Lab 2: Scanning Network on the LAN

Objective:

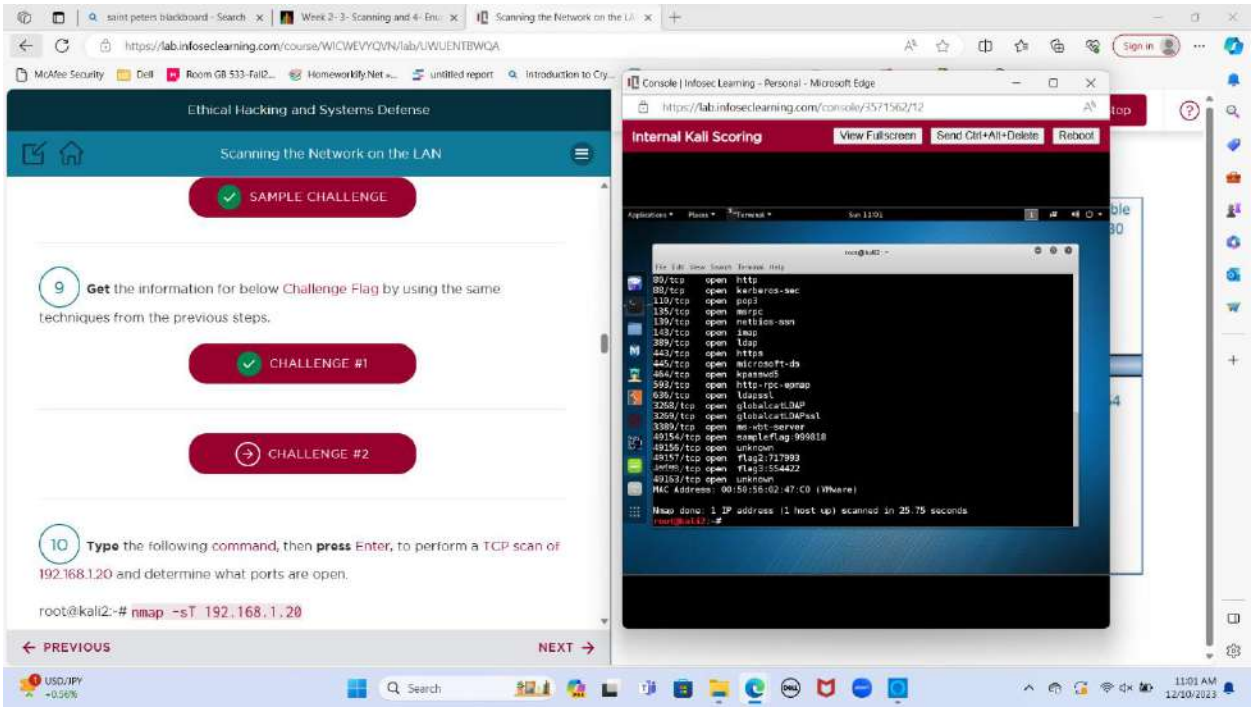
1. Scanning hosts on LAN
2. Scanning with Metasploit and Armitage
3. Exploitation

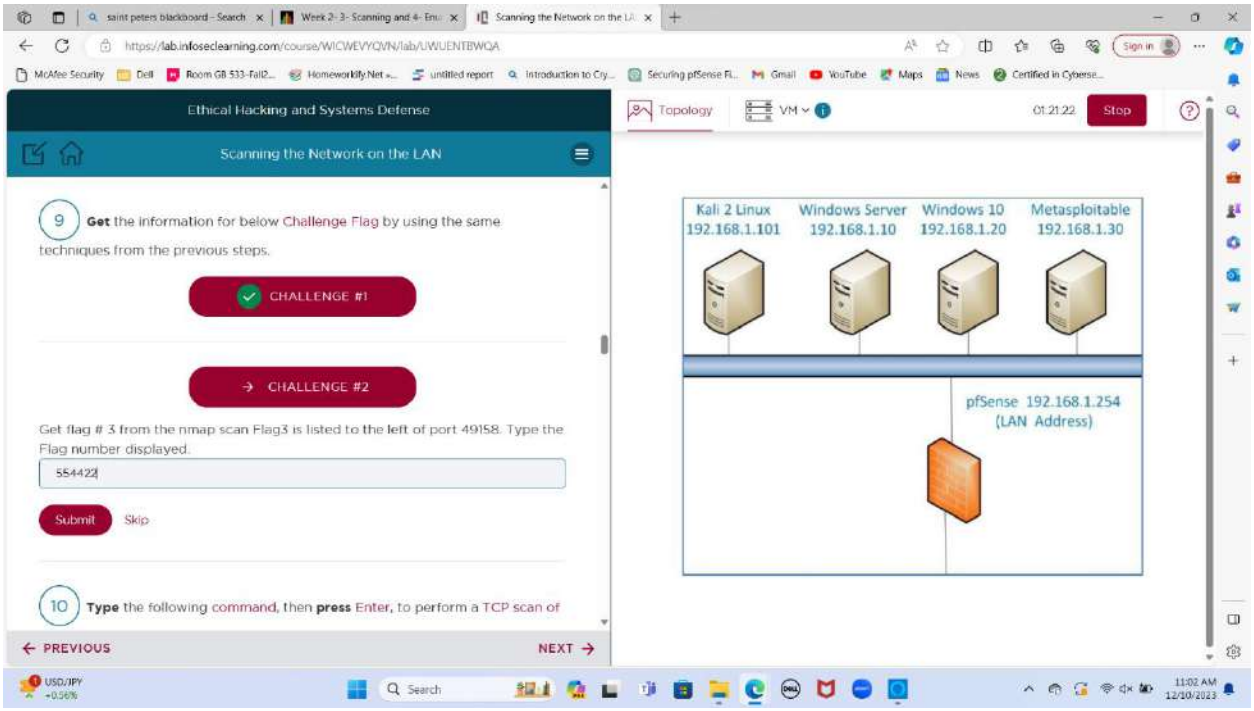
Takeaways:

1. ARP (Address Resolution Protocol) is a networking protocol used to map IP addresses to MAC addresses in a local network, enabling devices to communicate with each other.
2. The nmap option for performing a TCP scan is "-sT."
3. The nmap option for performing an OS detection scan is "-O".
4. Zenmap is a user-friendly graphical interface built on top of the Nmap network scanning tool. It provides an accessible way for users to conduct network discovery, perform security audits, and visualize the results of network scans, allowing easier interpretation and analysis of gathered data about hosts, services, and potential vulnerabilities within a network.
5. Armitage is a visual interface that simplifies cyber-attack simulations and penetration testing by serving as a front-end for the Metasploit Framework.
6. The "db_nmap" scan is a command within Metasploit that performs an Nmap scan and stores the results directly into the Metasploit database for subsequent analysis and exploitation of vulnerabilities.
7. A java_rmi_server attack involves exploiting vulnerabilities in Java's Remote Method Invocation protocol to gain unauthorized access or execute remote code on a system.

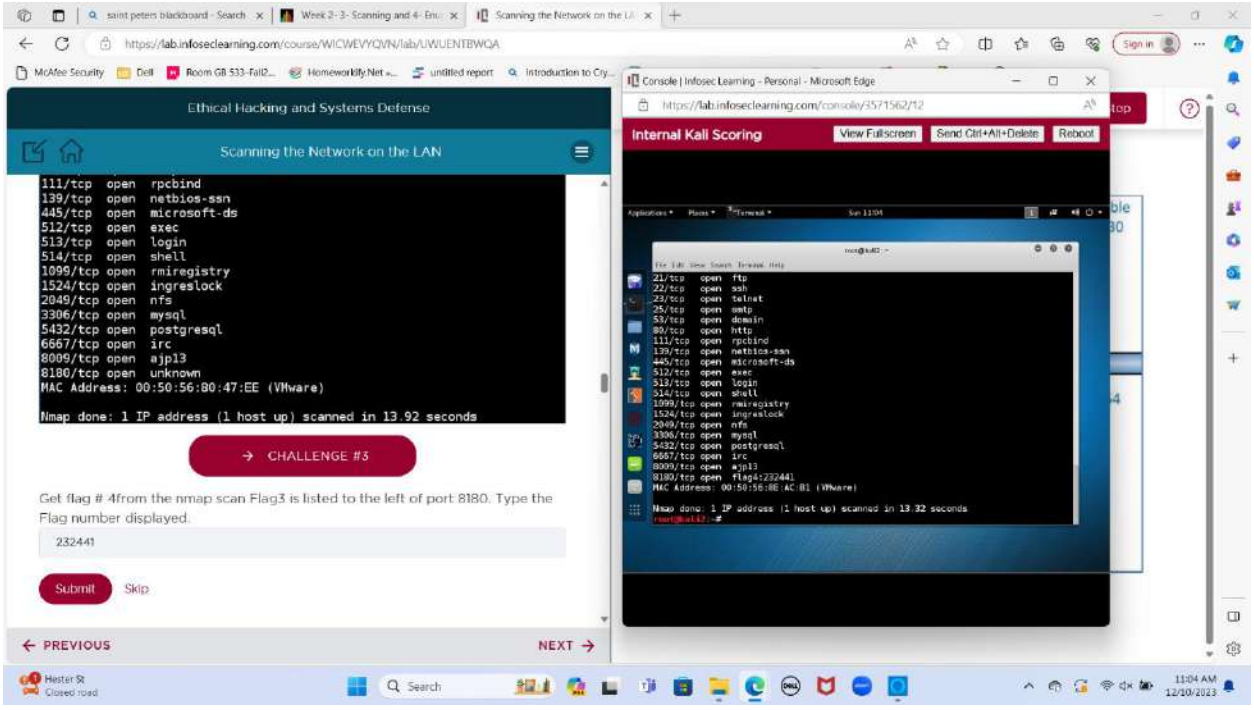
8. Meterpreter is an advanced, dynamically extensible payload within the Metasploit Framework, providing post-exploitation capabilities and allowing control over compromised systems.

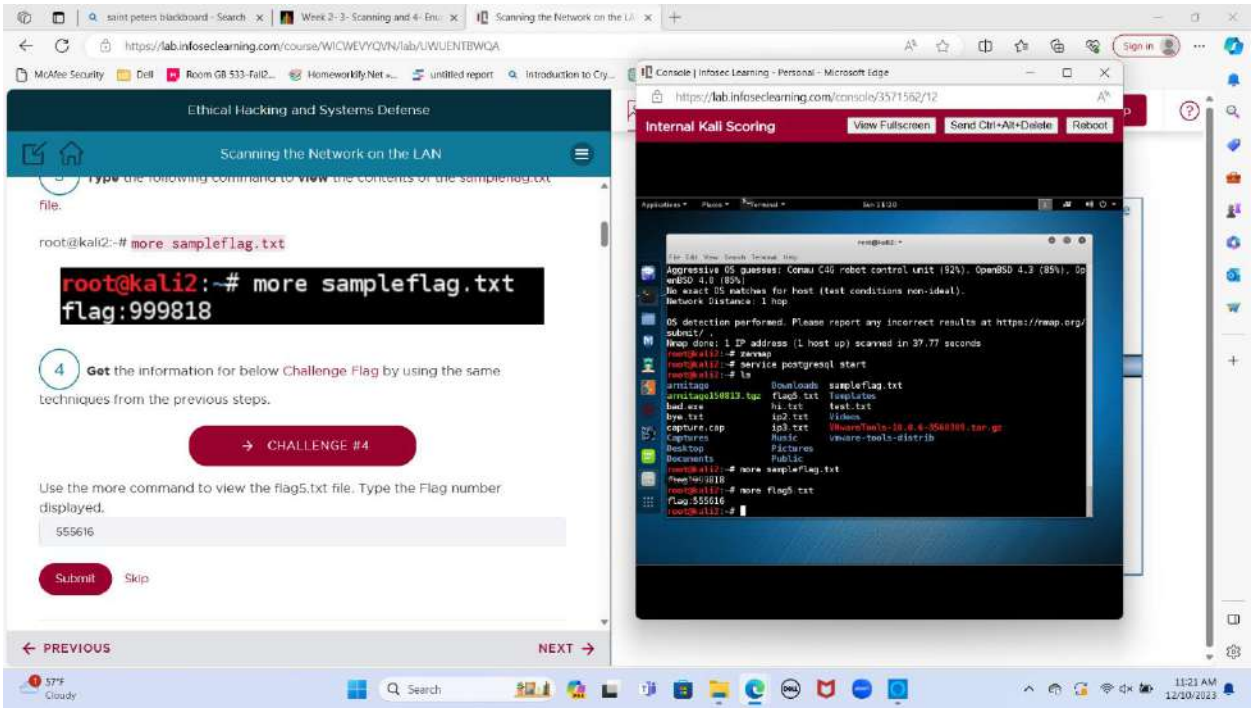
Challenges:

