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

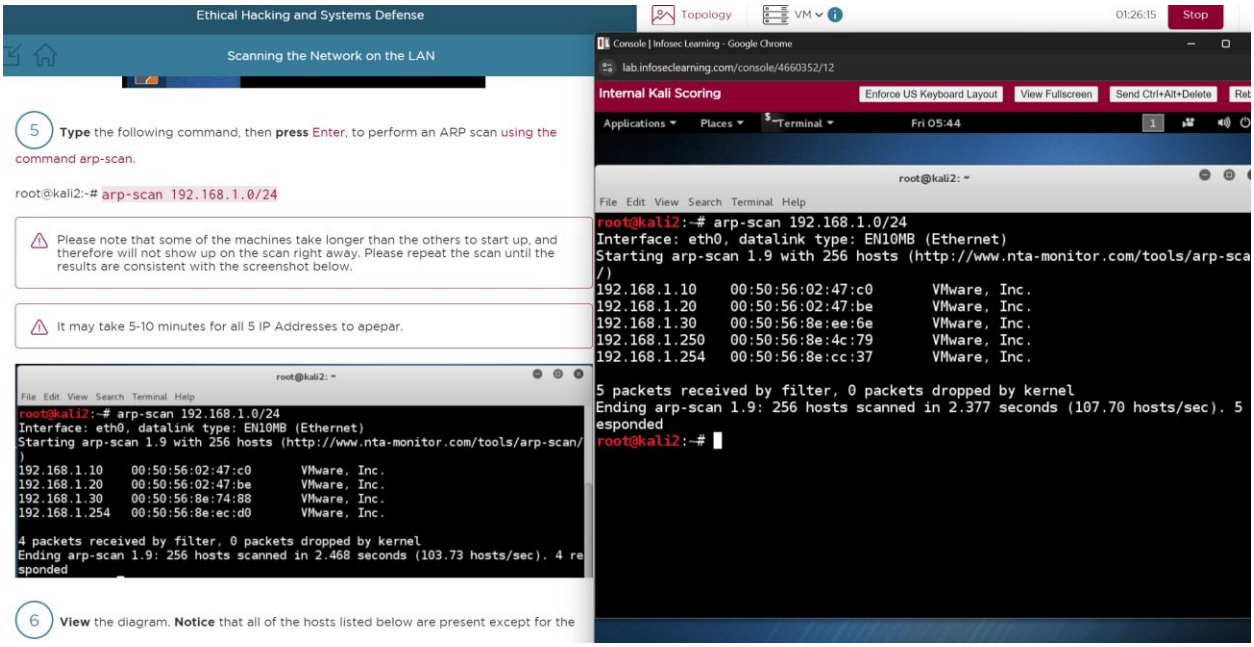
> *In this lab, I will perform a network scan using Kali Linux to identify hosts and open TCP ports on a local area network (LAN). I'll use nmap/Zenmap for scanning, followed by exploiting vulnerabilities using Metasploit and Armitage*

Objectives

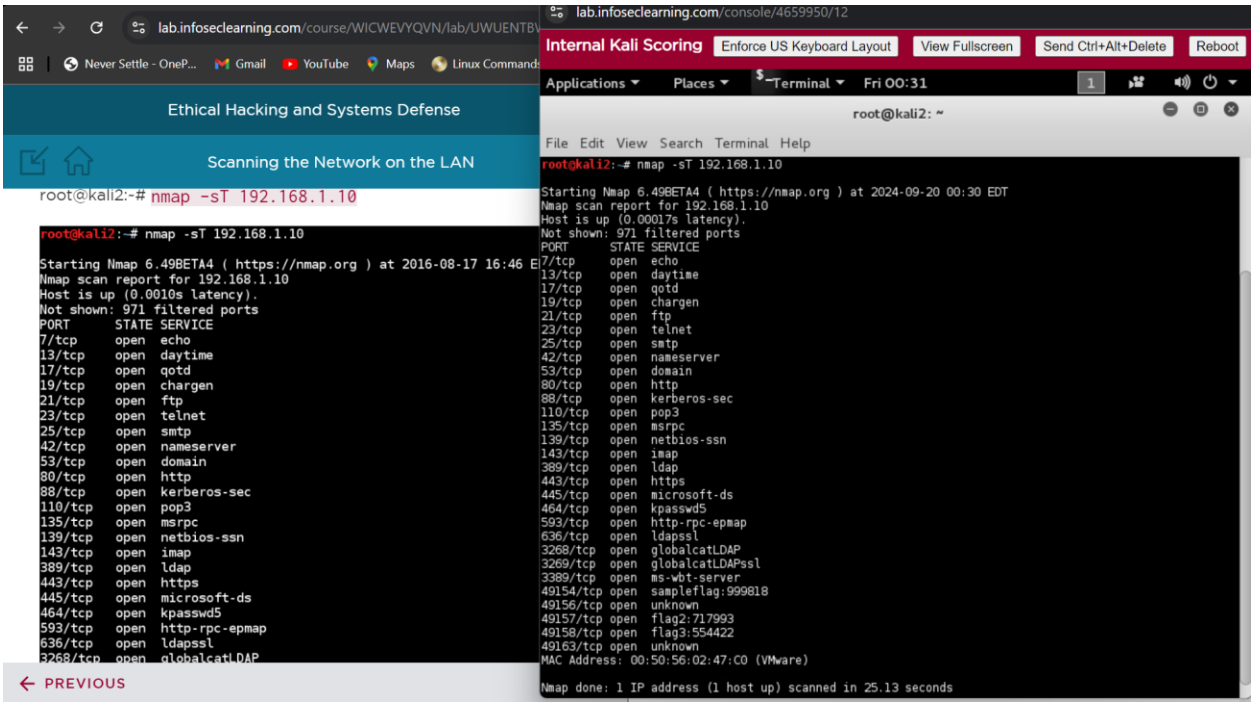
> *The objective of this lab is for me to scan the LAN for active machines, identify their open ports, and exploit the vulnerabilities found using Metasploit and Armitage to gain control of a target machine.*

