MODULE 03 FOOTPRINTIG AND RECONNAISSANCE LAB SCREENSHOTS

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

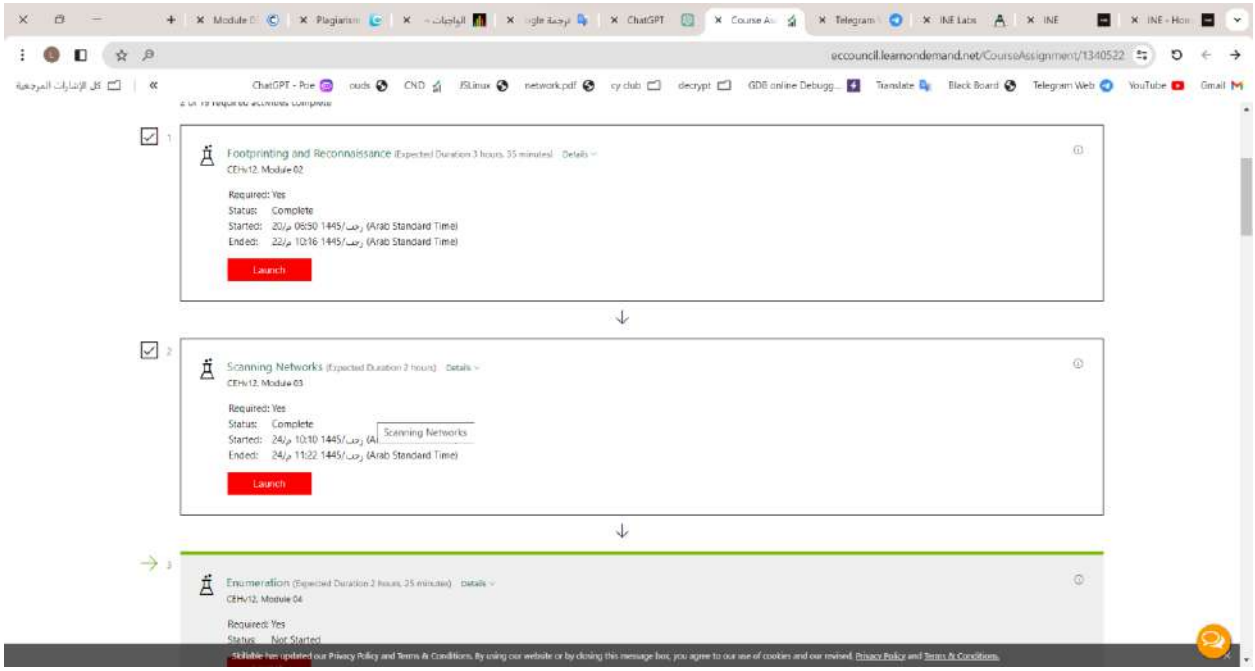
1. https://labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10

2. https://labclient.labondemand.com/LabClient/c7ae60a5-feb4-47a5-8dc2-7a96eb51daaa?rc=10

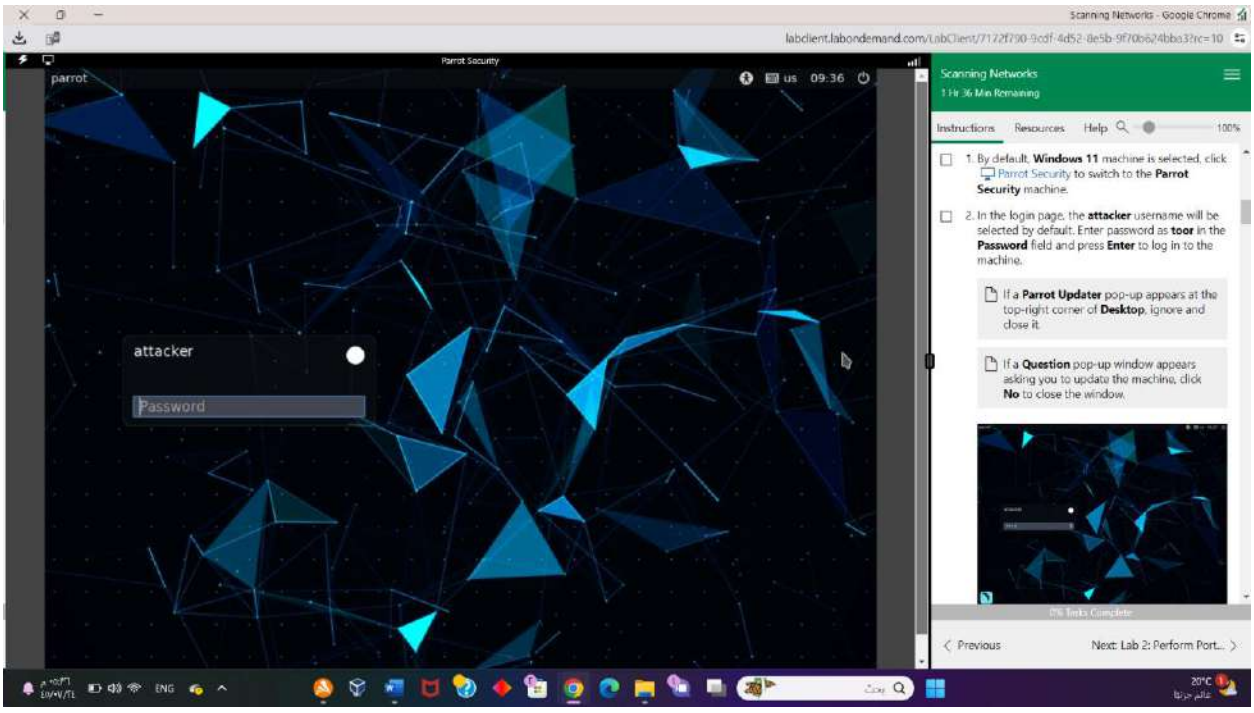
3. https://labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10

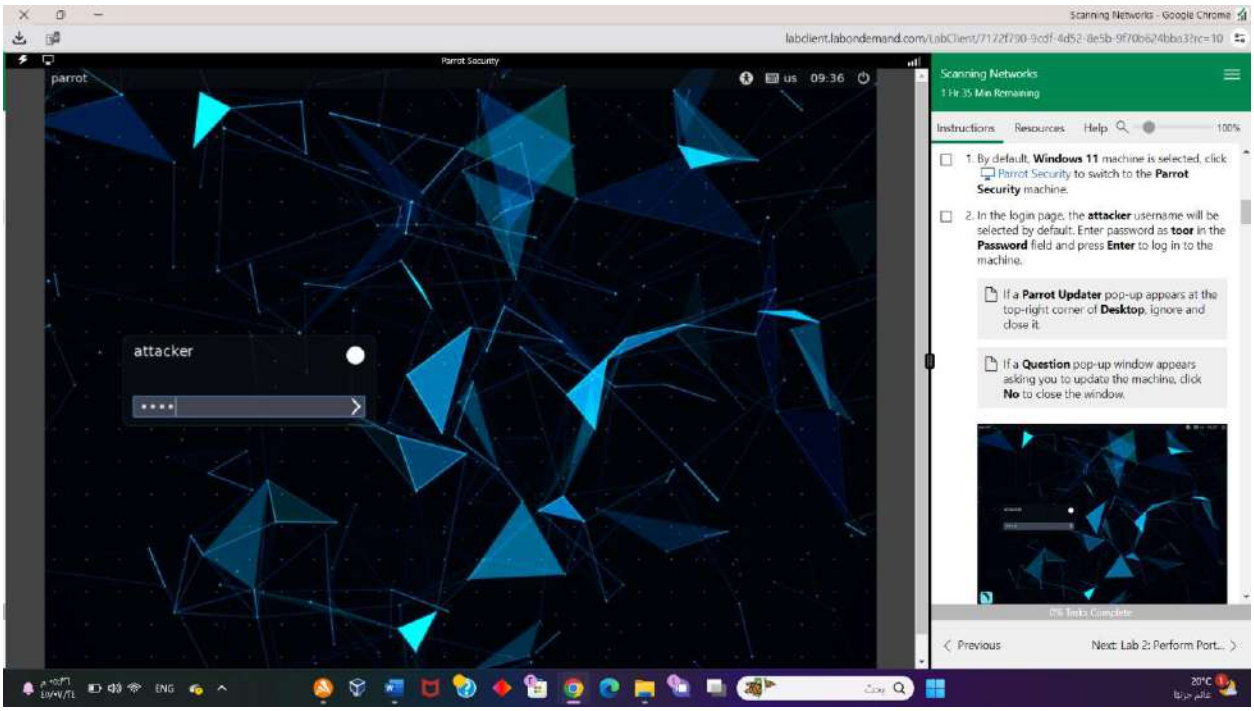
Username on EC-Council System

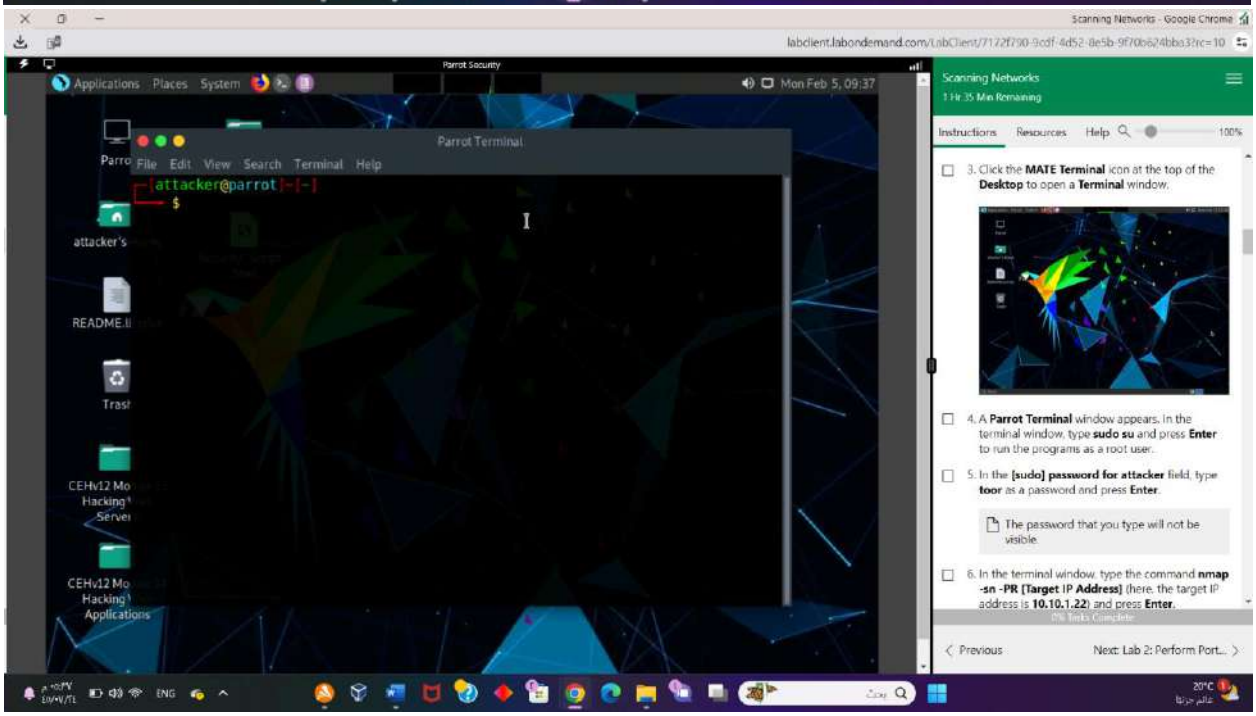
1. 2110886@uj.edu.sa

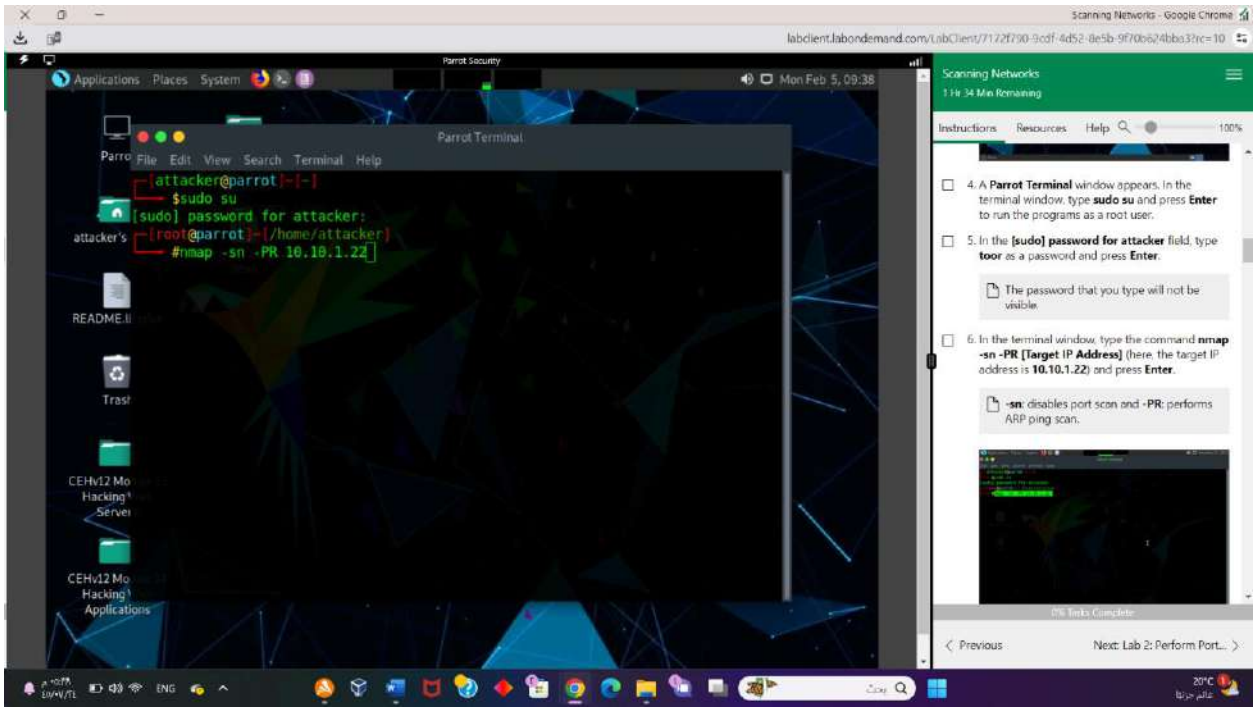


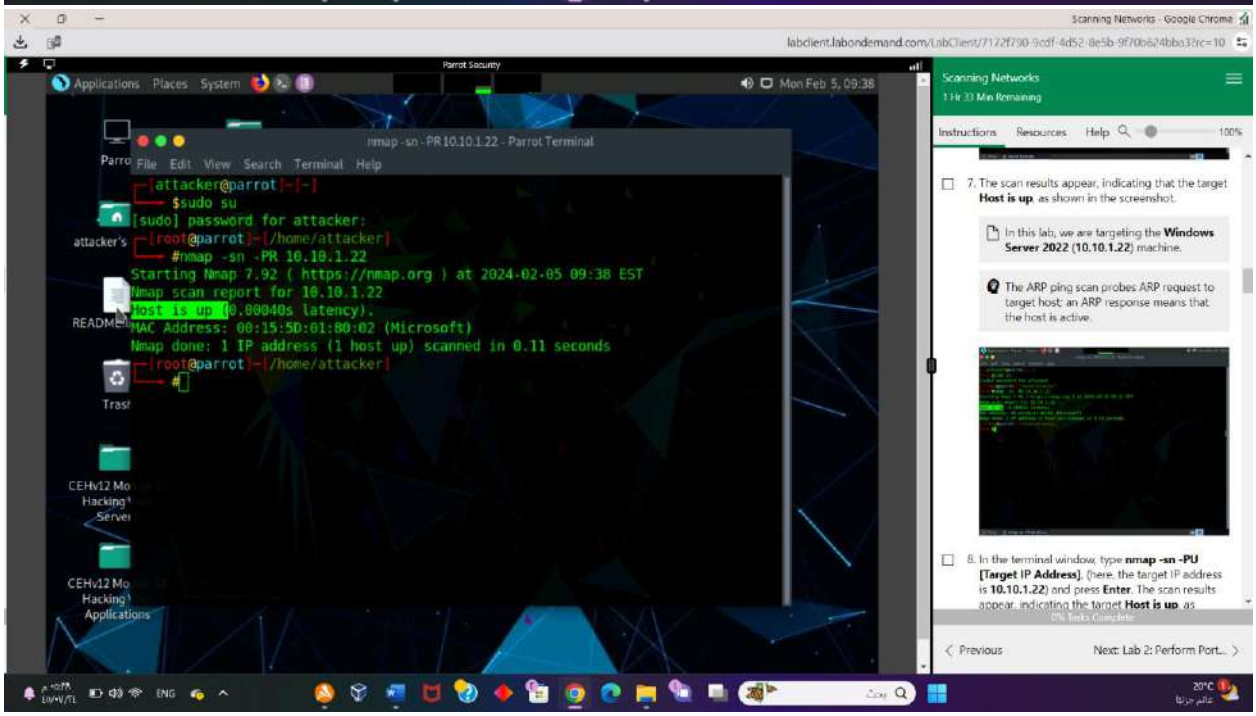
Lab 01 - Task 01

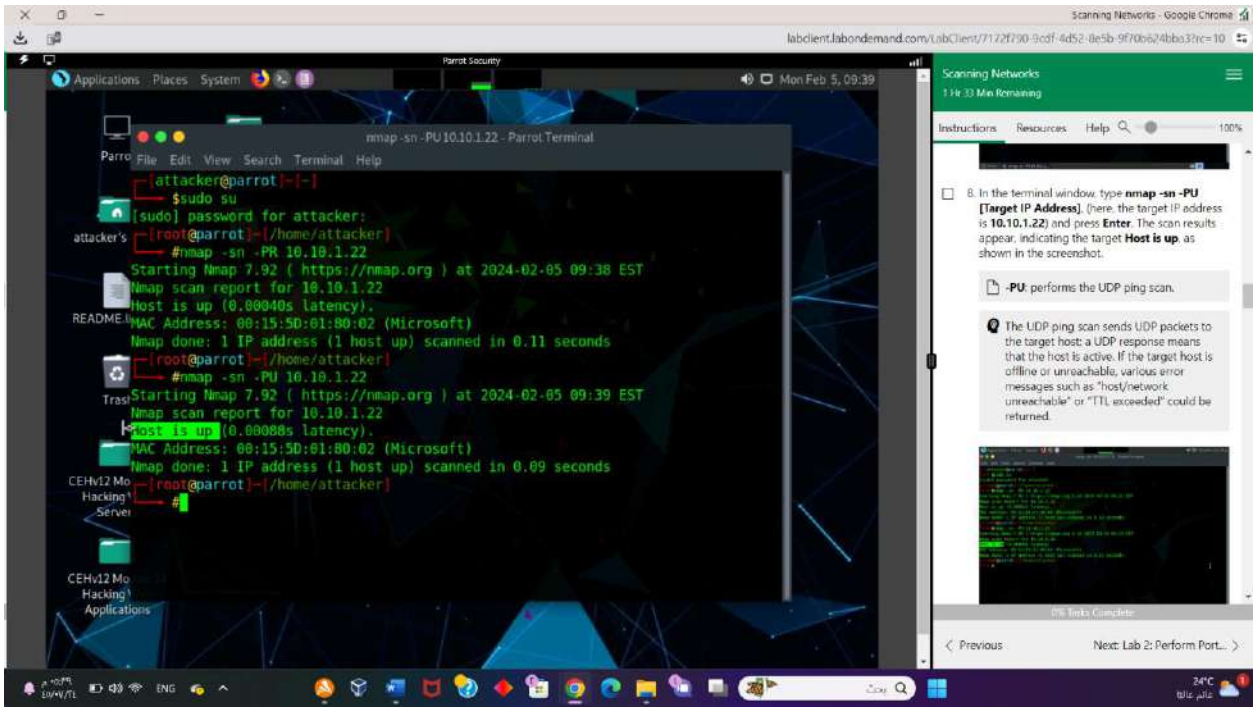

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7122f700-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
parrot
us 09:36
attacker
Password
Scanning Networks
1 Hr 36 Min Remaining
Instructions
Resources
Help
100%
1. By default, Windows 11 machine is selected, click Parrot Security to switch to the Parrot Security machine.
2. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.
If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.
If a Question pop-up window appears asking you to update the machine, click No to close the window.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
20°C

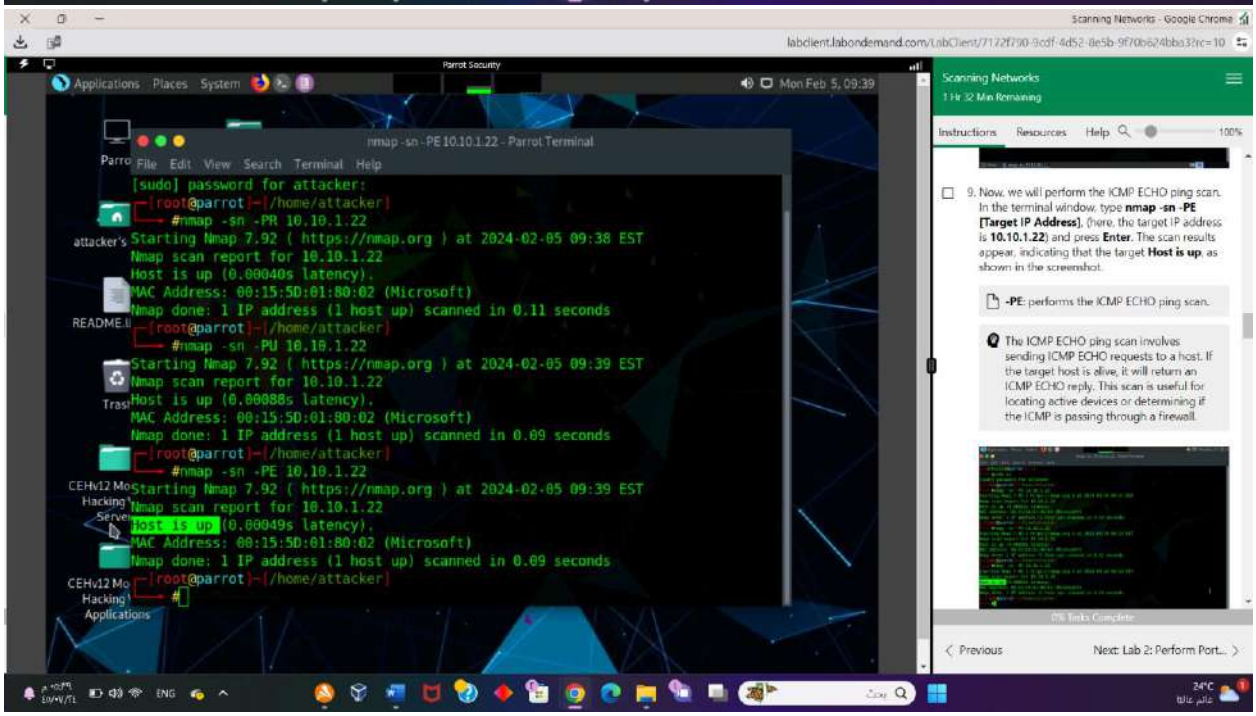

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
parrot
us 09:36
attacker
Scanning Networks
1 Hr 35 Min Remaining
Instructions
Resources
Help
100%
1. By default, Windows 11 machine is selected, click Parrot Security to switch to the Parrot Security machine.
2. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.
If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.
If a Question pop-up window appears asking you to update the machine, click No to close the window.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
20°C