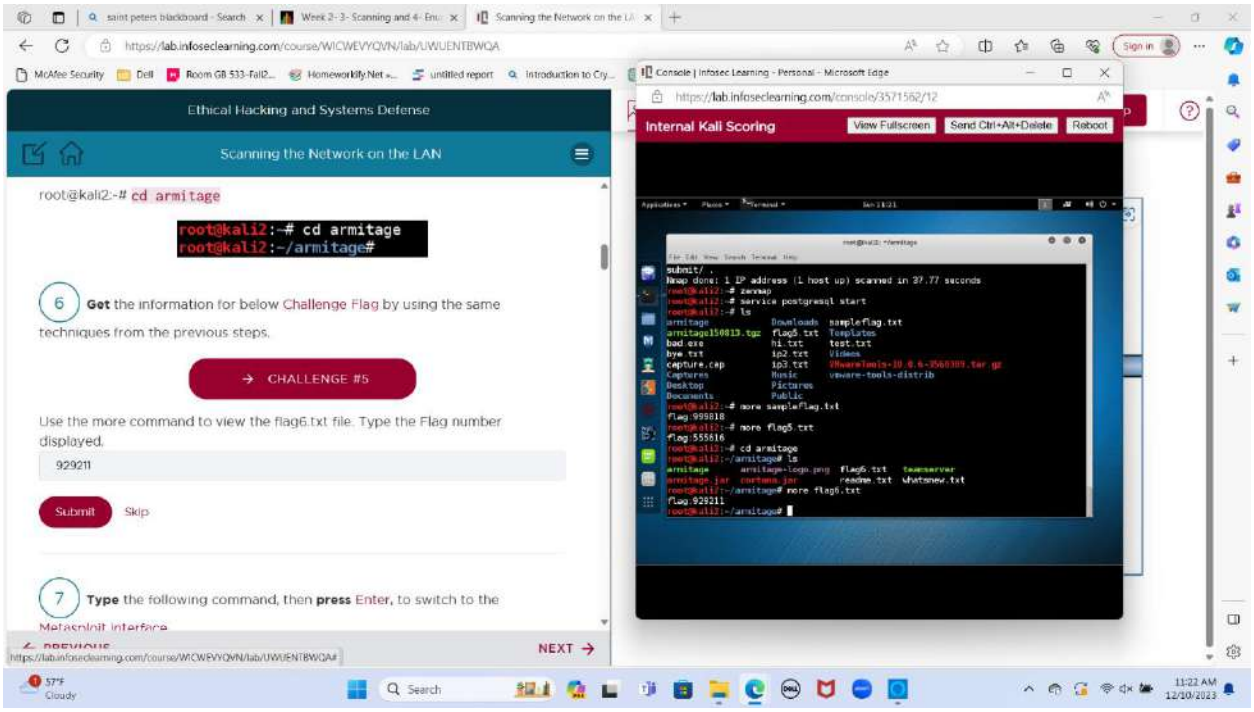



Ethical Hacking and Systems Defense
Scanning the Network on the LAN
Topology
VM
01.21.22
Stop
9 Get the information for below Challenge Flag by using the same techniques from the previous steps.
CHALLENGE #1
CHALLENGE #2
Get flag # 3 from the nmap scan Flag3 is listed to the left of port 49158. Type the Flag number displayed.
554422
Submit
Skip
10 Type the following command, then press Enter, to perform a TCP scan of
PREVIOUS
NEXT
Kali 2 Linux 192.168.1.101
Windows Server 192.168.1.10
Windows 10 192.168.1.20
Metasploitable 192.168.1.30
pfSense 192.168.1.254 (LAN Address)

re


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
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: 00:50:56:80:47:EE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
CHALLENGE #3
Get flag # 4from the nmap scan Flag3 is listed to the left of port 8180. Type the Flag number displayed.
232441
Submit
Skip
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
file.
root@kali2:-# more sampleflag.txt
root@kali2:~# more sampleflag.txt
flag:999818
4 Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #4
Use the more command to view the flag5.txt file. Type the Flag number displayed.
555616
Submit
Skip
← PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3571562/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

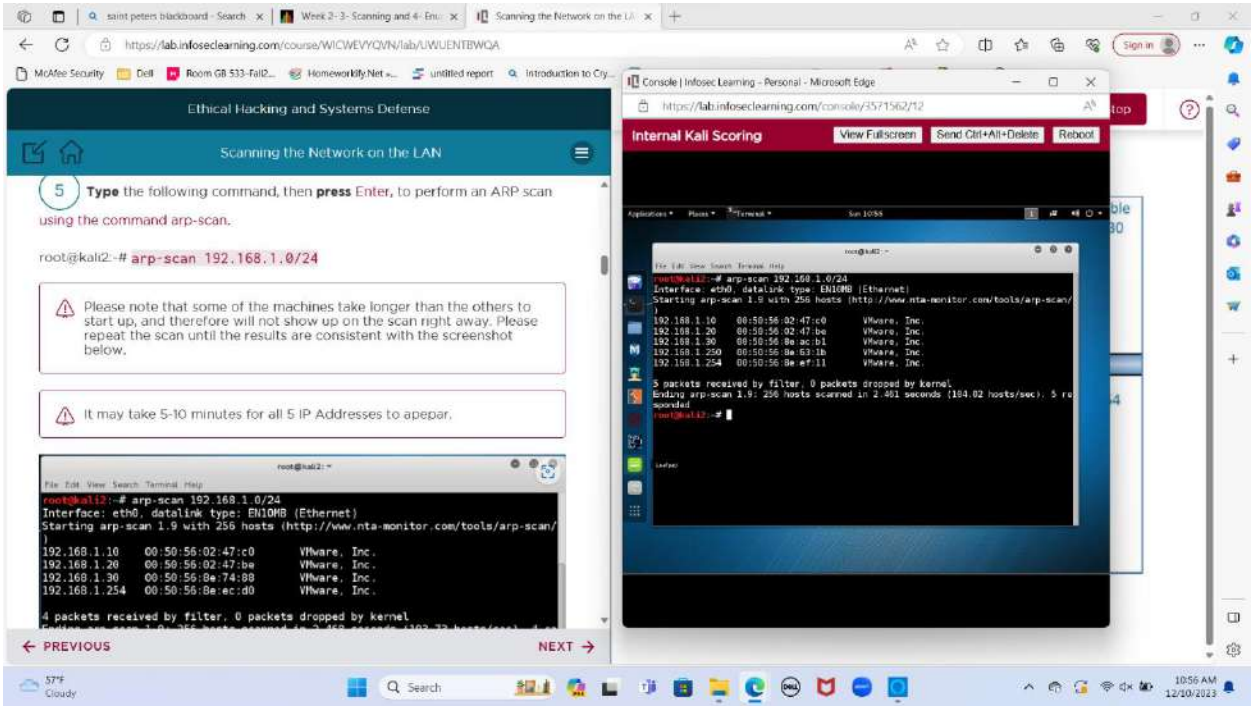

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
root@kali2:-# cd armitage
root@kali2:~# cd armitage
root@kali2:~/armitage#
6 Get the information for below Challenge Flag by using the same techniques from the previous steps.
→ CHALLENGE #5
Use the more command to view the flag6.txt file. Type the Flag number displayed.
929211
Submit
Skip
7 Type the following command, then press Enter, to switch to the Metasploit interface
NEXT →
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

The flags are:

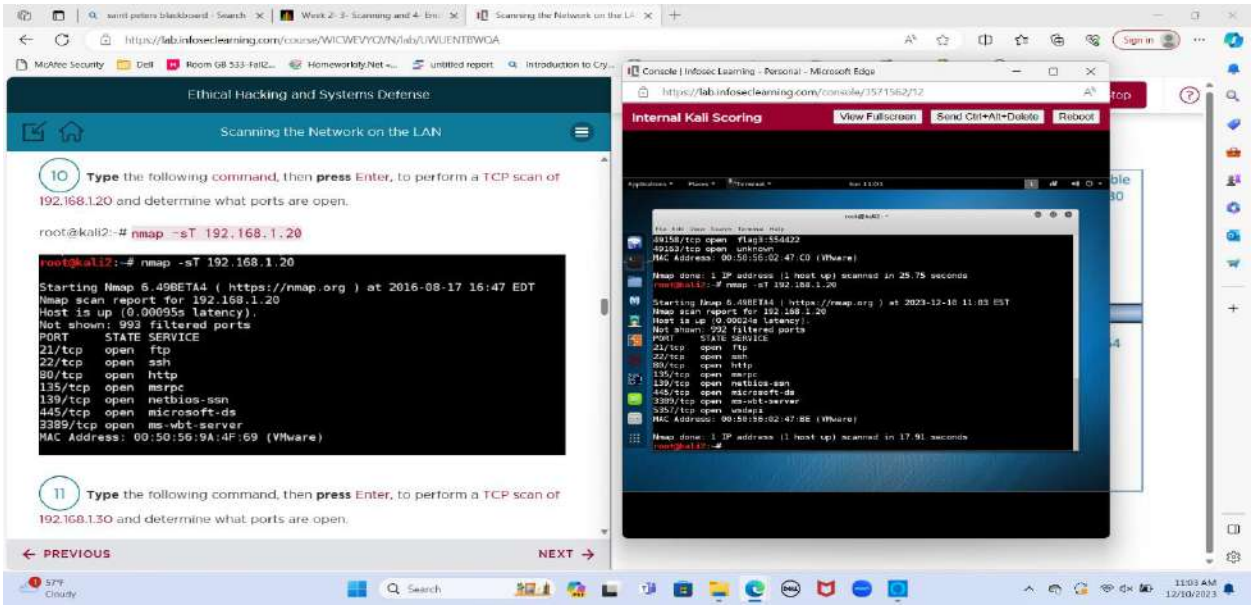
- Flag 1: 999818
- Flag 2: 717993
- Flag 3: 554422
- Flag 4: 232441
- Flag 5: 555616
- Flag 6: 929211

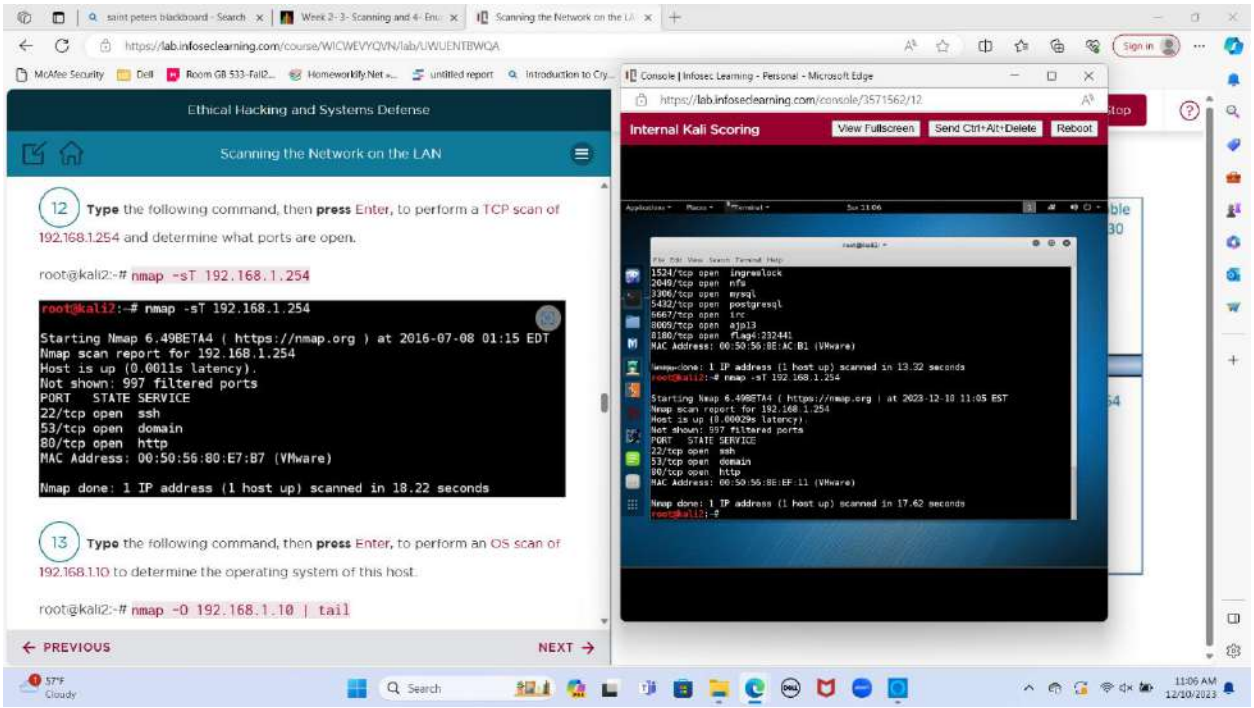
Screenshots:

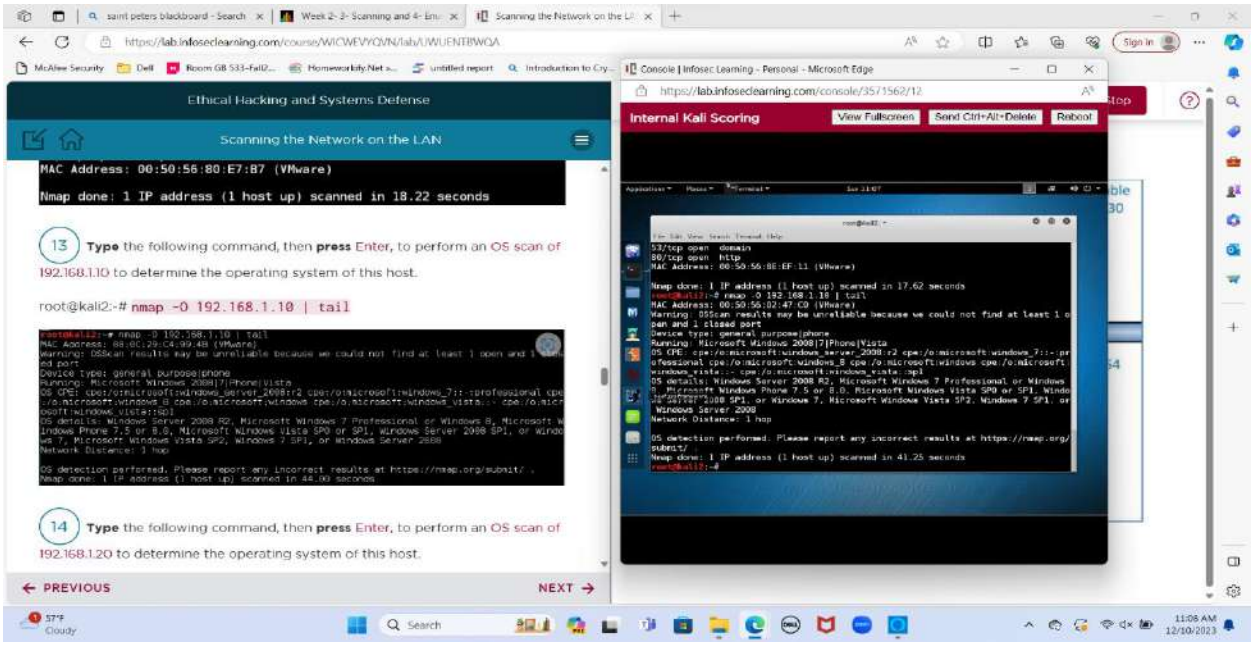
Arp Scan



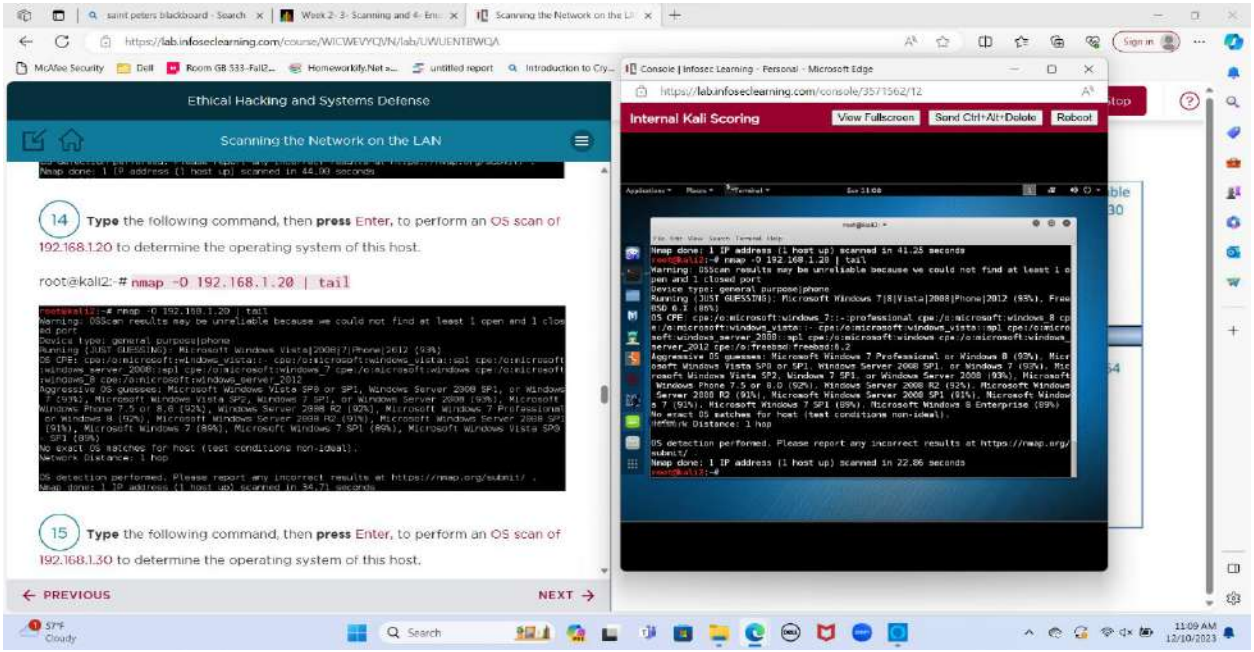
TCP scan

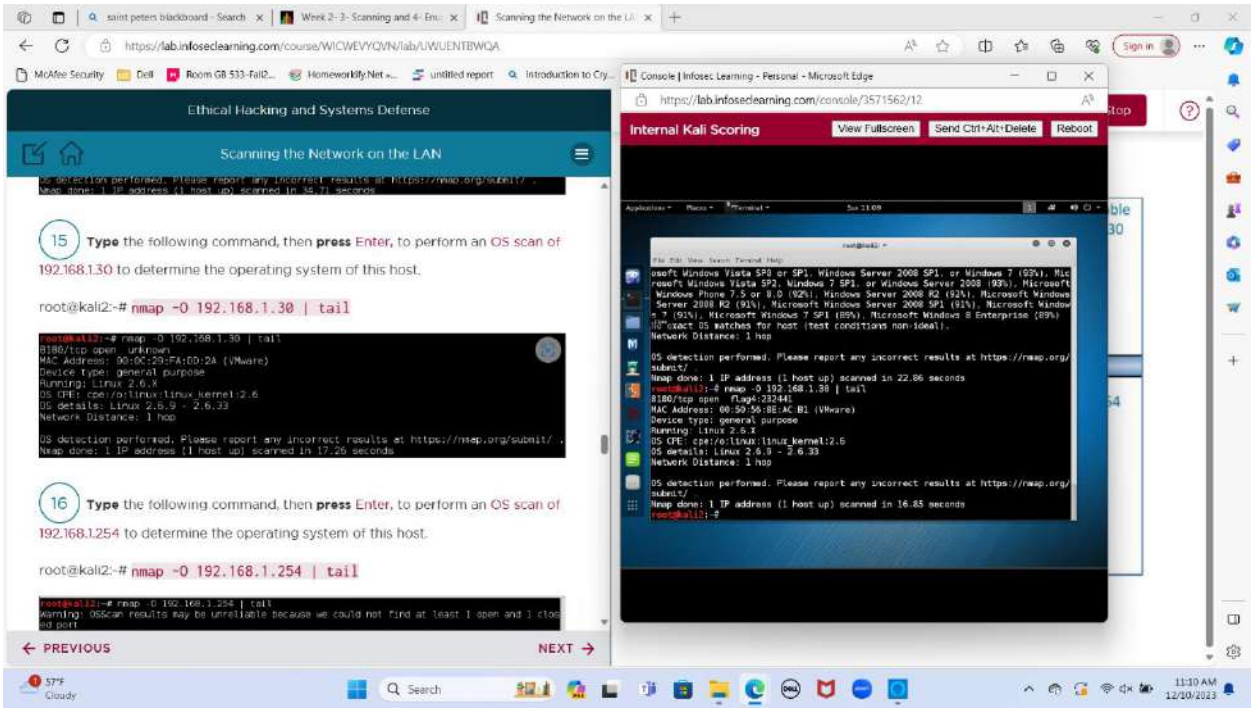

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
10 Type the following command, then press Enter, to perform a TCP scan of 192.168.1.20 and determine what ports are open.
root@kali2:~# nmap -sT 192.168.1.20
root@kali2:~# nmap -sT 192.168.1.20
Starting Nmap 6.49BETA4 (https://nmap.org) at 2016-08-17 16:47 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00095s latency).
Not shown: 993 filtered ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:50:56:9A:4F:69 (VMware)
11 Type the following command, then press Enter, to perform a TCP scan of 192.168.1.30 and determine what ports are open.
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


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
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
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
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

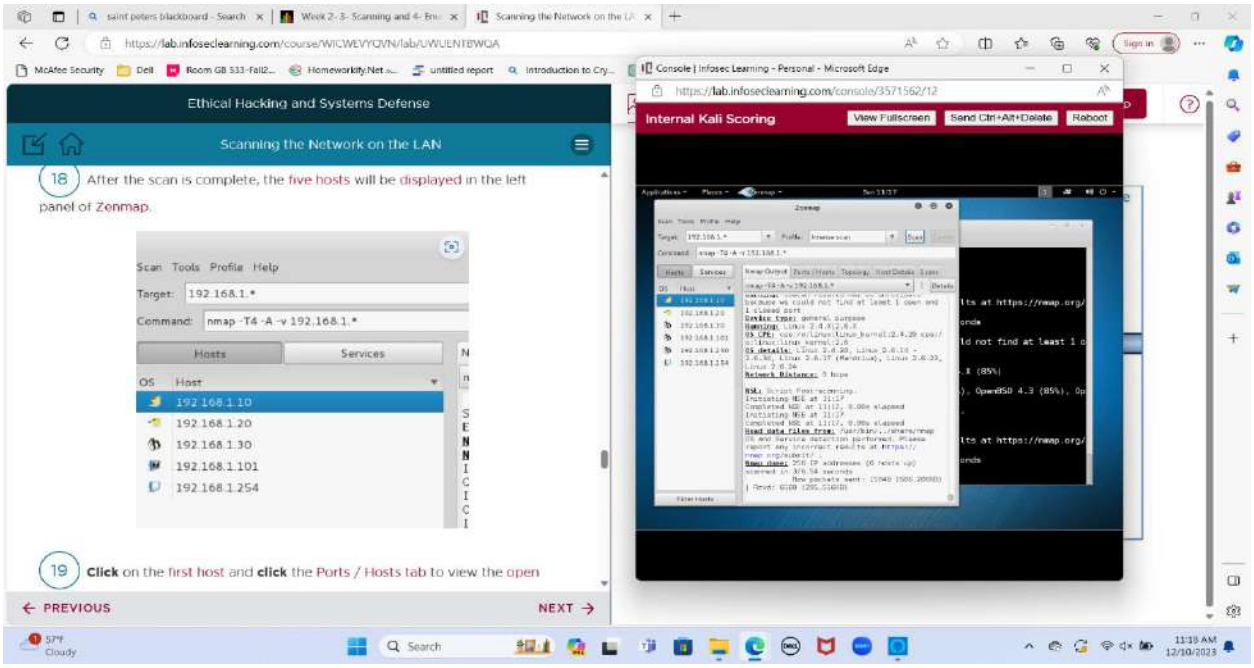

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
MAC Address: 00:50:56:80:E7:87 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 18.22 seconds
13 Type the following command, then press Enter, to perform an OS scan of 192.168.1.10 to determine the operating system of this host.
root@kali2:~# nmap -O 192.168.1.10 | tail
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.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