Lab Description Details

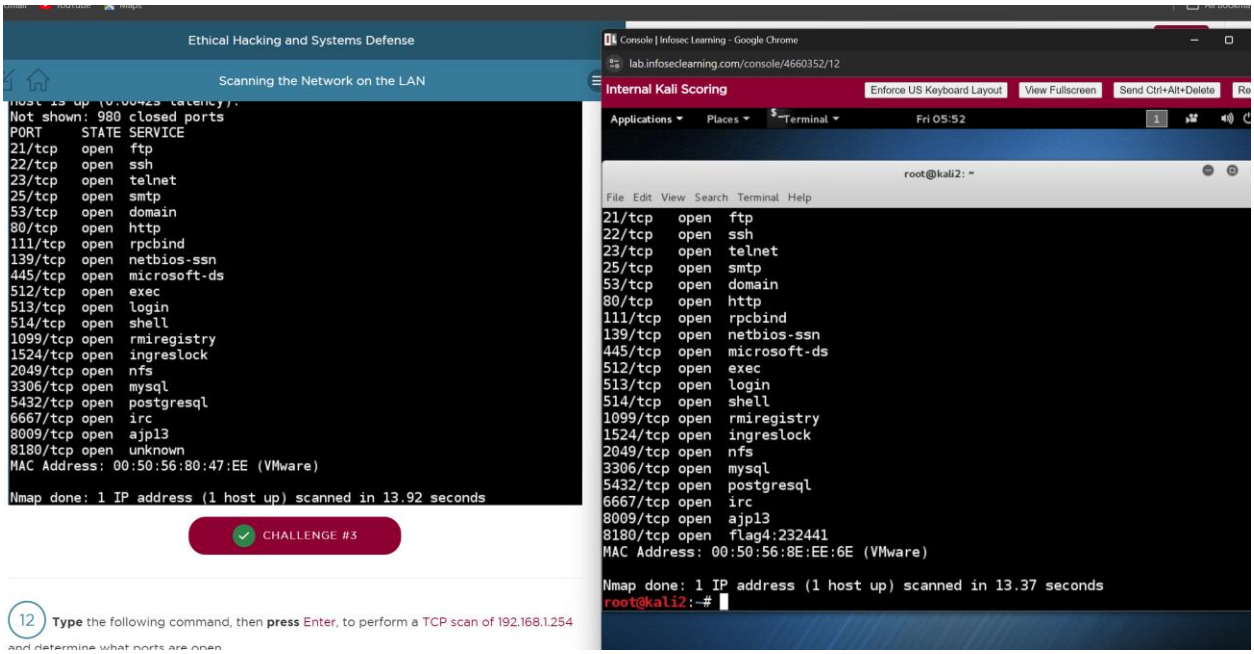
Arp-scan 192.168.1.0/24



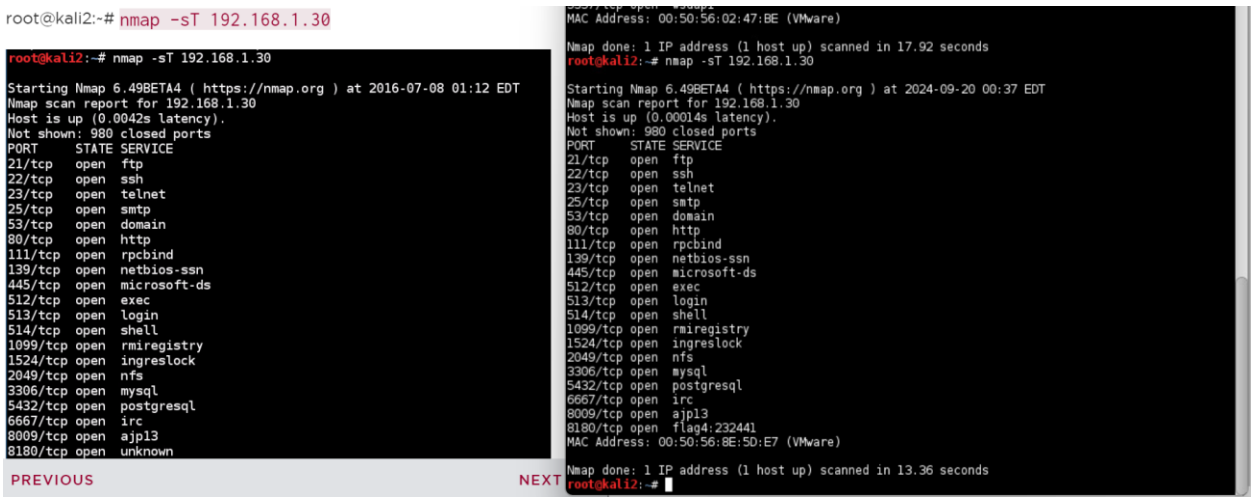
Nmap -sT 192.168.1.10



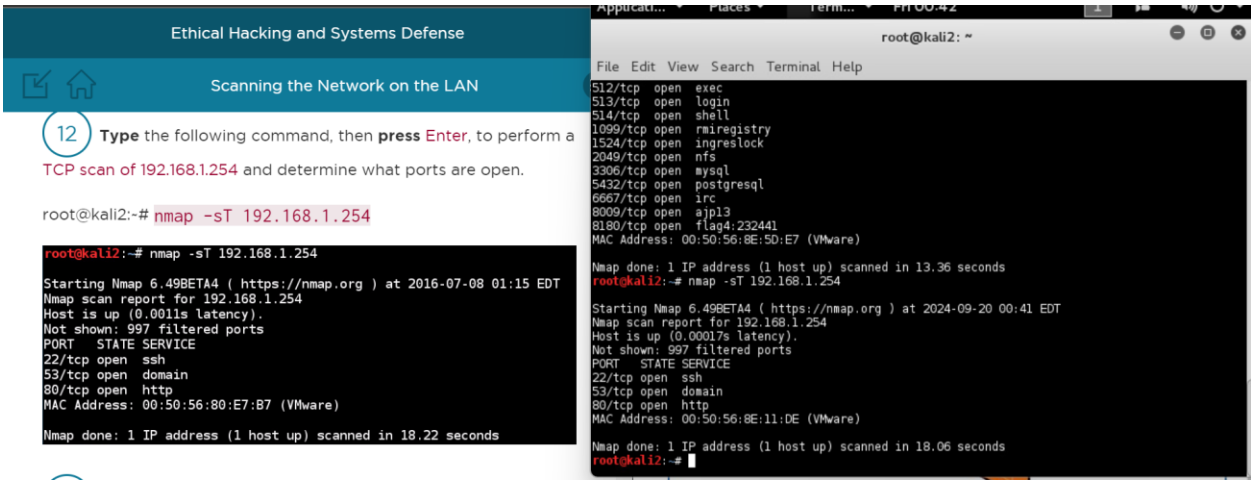
Nmap -sT 192.168.1.20



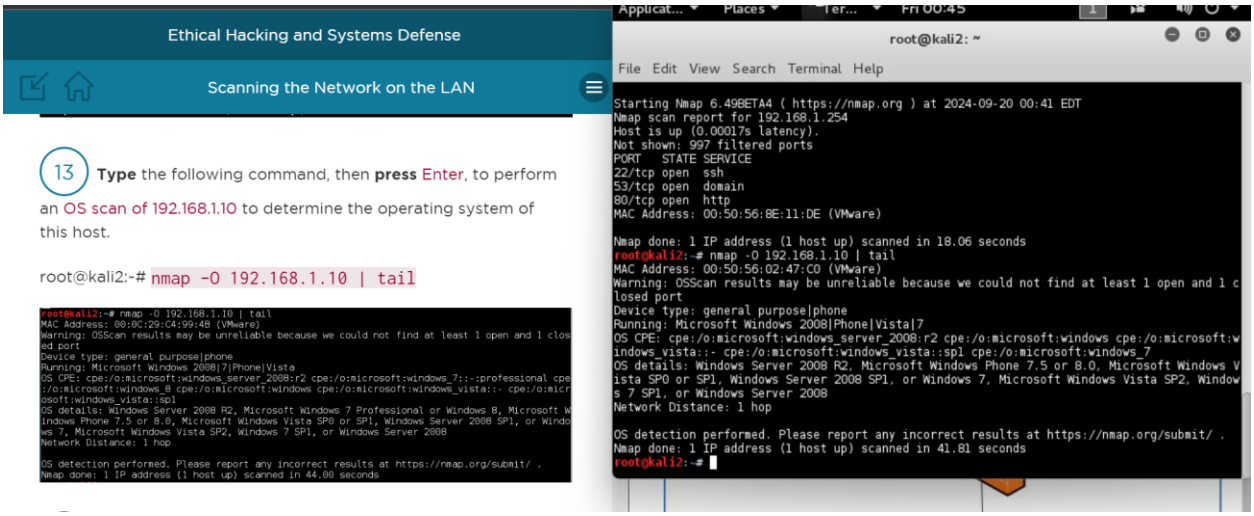
Nmap -sT 192.168.1.30



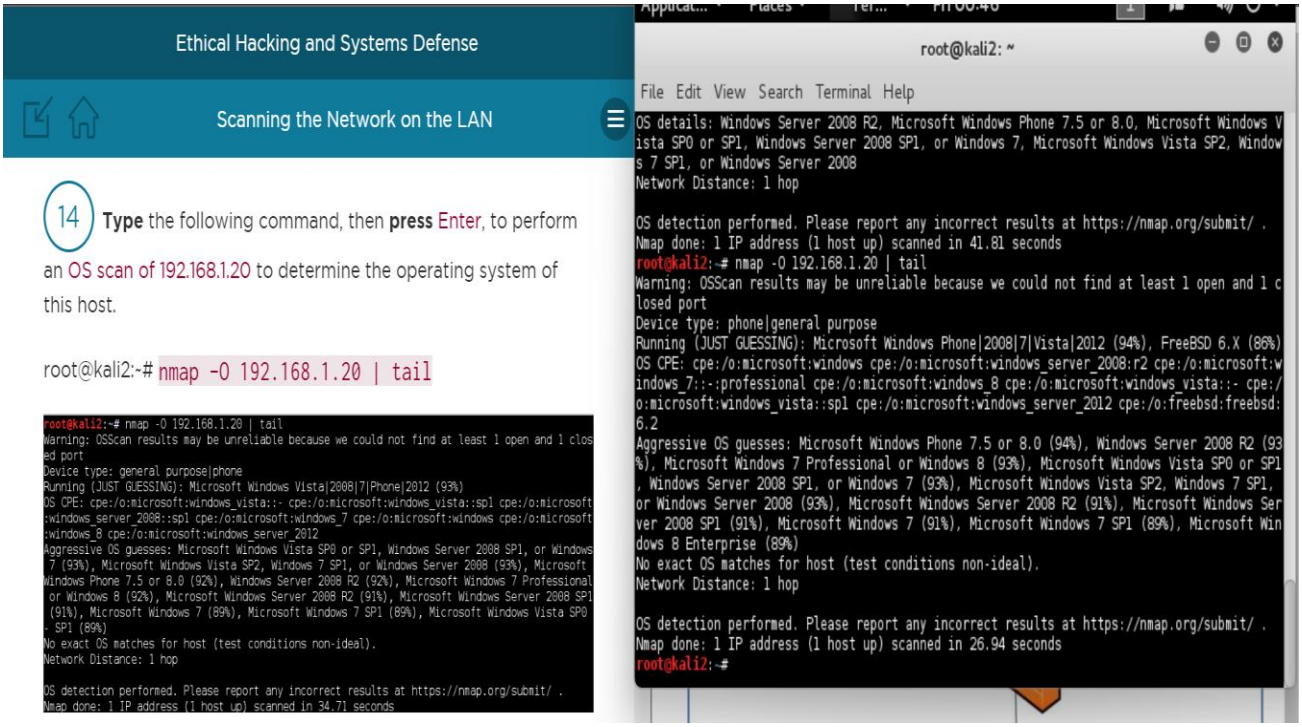
Nmap -sT 192.168.1.254



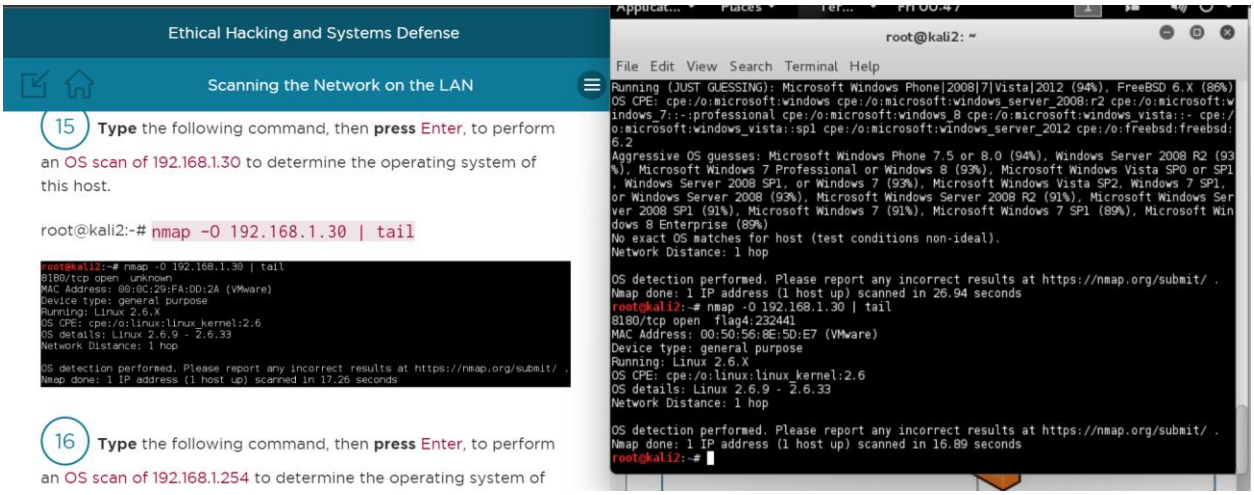
Nmap -O 192.168.1.10 | tail



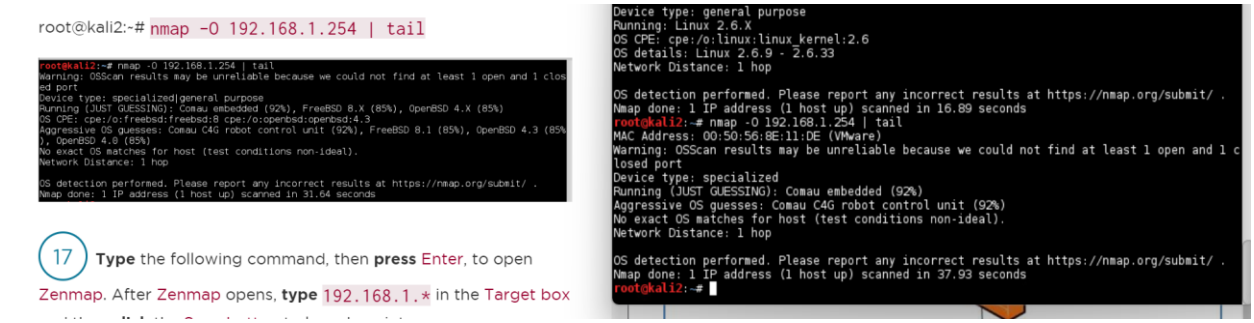
Nmap -O 192.168.1.20 | tail



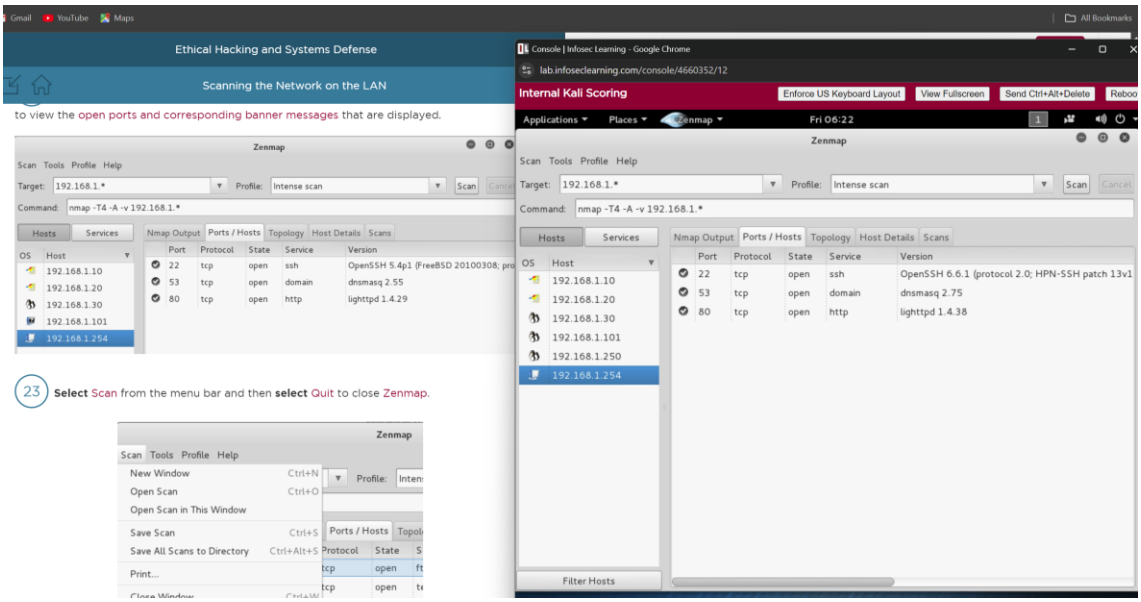
Nmap -O 192.168.1.30 | tail

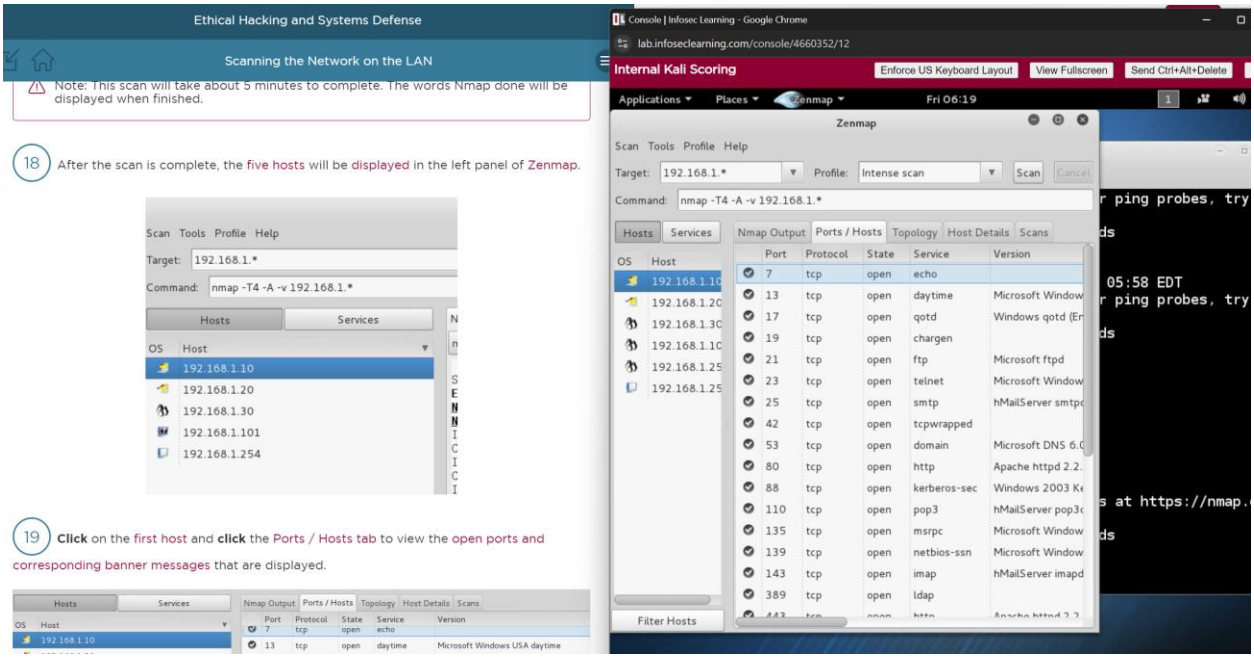


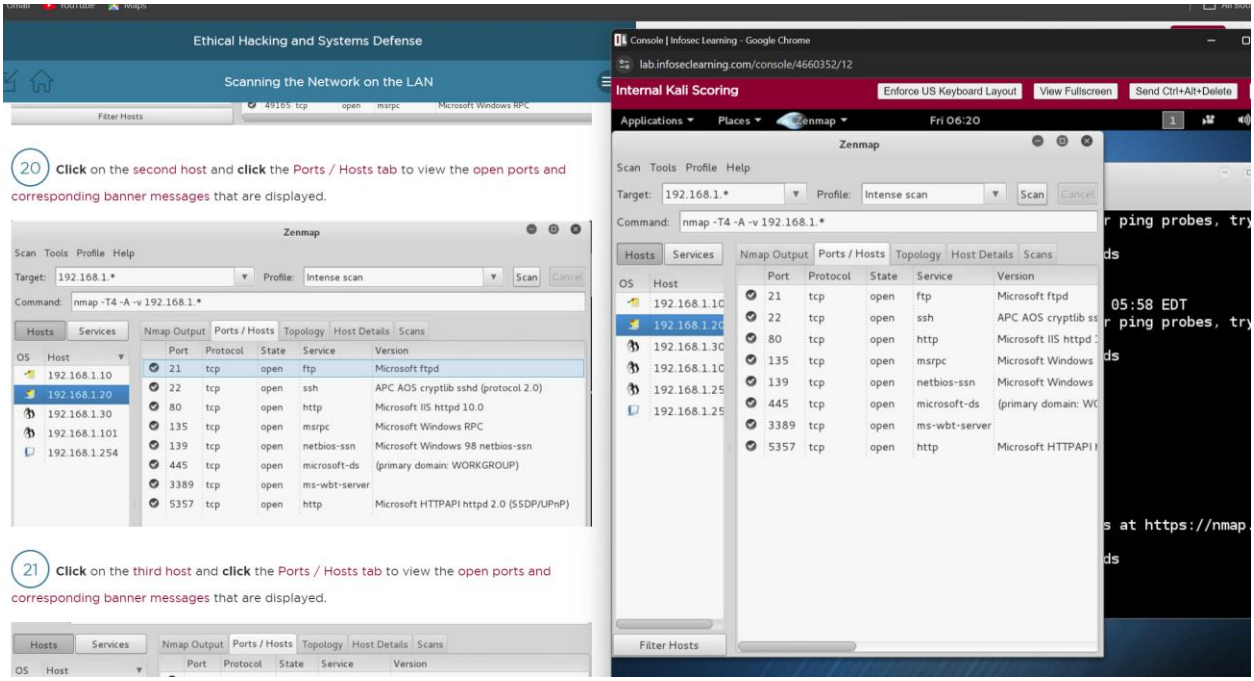
Nmap -O 192.168.1.254 | tail

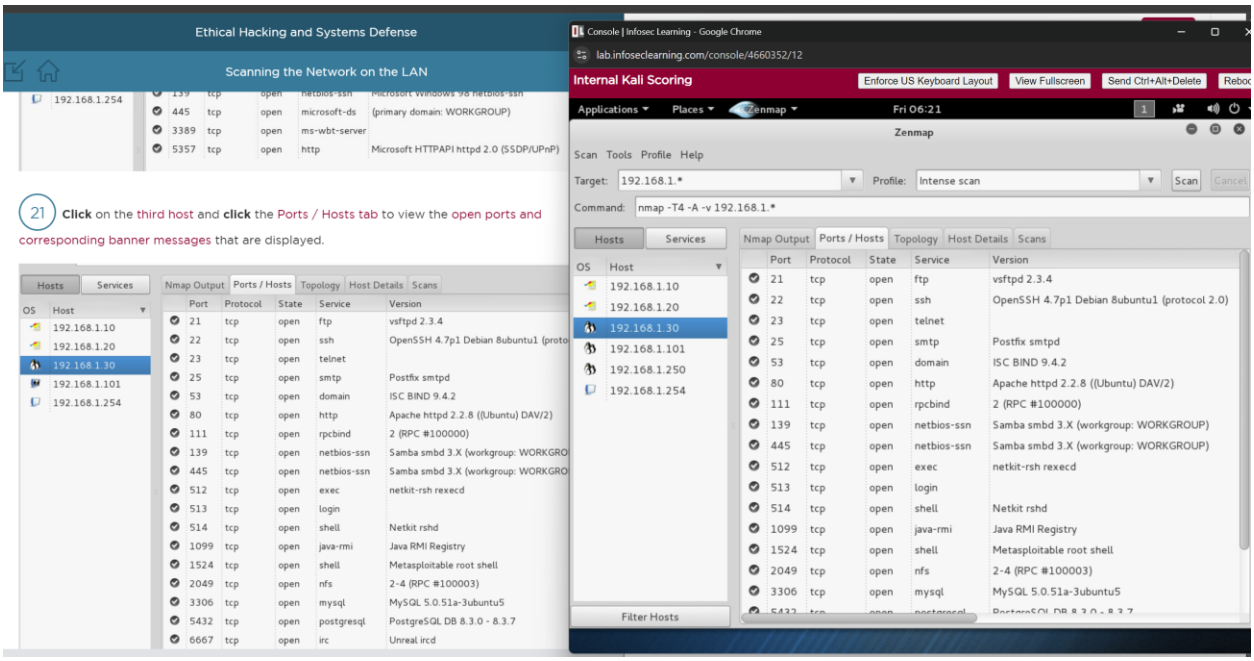


I had run 192.168.1.* in Zenmap

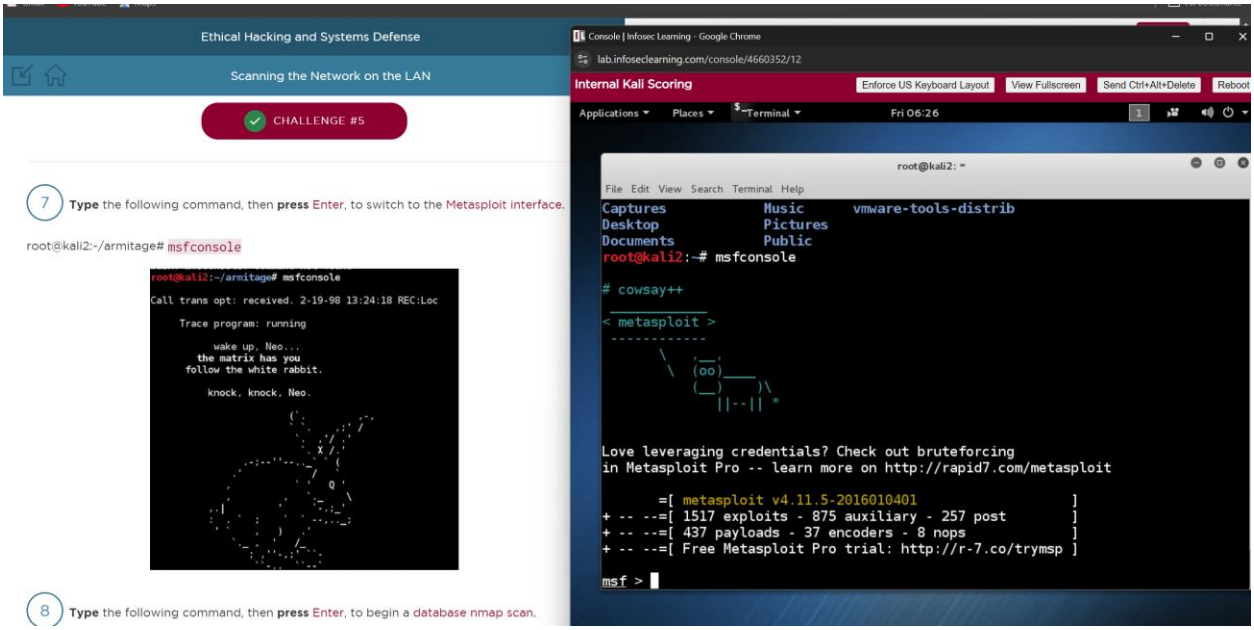

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
to view the open ports and corresponding banner messages that are displayed.
Zenmap
Scan Tools Profile Help
Target: 192.168.1.*
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.*
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
192.168.1.10
192.168.1.20
192.168.1.30
192.168.1.101
192.168.1.254
Port Protocol State Service Version
22 tcp open ssh OpenSSH 5.4p1 (FreeBSD 20100308;