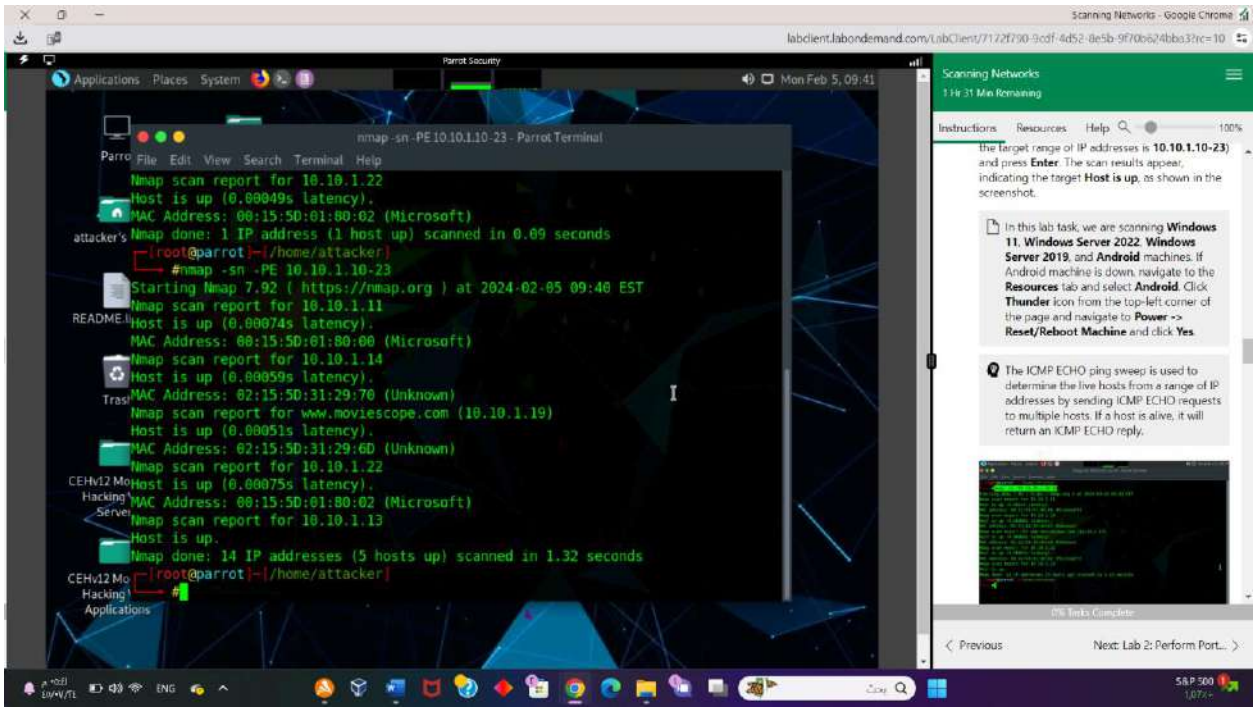

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:37
Parrot Terminal
File Edit View Search Terminal Help
attacker@parrot~[~]
$
attacker's
README.li
Trash
CEHv12 Mo
Hacking
Server
CEHv12 Mo
Hacking
Applications
Scanning Networks
1 Hr 35 Min Remaining
Instructions
Resources
Help
100%
3. Click the MATE Terminal icon at the top of the Desktop to open a Terminal window.
4. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
5. In the [sudo] password for attacker field, type toor as a password and press Enter.
The password that you type will not be visible.
6. In the terminal window, type the command nmap -sn -PR [Target IP Address] (here, the target IP address is 10.10.1.22) and press Enter.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
20°C

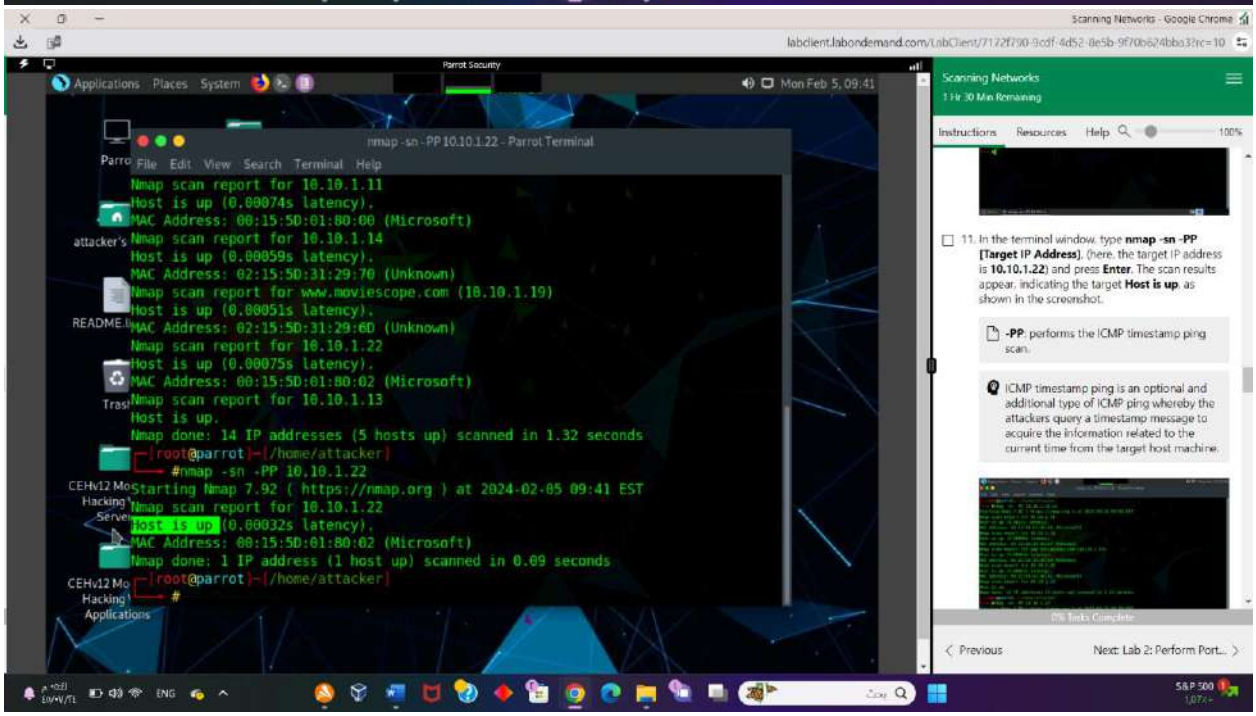

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:38
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#nmap -sn -PR 10.10.1.22
Scanning Networks
1 Hr 34 Min Remaining
Instructions Resources Help 100%
4. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
5. In the [sudo] password for attacker field, type toor as a password and press Enter.
The password that you type will not be visible.
6. In the terminal window, type the command nmap -sn -PR [Target IP Address] (here, the target IP address is 10.10.1.22) and press Enter.
-sn: disables port scan and -PR: performs ARP ping scan.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
20°C

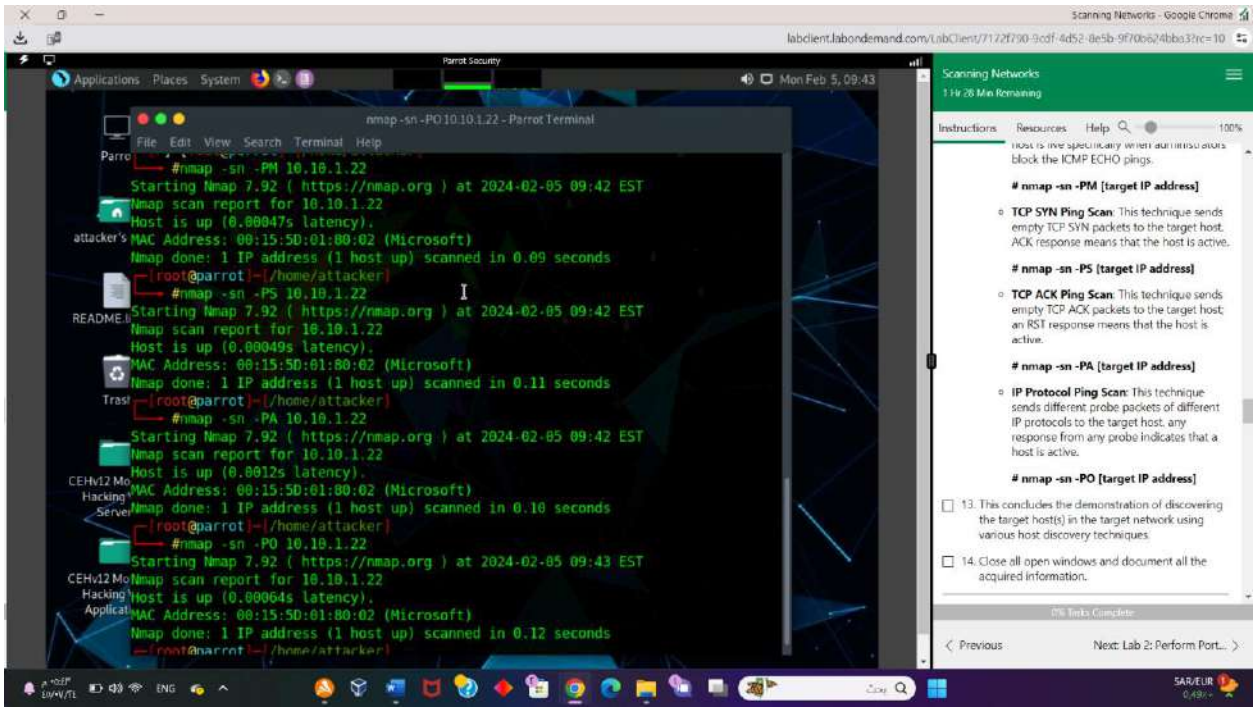

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:38
nmap -sn -PR 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:38 EST
Nmap scan report for 10.10.1.22
Host is up (0.00040s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[root@parrot]~[/home/attacker]
#
Scanning Networks
1 Hr 33 Min Remaining
Instructions Resources Help 100%
7. The scan results appear, indicating that the target Host is up, as shown in the screenshot.
In this lab, we are targeting the Windows Server 2022 (10.10.1.22) machine.
The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.
8. In the terminal window, type nmap -sn -PU [Target IP Address], (here, the target IP address is 10.10.1.22) and press Enter. The scan results appear, indicating the target Host is up, as
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
20°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:39
nmap -sn -PU 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:38 EST
Nmap scan report for 10.10.1.22
Host is up (0.00040s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[root@parrot]~[/home/attacker]
#nmap -sn -PU 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:39 EST
Nmap scan report for 10.10.1.22
Host is up (0.00088s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@parrot]~[/home/attacker]
#
attacker's
README.li
Trash
CEHv12 Mo Hacking Server
CEHv12 Mo Hacking Applications
Scanning Networks
1 Hr 33 Min Remaining
Instructions
Resources
Help
100%
8. In the terminal window, type nmap -sn -PU [Target IP Address], (here, the target IP address is 10.10.1.22) and press Enter. The scan results appear, indicating the target Host is up, as shown in the screenshot.
-PU: performs the UDP ping scan.
The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
24°C

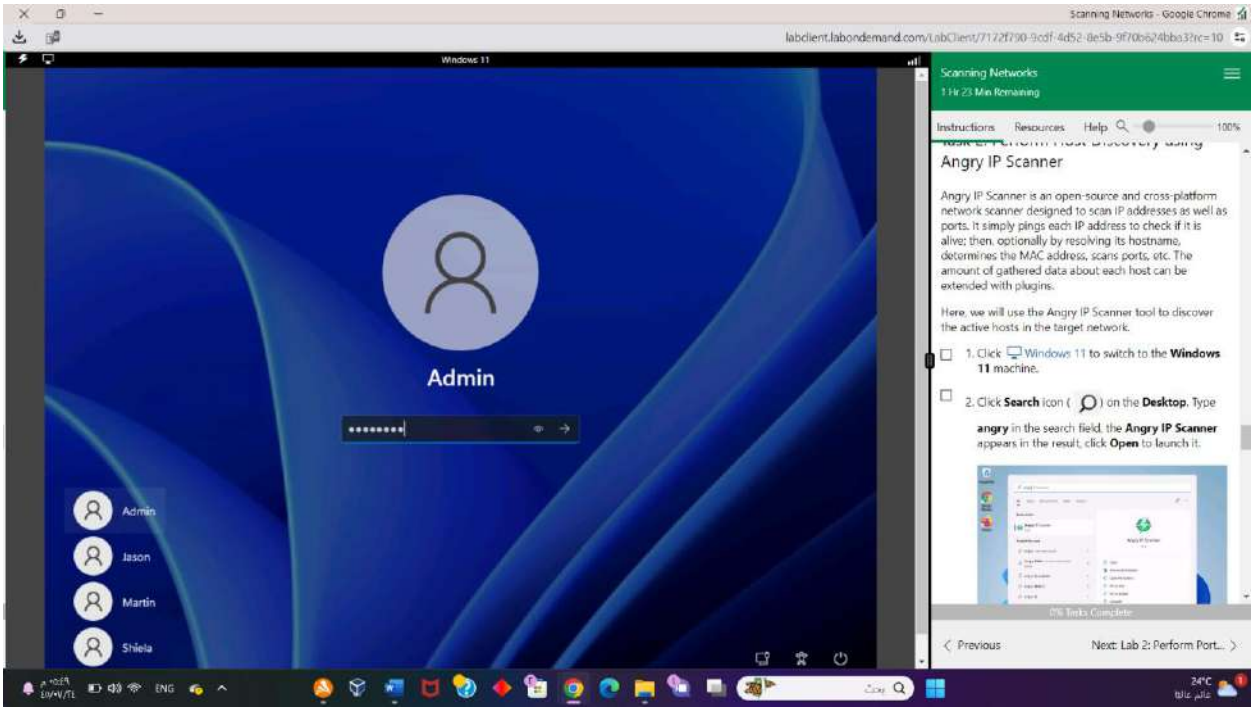

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:39
nmap -sn -PE 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:38 EST
Nmap scan report for 10.10.1.22
Host is up (0.00040s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[root@parrot]~[/home/attacker]
#nmap -sn -PU 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:39 EST
Nmap scan report for 10.10.1.22
Host is up (0.00088s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@parrot]~[/home/attacker]
#nmap -sn -PE 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:39 EST
Nmap scan report for 10.10.1.22
Host is up (0.00049s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@parrot]~[/home/attacker]
#
attacker's
README.li
Trash
CEHv12 Mo Hacking Server
CEHv12 Mo Hacking Applications
Scanning Networks
1 Hr 32 Min Remaining
Instructions
Resources
Help
100%
9. Now, we will perform the ICMP ECHO ping scan. In the terminal window, type nmap -sn -PE [Target IP Address], (here, the target IP address is 10.10.1.22) and press Enter. The scan results appear, indicating that the target Host is up, as shown in the screenshot.
-PE: performs the ICMP ECHO ping scan.
The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
24°C

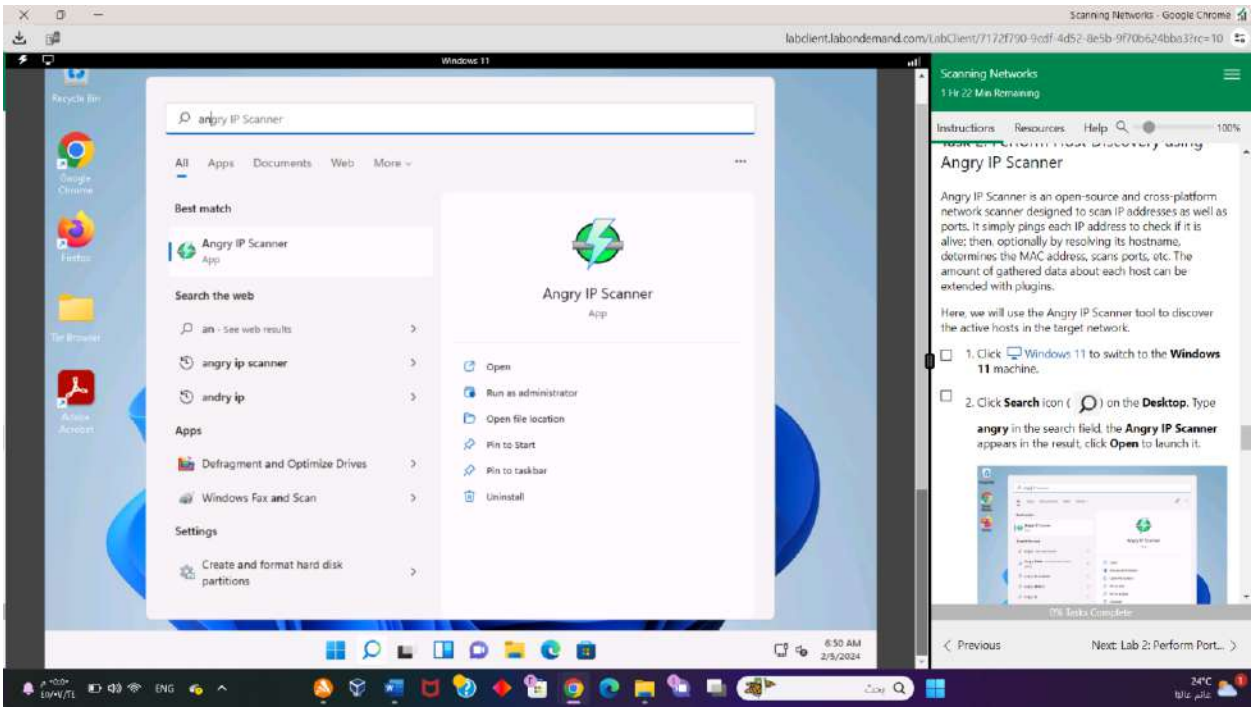

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:41
nmap -sn -PE 10.10.1.10-23 - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.22
Host is up (0.00049s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@parrot]-[/home/attacker]
#nmap -sn -PE 10.10.1.10-23
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:40 EST
Nmap scan report for 10.10.1.11
Host is up (0.00074s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00059s latency).
MAC Address: 02:15:5D:31:29:70 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00051s latency).
MAC Address: 02:15:5D:31:29:6D (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00075s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 14 IP addresses (5 hosts up) scanned in 1.32 seconds
[root@parrot]-[/home/attacker]
#
Scanning Networks
1 Hr 31 Min Remaining
Instructions Resources Help 100%
the target range of IP addresses is 10.10.1.10-23) and press Enter. The scan results appear, indicating the target Host is up, as shown in the screenshot.
In this lab task, we are scanning Windows 11, Windows Server 2022, Windows Server 2019, and Android machines. If Android machine is down, navigate to the Resources tab and select Android. Click Thunder icon from the top-left corner of the page and navigate to Power -> Reset/Reboot Machine and click Yes.
The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...

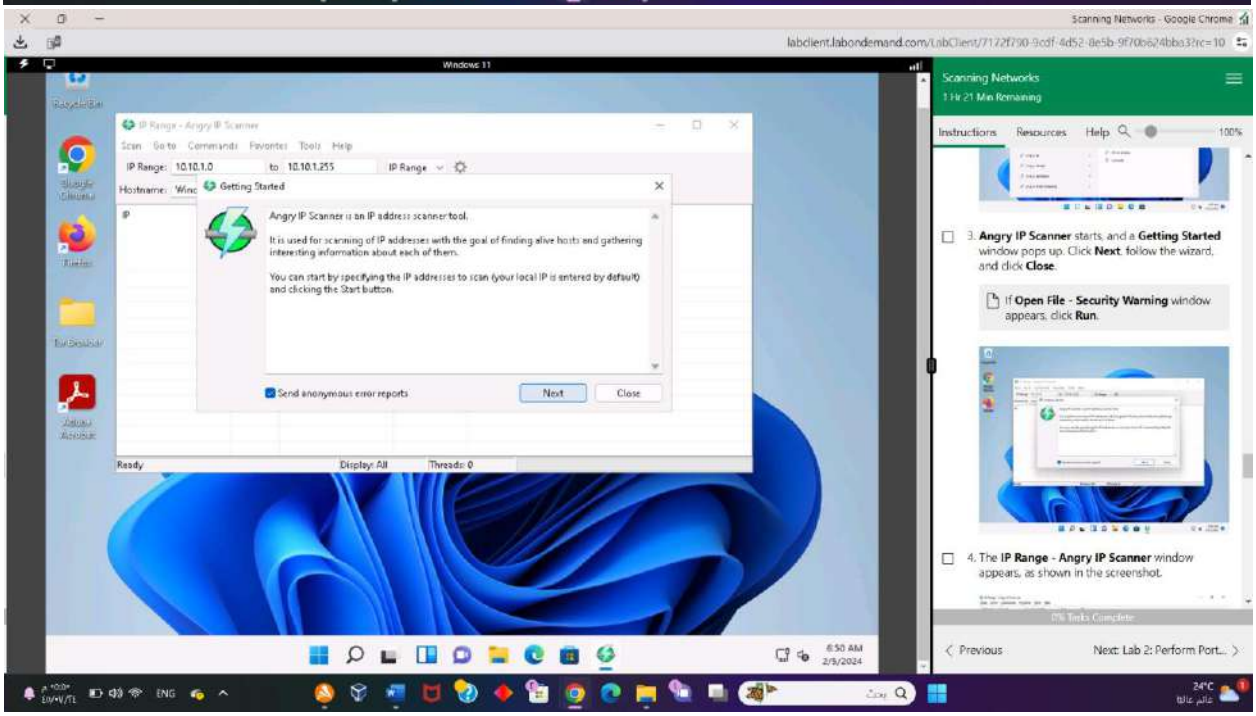

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 09:41
nmap -sn -PP 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.11
Host is up (0.00074s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00059s latency).
MAC Address: 02:15:5D:31:29:70 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00051s latency).
MAC Address: 02:15:5D:31:29:6D (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00075s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 14 IP addresses (5 hosts up) scanned in 1.32 seconds
[root@parrot]-[/home/attacker]
#nmap -sn -PP 10.10.1.22
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:41 EST
Nmap scan report for 10.10.1.22
Host is up (0.00032s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@parrot]-[/home/attacker]
#
Scanning Networks
1 Hr 30 Min Remaining
Instructions Resources Help 100%
11. In the terminal window, type nmap -sn -PP [Target IP Address], (here, the target IP address is 10.10.1.22) and press Enter. The scan results appear, indicating the target Host is up, as shown in the screenshot.
-PP: performs the ICMP timestamp ping scan.
ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...