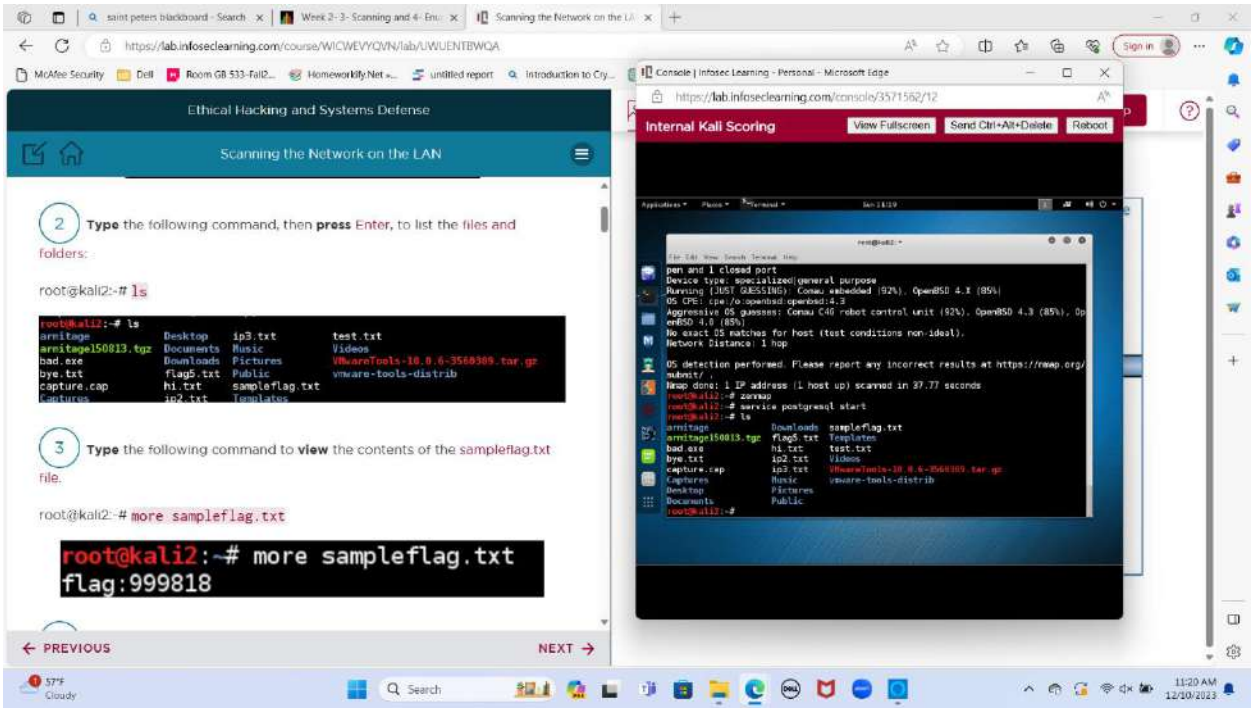
OS Scan

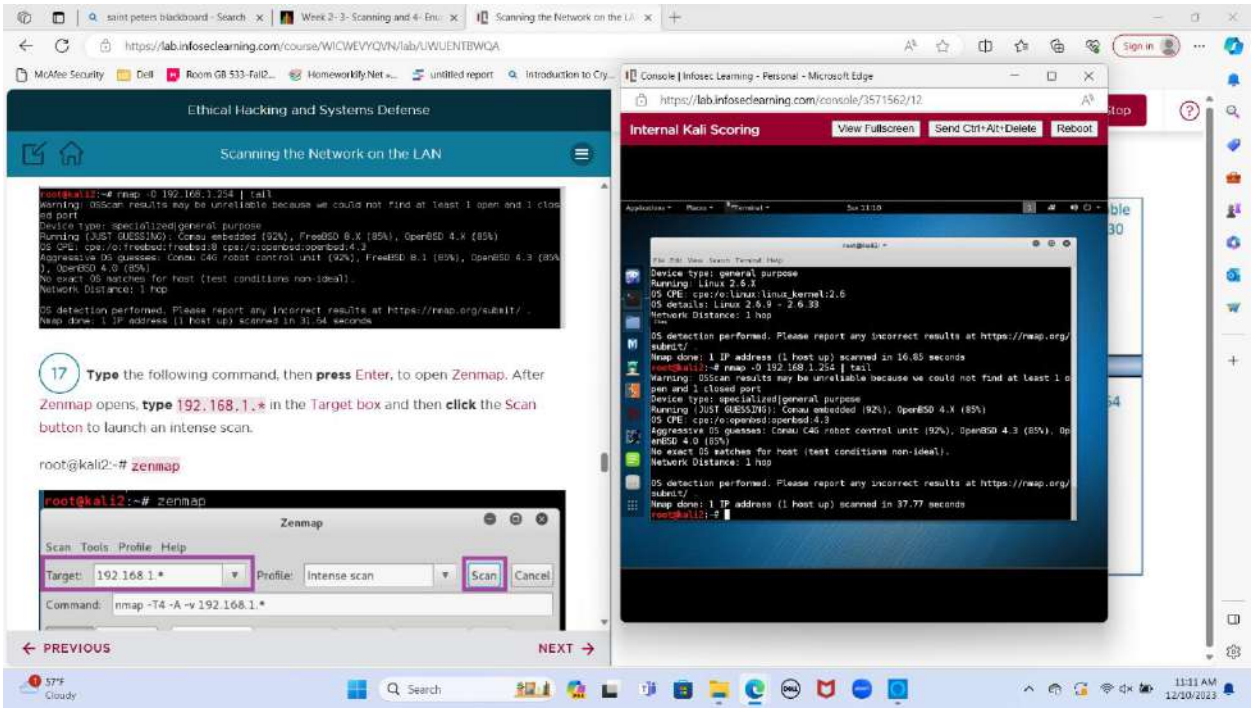

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
14 Type the following command, then press Enter, to perform an OS scan of 192.168.1.20 to determine the operating system of this host.
root@kali2:~# nmap -O 192.168.1.20 | tail
15 Type the following command, then press Enter, to perform an OS scan of 192.168.1.30 to determine the operating system of this host.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


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
16 Type the following command, then press Enter, to perform an OS scan of 192.168.1.254 to determine the operating system of this host.
root@kali2:~# nmap -O 192.168.1.254 | tail
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

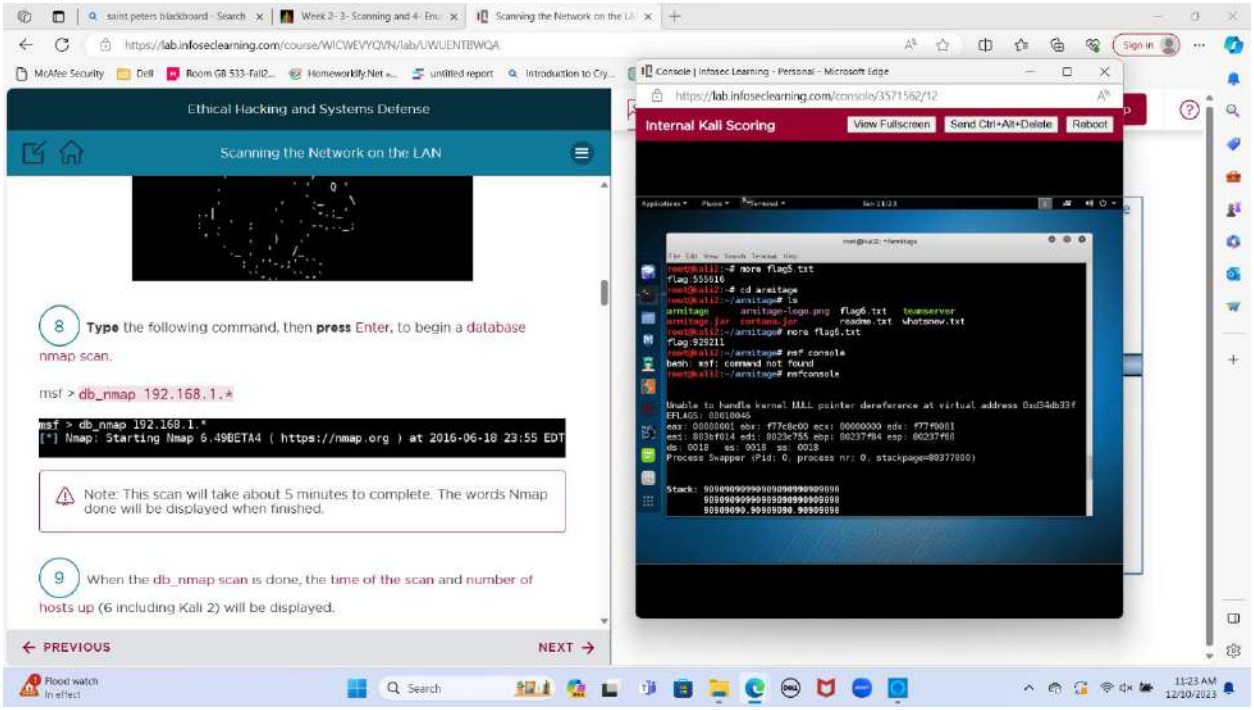
Zenmap

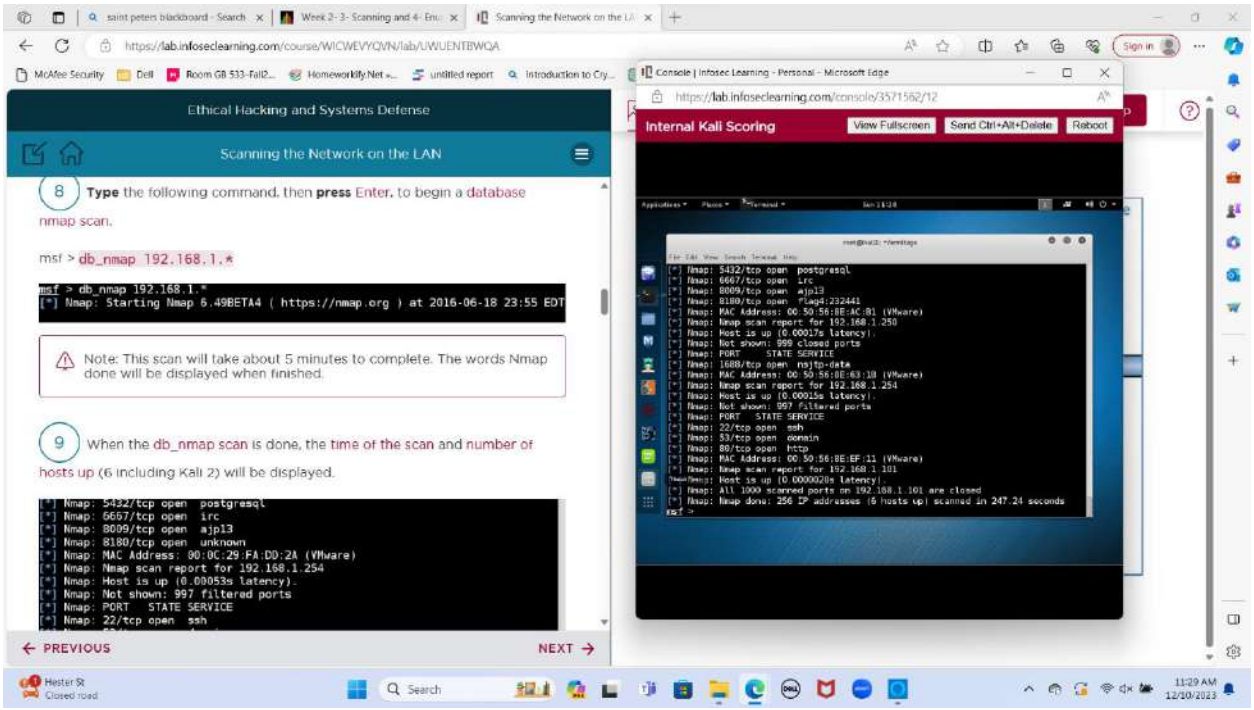

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
18 After the scan is complete, the five hosts will be displayed in the left panel of Zenmap.
Scan Tools Profile Help
Target: 192.168.1.*
Command: nmap -T4 -A -v 192.168.1.*
Hosts
Services
OS Host
192.168.1.10
192.168.1.20
192.168.1.30
192.168.1.101
192.168.1.254
19 Click on the first host and click the Ports / Hosts tab to view the open
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
2 Type the following command, then press Enter, to list the files and folders:
root@kali2:~# ls
3 Type the following command to view the contents of the sampleflag.txt file.
root@kali2:~# more sampleflag.txt
root@kali2:~# more sampleflag.txt
flag:999818
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

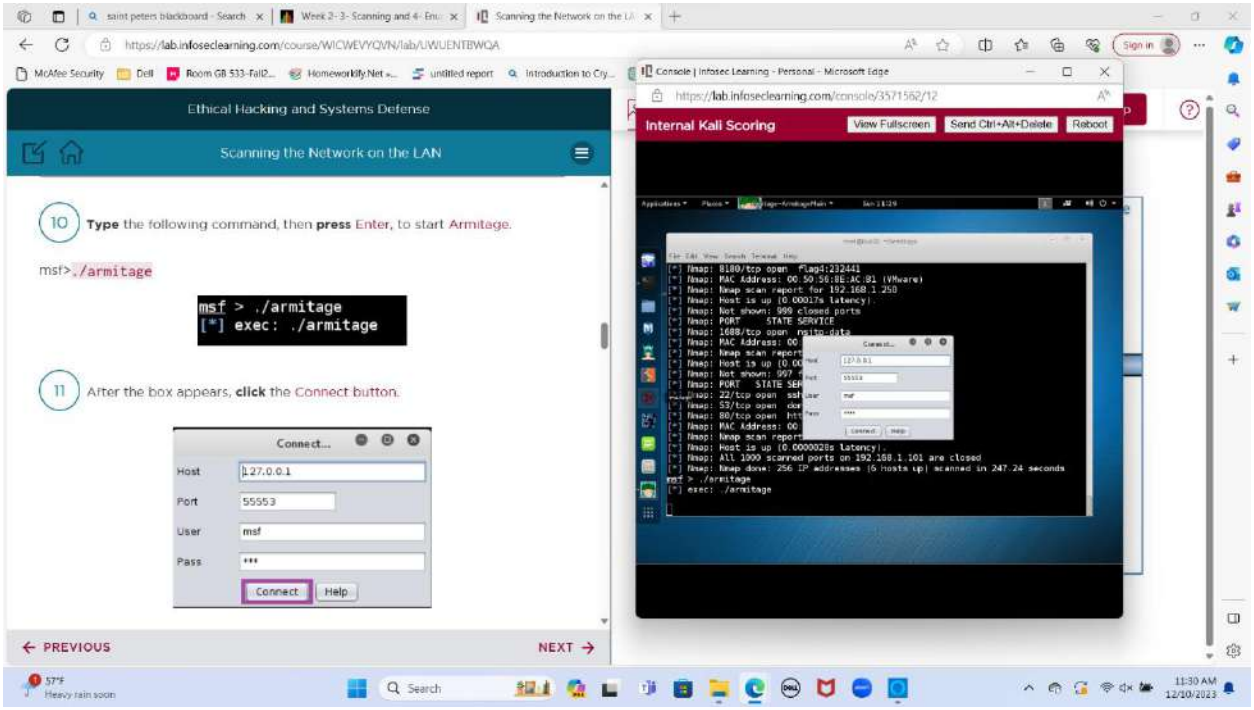

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
17 Type the following command, then press Enter, to open Zenmap. After Zenmap opens, type 192.168.1.* in the Target box and then click the Scan button to launch an intense scan.
root@kali2:~# zenmap
Zenmap
Scan Tools Profile Help
Target: 192.168.1.*
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.1.*
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