53 tcp open domain dnsmasq 2.55
80 tcp open http lighttpd 1.4.29
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660352/12
Internal Kali Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Applications Places Zenmap Fri 06:22
Zenmap
Scan Tools Profile Help
Target: 192.168.1.*
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.*
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
192.168.1.10
192.168.1.20
192.168.1.30
192.168.1.101
192.168.1.250
192.168.1.254
Port Protocol State Service Version
22 tcp open ssh OpenSSH 6.6.1 (protocol 2.0; HPN-SSH patch 13v1
53 tcp open domain dnsmasq 2.75
80 tcp open http lighttpd 1.4.38
Filter Hosts
23 Select Scan from the menu bar and then select Quit to close Zenmap.
Zenmap
Scan Tools Profile Help
New Window Ctrl+N
Open Scan Ctrl+O
Open Scan in This Window
Save Scan Ctrl+S
Save All Scans to Directory Ctrl+Alt+S
Print...
Profile:
Ports / Hosts
Protocol State


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.
18 After the scan is complete, the five hosts will be displayed in the left panel of Zenmap.
Scan Tools Profile Help
Target: 192.168.1.*
Command: nmap -T4 -A -v 192.168.1.*
Hosts Services
OS Host
192.168.1.10
192.168.1.20
192.168.1.30
192.168.1.101
192.168.1.254
19 Click on the first host and click the Ports / Hosts tab to view the open ports and corresponding banner messages that are displayed.
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
7 tcp open echo
13 tcp open daytime Microsoft Windows USA daytime
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660352/12
Internal Kali Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Applications Places Zenmap Fri 06:19
Zenmap
Scan Tools Profile Help
Target: 192.168.1.*
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.*
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Port Protocol State Service Version
7 tcp open echo
13 tcp open daytime Microsoft Window
17 tcp open qotd Windows qotd (Er
19 tcp open chargen
21 tcp open ftp Microsoft ftpd
23 tcp open telnet Microsoft Window
25 tcp open smtp hMailServer smtpc
42 tcp open tcpwrapped
53 tcp open domain Microsoft DNS 6.0
80 tcp open http Apache httpd 2.2.
88 tcp open kerberos-sec Windows 2003 Ke
110 tcp open pop3 hMailServer pop3c
135 tcp open msrpc Microsoft Window
139 tcp open netbios-ssn Microsoft Window
143 tcp open imap hMailServer imapd
389 tcp open ldap
Filter Hosts
r ping probes, try
ds
05:58 EDT
r ping probes, try
ds
s at https://nmap.
ds