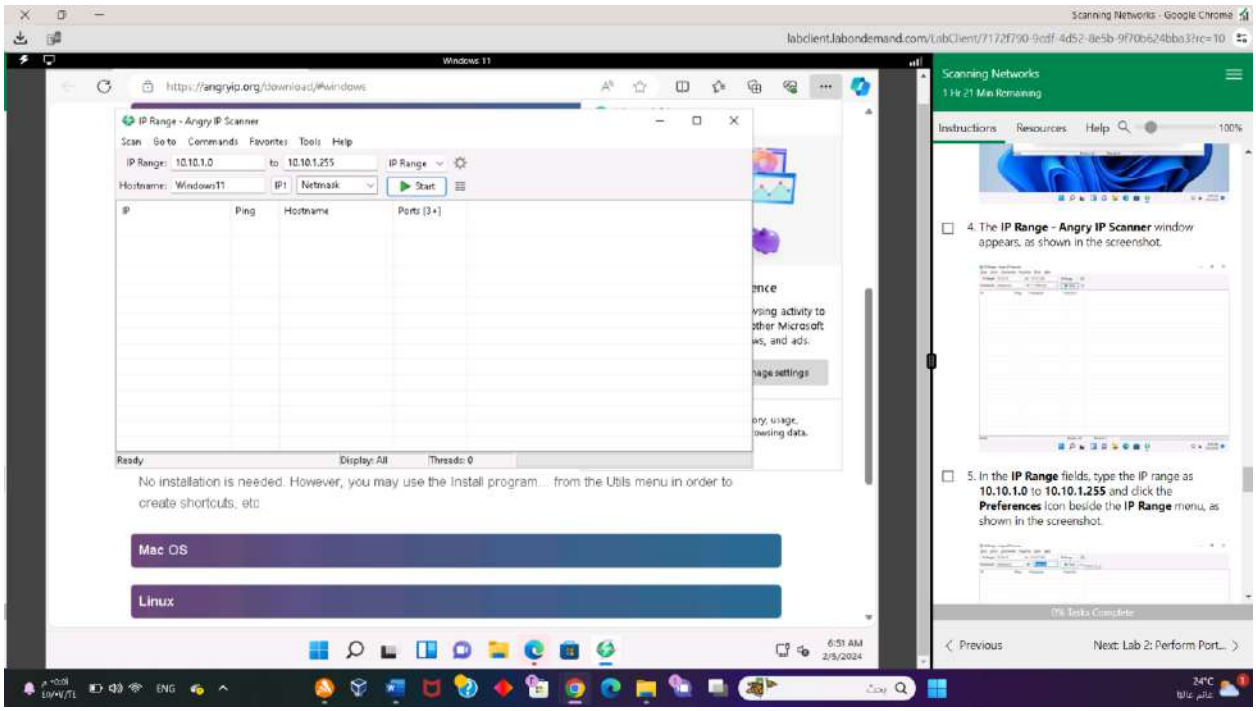


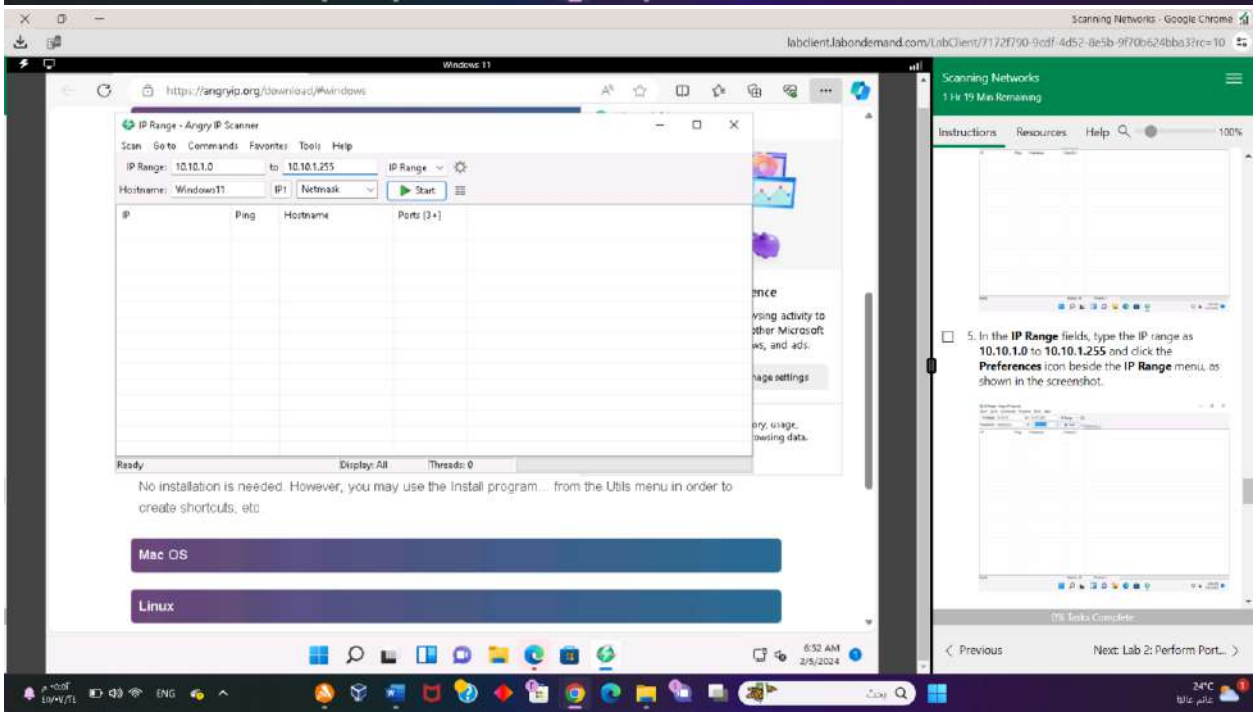
Lab 01 – Task 02

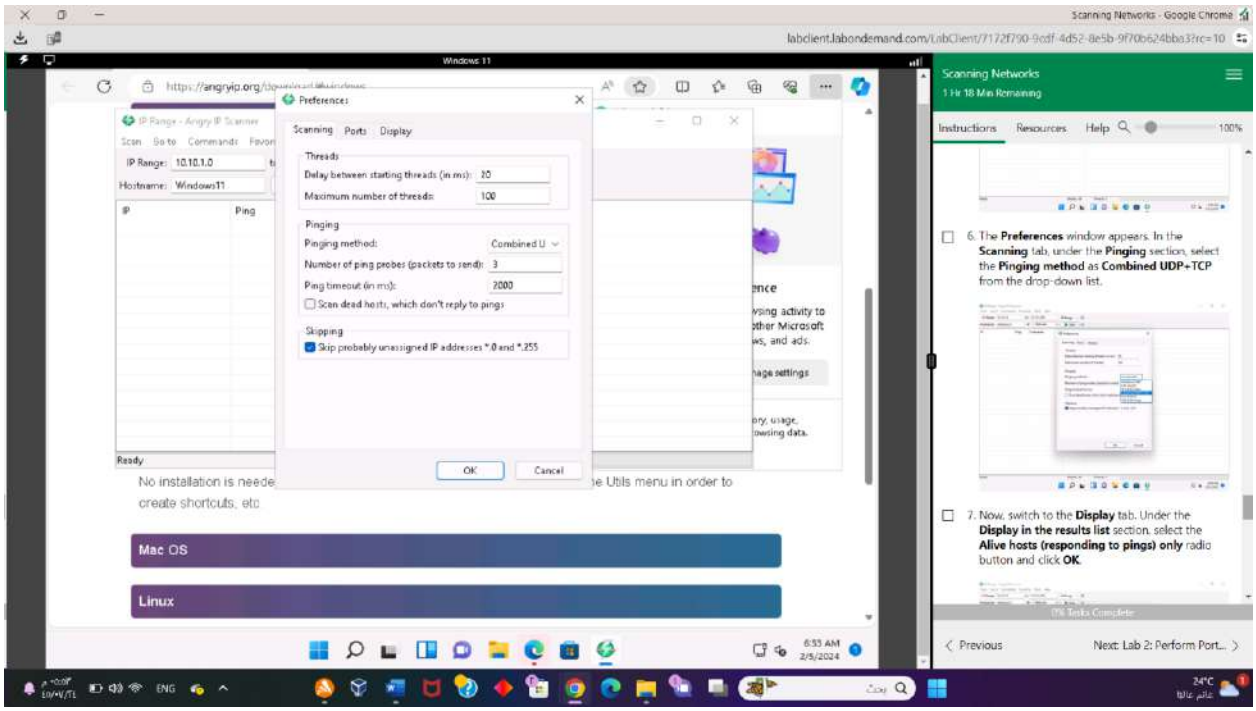


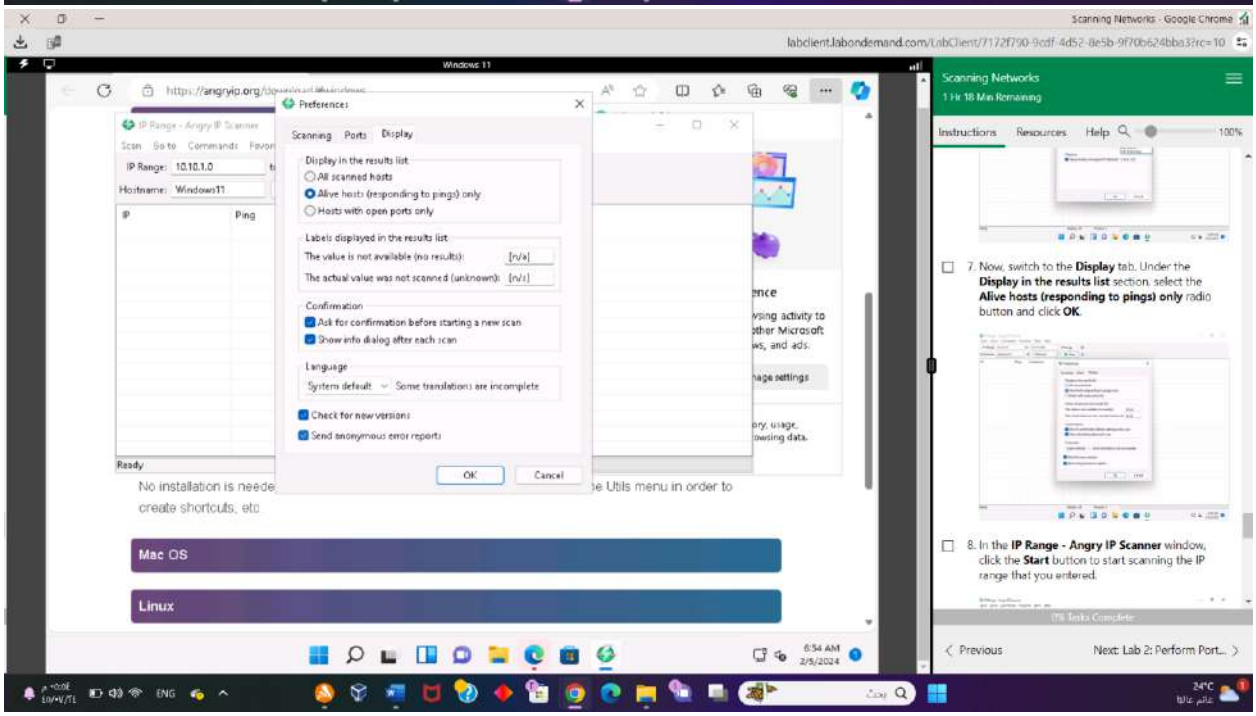

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
angry IP Scanner
All Apps Documents Web More
Best match
Angry IP Scanner
App
Search the web
an - See web results
angry ip scanner
andry ip
Apps
Defragment and Optimize Drives
Windows Fax and Scan
Settings
Create and format hard disk partitions
Angry IP Scanner
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall
Scanning Networks
1 Hr 22 Min Remaining
Instructions Resources Help 100%
Angry IP Scanner
Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins.
Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.
1. Click Windows 11 to switch to the Windows 11 machine.
2. Click Search icon ( ) on the Desktop. Type angry in the search field, the Angry IP Scanner appears in the result, click Open to launch it.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...

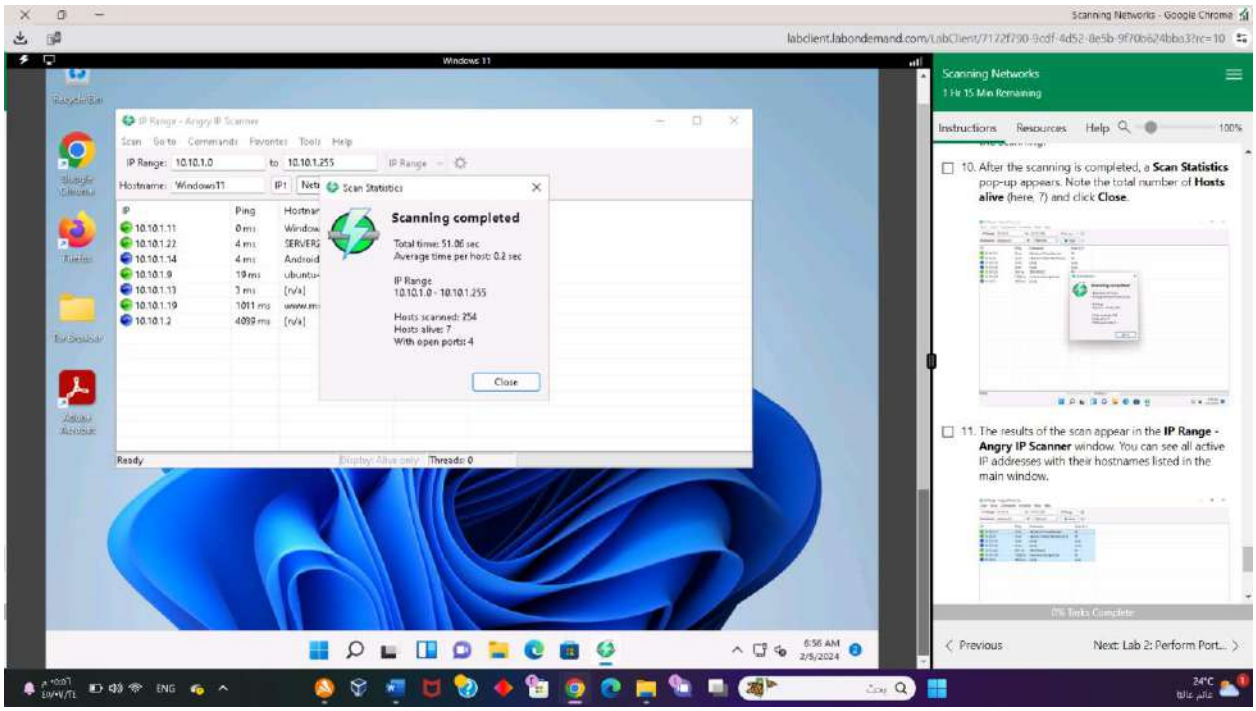

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 10.10.1.0 to 10.10.1.255 IP Range
Hostname:
Getting Started
Angry IP Scanner is an IP address scanner tool.
It is used for scanning of IP addresses with the goal of finding alive hosts and gathering interesting information about each of them.
You can start by specifying the IP addresses to scan (your local IP is entered by default) and clicking the Start button.
Send anonymous error reports
Next
Close
Ready
Display: All
Threads: 0
Scanning Networks
1 Hr 21 Min Remaining
Instructions Resources Help 100%
3. Angry IP Scanner starts, and a Getting Started window pops up. Click Next, follow the wizard, and click Close.
If Open File - Security Warning window appears, click Run.
4. The IP Range - Angry IP Scanner window appears, as shown in the screenshot.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
https://angryip.org/download/#windows
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 10.10.1.0 to 10.10.1.255 IP Range
Hostname: Windows11 IP1 Netmask Start
IP Ping Hostname Ports [3+]
Ready Display: All Threads: 0
No installation is needed. However, you may use the Install program... from the Utils menu in order to create shortcuts, etc
Mac OS
Linux
6:51 AM 2/5/2024
Scanning Networks
1 Hr 21 Min Remaining
Instructions Resources Help 100%
4. The IP Range - Angry IP Scanner window appears, as shown in the screenshot.
5. In the IP Range fields, type the IP range as 10.10.1.0 to 10.10.1.255 and click the Preferences icon beside the IP Range menu, as shown in the screenshot.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
24°C

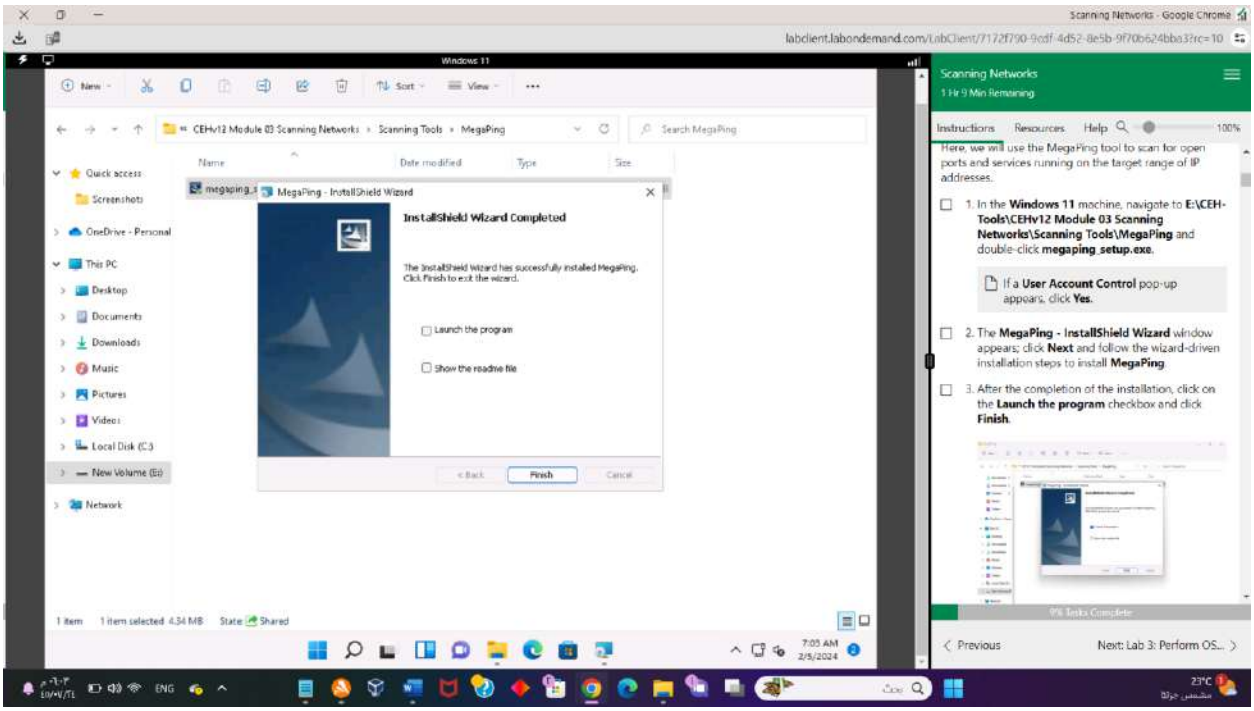

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
https://angryip.org/download/#windows
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 10.10.1.0 to 10.10.1.255 IP Range
Hostname: Windows11 IP1 Netmask Start
IP Ping Hostname Ports [3+]
Ready Display: All Threads: 0
No installation is needed. However, you may use the Install program... from the Utils menu in order to create shortcuts, etc
Mac OS
Linux
6:52 AM 2/5/2024
Scanning Networks
1 Hr 19 Min Remaining
Instructions Resources Help 100%
5. In the IP Range fields, type the IP range as 10.10.1.0 to 10.10.1.255 and click the Preferences icon beside the IP Range menu, as shown in the screenshot.
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...
ENG
24°C

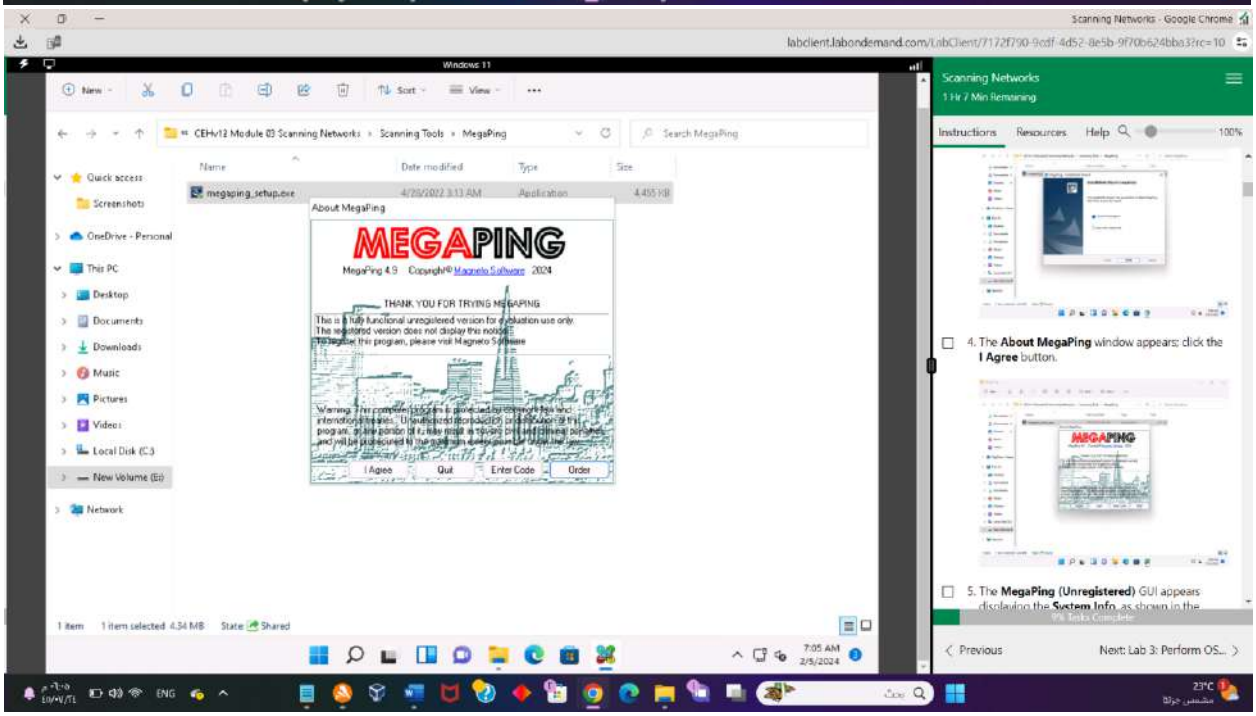

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
6. The Preferences window appears. In the Scanning tab, under the Pinging section, select the Pinging method as Combined UDP+TCP from the drop-down list.
7. Now, switch to the Display tab. Under the Display in the results list section, select the Alive hosts (responding to pings) only radio button and click OK.
Preferences
Scanning
Ports
Display
Threads
Delay between starting threads (in ms):
Maximum number of threads:
Pinging
Pinging method:
Number of ping probes (packets to send):
Ping timeout (in ms):
Scan dead hosts, which don't reply to pings
Skipping
Skip probably unassigned IP addresses *.0 and *.255
OK
Cancel
Mac OS
Linux
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...

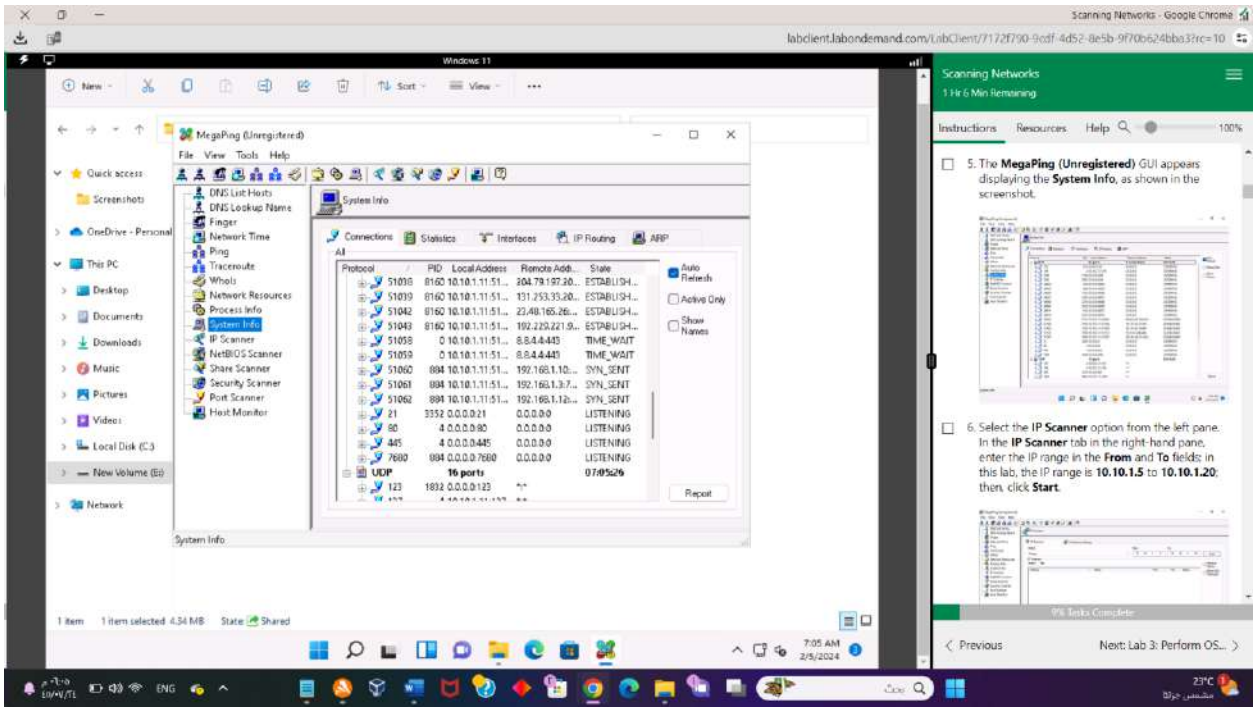

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
7. Now, switch to the Display tab. Under the Display in the results list section, select the Alive hosts (responding to pings) only radio button and click OK.
8. In the IP Range - Angry IP Scanner window, click the Start button to start scanning the IP range that you entered.
Preferences
Scanning
Ports
Display
Display in the results list
All scanned hosts
Alive hosts (responding to pings) only
Hosts with open ports only
Labels displayed in the results list
The value is not available (no results):
The actual value was not scanned (unknown):
Confirmation
Ask for confirmation before starting a new scan
Show info dialog after each scan
Language
System default
Some translations are incomplete
Check for new versions
Send anonymous error reports
OK
Cancel
Mac OS
Linux
0% Tasks Complete
Previous
Next: Lab 2: Perform Port...