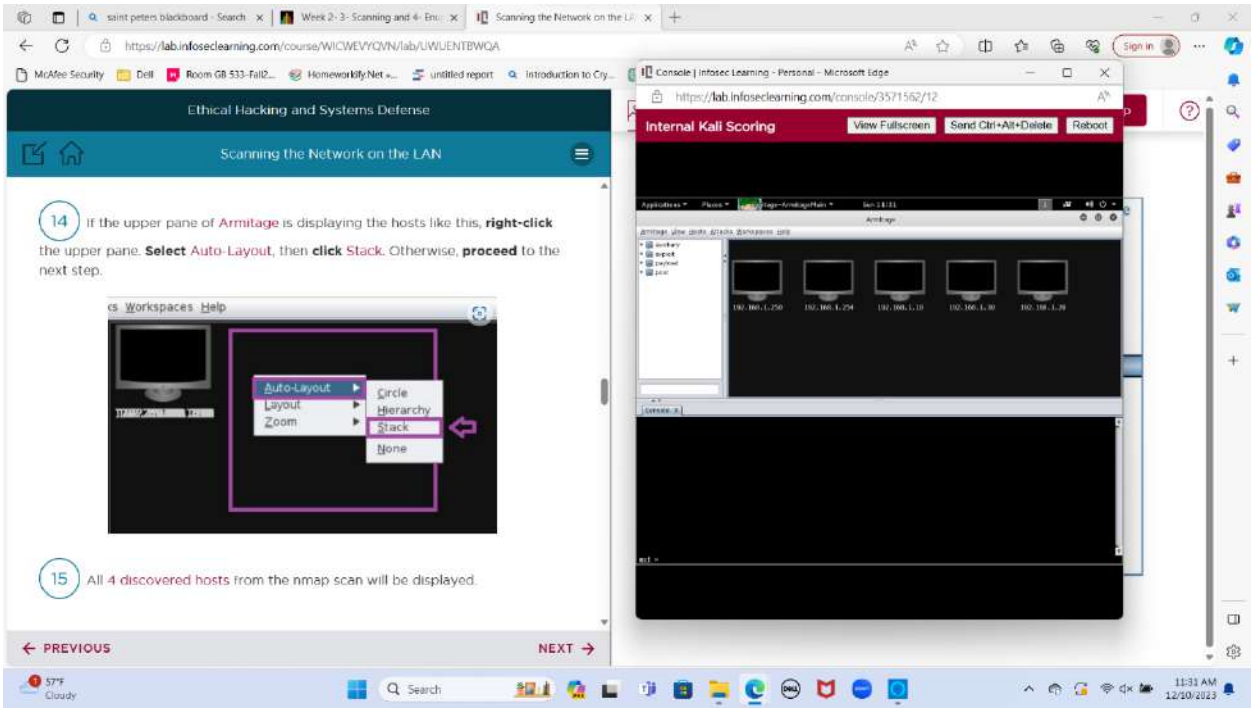
Database nmap scan



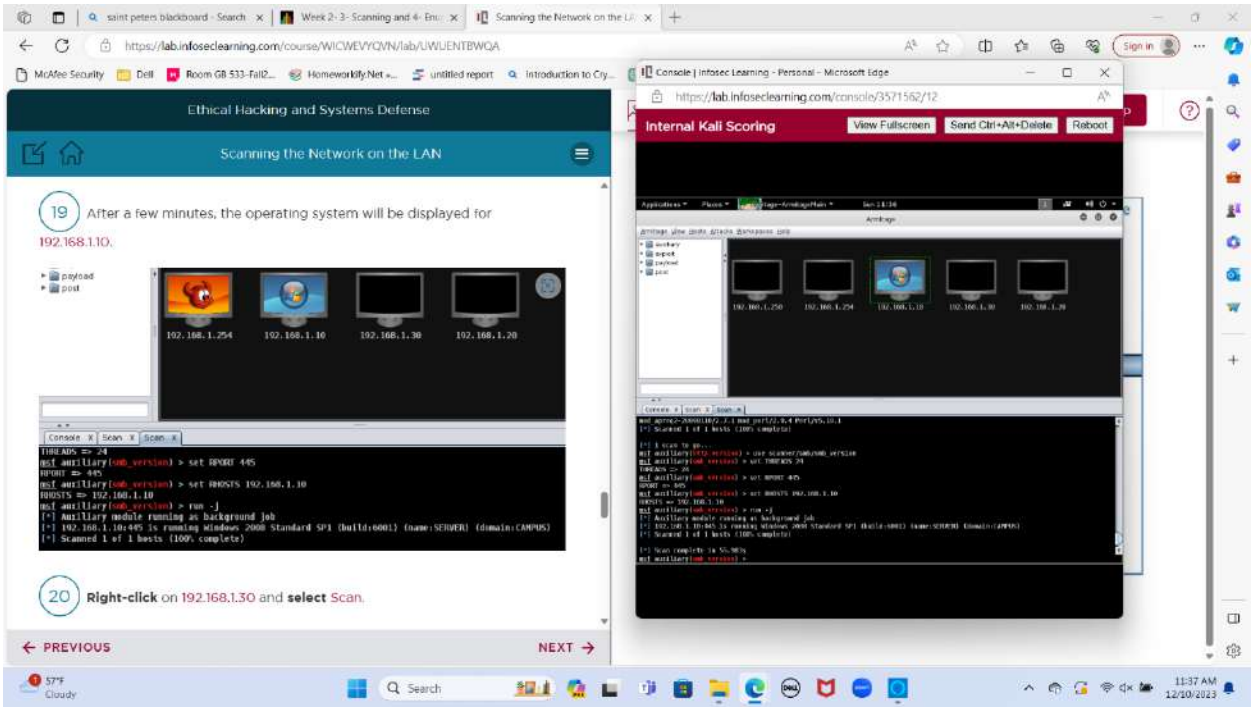


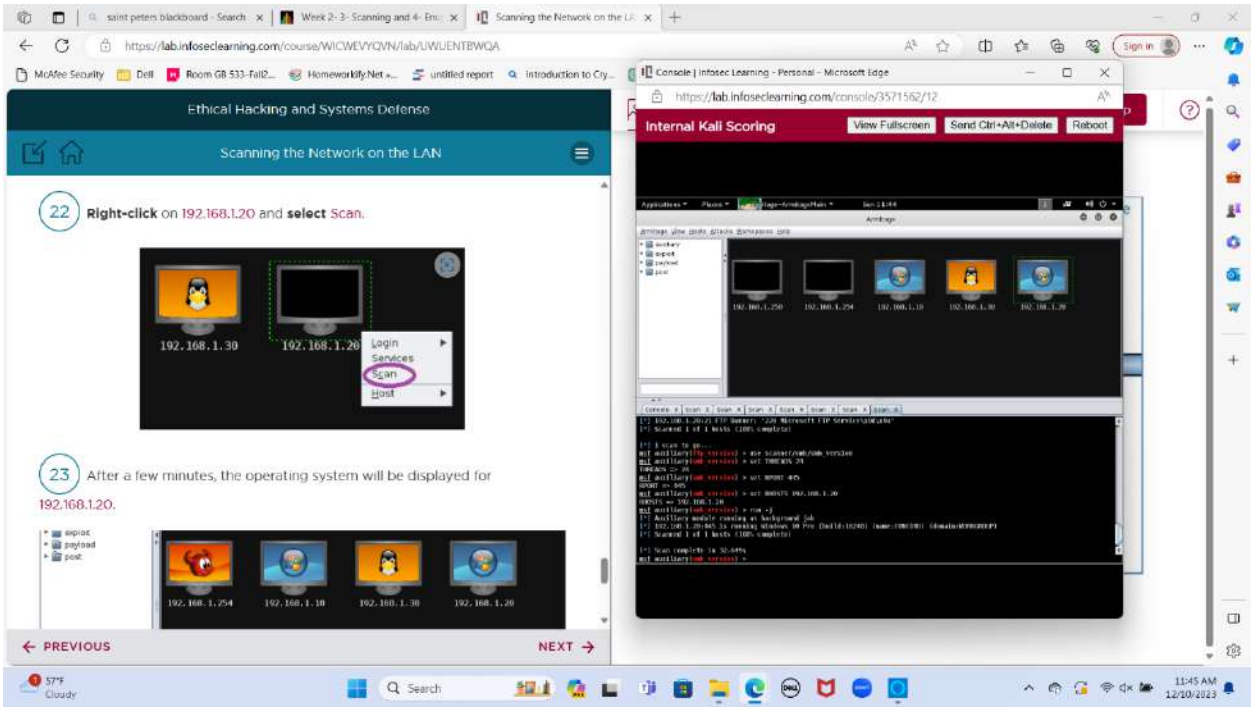
Armitage


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
10 Type the following command, then press Enter, to start Armitage.
msf>./armitage
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
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

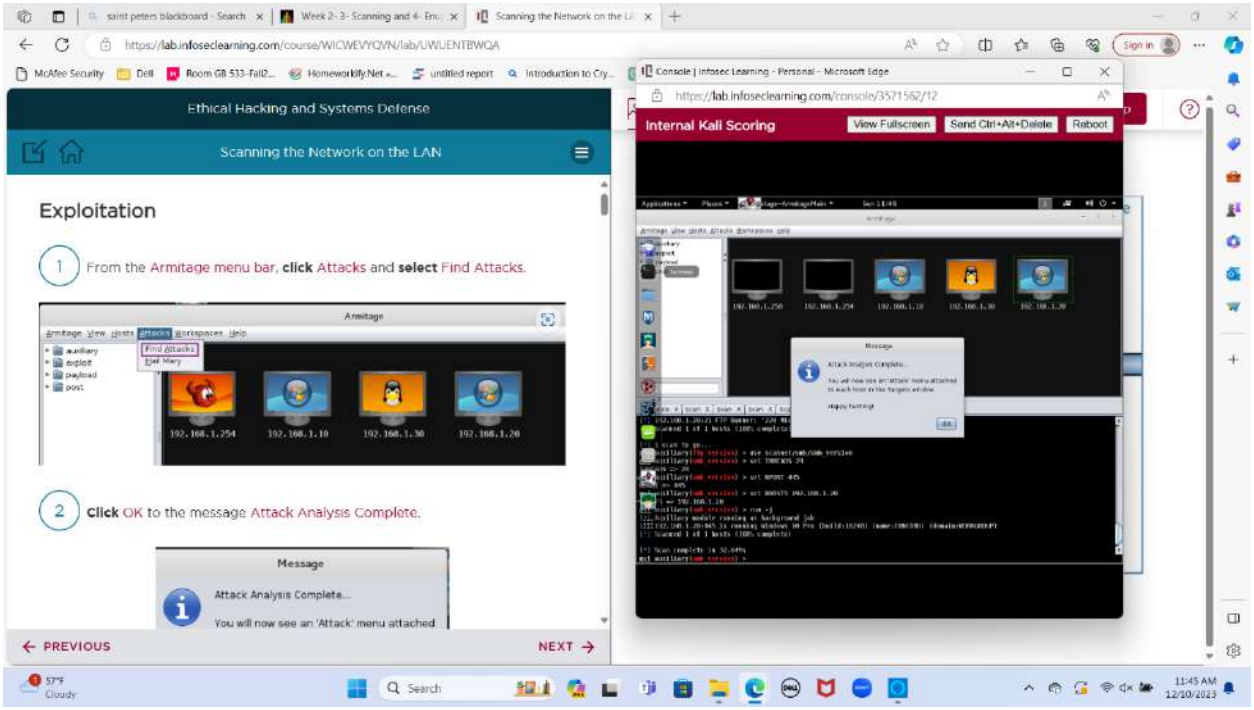

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
14 If the upper pane of Armitage is displaying the hosts like this, right-click the upper pane. Select Auto-Layout, then click Stack. Otherwise, proceed to the next step.
Workspaces Help
Auto-Layout
Layout
Zoom
Circle
Hierarchy
Stack
None
15 All 4 discovered hosts from the nmap scan will be displayed.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

