4659950/12

Internal Kali Scoring

Applications ▾ Places ▾ Terminal ▾ Fri 01:22 root@kali2: ~/armitage

```
File Edit View Search Terminal Help
[*] Nmap: Not shown: 990 closed ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 21/tcp open  ftp
[*] Nmap: 22/tcp open ssh
[*] Nmap: 23/tcp open telnet
[*] Nmap: 25/tcp open smtp
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open nfs
[*] Nmap: 3306/tcp open mysql
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 6667/tcp open irc
[*] Nmap: 8009/tcp open ajp13
[*] Nmap: 8180/tcp open flag4:232441
[*] Nmap: MAC Address: 00:50:56:8E:5D:E7 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.250
[*] Nmap: Host is up (0.00014s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 1688/tcp open nsjip-data
[*] Nmap: MAC Address: 00:50:56:8E:AD:5E (VMware)
[*] Nmap: Nmap scan report for 192.168.1.254
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 22/tcp open ssh
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
```

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

Note: This scan will take about 5 minutes to complete. The words Nmap done will be displayed when finished.

9 When the db_nmap scan is done, the time of the scan and number of hosts up (6 including Kali 2) will be displayed.

```
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 6667/tcp open irc
[*] Nmap: 8009/tcp open ajp13
[*] Nmap: 8180/tcp open unknown
[*] Nmap: MAC Address: 00:0C:29:FA:D0:2A (VMware)
[*] Nmap: Nmap scan report for 192.168.1.254
[*] Nmap: Host is up (0.00053s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 22/tcp open ssh
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: MAC Address: 00:0C:29:D6:01:96 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000090s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 238.20 seconds
```

NOTE: If the scan does not show at least 6 hosts up then rerun it until it does. This will affect the completion of the scan.

PREVIOUS NEX... msf > []

```
[*] Nmap: 22/tcp open ssh
[*] Nmap: 23/tcp open telnet
[*] Nmap: 25/tcp open smtp
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open nfs
[*] Nmap: 3306/tcp open mysql
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 6667/tcp open irc
[*] Nmap: 8009/tcp open ajp13
[*] Nmap: 8180/tcp open flag4:232441
[*] Nmap: MAC Address: 00:50:56:8E:5D:E7 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.250
[*] Nmap: Host is up (0.00014s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 1688/tcp open nsjip-data
[*] Nmap: MAC Address: 00:50:56:8E:AD:5E (VMware)
[*] Nmap: Nmap scan report for 192.168.1.254
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 22/tcp open ssh
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 244.26 seconds
```

Msf > ./Armitage And we connected

lab.infoseclearning.com/course/WICWEVYQVN/lab/UWUENTBWQA

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

```
msf > ./armitage
[*] exec: ./armitage
```

11 After the box appears, click the Connect button.



```
Internal Kali S... Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Reboot
Applications Places armitage Fri 01:43
root@kali2: ~/armitage
File Edit View Search Terminal Help
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open m
[*] Nmap: 5432/tcp open m
[*] Nmap: 6667/tcp open i Host
[*] Nmap: 8009/tcp open a
[*] Nmap: 8180/tcp open a
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 1688/tcp open n Pass
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 244.26 seconds
msf > ./armitage
[*] exec: ./armitage
```

12 Click Yes when you are asked if you want to Start

← PREVIOUS NEXT →

lab.infoseclearning.com/course/WICWEVYQVN/lab/UWUENTBWQA

Ethical Hacking and Systems Defense

Scanning the Network on the LAN

```
msf > ./armitage
[*] exec: ./armitage
```

11 After the box appears, click the Connect button.



```
Internal Kali S... Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Reboot
Applications Places armitage Fri 01:43
root@kali2: ~/armitage
File Edit View Search Terminal Help
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open m
[*] Nmap: 3306/tcp open m
[*] Nmap: 5432/tcp open m
[*] Nmap: 6667/tcp open i Host
[*] Nmap: 8009/tcp open a
[*] Nmap: 8180/tcp open a
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 1688/tcp open n Pass
[*] Nmap: MAC Address: 00:50:56:8E:11:DE (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 244.26 seconds
msf > ./armitage
[*] exec: ./armitage
```