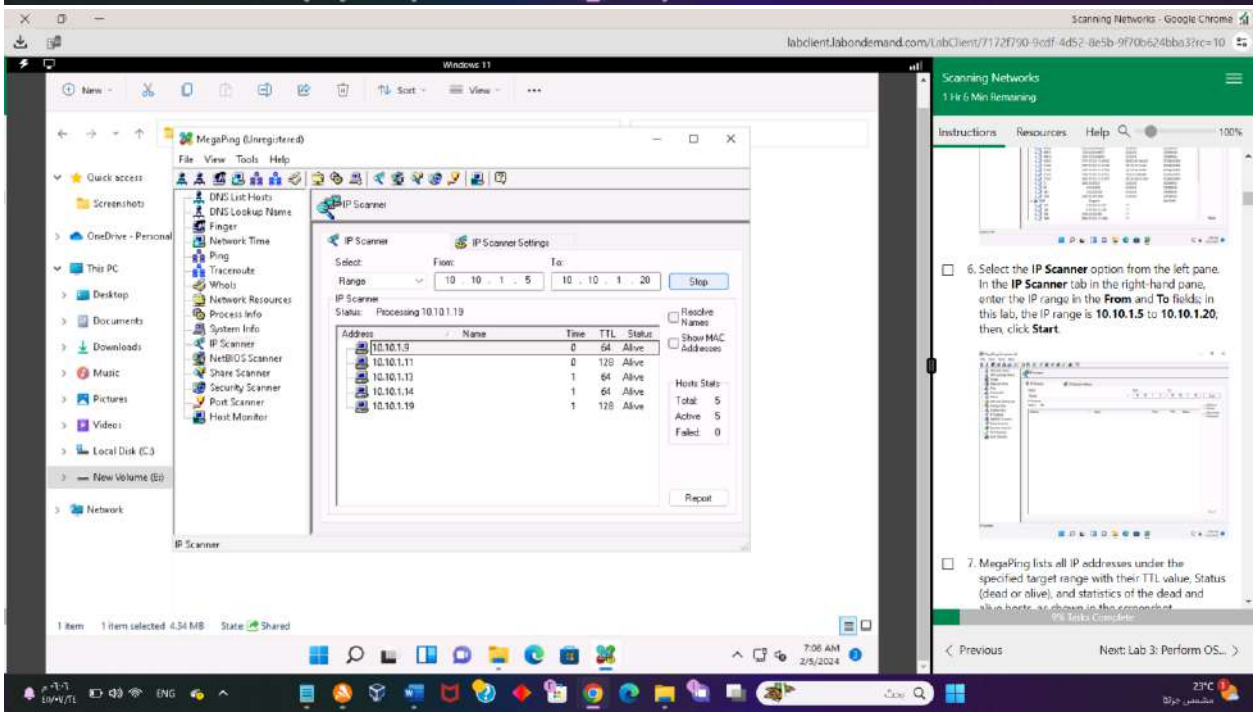


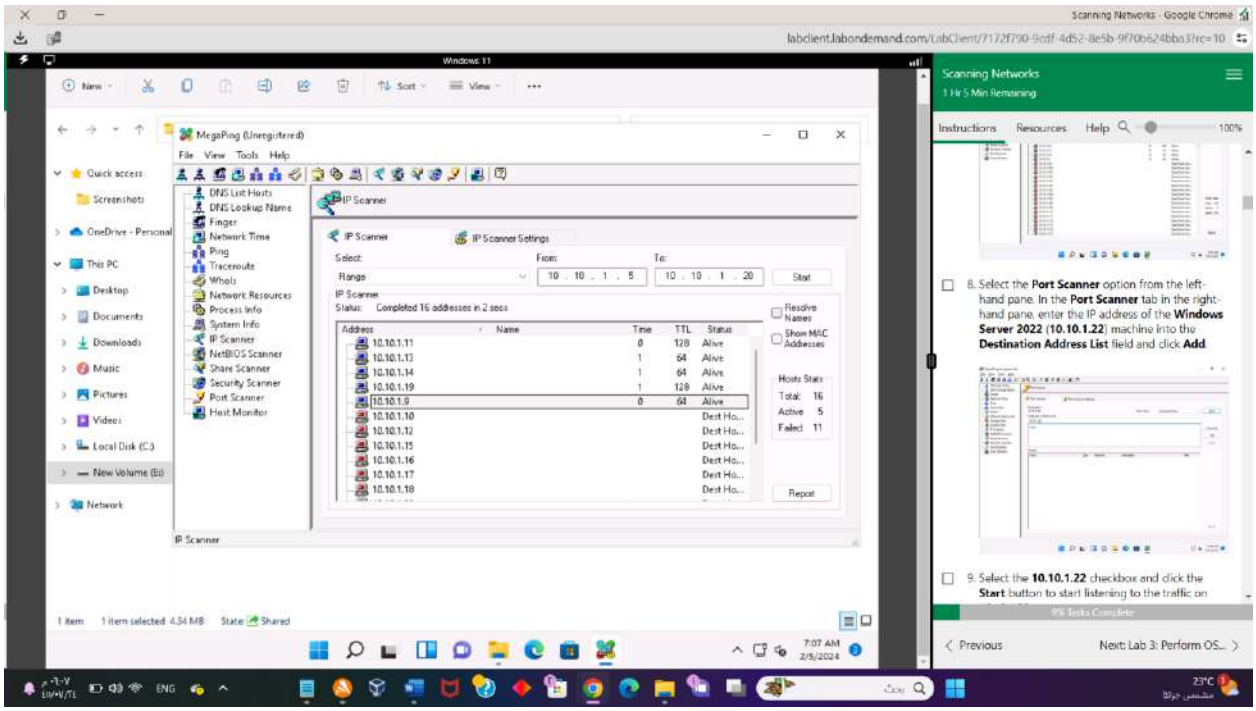
Lab 02 – Task 01

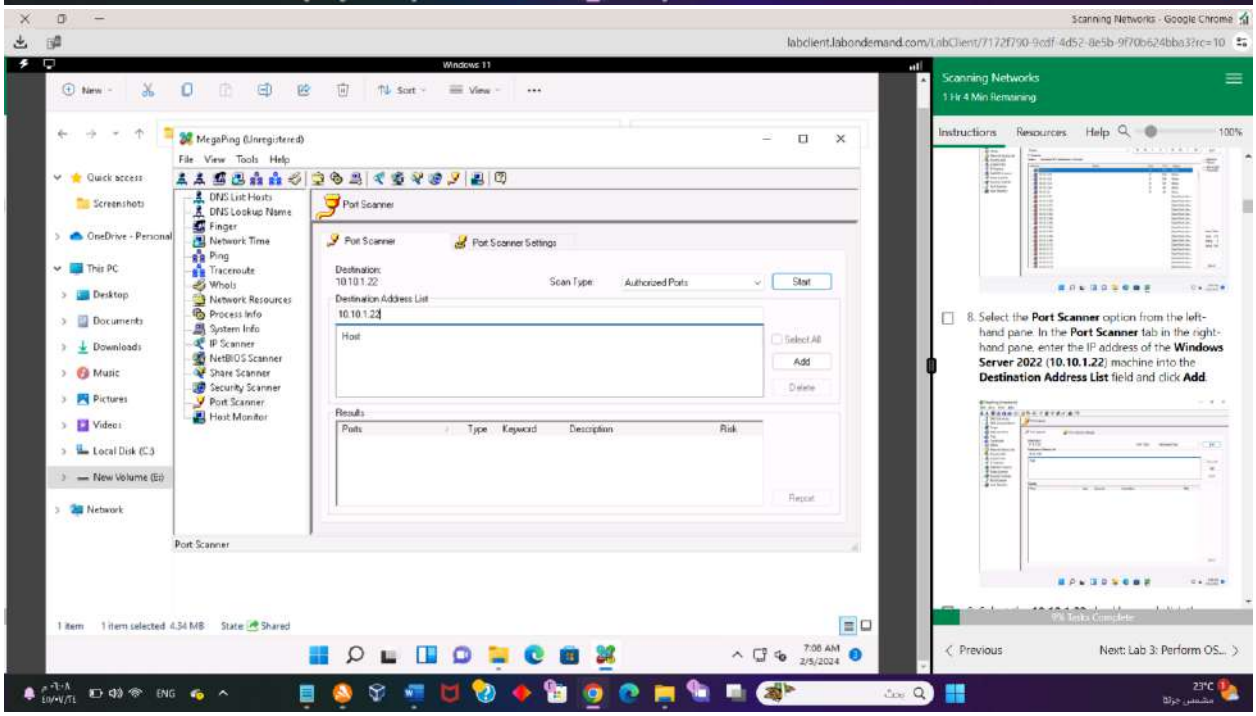

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
CEHv12 Module 03 Scanning Networks › Scanning Tools › MegaPing
MegaPing - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed MegaPing. Click Finish to exit the wizard.
Launch the program
Show the readme file
Finish
Cancel
Scanning Networks
1 Hr 9 Min Remaining
Instructions
Resources
Help
100%
Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.
1. In the Windows 11 machine, navigate to E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\MegaPing and double-click megaping_setup.exe.
If a User Account Control pop-up appears, click Yes.
2. The MegaPing - InstallShield Wizard window appears; click Next and follow the wizard-driven installation steps to install MegaPing.
3. After the completion of the installation, click on the Launch the program checkbox and click Finish.
9% Tasks Complete
Previous
Next: Lab 3: Perform OS...

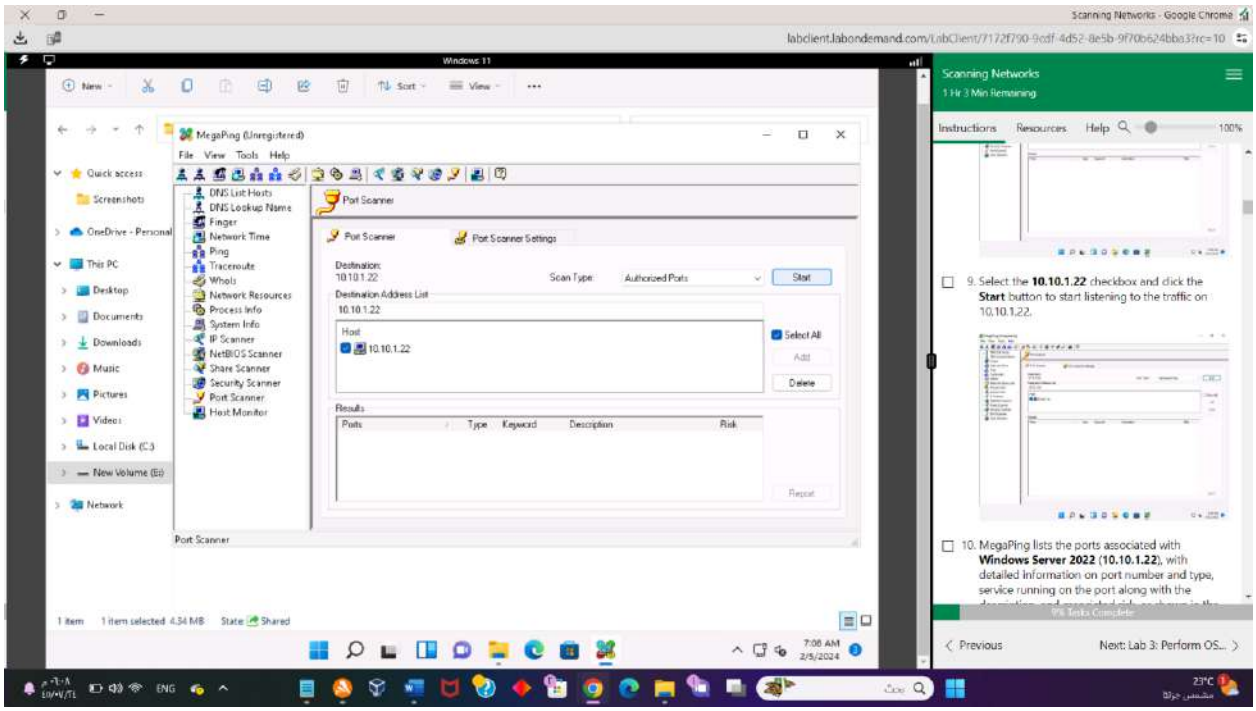

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
CEHv12 Module 03 Scanning Networks › Scanning Tools › MegaPing
megaping_setup.exe
About MegaPing
MEGAPING
MegaPing 4.9 Copyright© Magneto Software 2024
THANK YOU FOR TRYING MEGAPING
This is a fully functional unregistered version for evaluation use only.
The registered version does not display this notice.
To register this program, please visit Magneto Software
I Agree
Quit
Enter Code
Order
Scanning Networks
1 Hr 7 Min Remaining
Instructions
Resources
Help
100%
4. The About MegaPing window appears; click the I Agree button.
5. The MegaPing (Unregistered) GUI appears displaying the System Info, as shown in the
9% Tasks Complete
Previous
Next: Lab 3: Perform OS...

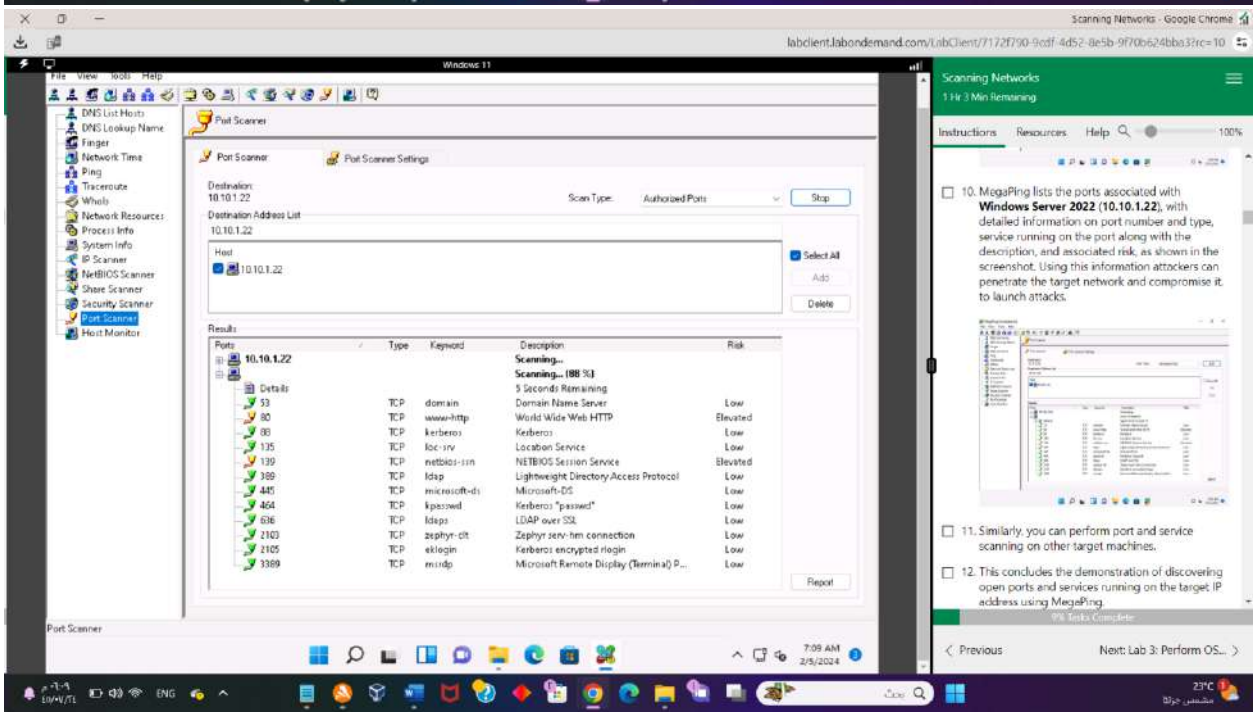

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
Whois
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
Connections
Statistics
Interfaces
IP Routing
ARP
Auto Refresh
Active Only
Show Names
Report
Scanning Networks
1 Hr 6 Min Remaining
Instructions
Resources
Help
100%
5. The MegaPing (Unregistered) GUI appears displaying the System Info, as shown in the screenshot.
6. Select the IP Scanner option from the left pane. In the IP Scanner tab in the right-hand pane, enter the IP range in the From and To fields; in this lab, the IP range is 10.10.1.5 to 10.10.1.20; then, click Start.
9% Tasks Complete
Previous
Next: Lab 3: Perform OS...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
MegaPing (Unregistered)
File View Tools Help
IP Scanner
IP Scanner Settings
Select:
From:
To:
Range
10 . 10 . 1 . 5
10 . 10 . 1 . 20
Stop
IP Scanner
Status: Processing 10.10.1.19
Address
Name
Time
TTL
Status
10.10.1.9 0 64 Alive
10.10.1.11 0 128 Alive
10.10.1.13 1 64 Alive
10.10.1.14 1 64 Alive
10.10.1.19 1 128 Alive
Resolve Names
Show MAC Addresses
Hosts Stats
Total: 5
Active: 5
Failed: 0
Report
Scanning Networks
1 Hr 6 Min Remaining
Instructions
Resources
Help
100%
6. Select the IP Scanner option from the left pane. In the IP Scanner tab in the right-hand pane, enter the IP range in the From and To fields; in this lab, the IP range is 10.10.1.5 to 10.10.1.20; then, click Start.
7. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and
Previous
Next: Lab 3: Perform OS...

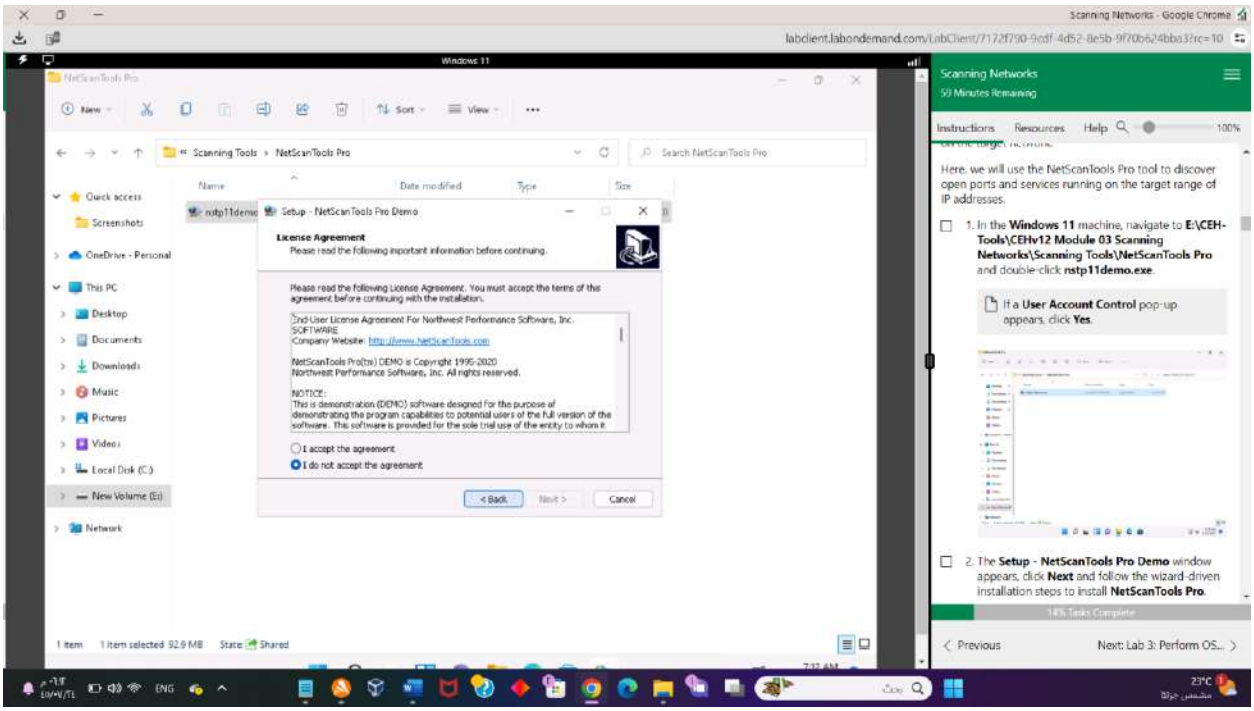

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
MegaPing (Unregistered)
File View Tools Help
IP Scanner
IP Scanner Settings
Select: Range
From: 10 . 10 . 1 . 5
To: 10 . 10 . 1 . 20
Start
Status: Completed 16 addresses in 2 secs
Resolve Names
Show MAC Addresses
Address Name Time TTL Status
10.10.1.11 0 128 Alive
10.10.1.13 1 64 Alive
10.10.1.14 1 64 Alive
10.10.1.19 1 128 Alive
10.10.1.9 0 64 Alive
Hosts Stats
Total: 16
Active: 5
Failed: 11
Report
Scanning Networks
1 Hr 5 Min Remaining
Instructions Resources Help 100%
8. Select the Port Scanner option from the left-hand pane. In the Port Scanner tab in the right-hand pane, enter the IP address of the Windows Server 2022 (10.10.1.22) machine into the Destination Address List field and click Add.
9. Select the 10.10.1.22 checkbox and click the Start button to start listening to the traffic on
Previous
Next: Lab 3: Perform OS...

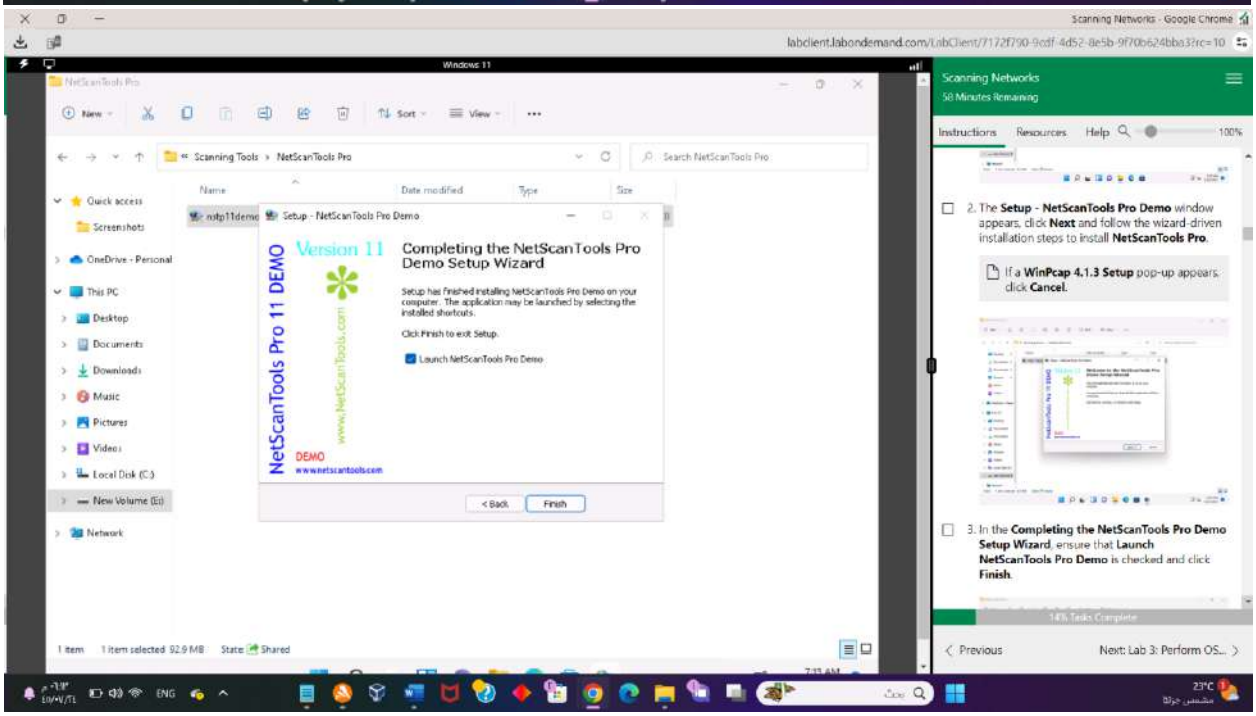

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
MegaPing (Unregistered)
File View Tools Help
Port Scanner
Port Scanner Settings
Destination: 10.10.1.22
Scan Type: Authorized Ports
Start
Destination Address List
10.10.1.22
Host
Select All
Add
Delete
Results
Ports Type Keyword Description Risk
Report
Scanning Networks
1 Hr 4 Min Remaining
Instructions Resources Help 100%
8. Select the Port Scanner option from the left-hand pane. In the Port Scanner tab in the right-hand pane, enter the IP address of the Windows Server 2022 (10.10.1.22) machine into the Destination Address List field and click Add.
Previous
Next: Lab 3: Perform OS...