Scanning

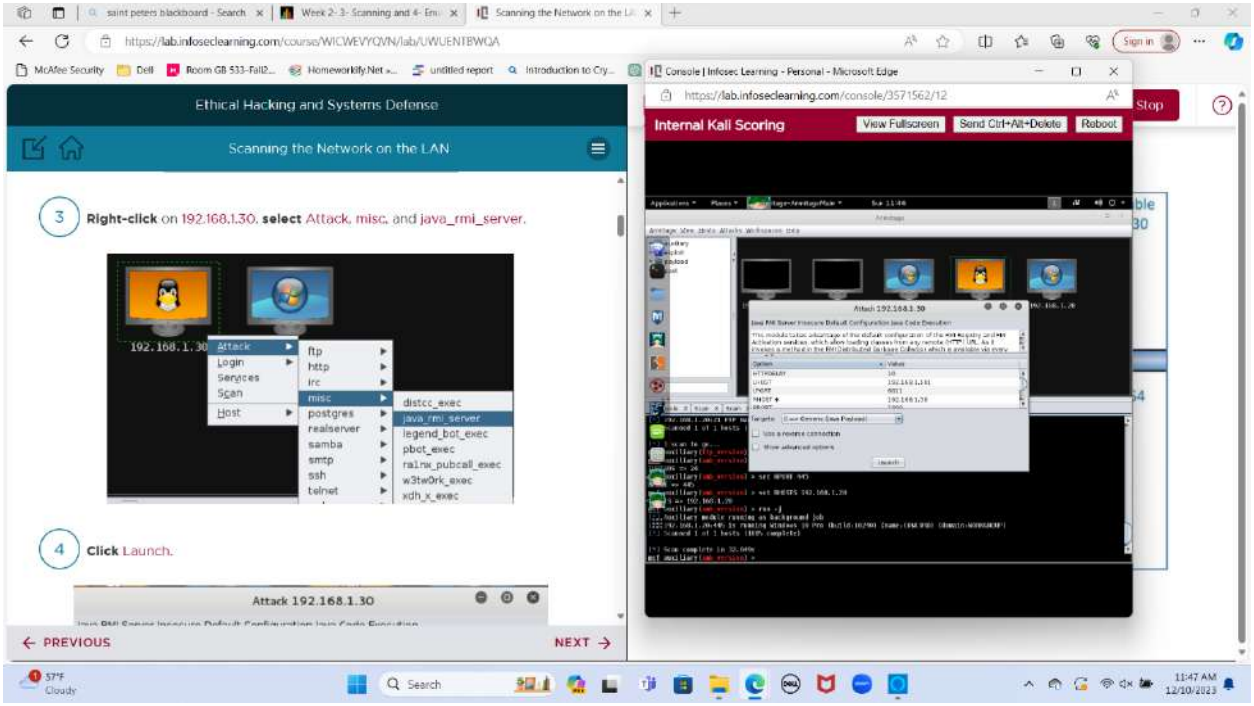

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
19 After a few minutes, the operating system will be displayed for 192.168.1.10.
20 Right-click on 192.168.1.30 and select Scan.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
22 Right-click on 192.168.1.20 and select Scan.
192.168.1.30
192.168.1.20
Login
Services
Scan
Host
23 After a few minutes, the operating system will be displayed for 192.168.1.20.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