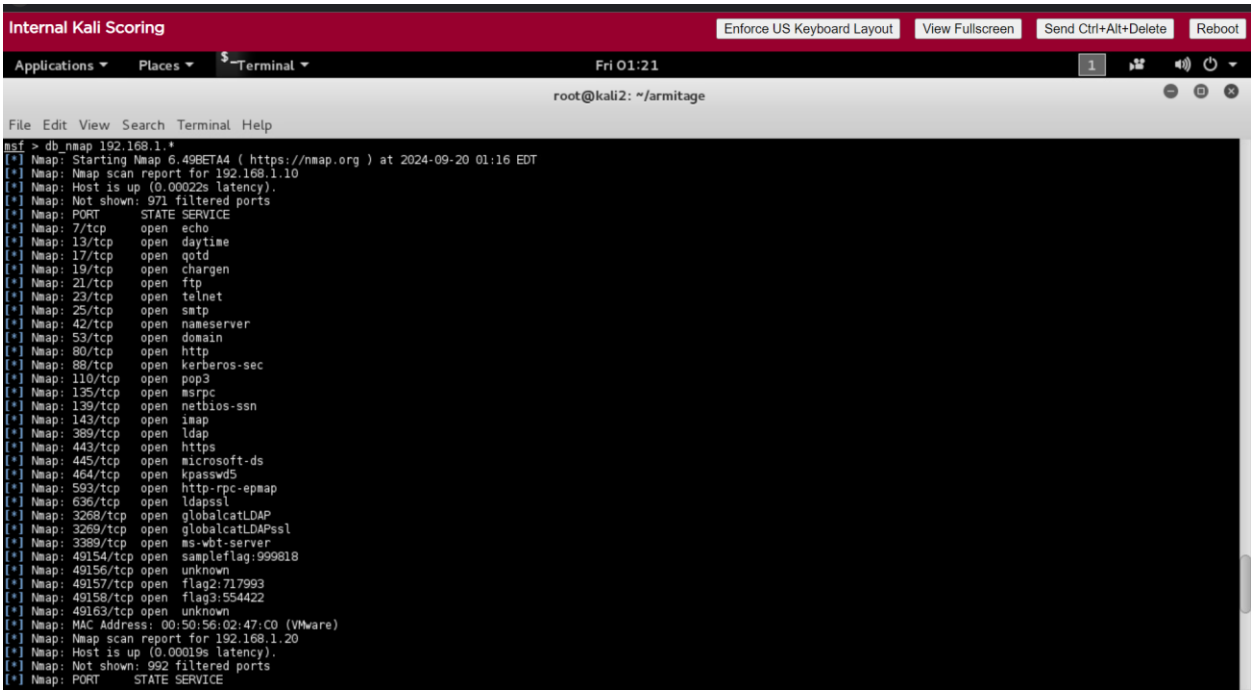


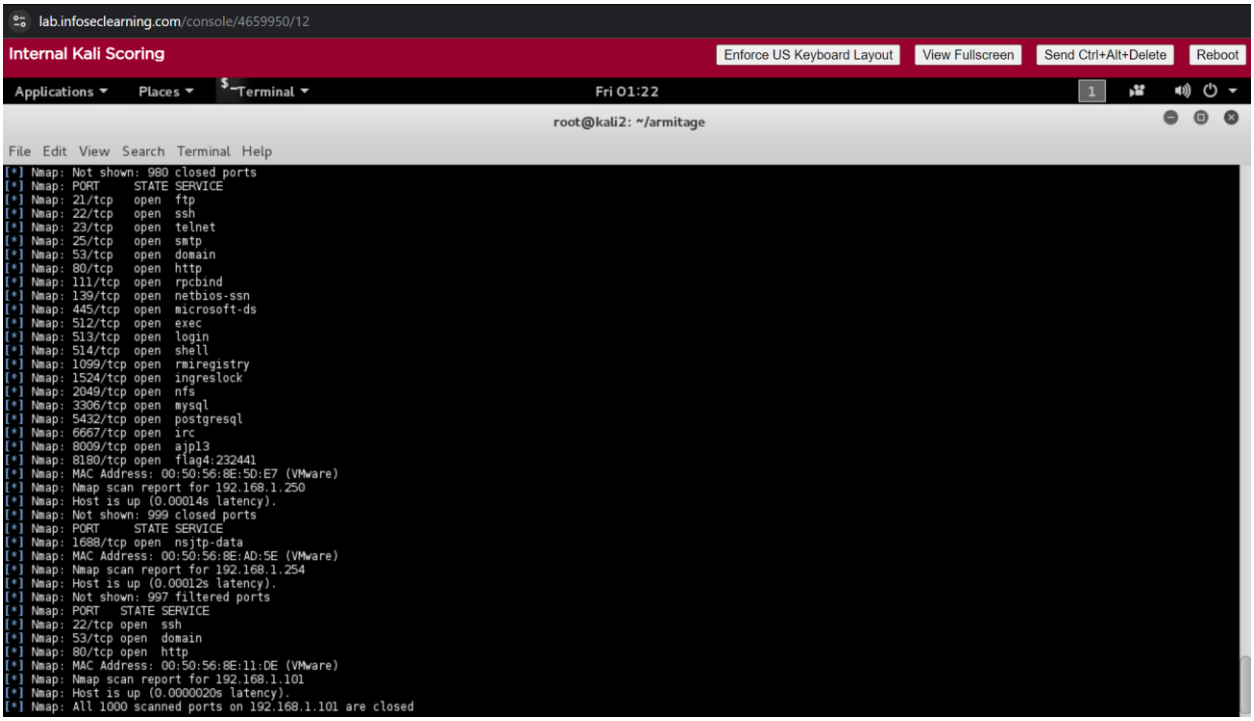


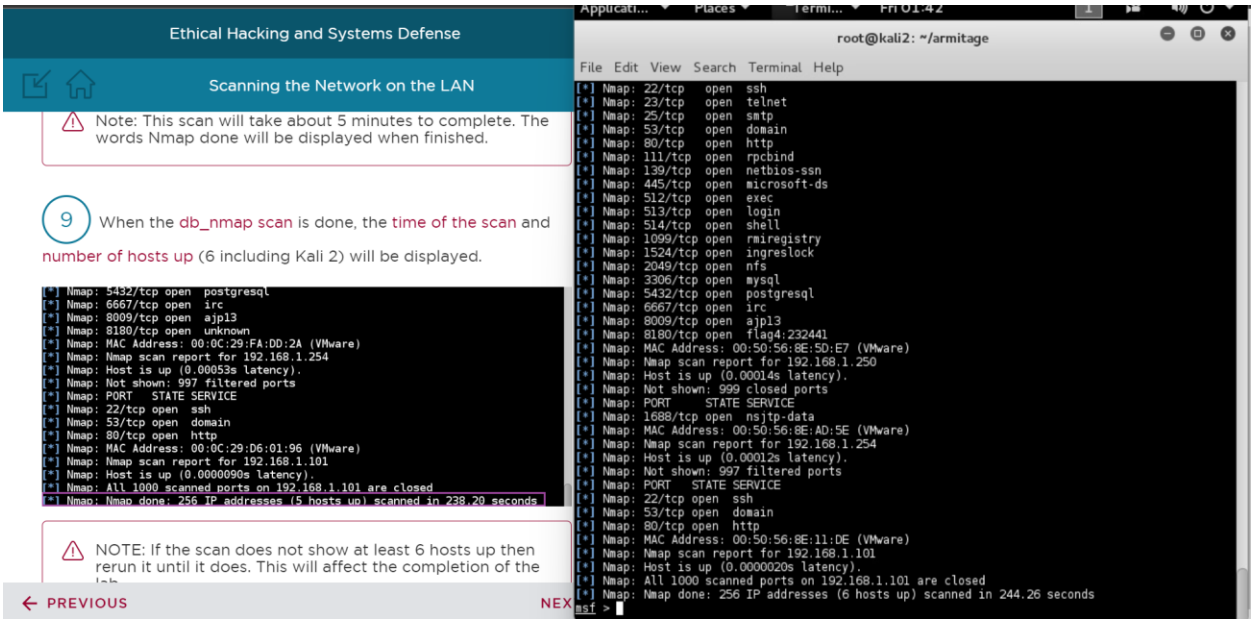
I had used msfconsole in/armitage



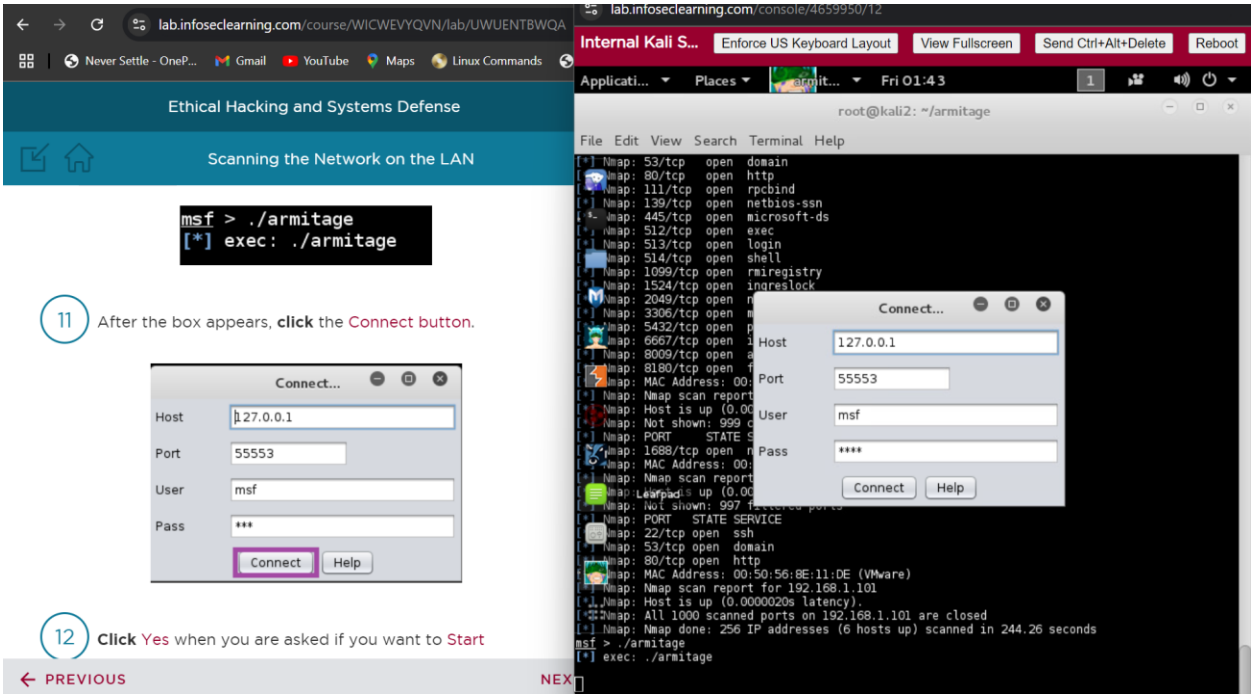
Msf > db_nmap 192.168.1.*

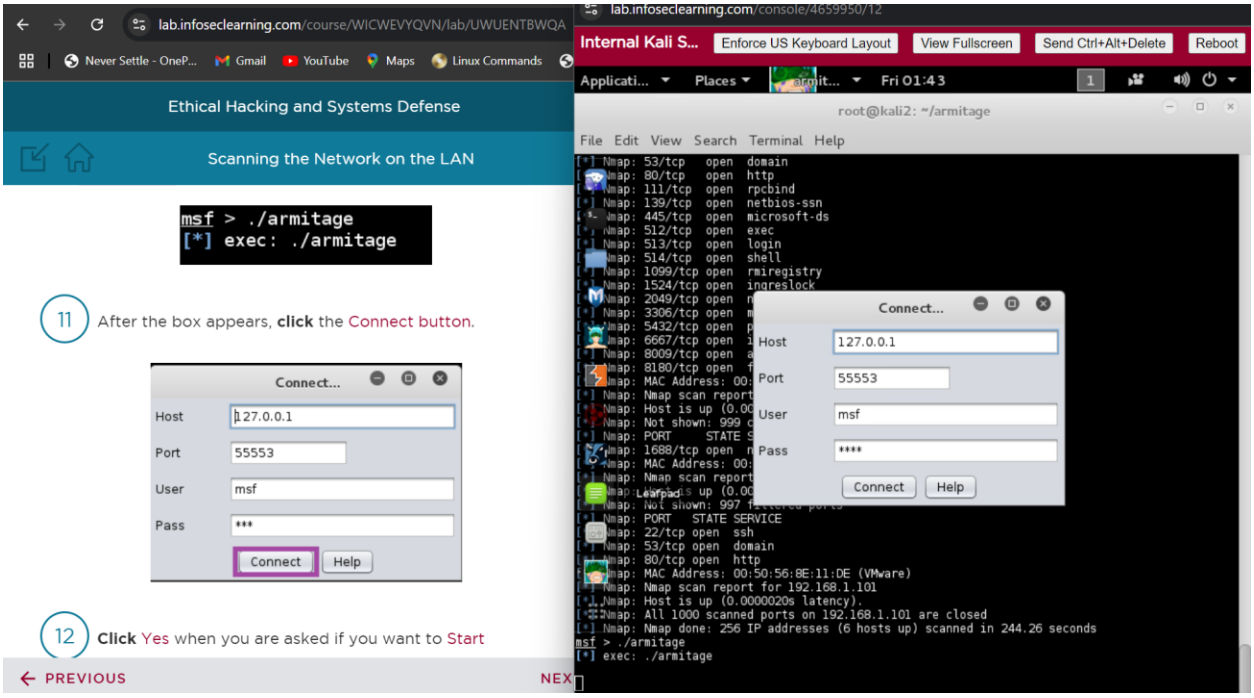


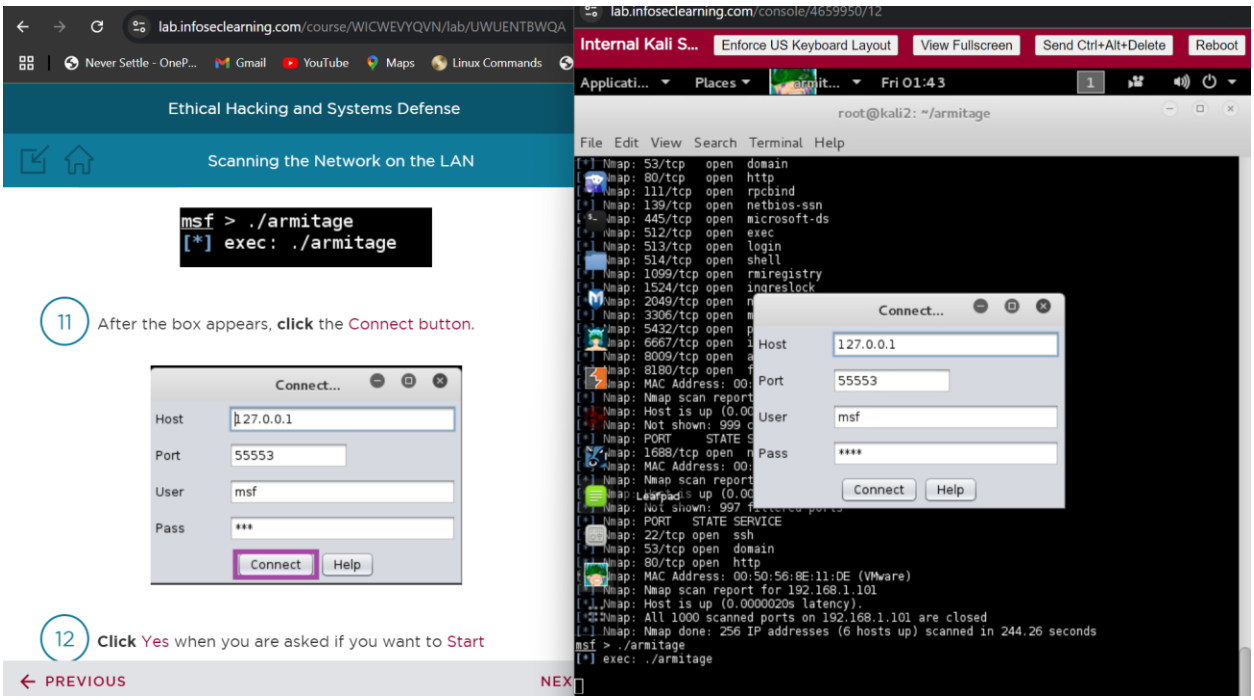


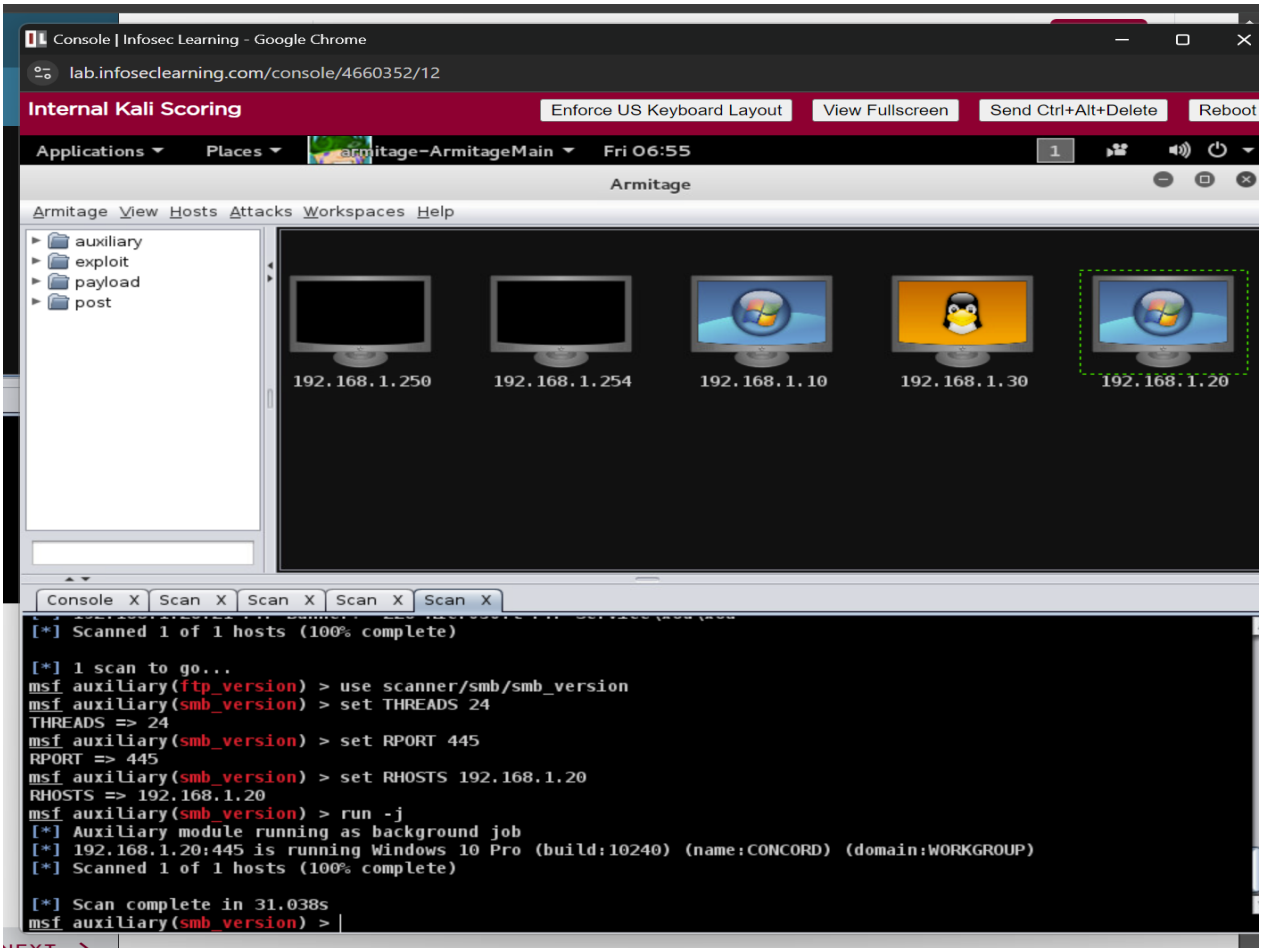


Msf > ./Armitage And we connected

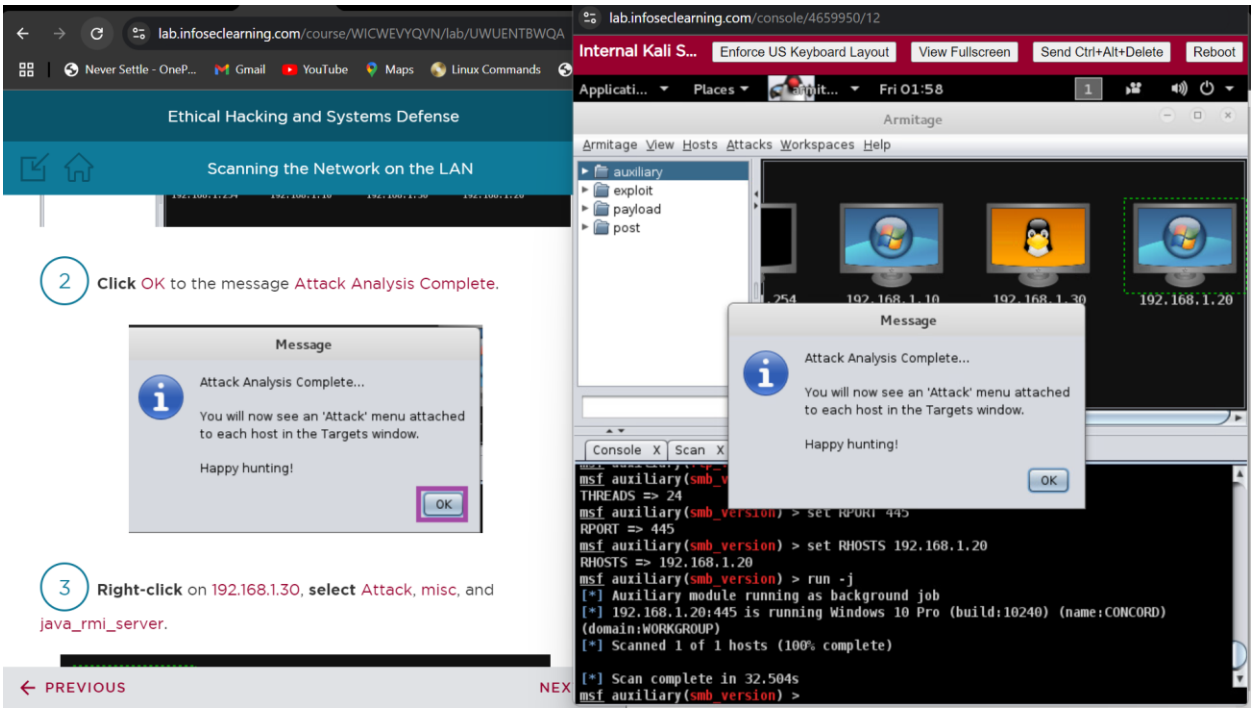

lab.infoseclearning.com/course/WICWEVYQVN/lab/UWUENTBWQA
Never Settle - OneP...
Gmail
YouTube
Maps
Linux Commands
Ethical Hacking and Systems Defense
Scanning the Network on the LAN
msf > ./armitage
[*] exec: ./armitage
11
After the box appears, click the Connect button.
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
***
Connect
Help
12
Click Yes when you are asked if you want to Start
PREVIOUS
NEX
lab.infoseclearning.com/console/4659950/12
Internal Kali S...
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applicati...
Places
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: 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 (0.0000020s 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
Leafpad