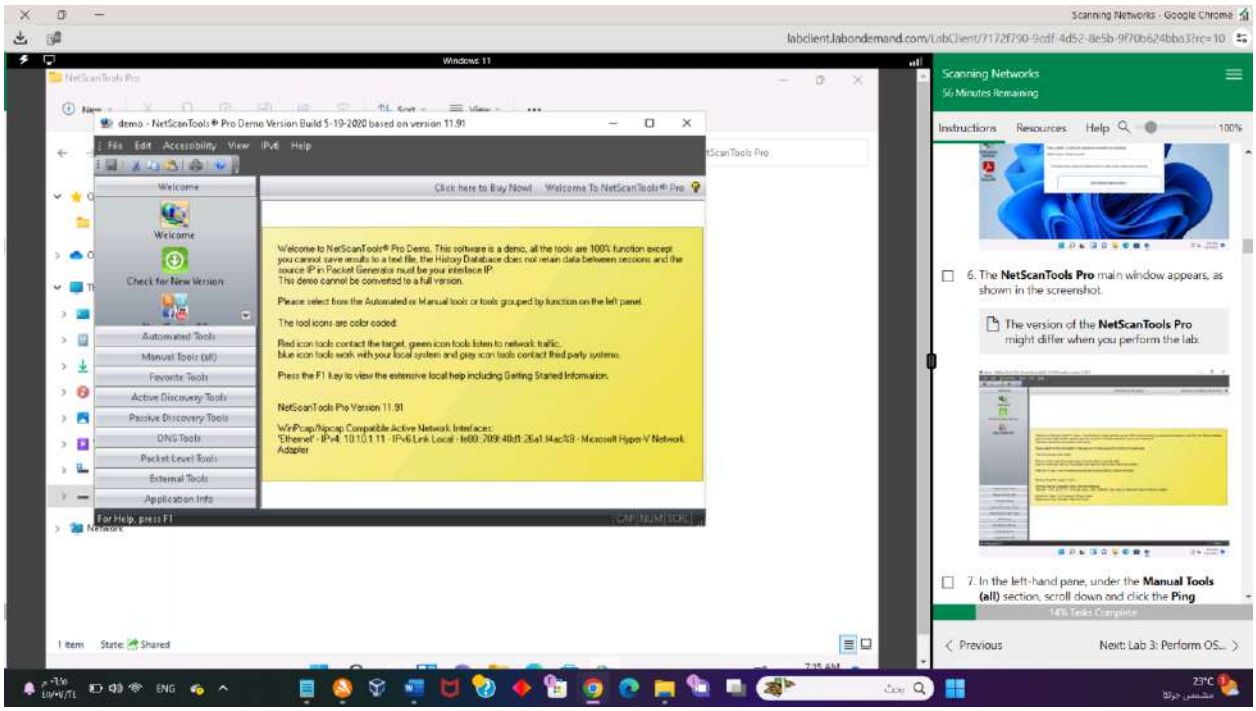


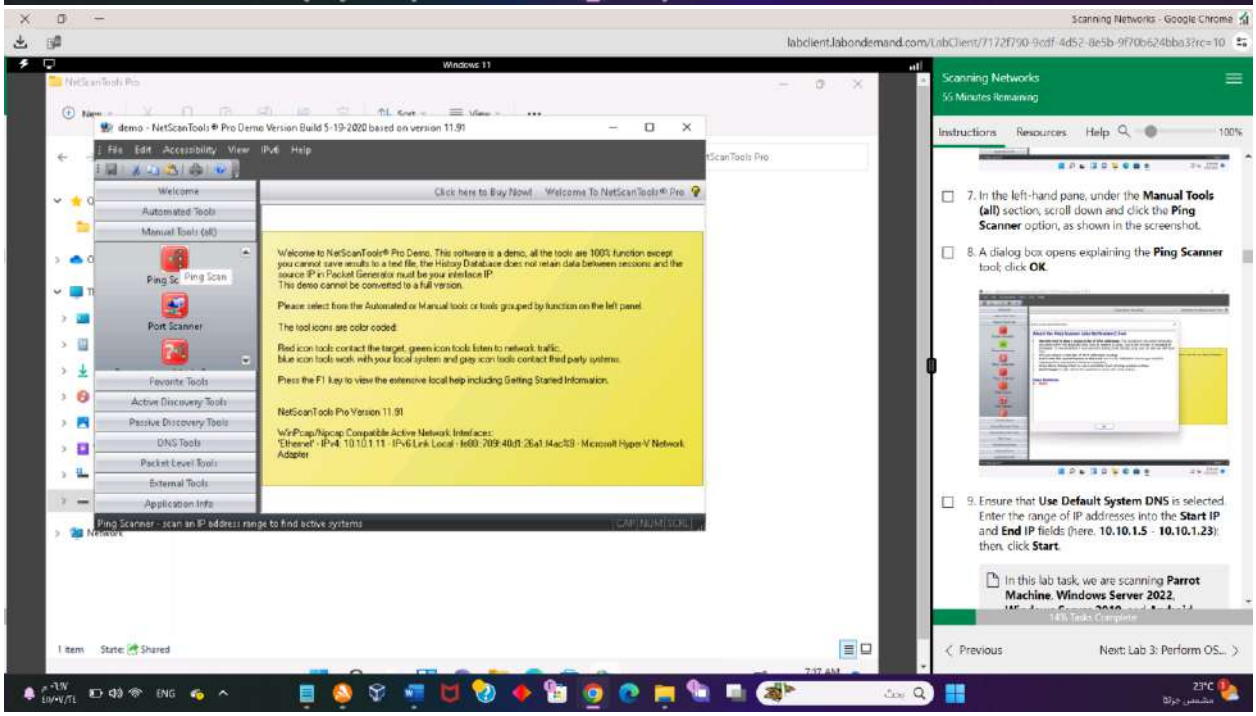


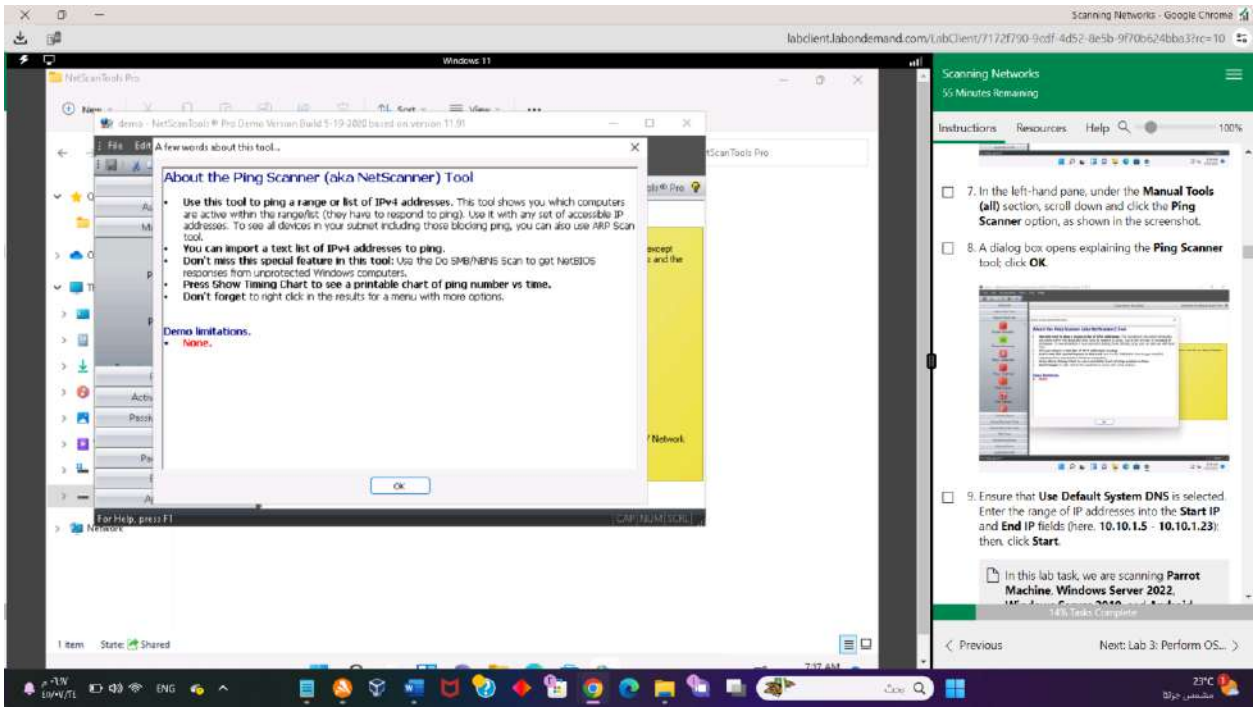
Lab 02 – Task 02

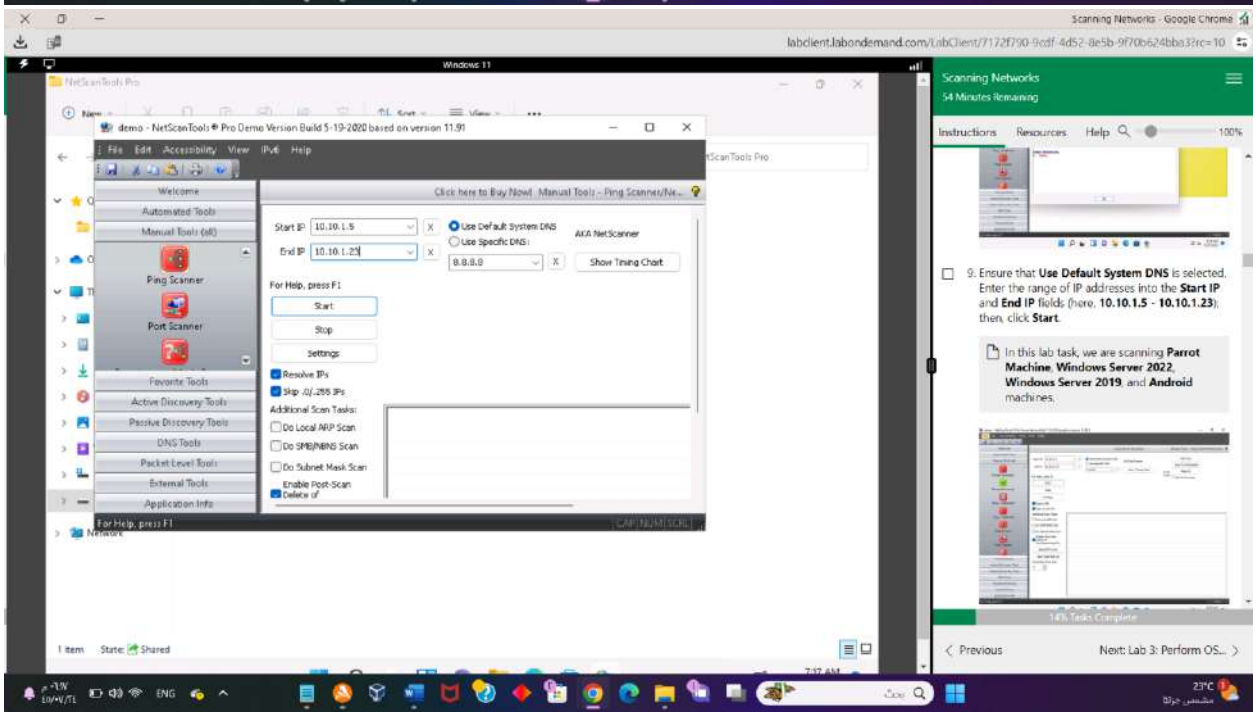

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
59 Minutes Remaining
Instructions
Resources
Help
100%
Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.
1. In the Windows 11 machine, navigate to E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro and double-click nstp11demo.exe.
If a User Account Control pop-up appears, click Yes.
2. The Setup - NetScanTools Pro Demo window appears, click Next and follow the wizard-driven installation steps to install NetScanTools Pro.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
Setup - NetScanTools Pro Demo
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel
1 item
1 item selected 92.9 MB
State: Shared

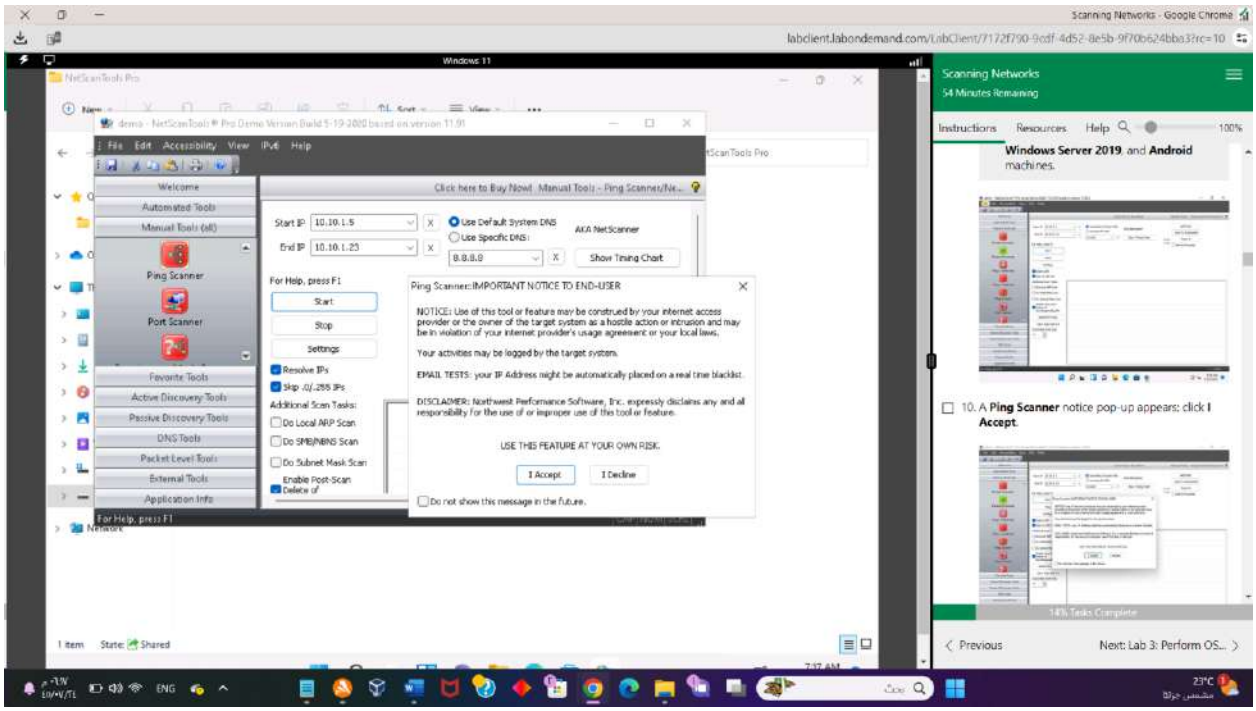

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
58 Minutes Remaining
Instructions
Resources
Help
100%
2. The Setup - NetScanTools Pro Demo window appears, click Next and follow the wizard-driven installation steps to install NetScanTools Pro.
If a WinPcap 4.1.3 Setup pop-up appears, click Cancel.
3. In the Completing the NetScanTools Pro Demo Setup Wizard, ensure that Launch NetScanTools Pro Demo is checked and click Finish.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
Setup - NetScanTools Pro Demo
Version 11
Completing the NetScanTools Pro Demo Setup Wizard
Setup has finished installing NetScanTools Pro Demo on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch NetScanTools Pro Demo
NetScanTools Pro 11 DEMO
www.NetScanTools.com
DEMO
www.netscantools.com
< Back
Finish
1 item
1 item selected 92.9 MB
State: Shared

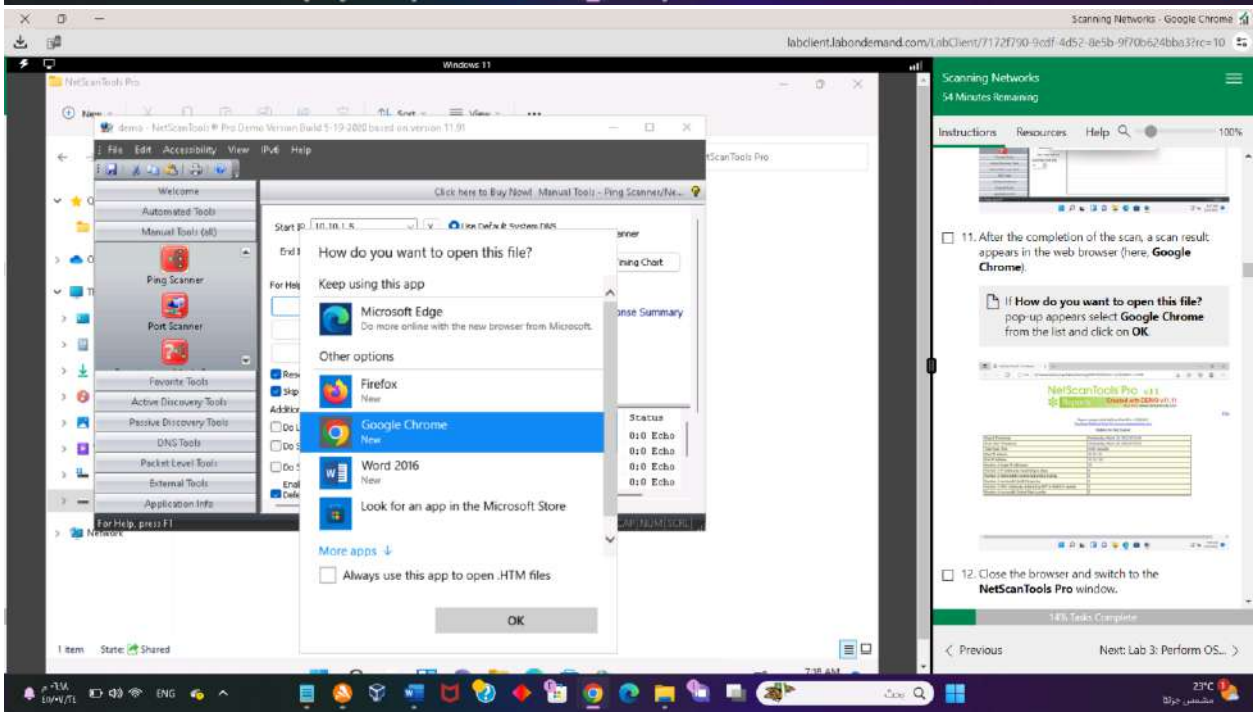

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Click here to Buy Now! Welcome To NetScanTools® Pro
Welcome
Check for New Version
Automated Tools
Manual Tools (all)
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not retain data between sessions and the source IP in Packet Generator must be your interface IP.
This demo cannot be converted to a full version.
Please select from the Automated or Manual tools or tools grouped by function on the left panel.
The tool icons are color coded:
Red icon tools contact the target, green icon tools listen to network traffic.
blue icon tools work with your local system and gray icon tools contact third party systems.
Press the F1 key to view the extensive local help including Getting Started Information.
NetScanTools Pro Version 11.91
WinPcap/Nipcap Compatible Active Network Interfaces:
'Ethernet' - IPv4: 10.10.1.11 - IPv6 Link Local - fe80::709:40d1:26a1:f4ac%9 - Microsoft Hyper-V Network Adapter
For Help, press F1
1 item State: Shared
Scanning Networks
56 Minutes Remaining
Instructions Resources Help 100%
6. The NetScanTools Pro main window appears, as shown in the screenshot.
The version of the NetScanTools Pro might differ when you perform the lab.
7. In the left-hand pane, under the Manual Tools (all) section, scroll down and click the Ping
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...

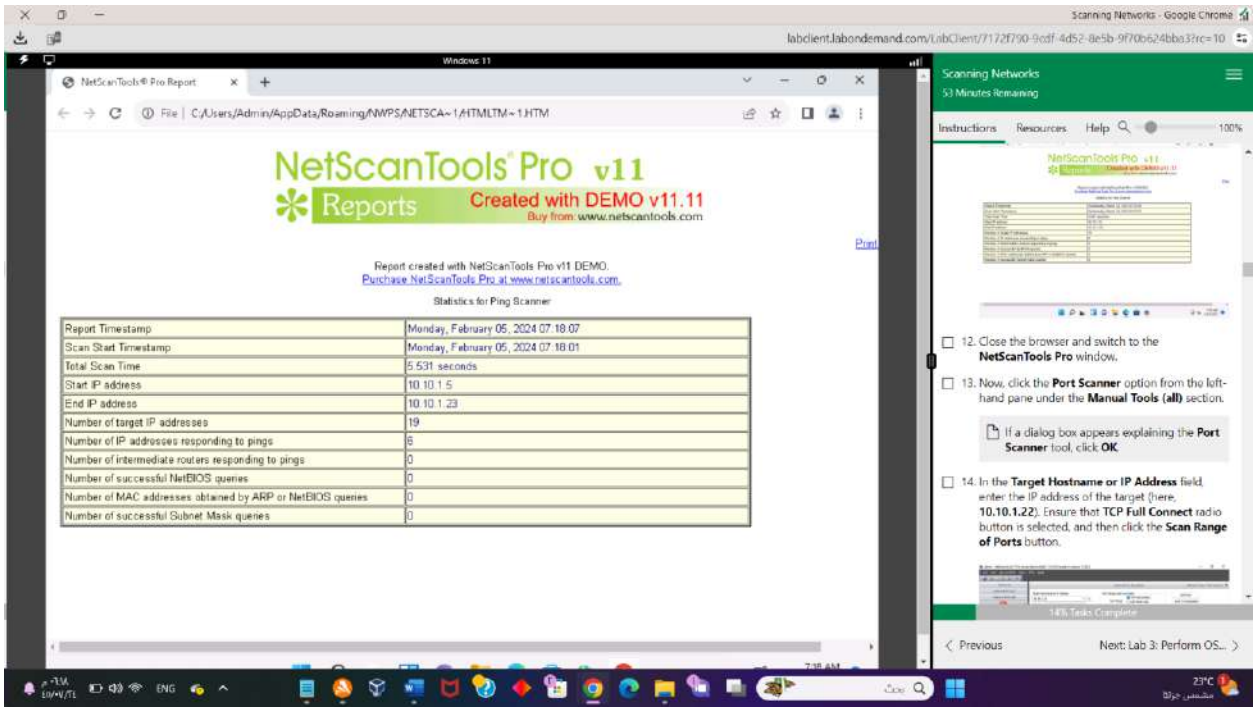

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Ping Scan
Port Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not retain data between sessions and the source IP in Packet Generator must be your interface IP.
This demo cannot be converted to a full version.
Please select from the Automated or Manual tools or tools grouped by function on the left panel.
The tool icons are color coded:
Red icon tools contact the target, green icon tools listen to network traffic.
blue icon tools work with your local system and gray icon tools contact third party systems.
Press the F1 key to view the extensive local help including Getting Started Information.
NetScanTools Pro Version 11.91
WinPcap/Nipcap Compatible Active Network Interfaces:
'Ethernet' - IPv4: 10.10.1.11 - IPv6 Link Local - fe80::709:40d1:26a1:f4ac%9 - Microsoft Hyper-V Network Adapter
Ping Scanner - scan an IP address range to find active systems
1 item State: Shared
Scanning Networks
55 Minutes Remaining
Instructions Resources Help 100%
7. In the left-hand pane, under the Manual Tools (all) section, scroll down and click the Ping Scanner option, as shown in the screenshot.
8. A dialog box opens explaining the Ping Scanner tool; click OK.
9. Ensure that Use Default System DNS is selected. Enter the range of IP addresses into the Start IP and End IP fields (here, 10.10.1.5 - 10.10.1.23); then, click Start.
In this lab task, we are scanning Parrot Machine, Windows Server 2022,
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...