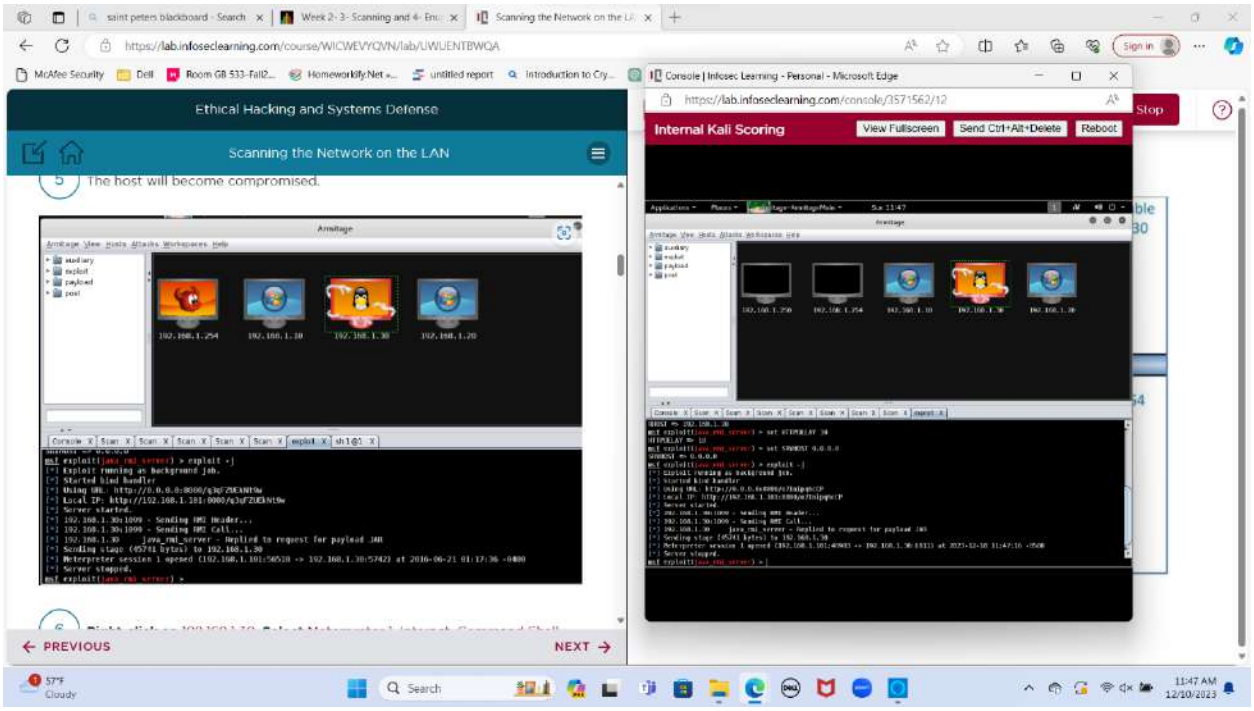
Finding attacks



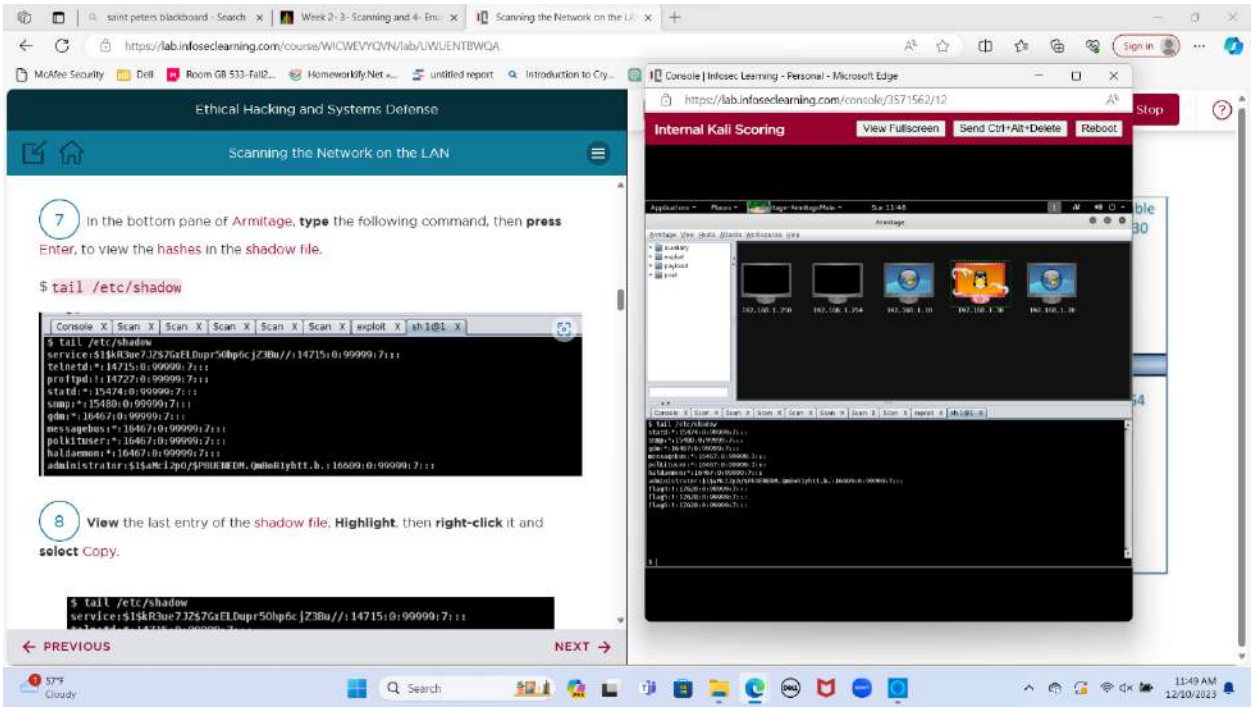
Selecting attack



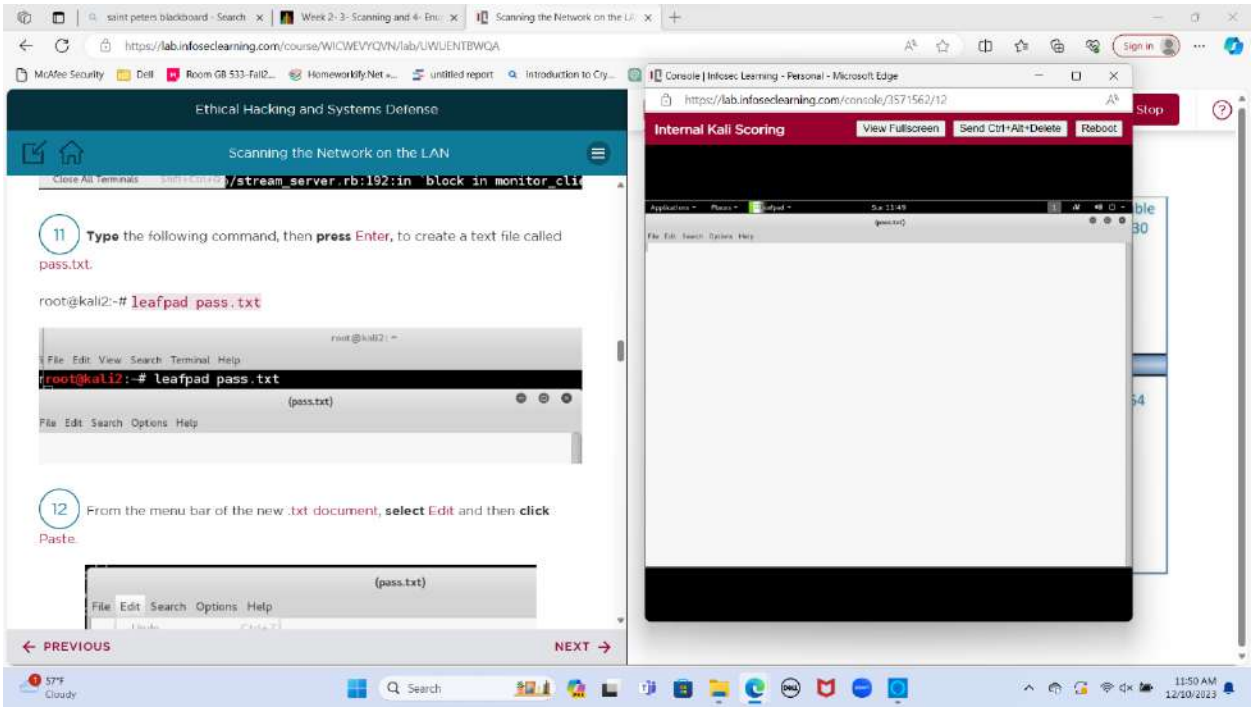
Host compromised



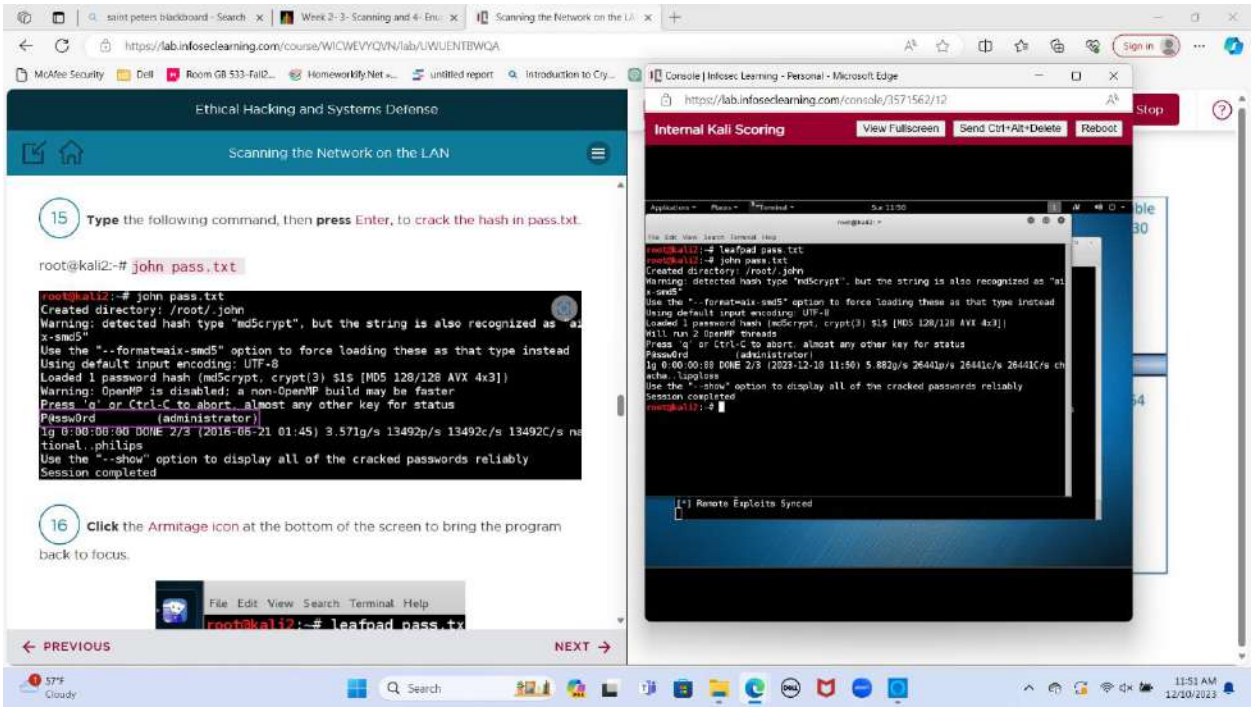
Viewing hashes



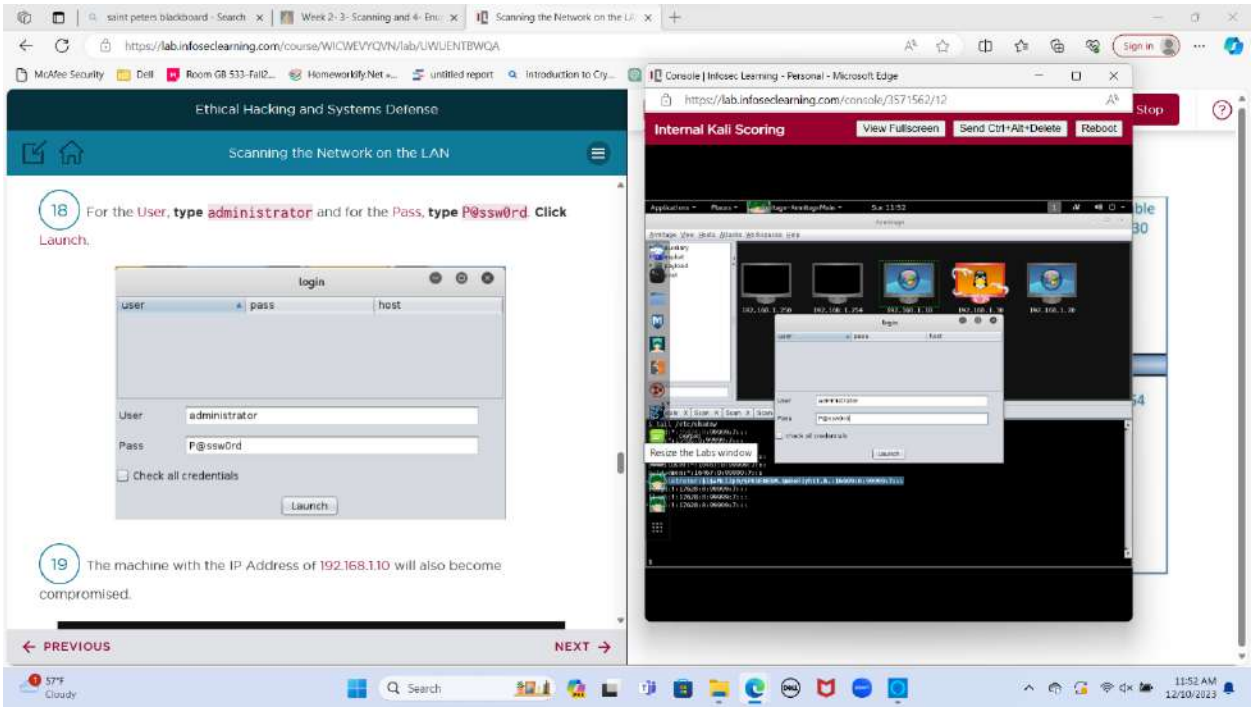
Creating text file

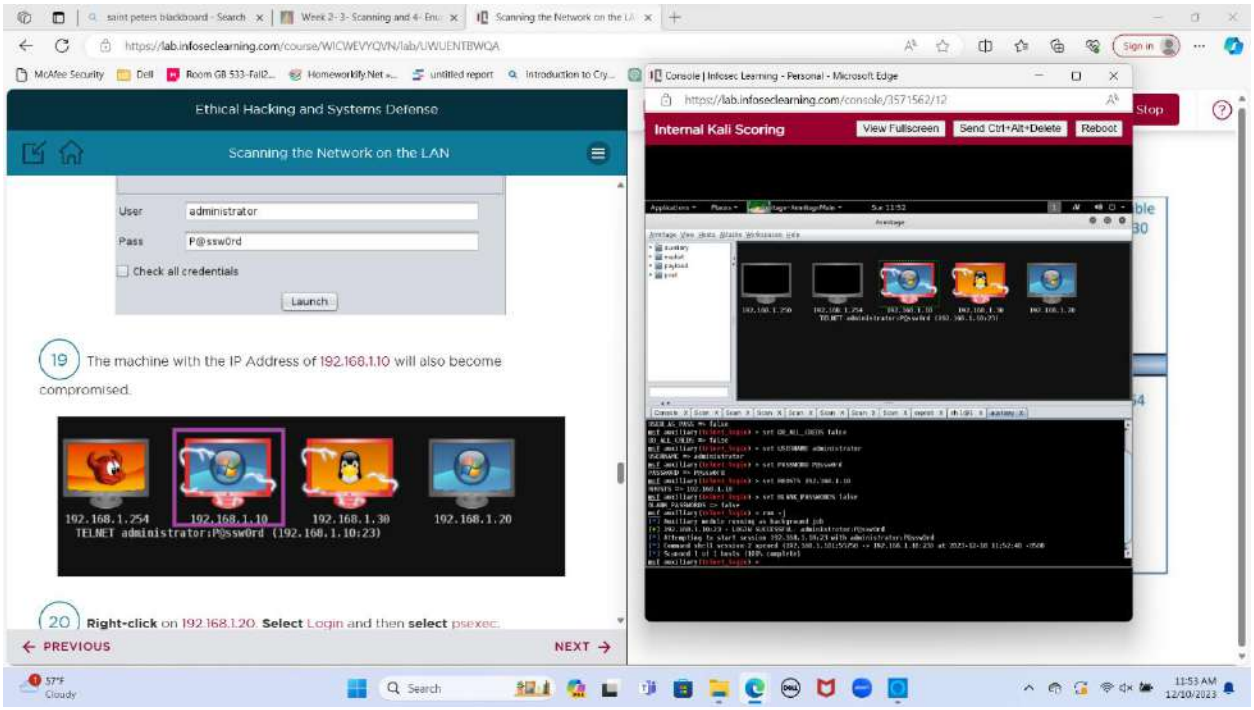


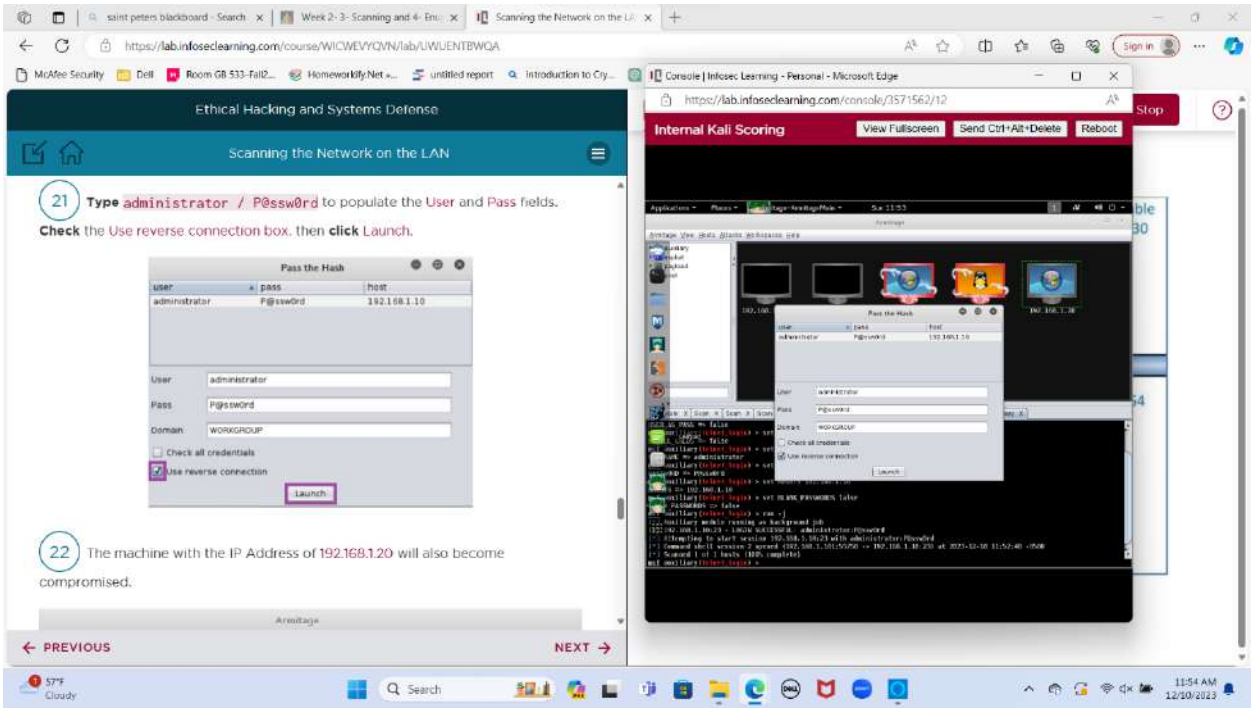
Cracking the hash

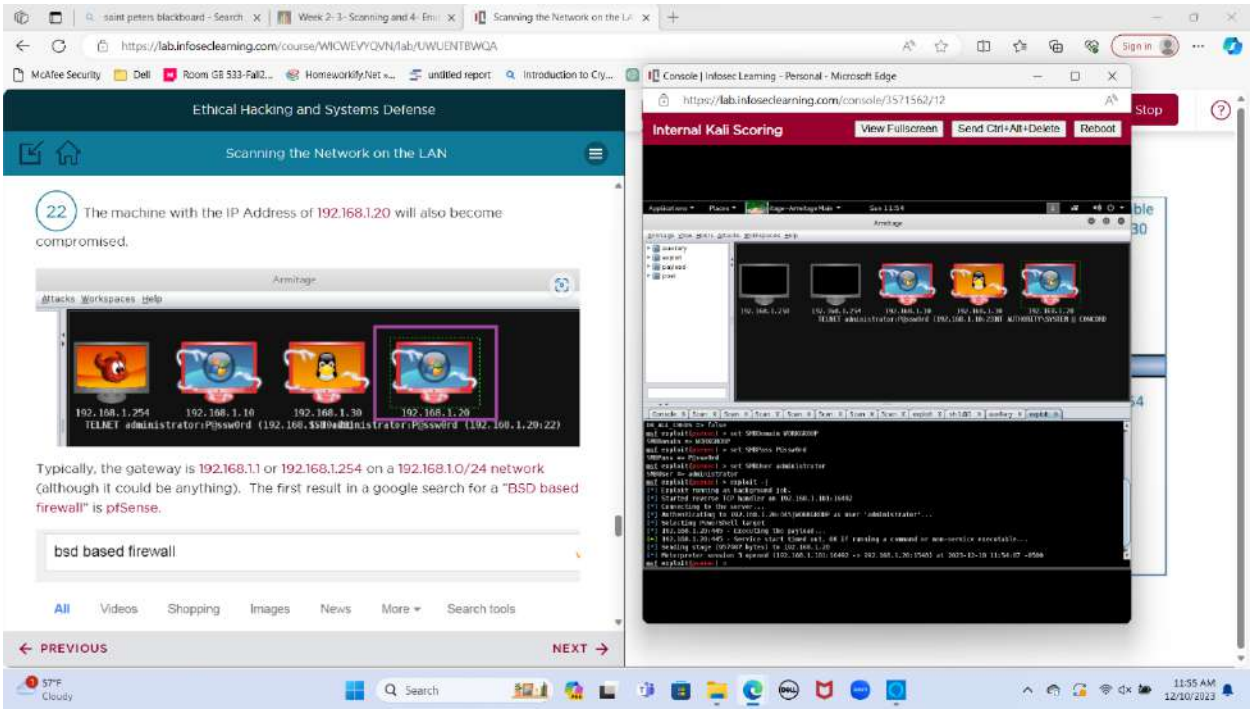


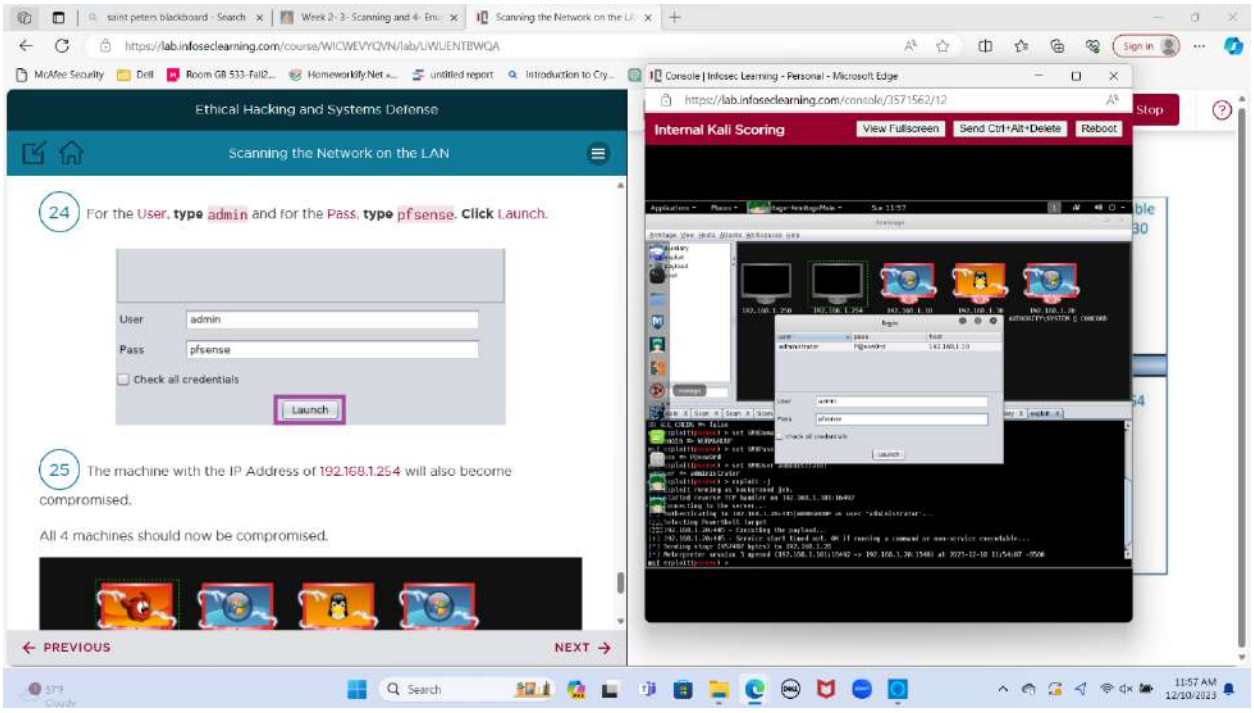
Logging in

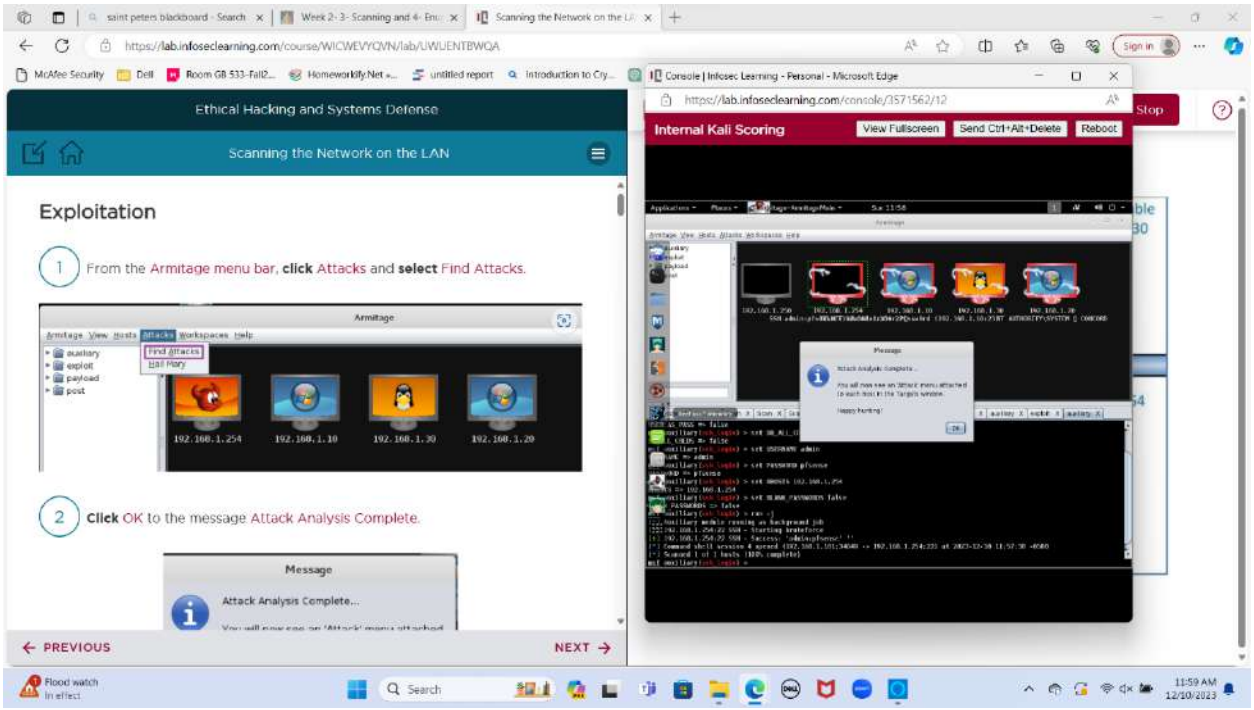

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
18 For the User, type administrator and for the Pass, type P@ssw0rd. Click Launch.
login
user
pass
host
User
administrator
Pass
P@ssw0rd
Check all credentials
Launch
19 The machine with the IP Address of 192.168.1.10 will also become compromised.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Resize the Labs window

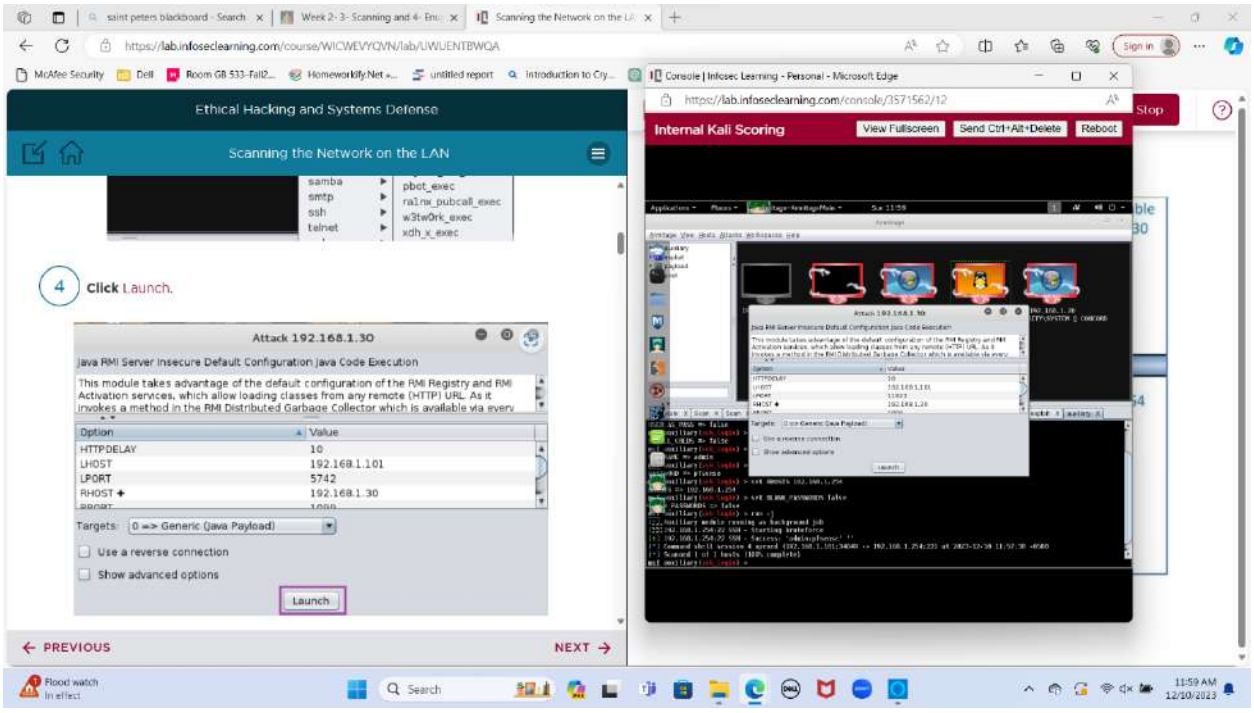

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
User
administrator
Pass
P@ssw0rd
Check all credentials
Launch
19 The machine with the IP Address of 192.168.1.10 will also become compromised.
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
TELNET administrator:P@ssw0rd (192.168.1.10:23)
20 Right-click on 192.168.1.20. Select Login and then select psexec.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop

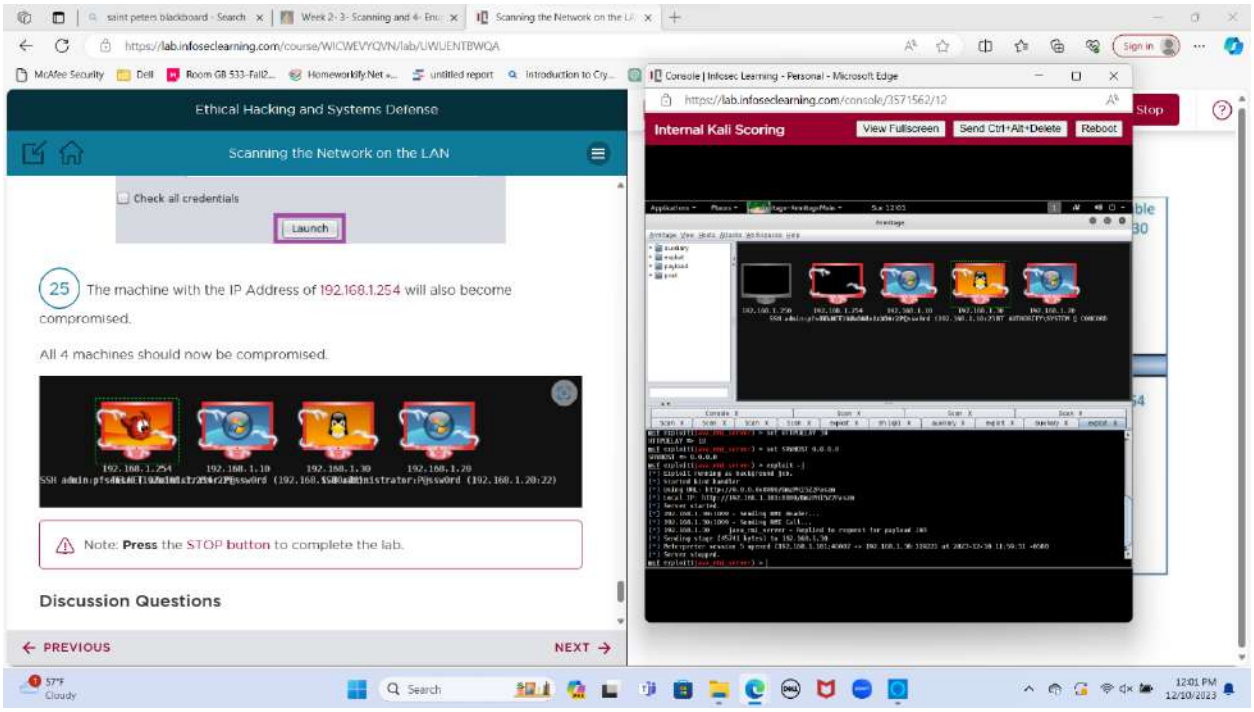

Ethical Hacking and Systems Defense
Scanning the Network on the LAN
21 Type administrator / P@ssw0rd to populate the User and Pass fields.