12 Click Yes when you are asked if you want to Start

← PREVIOUS NEXT →

Scanning the Network on the LAN

```
msf > ./armitage
[*] exec: ./armitage
```

11 After the box appears, click the Connect button.

12 Click Yes when you are asked if you want to Start

← PREVIOUS NEX↑

File Edit View Search Terminal Help

```
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open n
[*] Nmap: 5422/tcp open m
[*] Nmap: 6667/tcp open P
[*] Nmap: 8009/tcp open a
[*] Nmap: 8180/tcp open a
[*] Nmap: MAC Address: 00:50:56:8E:11:D
[*] Nmap: Host is up (0.0000020s latency).
[*] Nmap: Not shown: 999 c
[*] Nmap: PORT STATE S
[*] Nmap: 1688/tcp open n Pass
[*] Nmap: MAC Address: 00:50:56:8E:11:D
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.0000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 244.26 seconds
msf > ./armitage
[*] exec: ./armitage
```

Internal Kali Scoring

Applications Places Armitage-ArmitageMain Fri 06:55

Armitage

Armitage View Hosts Attacks Workspaces Help

auxiliary exploit payload post

192.168.1.250 192.168.1.254 192.168.1.10 192.168.1.30 192.168.1.20

Console Scan Scan Scan Scan Scan

```
[*] Scanned 1 of 1 hosts (100% complete)

[*] 1 scan to go...
msf auxiliary(ftp_version) > use scanner/smb/smb_version
msf auxiliary(smb_version) > set THREADS 24
THREADS => 24
msf auxiliary(smb_version) > set RPOR
RPOR => 445
msf auxiliary(smb_version) > set RHOSTS 192.168.1.20
RHOSTS => 192.168.1.20
msf auxiliary(smb_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.1.20:445 is running Windows 10 Pro (build:10240) (name:CONCORD) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 31.038s
msf auxiliary(smb_version) > |
```

I tried to attack analysis and completed.

2 Click OK to the message Attack Analysis Complete.

Message

Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

Happy hunting!

OK

Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

Happy hunting!

OK

3 Right-click on 192.168.1.30, select Attack, misc, and java_rmi_server.

← PREVIOUS NEX →

msf auxiliary(smb_version) > set RHOST 192.168.1.20
RHOSTS => 192.168.1.20
msf auxiliary(smb_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.1.20:445 is running Windows 10 Pro (build:10240) (name:CONCORD)
(domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 32.504s
msf auxiliary(smb_version) >

4 Click Launch.

Attack 192.168.1.30

Java RMI Server Insecure Default Configuration Java Code Execution

This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every

Option	Value
HTTPDELAY	10
LHOST	192.168.1.101
LPORT	5742
RHOST +	192.168.1.30
RPRT	1000

Targets: 0 => Generic (Java Payload)

Use a reverse connection

Show advanced options

Launch

Attack 192.168.1.30

Java RMI Server Insecure Default Configuration Java Code Execution

This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every

Option	Value
HTTPDELAY	10
LHOST	192.168.1.101
LPORT	17843
RHOST +	192.168.1.30
RPRT	1000

Targets: 0 => Generic (Java Payload)