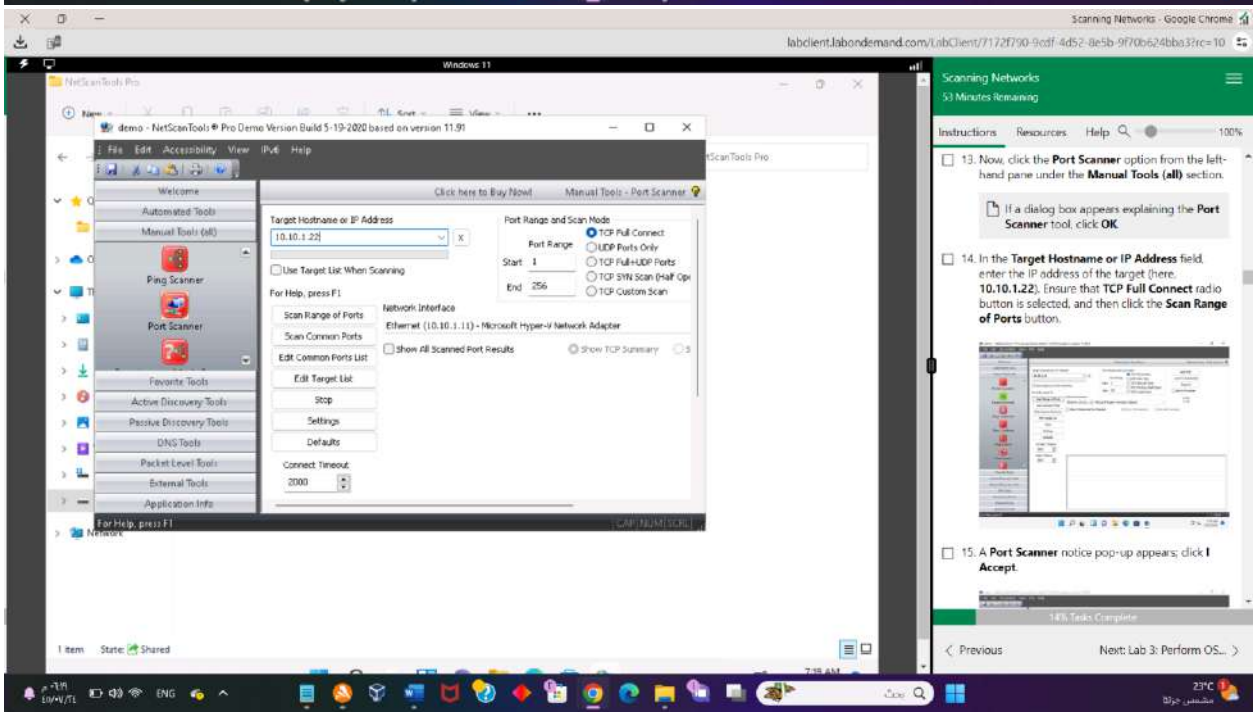

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
55 Minutes Remaining
Instructions
Resources
Help
100%
About the Ping Scanner (aka NetScanner) Tool
Use this tool to ping a range or list of IPv4 addresses. This tool shows you which computers are active within this range/list (they have to respond to ping). Use it with any set of accessible IP addresses. To see all devices in your subnet including those blocking ping, you can also use ARP Scan tool.
You can import a text list of IPv4 addresses to ping.
Don't miss this special feature in this tool: Use the Do SMB/NBNS Scan to get NetBIOS responses from unprotected Windows computers.
Press Show Timing Chart to see a printable chart of ping number vs time.
Don't forget to right click in the results for a menu with more options.
Demo limitations.
None.
Ok
7. In the left-hand pane, under the Manual Tools (all) section, scroll down and click the Ping Scanner option, as shown in the screenshot.
8. A dialog box opens explaining the Ping Scanner tool; click OK.
9. Ensure that Use Default System DNS is selected. Enter the range of IP addresses into the Start IP and End IP fields (here, 10.10.1.5 - 10.10.1.23); then, click Start.
In this lab task, we are scanning Parrot Machine, Windows Server 2022,
Previous
Next: Lab 3: Perform OS...

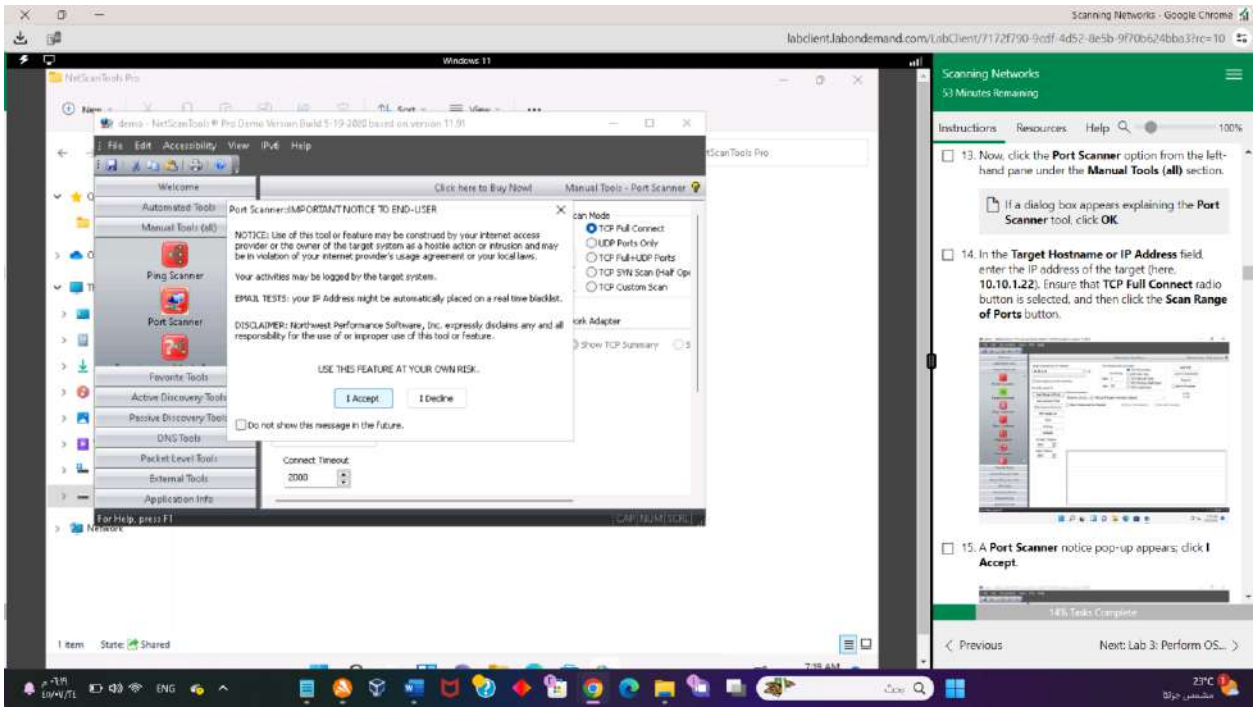

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
54 Minutes Remaining
Instructions
Resources
Help
100%
demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
Start IP: 10.10.1.5
End IP: 10.10.1.23
Use Default System DNS
Use Specific DNS:
8.8.8.8
AKA NetScanner
Show Timing Chart
Ping Scanner
Port Scanner
Start
Stop
Settings
Resolve IPs
Do Local ARP Scan
Do SMB/NBNS Scan
Do Subnet Mask Scan
9. Ensure that Use Default System DNS is selected. Enter the range of IP addresses into the Start IP and End IP fields (here, 10.10.1.5 - 10.10.1.23); then, click Start.
In this lab task, we are scanning Parrot Machine, Windows Server 2022, Windows Server 2019, and Android machines.
Previous
Next: Lab 3: Perform OS...

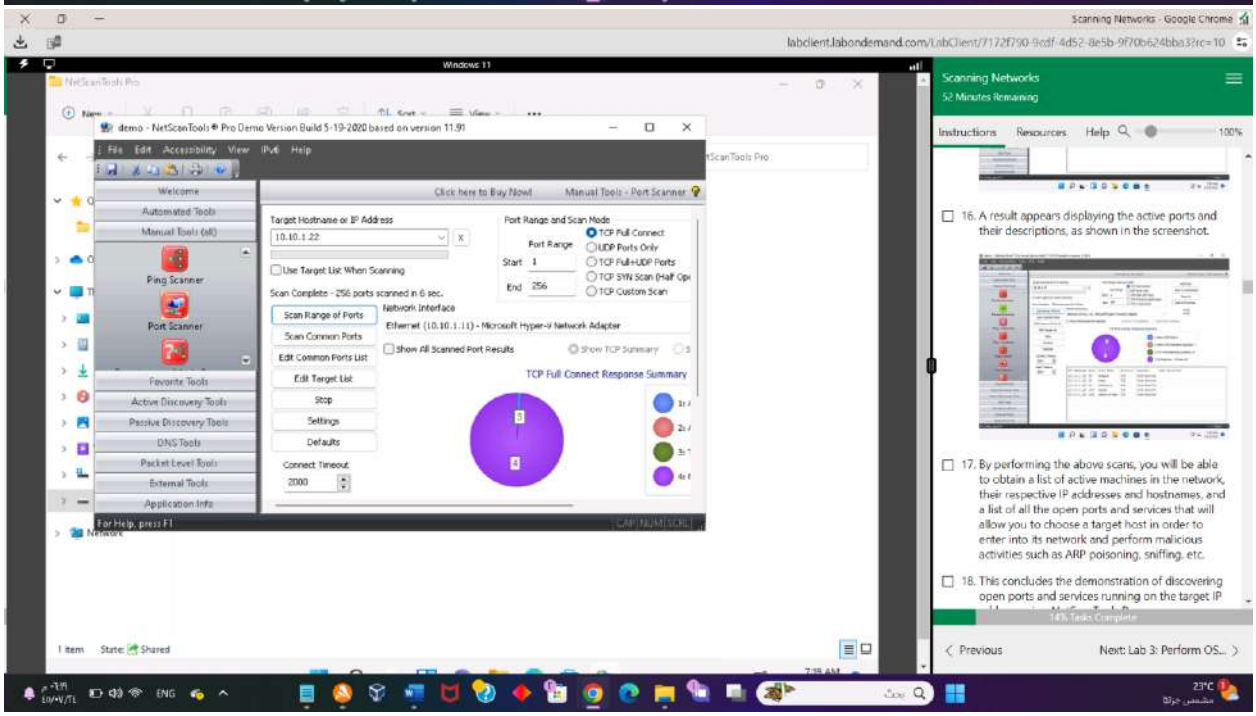

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
54 Minutes Remaining
Instructions
Resources
Help
100%
Windows Server 2019, and Android machines.
10. A Ping Scanner notice pop-up appears; click I Accept.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
Ping Scanner::IMPORTANT NOTICE TO END-USER
NOTICE: Use of this tool or feature may be construed by your internet access provider or the owner of the target system as a hostile action or intrusion and may be in violation of your internet provider's usage agreement or your local laws.
Your activities may be logged by the target system.
EMAIL TESTS: your IP Address might be automatically placed on a real time blacklist.
DISCLAIMER: Northwest Performance Software, Inc., expressly disclaims any and all responsibility for the use of or improper use of this tool or feature.
USE THIS FEATURE AT YOUR OWN RISK.
I Accept
I Decline
Do not show this message in the future.


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
54 Minutes Remaining
Instructions
Resources
Help
100%
How do you want to open this file?
Keep using this app
Microsoft Edge
Do more online with the new browser from Microsoft.
Other options
Firefox
New
Google Chrome
New
Word 2016
New
Look for an app in the Microsoft Store
More apps
Always use this app to open .HTM files
OK
11. After the completion of the scan, a scan result appears in the web browser (here, Google Chrome).
If How do you want to open this file? pop-up appears select Google Chrome from the list and click on OK.
12. Close the browser and switch to the NetScanTools Pro window.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...

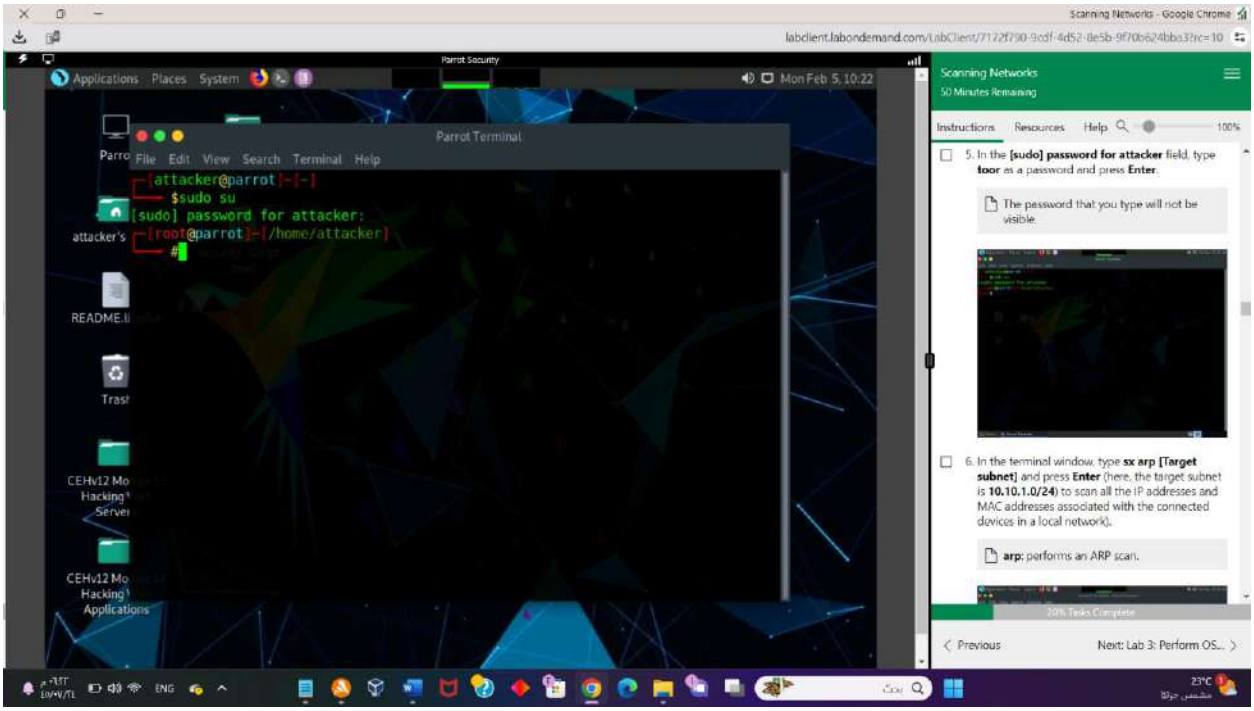

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
NetScanTools® Pro Report
File | C:/Users/Admin/AppData/Roaming/NWPS/NETSCA~1/HTMLTM~1.HTM
NetScanTools® Pro v11
Reports
Created with DEMO v11.11
Buy from: www.netscantools.com
Print
Report created with NetScanTools Pro v11 DEMO.
Purchase NetScanTools Pro at www.netscantools.com.
Statistics for Ping Scanner
Report Timestamp | Monday, February 05, 2024 07:18:07
Scan Start Timestamp | Monday, February 05, 2024 07:18:01
Total Scan Time | 5.531 seconds
Start IP address | 10.10.1.5
End IP address | 10.10.1.23
Number of target IP addresses | 19
Number of IP addresses responding to pings | 6
Number of intermediate routers responding to pings | 0
Number of successful NetBIOS queries | 0
Number of MAC addresses obtained by ARP or NetBIOS queries | 0
Number of successful Subnet Mask queries | 0
Scanning Networks
53 Minutes Remaining
Instructions
Resources
Help
100%
12. Close the browser and switch to the NetScanTools Pro window.
13. Now, click the Port Scanner option from the left-hand pane under the Manual Tools (all) section.
If a dialog box appears explaining the Port Scanner tool, click OK.
14. In the Target Hostname or IP Address field, enter the IP address of the target (here, 10.10.1.22). Ensure that TCP Full Connect radio button is selected, and then click the Scan Range of Ports button.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
23°C

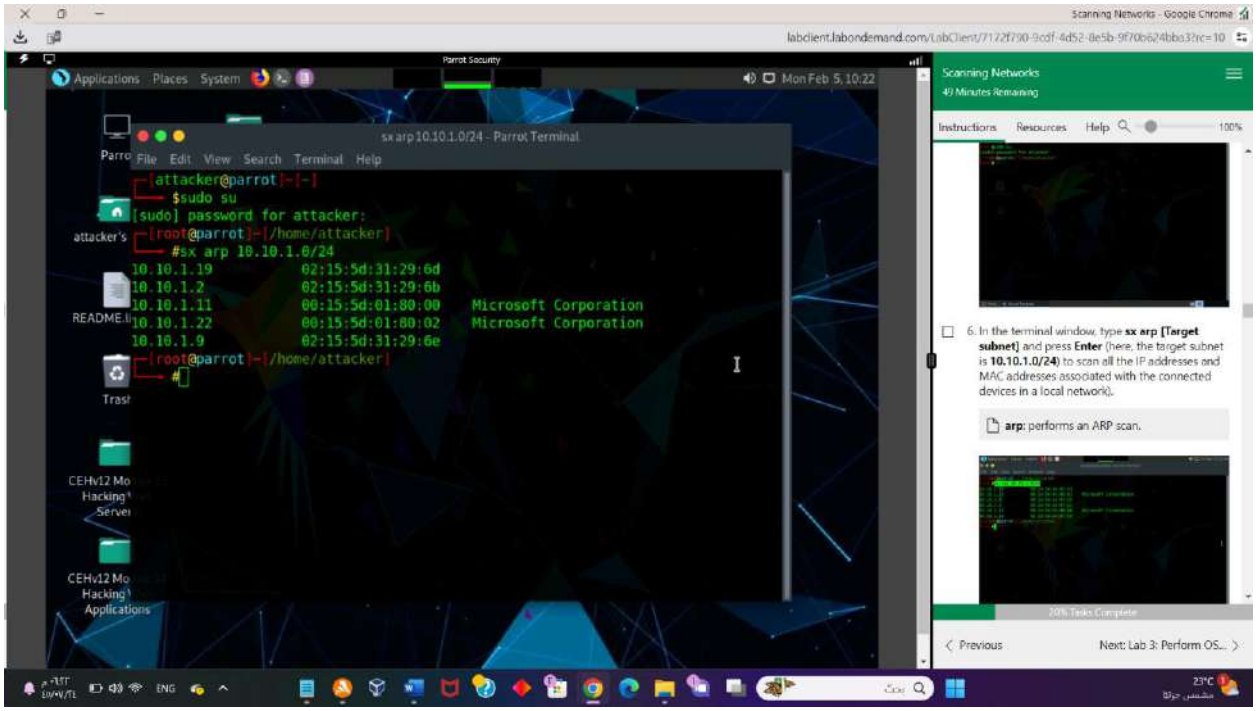

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Ping Scanner
Port Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - Port Scanner
Target Hostname or IP Address
10.10.1.22
Use Target List When Scanning
For Help, press F1
Port Range and Scan Mode
TCP Full Connect
UDP Ports Only
TCP Full+UDP Ports
TCP SYN Scan (Half Ope
TCP Custom Scan
Port Range
Start 1
End 256
Network Interface
Ethernet (10.10.1.11) - Microsoft Hyper-V Network Adapter
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Connect Timeout
2000
Show All Scanned Port Results
Show TCP Summary
For Help, press F1
1 item State: Shared
Scanning Networks
53 Minutes Remaining
Instructions
Resources
Help
100%
13. Now, click the Port Scanner option from the left-hand pane under the Manual Tools (all) section.
If a dialog box appears explaining the Port Scanner tool, click OK.
14. In the Target Hostname or IP Address field, enter the IP address of the target (here, 10.10.1.22). Ensure that TCP Full Connect radio button is selected, and then click the Scan Range of Ports button.
15. A Port Scanner notice pop-up appears; click I Accept.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
23°C

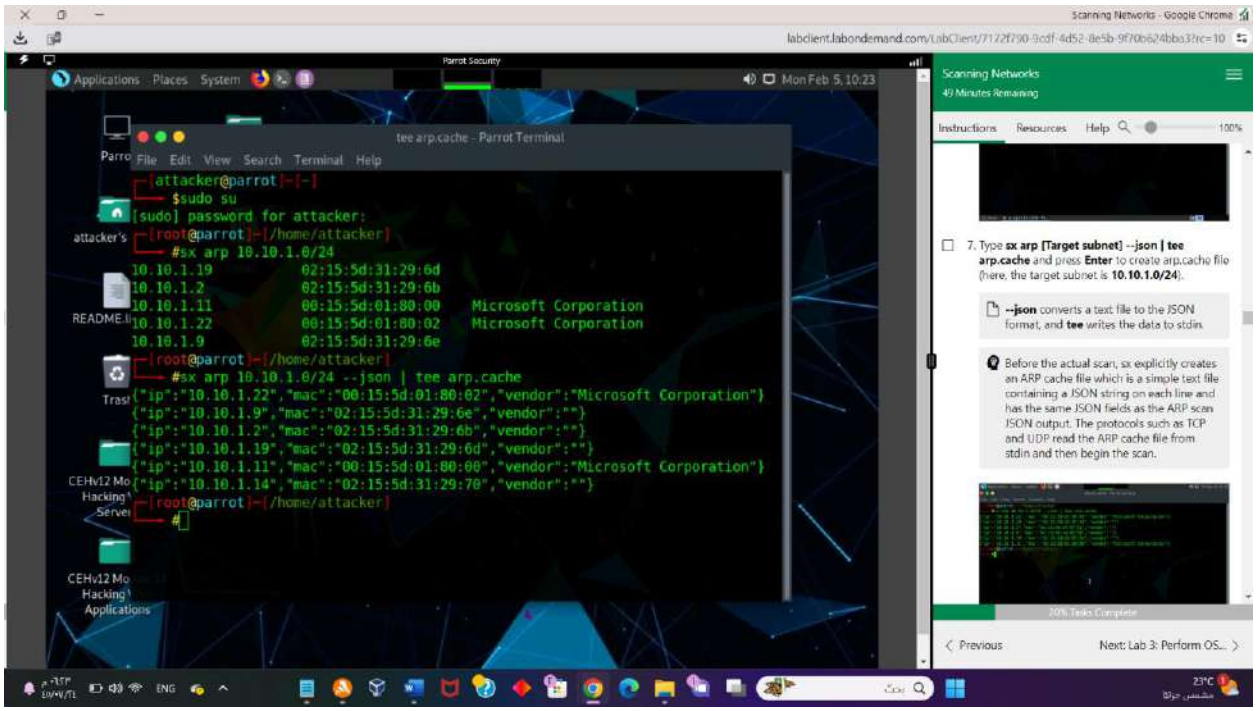

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
53 Minutes Remaining
Instructions
Resources
Help
100%
13. Now, click the Port Scanner option from the left-hand pane under the Manual Tools (all) section.
If a dialog box appears explaining the Port Scanner tool, click OK.
14. In the Target Hostname or IP Address field, enter the IP address of the target (here, 10.10.1.22). Ensure that TCP Full Connect radio button is selected, and then click the Scan Range of Ports button.
15. A Port Scanner notice pop-up appears; click I Accept.
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
Port Scanner:IMPORTANT NOTICE TO END-USER
NOTICE: Use of this tool or feature may be construed by your internet access provider or the owner of the target system as a hostile action or intrusion and may be in violation of your internet provider's usage agreement or your local laws.
Your activities may be logged by the target system.
EMAIL TESTS: your IP address might be automatically placed on a real time blacklist.
DISCLAIMER: Northwest Performance Software, Inc. expressly disclaims any and all responsibility for the use of or improper use of this tool or feature.
USE THIS FEATURE AT YOUR OWN RISK.
I Accept
I Decline
Do not show this message in the future.