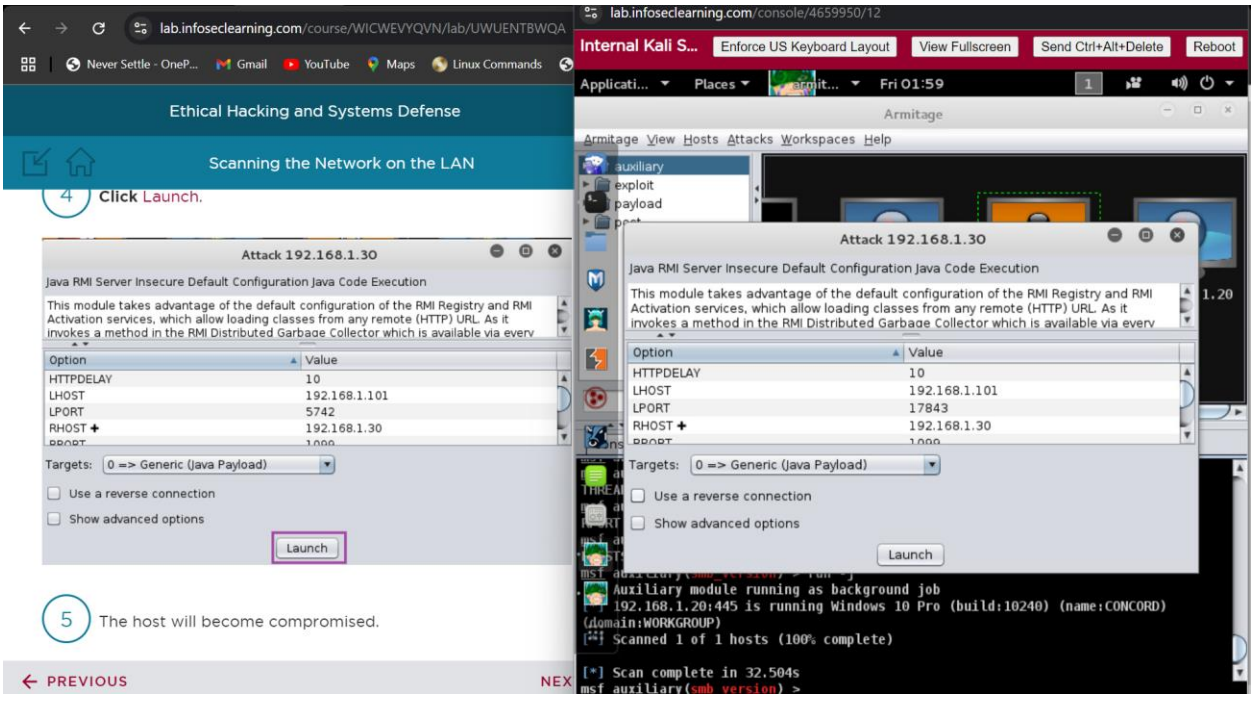

lab.infoseclearning.com/course/WICWEVYQVN/lab/UWUENTBWQA
Never Settle - OneP...
Gmail
YouTube
Maps
Linux Commands
Ethical Hacking and Systems Defense
Scanning the Network on the LAN
msf > ./armitage
[*] exec: ./armitage
11
After the box appears, click the Connect button.
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
***
Connect
Help
12
Click Yes when you are asked if you want to Start
PREVIOUS
NEX
lab.infoseclearning.com/console/4659950/12
Internal Kali S...
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applicati...
Places
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: 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 (0.0000020s 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
Leafpad


lab.infoseclearning.com/course/WICWEVYQVN/lab/UWUENTBWQA
Never Settle - OneP...
Gmail
YouTube
Maps
Linux Commands
Ethical Hacking and Systems Defense
Scanning the Network on the LAN
msf > ./armitage
[*] exec: ./armitage
11
After the box appears, click the Connect button.
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
***
Connect
Help
12
Click Yes when you are asked if you want to Start
PREVIOUS
NEX
lab.infoseclearning.com/console/4659950/12
Internal Kali S...
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applicati...
Places
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
[*] Nmap: 3306/tcp open
[*] Nmap: 5432/tcp open
[*] Nmap: 6667/tcp open
[*] Nmap: 8009/tcp open
[*] Nmap: 8180/tcp open
[*] Nmap: MAC Address: 00:
[*] Nmap: Nmap scan report
[*] Nmap: Host is up (0.00
[*] Nmap: Not shown: 999
[*] Nmap: PORT STATE
[*] Nmap: 1688/tcp open
[*] Nmap: MAC Address: 00:
[*] Nmap: Nmap scan report
[*] Nmap: Not shown: 997
[*] 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 (0.0000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap done: 256 IP addresses (6 hosts up) scanned in 244.26 seconds
msf > ./armitage
[*] exec: ./armitage
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
****
Connect
Help

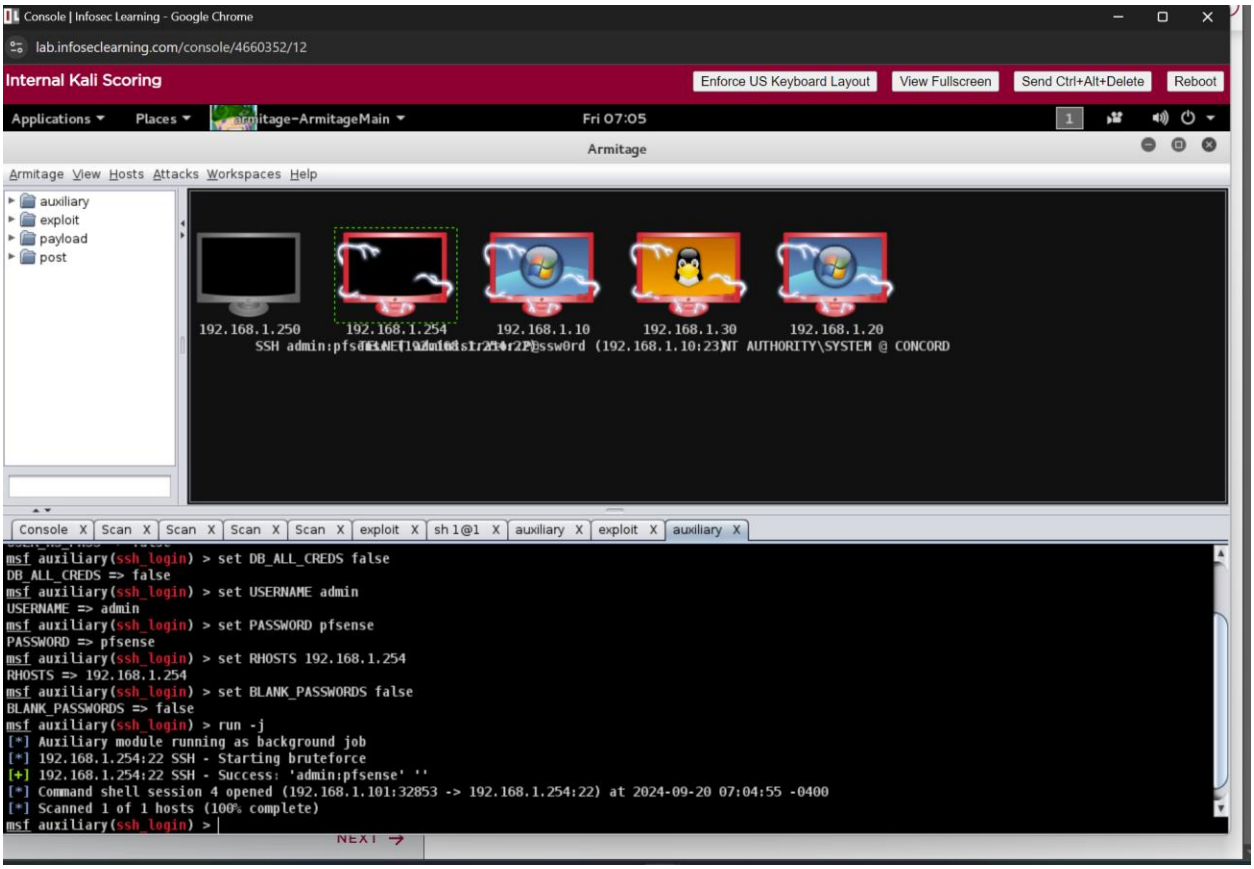

Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4660352/12
Internal Kali Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
armitage-ArmitageMain
Fri 06:55
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.250
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
Console X
Scan X
Scan X
Scan X
Scan X
[*] 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 RPORT 445
RPORT => 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.