Check the Use reverse connection box, then click Launch.
Pass the Hash
user
pass
host
administrator
P@ssw0rd
192.168.1.10
User
administrator
Pass
P@ssw0rd
Domain
WORKGROUP
Check all credentials
Use reverse connection
Launch
22 The machine with the IP Address of 192.168.1.20 will also become compromised.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
22 The machine with the IP Address of 192.168.1.20 will also become compromised.
Armitage
Attacks Workspaces Help
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
Typically, the gateway is 192.168.1.1 or 192.168.1.254 on a 192.168.1.0/24 network (although it could be anything). The first result in a google search for a "BSD based firewall" is pfSense.
bsd based firewall
All
Videos
Shopping
Images
News
More
Search tools
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
24 For the User, type admin and for the Pass, type pfsense. Click Launch.
User
admin
Pass
pfsense
Check all credentials
Launch
25 The machine with the IP Address of 192.168.1.254 will also become compromised.
All 4 machines should now be compromised.
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop


Ethical Hacking and Systems Defense
Scanning the Network on the LAN
Exploitation
1 From the Armitage menu bar, click Attacks and select Find Attacks.
Armitage
Find Attacks
Hail Mary
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
2 Click OK to the message Attack Analysis Complete.
Message
Attack Analysis Complete...
PREVIOUS
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop





This is the last screen before the end of this lab.