Use a reverse connection

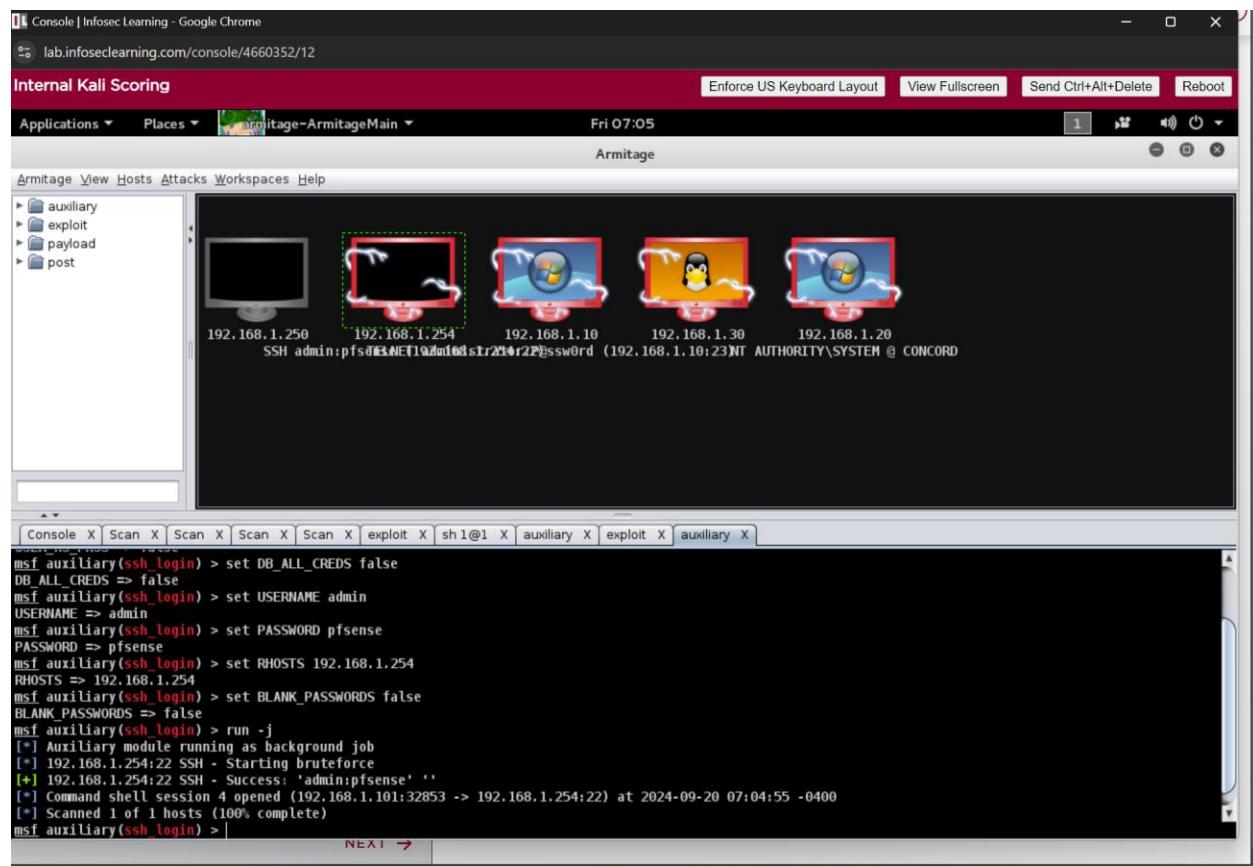
Show advanced options

Launch

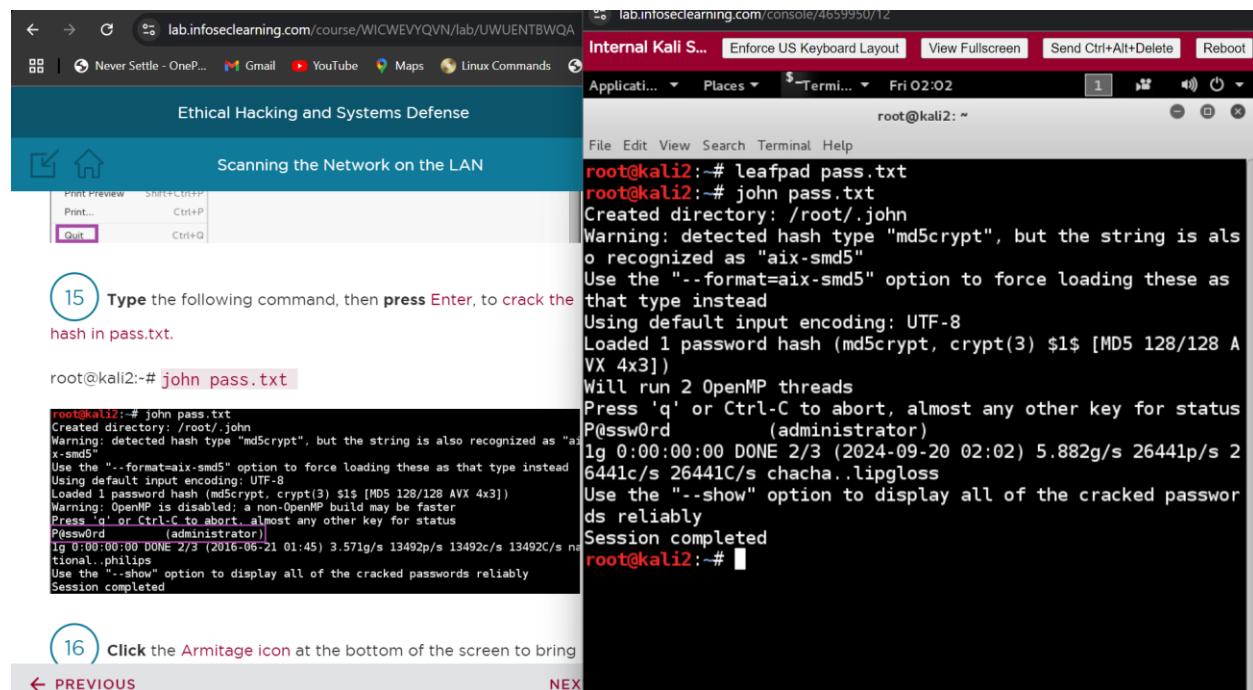
[*] Auxiliary module running as background job
[*] 192.168.1.20:445 is running Windows 10 Pro (build:10240) (name:CONCORD)
(domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 32.504s
msf auxiliary(smb_version) >