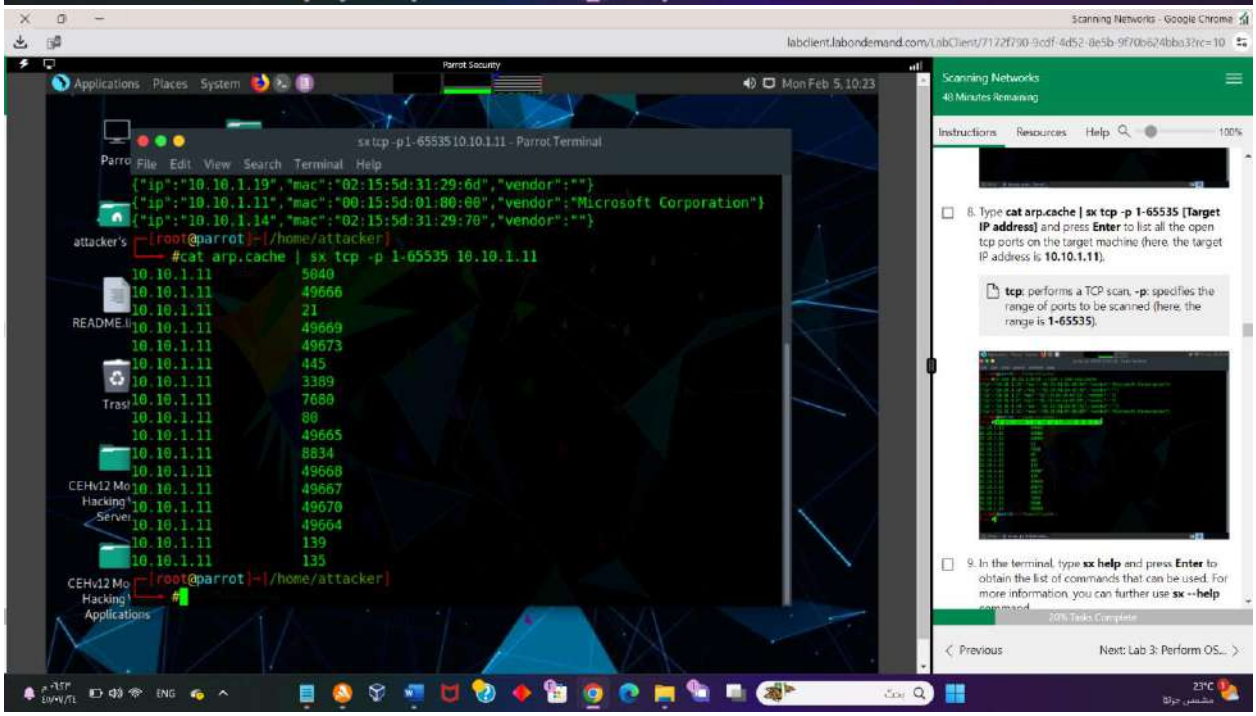

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Scanning Networks
52 Minutes Remaining
Instructions
Resources
Help
100%
16. A result appears displaying the active ports and their descriptions, as shown in the screenshot.
17. By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.
18. This concludes the demonstration of discovering open ports and services running on the target IP
14% Tasks Complete
Previous
Next: Lab 3: Perform OS...
Target Hostname or IP Address
10.10.1.22
Port Range and Scan Mode
Port Range
Start 1
End 256
TCP Full Connect
UDP Ports Only
TCP Full+UDP Ports
TCP SYN Scan (Half Ope
TCP Custom Scan
Use Target List When Scanning
Scan Complete - 256 ports scanned in 6 sec.
Network Interface
Ethernet (10.10.1.11) - Microsoft Hyper-V Network Adapter
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Show All Scanned Port Results
Show TCP Summary
TCP Full Connect Response Summary
Connect Timeout
2000

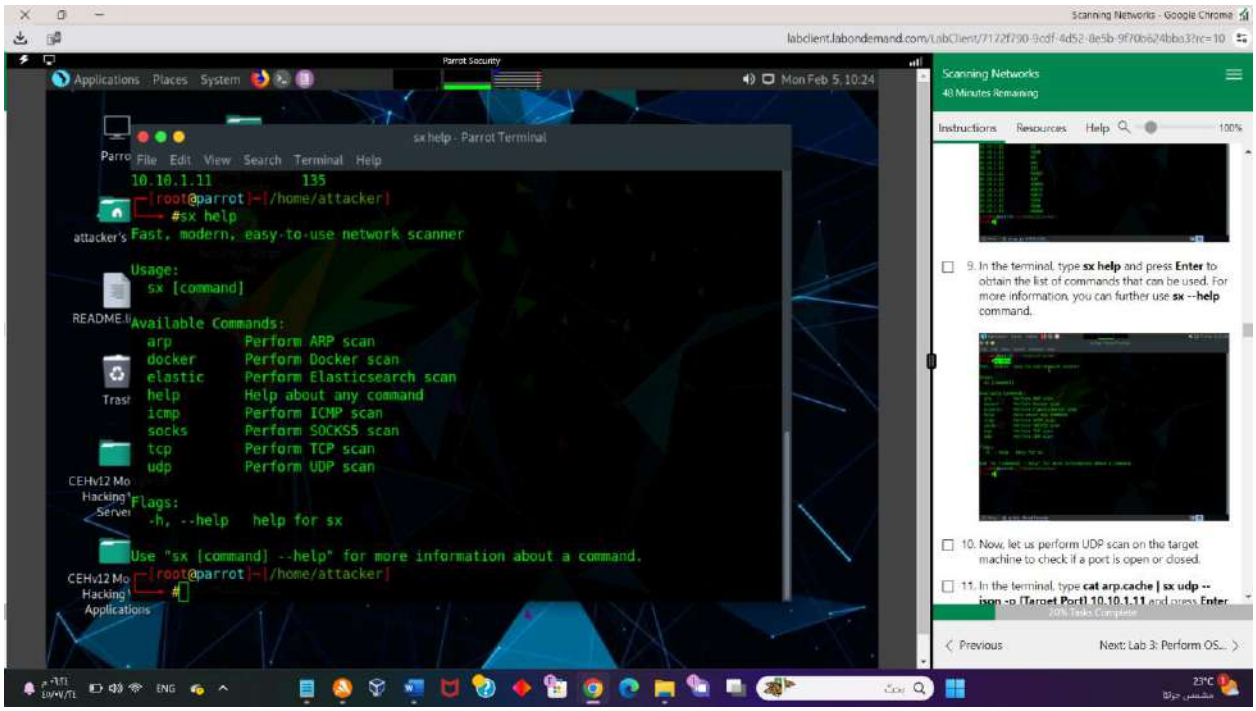
Lab 02 – Task 03

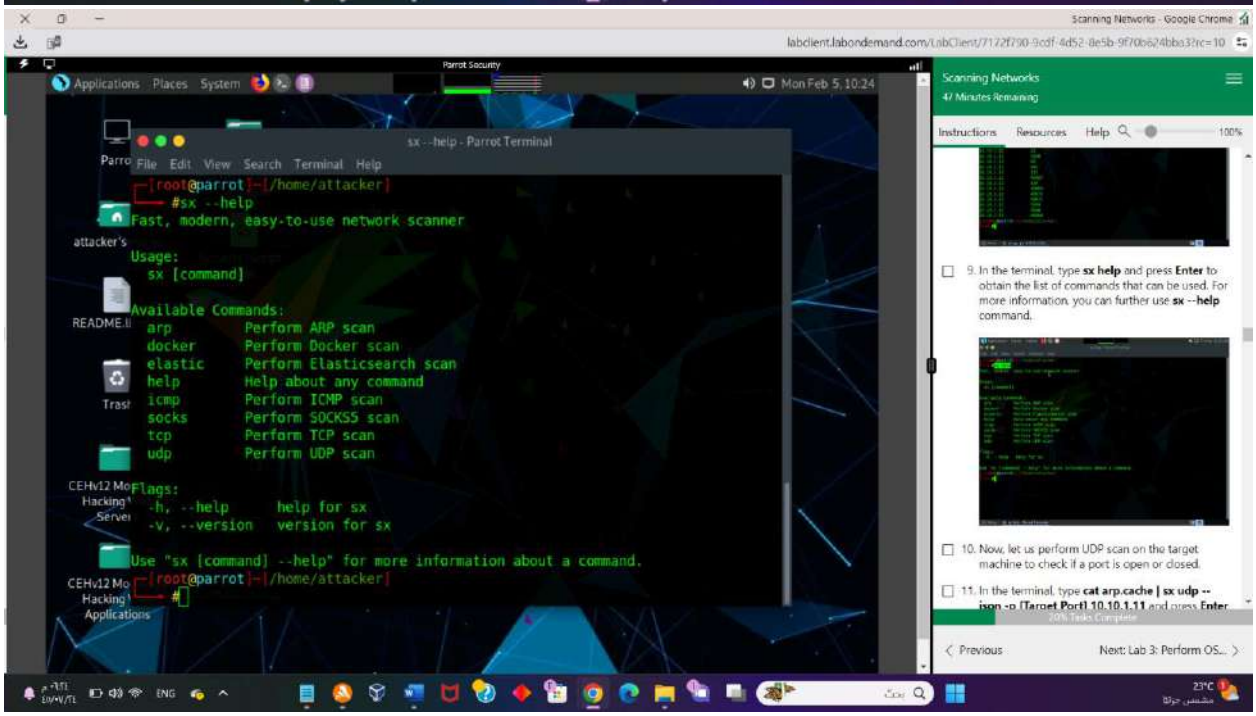


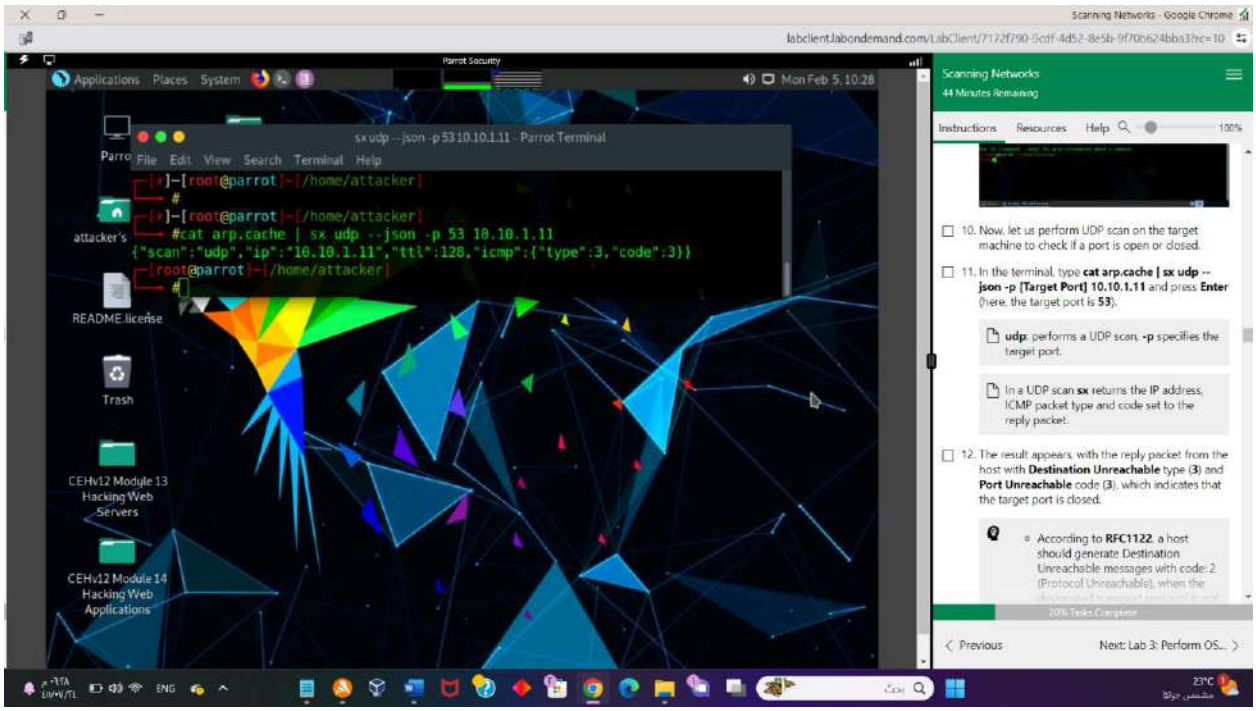


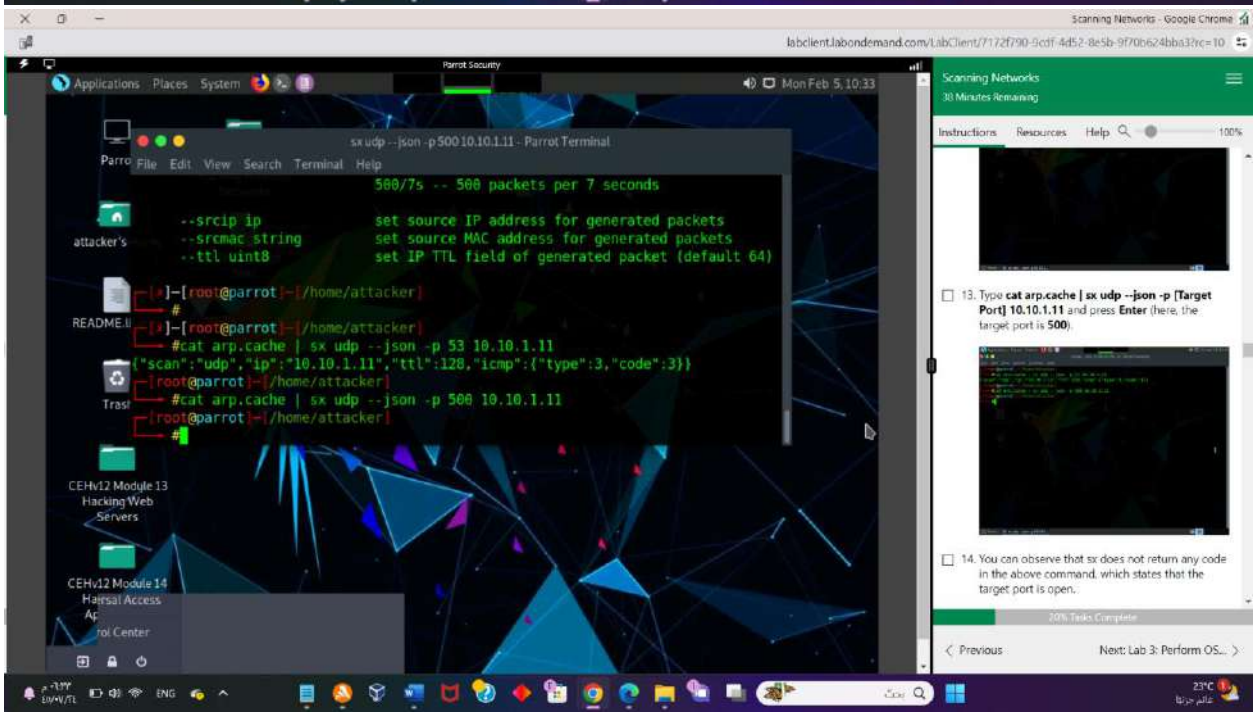

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:23
tee arp.cache - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#sx arp 10.10.1.0/24
10.10.1.19 02:15:5d:31:29:6d
10.10.1.2 02:15:5d:31:29:6b
10.10.1.11 00:15:5d:01:80:00 Microsoft Corporation
10.10.1.22 00:15:5d:01:80:02 Microsoft Corporation
10.10.1.9 02:15:5d:31:29:6e
[root@parrot]~[/home/attacker]
#sx arp 10.10.1.0/24 --json | tee arp.cache
{"ip":"10.10.1.22","mac":"00:15:5d:01:80:02","vendor":"Microsoft Corporation"}
{"ip":"10.10.1.9","mac":"02:15:5d:31:29:6e","vendor":""}
{"ip":"10.10.1.2","mac":"02:15:5d:31:29:6b","vendor":""}
{"ip":"10.10.1.19","mac":"02:15:5d:31:29:6d","vendor":""}
{"ip":"10.10.1.11","mac":"00:15:5d:01:80:00","vendor":"Microsoft Corporation"}
{"ip":"10.10.1.14","mac":"02:15:5d:31:29:70","vendor":""}
[root@parrot]~[/home/attacker]
#
Scanning Networks
49 Minutes Remaining
Instructions Resources Help 100%
7. Type sx arp [Target subnet] --json | tee arp.cache and press Enter to create arp.cache file (here, the target subnet is 10.10.1.0/24).
--json converts a text file to the JSON format, and tee writes the data to stdin.
Before the actual scan, sx explicitly creates an ARP cache file which is a simple text file containing a JSON string on each line and has the same JSON fields as the ARP scan JSON output. The protocols such as TCP and UDP read the ARP cache file from stdin and then begin the scan.
20% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
23°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:23
sx tcp -p 1-65535 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
{"ip":"10.10.1.19","mac":"02:15:5d:31:29:6d","vendor":""}
{"ip":"10.10.1.11","mac":"00:15:5d:01:80:00","vendor":"Microsoft Corporation"}
{"ip":"10.10.1.14","mac":"02:15:5d:31:29:70","vendor":""}
[root@parrot]~[/home/attacker]
#cat arp.cache | sx tcp -p 1-65535 10.10.1.11
10.10.1.11 5040
10.10.1.11 49666
10.10.1.11 21
10.10.1.11 49669
10.10.1.11 49673
10.10.1.11 445
10.10.1.11 3389
10.10.1.11 7680
10.10.1.11 80
10.10.1.11 49665
10.10.1.11 8834
10.10.1.11 49668
10.10.1.11 49667
10.10.1.11 49670
10.10.1.11 49664
10.10.1.11 139
10.10.1.11 135
[root@parrot]~[/home/attacker]
#
Scanning Networks
48 Minutes Remaining
Instructions Resources Help 100%
8. Type cat arp.cache | sx tcp -p 1-65535 [Target IP address] and press Enter to list all the open tcp ports on the target machine (here, the target IP address is 10.10.1.11).
tcp: performs a TCP scan, -p: specifies the range of ports to be scanned (here, the range is 1-65535).
9. In the terminal, type sx help and press Enter to obtain the list of commands that can be used. For more information, you can further use sx --help
20% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
23°C

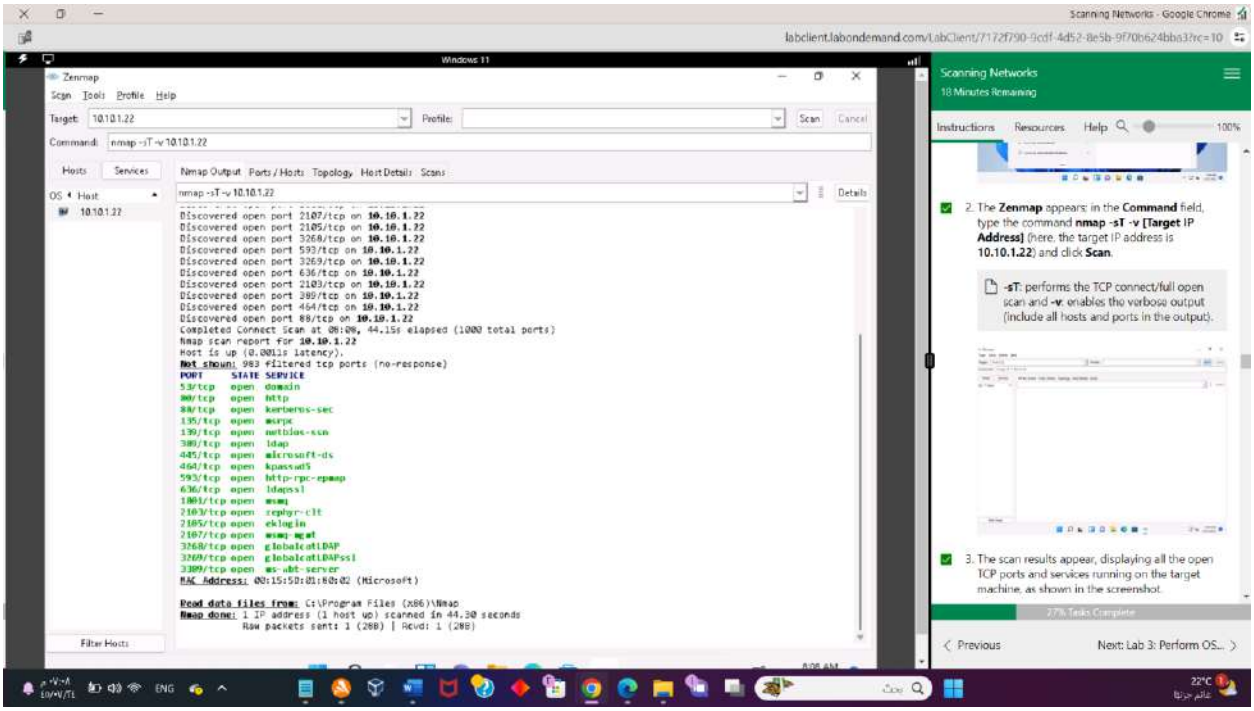

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:24
sx help - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.11 135
[root@parrot]~[/home/attacker]
#sx help
Fast, modern, easy-to-use network scanner
Usage:
sx [command]
Available Commands:
arp Perform ARP scan
docker Perform Docker scan
elastic Perform Elasticsearch scan
help Help about any command
icmp Perform ICMP scan
socks Perform SOCKS5 scan
tcp Perform TCP scan
udp Perform UDP scan
Flags:
-h, --help help for sx
Use "sx [command] --help" for more information about a command.
[root@parrot]~[/home/attacker]
#
Scanning Networks
48 Minutes Remaining
Instructions Resources Help 100%
9. In the terminal, type sx help and press Enter to obtain the list of commands that can be used. For more information, you can further use sx --help command.
10. Now, let us perform UDP scan on the target machine to check if a port is open or closed.
11. In the terminal, type cat arp.cache | sx udp --
Previous
Next: Lab 3: Perform OS...

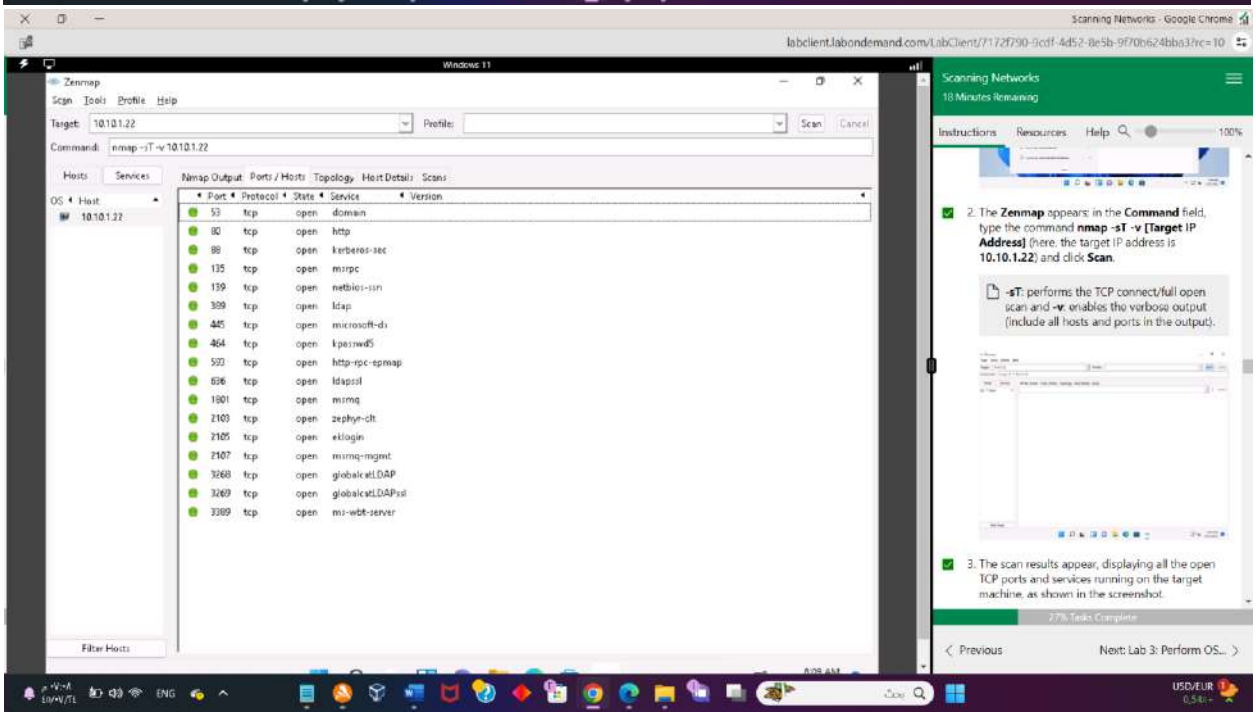

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:24
sx --help - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sx --help
Fast, modern, easy-to-use network scanner
Usage:
sx [command]
Available Commands:
arp Perform ARP scan
docker Perform Docker scan
elastic Perform Elasticsearch scan
help Help about any command
icmp Perform ICMP scan
socks Perform SOCKS5 scan
tcp Perform TCP scan
udp Perform UDP scan
Flags:
-h, --help help for sx
-v, --version version for sx
Use "sx [command] --help" for more information about a command.
[root@parrot]~[/home/attacker]
#
Scanning Networks
47 Minutes Remaining
Instructions Resources Help 100%
9. In the terminal, type sx help and press Enter to obtain the list of commands that can be used. For more information, you can further use sx --help command.
10. Now, let us perform UDP scan on the target machine to check if a port is open or closed.
11. In the terminal, type cat arp.cache | sx udp --
Previous
Next: Lab 3: Perform OS...