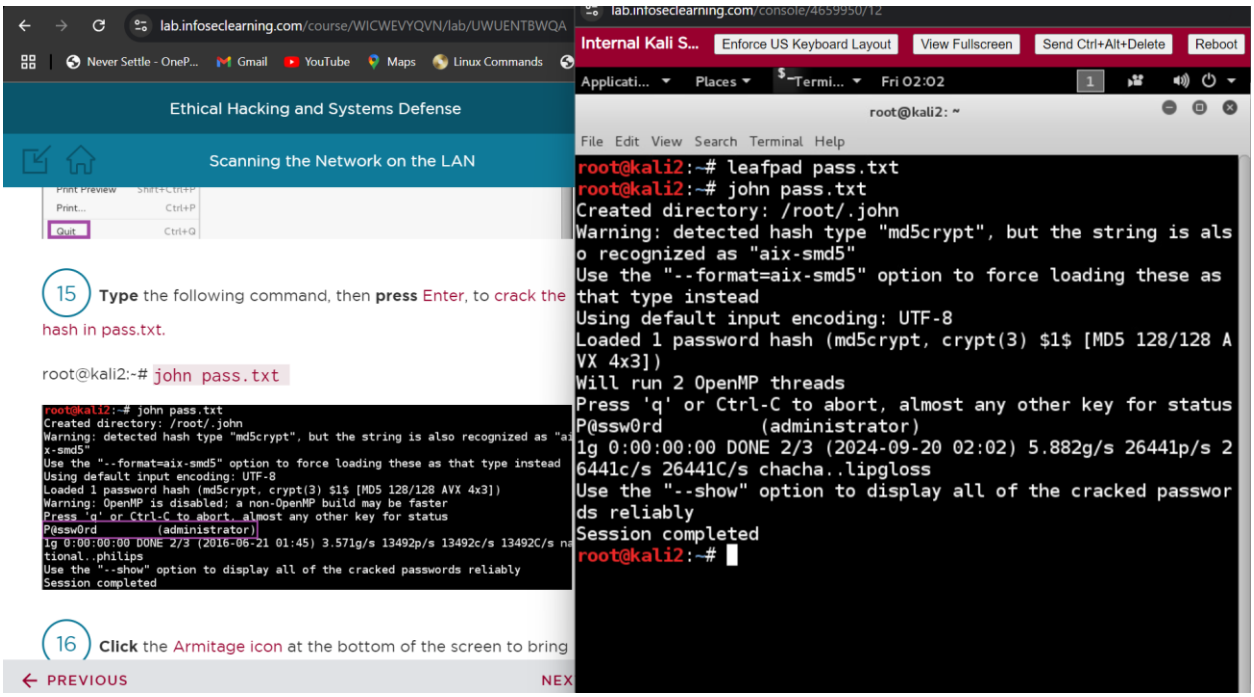




We exploited 192.168.1.* machine

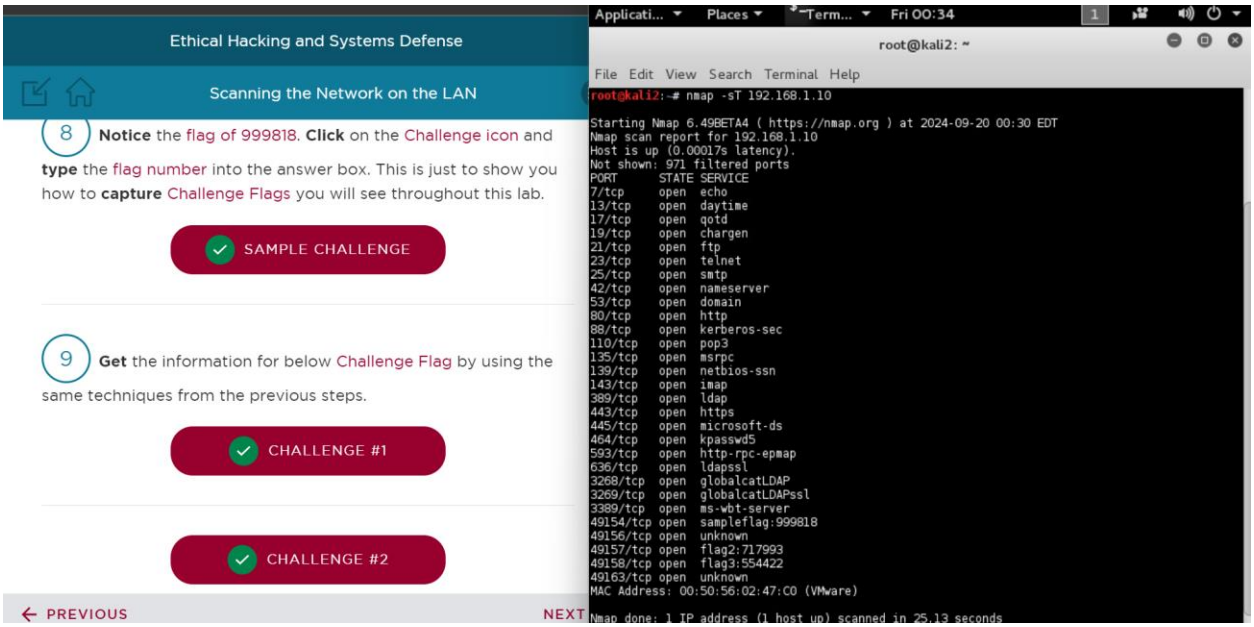


We pasted the hash in leafpad pass.txt and john got used for txt file

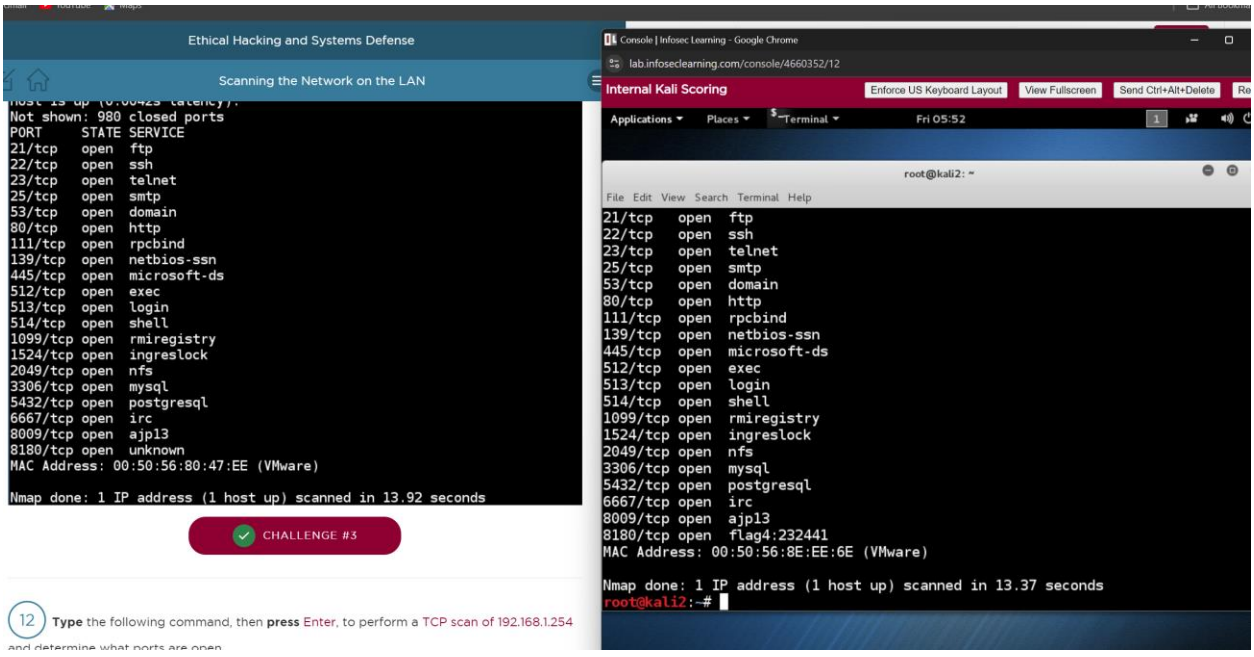


Supporting Evidence

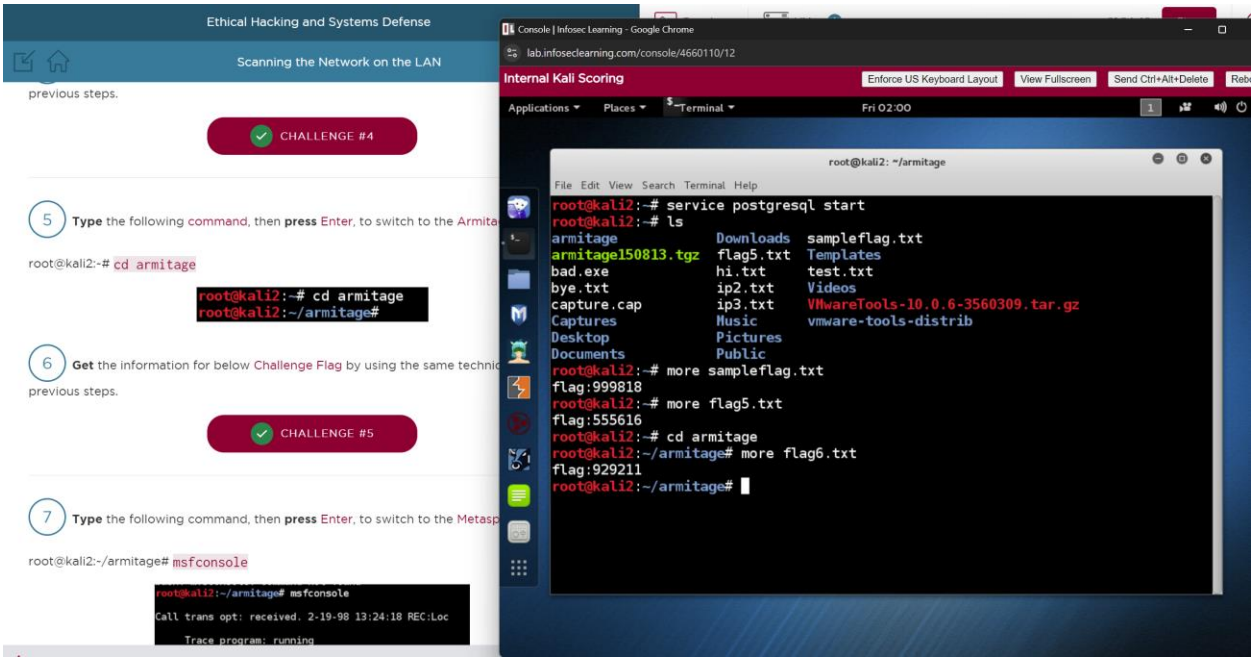
Nmap -sT 192.168.1.10



Nmap -sT 192.168.1.254



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.