We exploited 192.168.1.* machine



We pasted the hash in leafpad pass.txt and john got used for txt file



Supporting Evidence

Nmap -sT 192.168.1.10

The screenshot shows a two-panel interface. On the left, a web-based challenge interface titled "Scanning the Network on the LAN" displays a challenge step 8: "Notice the flag of 999818. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab." It includes three challenge buttons: "SAMPLE CHALLENGE", "CHALLENGE #1", and "CHALLENGE #2". On the right, a terminal window titled "root@kali2: ~" shows the command "nmap -sT 192.168.1.10" and its output, which lists various open ports on the target host.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:30 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00037s latency).
Not shown: 971 filtered ports
PORT      STATE SERVICE
7/tcp      open  echo
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
21/tcp     open  ftp
23/tcp     open  telnet
25/tcp     open  smtp
42/tcp     open  nameserver
53/tcp     open  domain
80/tcp     open  http
88/tcp     open  kerberos-sec
110/tcp    open  pop3
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
143/tcp    open  imap
389/tcp    open  ldap
443/tcp    open  https
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatDAPssl
389/tcp   open  ms-wbt-server
49154/tcp  open  sampleflag:999818
49156/tcp  open  unknown
49157/tcp  open  flag2:717993
49158/tcp  open  flag3:554422
49163/tcp  open  unknown
MAC Address: 00:50:56:02:47:C0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.13 seconds
```

Nmap -sT 192.168.1.254

The screenshot shows a two-panel interface. On the left, a web-based challenge interface titled "Scanning the Network on the LAN" displays a challenge step 12: "Type the following command, then press Enter, to perform a TCP scan of 192.168.1.254 and determine what ports are open." It includes a challenge button "CHALLENGE #3". On the right, a terminal window titled "root@kali2: ~" shows the command "nmap -sT 192.168.1.254" and its output, which lists various open ports on the target host.

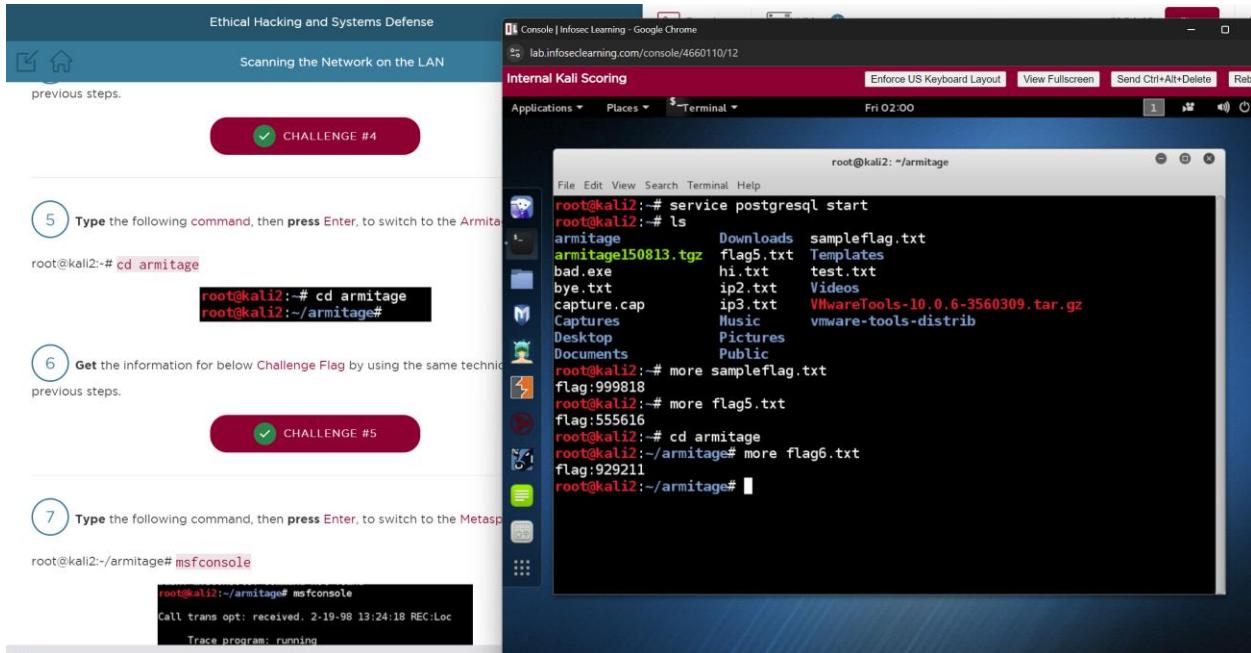
```
Host is up (0.0042s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingerlock
2049/tcp   open  nfs
3306/tcp   open  mysql
5432/tcp   open  postgresql
6667/tcp   open  irc
8009/tcp   open  ajp13
8180/tcp   open  unknown
MAC Address: 00:50:56:80:47:EE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

```
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingerlock
2049/tcp open  nfs
3306/tcp open  mysql
5432/tcp open  postgresql
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  flag4:232441
MAC Address: 00:50:56:8E:EE:6E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

We gathered the flag with more sampleflag.txt and Changed directory to Armitage by using “cd Armitage”



Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I used nmap to find other computers on the network and checked which ones had open ports. Then, I used tools called Metasploit and Armitage to access a computer that wasn't well-protected.

Identified risks

The main risks I found were from computers that weren't updated or secured properly, making it easy for someone to sneak in. Some computers had open ports that shouldn't be open, which could let attackers in easily.

Suggested recommendations

I recommend updating all computers regularly and closing ports that aren't needed. Also, setting up systems to detect when someone is trying to break in could help keep the network safe.

Your successes & failures

I did well in finding and getting into the vulnerable computer, but I struggled to tackle some tougher security on other machines. It was a good learning experience to see what works and what doesn't

Challenges

One of the biggest challenges was making sure my scanning activities didn't set off any alarms. It was also tricky to use Metasploit and Armitage effectively, especially when trying to make sure the attacks worked as planned.