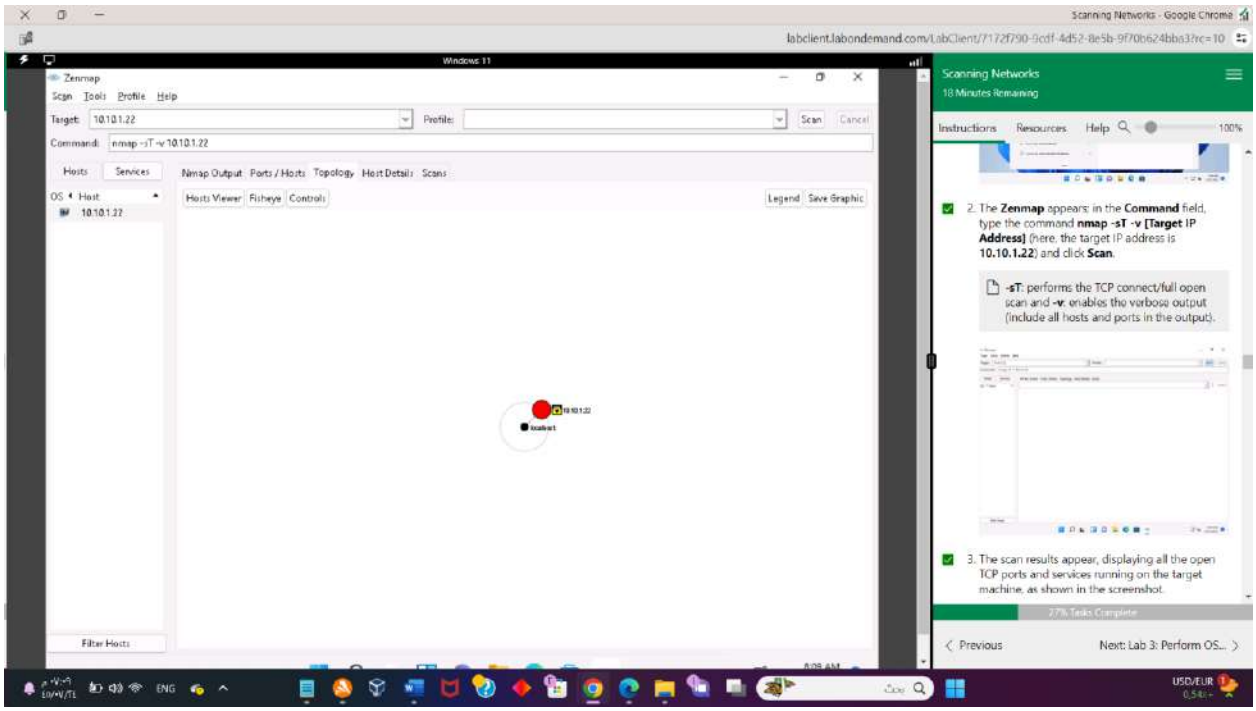

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:28
sx udp --json -p 53 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#
[root@parrot]-[/home/attacker]
#cat arp.cache | sx udp --json -p 53 10.10.1.11
{"scan":"udp","ip":"10.10.1.11","ttl":128,"icmp":{"type":3,"code":3}}
[root@parrot]-[/home/attacker]
#
attacker's
README.license
Trash
CEHv12 Module 13 Hacking Web Servers
CEHv12 Module 14 Hacking Web Applications
Scanning Networks
44 Minutes Remaining
Instructions Resources Help 100%
10. Now, let us perform UDP scan on the target machine to check if a port is open or closed.
11. In the terminal, type cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11 and press Enter (here, the target port is 53).
udp: performs a UDP scan, -p specifies the target port.
In a UDP scan sx returns the IP address, ICMP packet type and code set to the reply packet.
12. The result appears, with the reply packet from the host with Destination Unreachable type (3) and Port Unreachable code (3), which indicates that the target port is closed.
According to RFC1122, a host should generate Destination Unreachable messages with code: 2 (Protocol Unreachable), when the
20% Tasks Complete
Previous
Next: Lab 3: Perform OS...

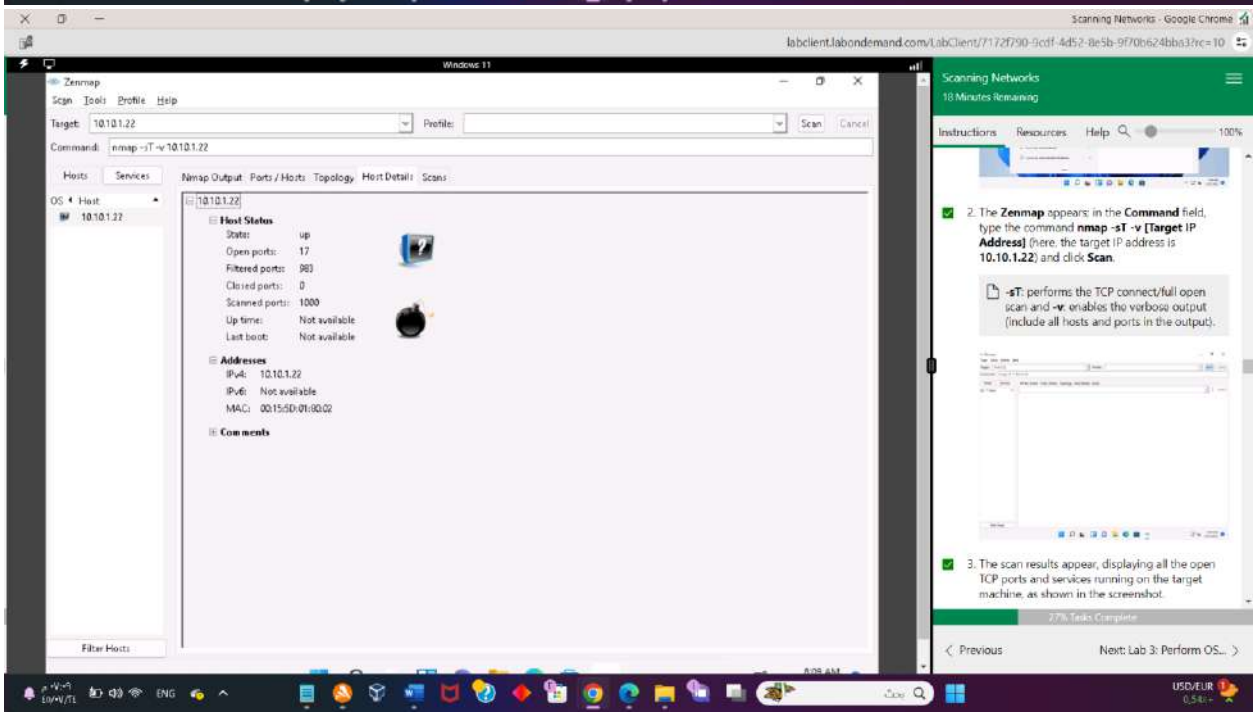

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 10:33
sx udp --json -p 500 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
500/7s -- 500 packets per 7 seconds
--srcip ip set source IP address for generated packets
--srcmac string set source MAC address for generated packets
--ttl uint8 set IP TTL field of generated packet (default 64)
[root@parrot]-[/home/attacker]
#
[root@parrot]-[/home/attacker]
#cat arp.cache | sx udp --json -p 53 10.10.1.11
{"scan":"udp","ip":"10.10.1.11","ttl":128,"icmp":{"type":3,"code":3}}
[root@parrot]-[/home/attacker]
#cat arp.cache | sx udp --json -p 500 10.10.1.11
[root@parrot]-[/home/attacker]
#
attacker's
README.li
Trash
CEHv12 Module 13 Hacking Web Servers
CEHv12 Module 14
Scanning Networks
38 Minutes Remaining
Instructions Resources Help 100%
13. Type cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11 and press Enter (here, the target port is 500).
14. You can observe that sx does not return any code in the above command, which states that the target port is open.
20% Tasks Complete
Previous
Next: Lab 3: Perform OS...

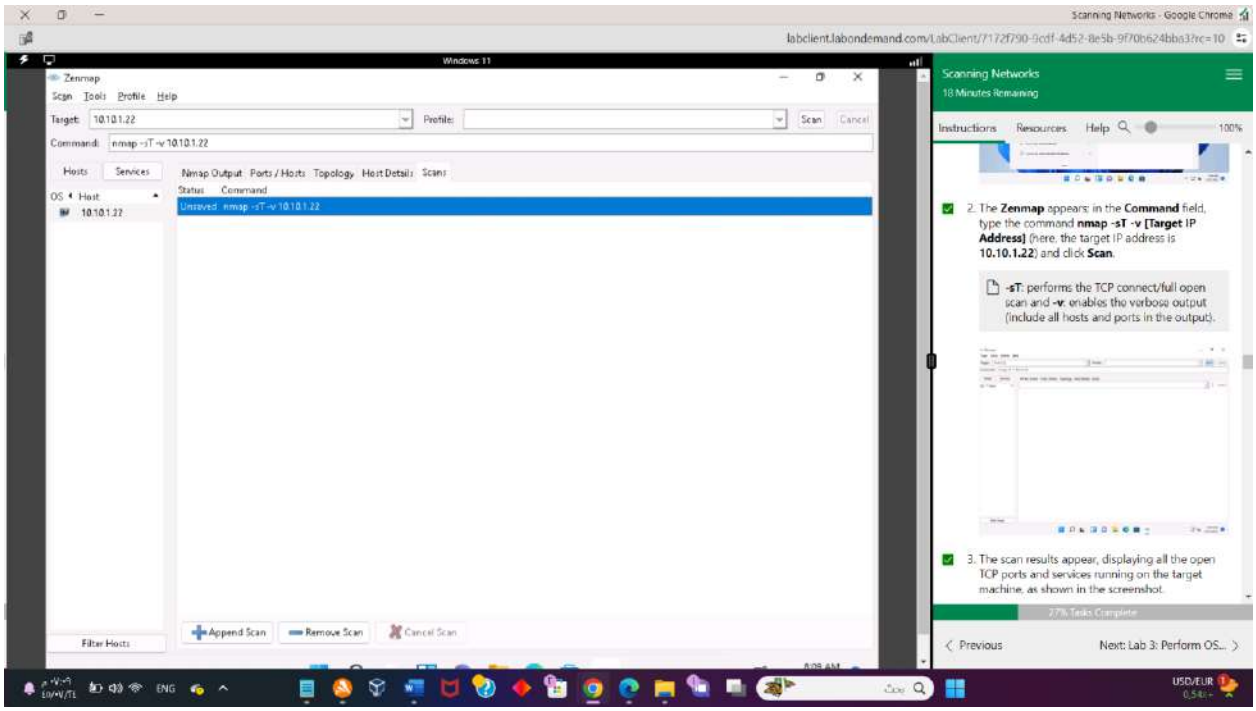
Lab 02 – Task 04

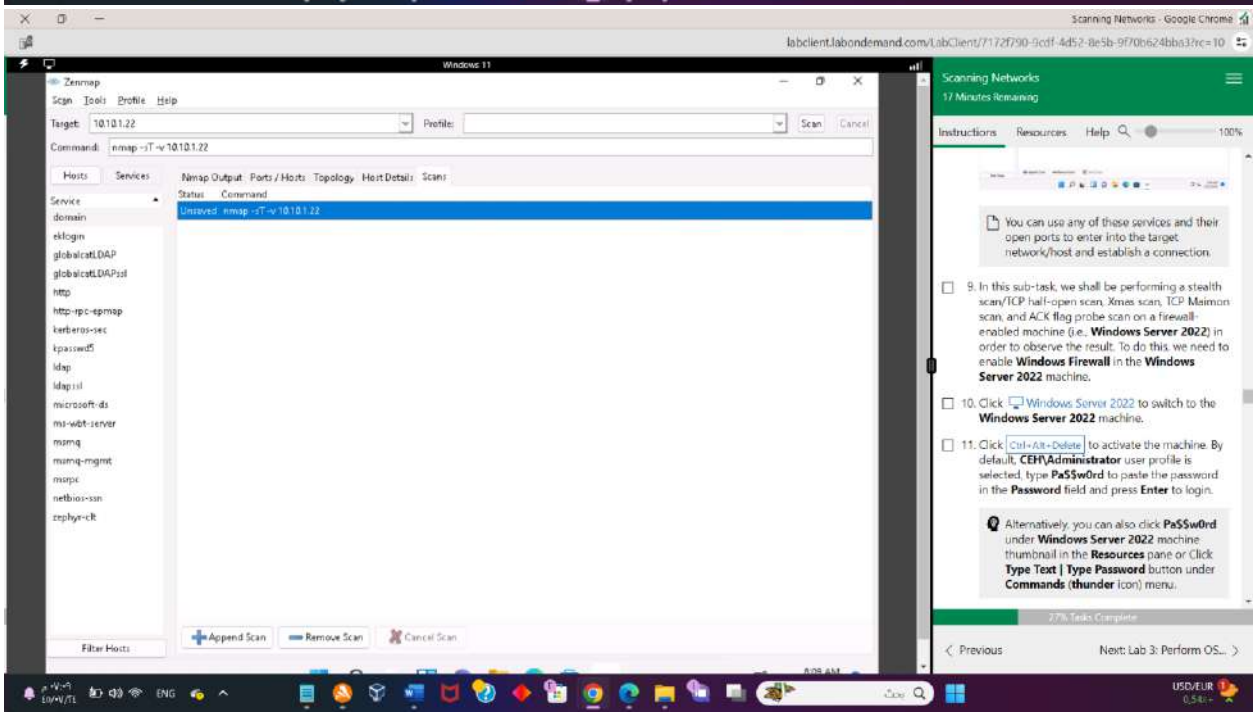


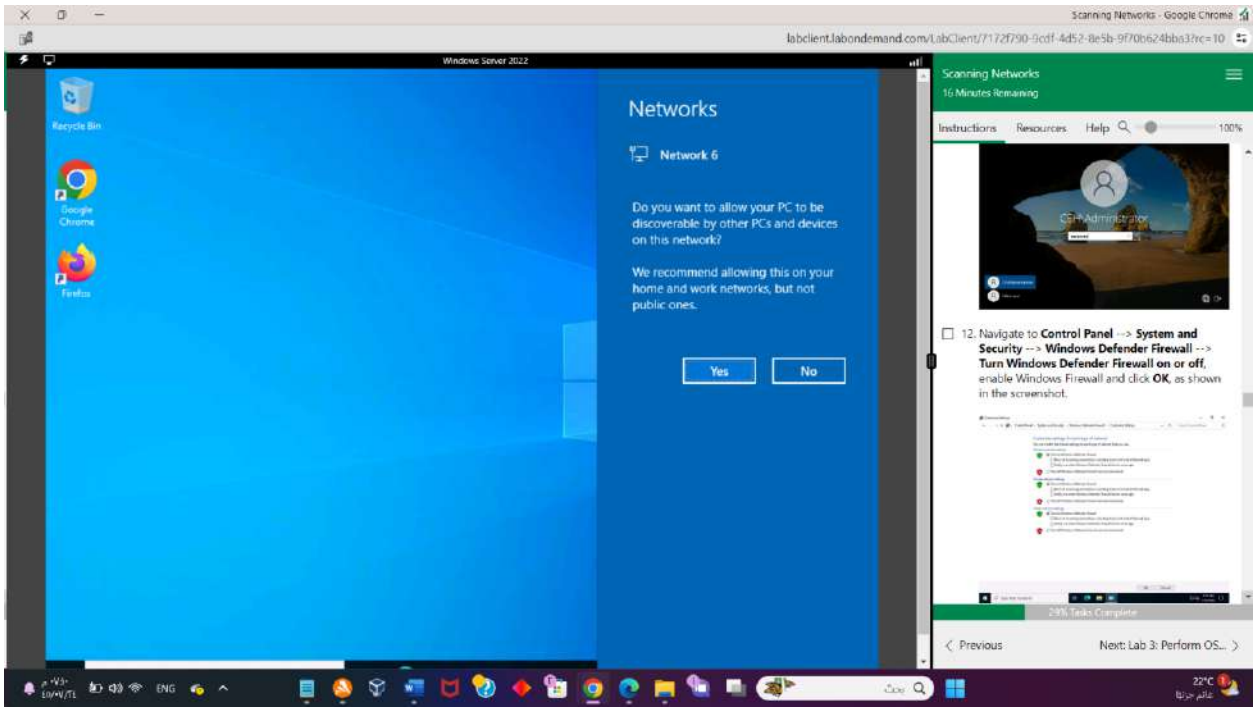


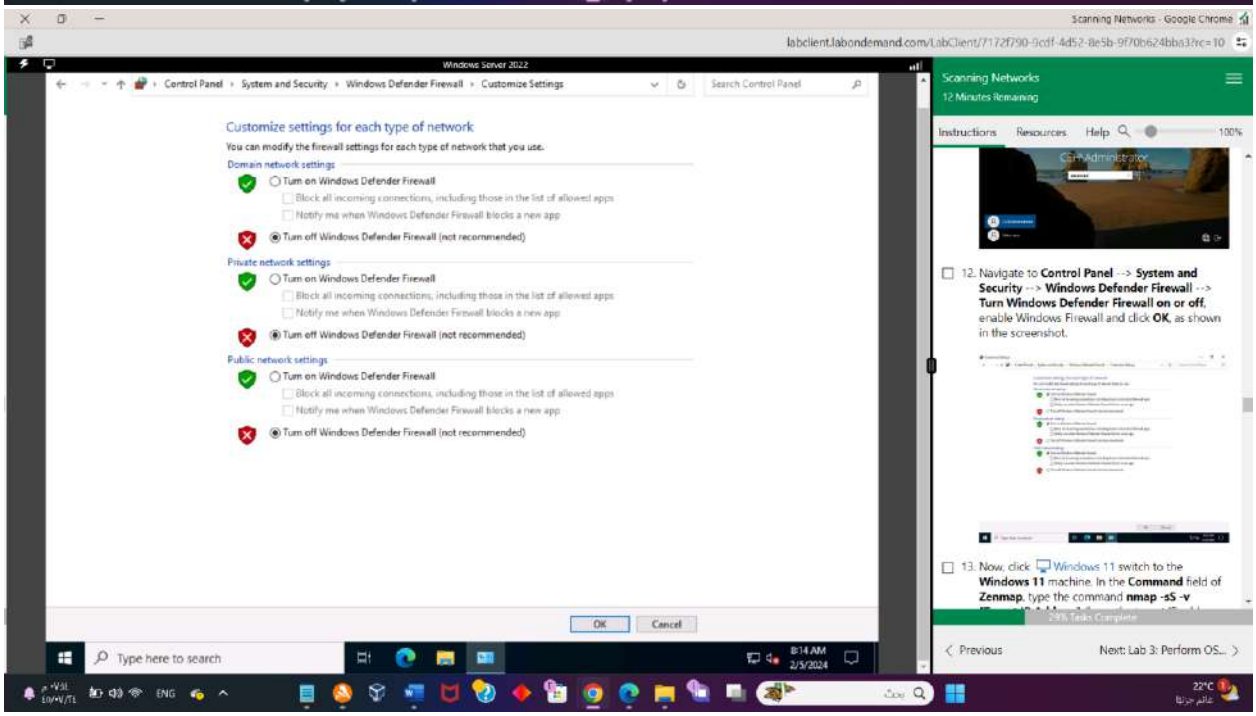

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
Hosts Viewer Fisheye Controls
Legend Save Graphic
Filter Hosts
Scanning Networks
18 Minutes Remaining
Instructions Resources Help 100%
2. The Zenmap appears in the Command field, type the command nmap -sT -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).
3. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.
27% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
USD/EUR

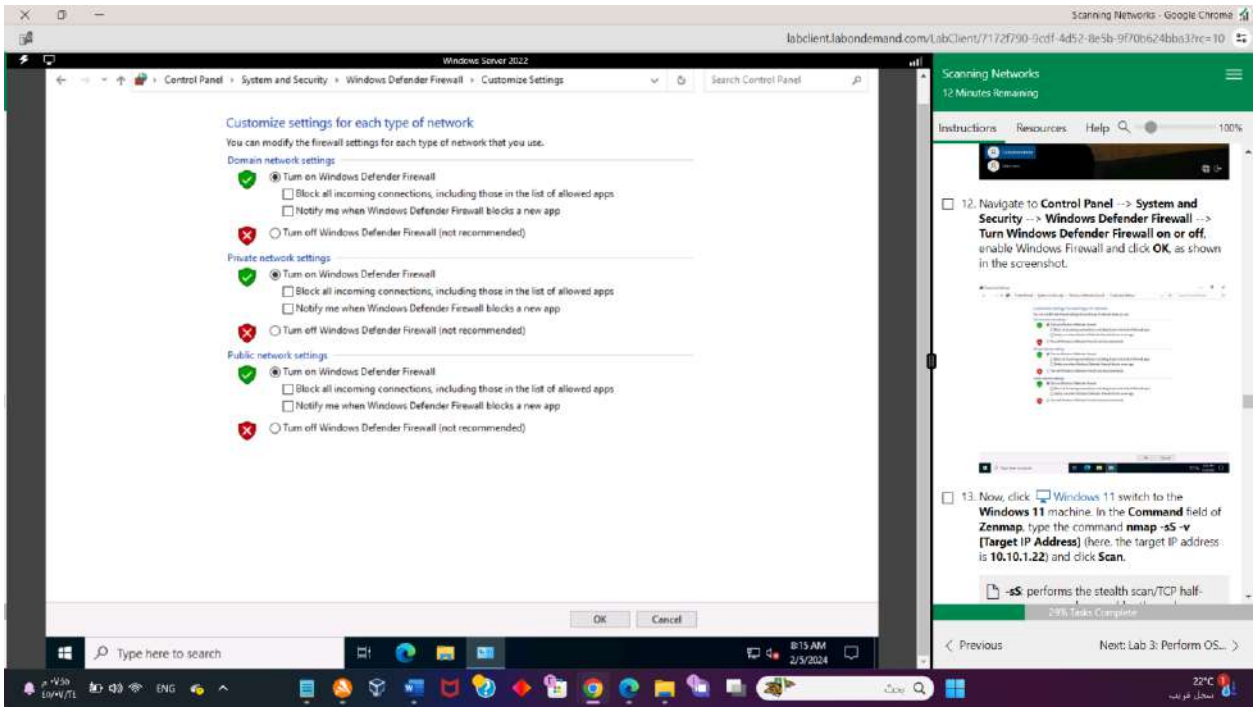

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
10.10.1.22
Host Status
State: up
Open ports: 17
Filtered ports: 983
Closed ports: 0
Scanned ports: 1000
Up time: Not available
Last boot: Not available
Addresses
IPv4: 10.10.1.22
IPv6: Not available
MAC: 00:15:5D:01:80:02
Comments
Filter Hosts
Scanning Networks
18 Minutes Remaining
Instructions Resources Help 100%
2. The Zenmap appears in the Command field, type the command nmap -sT -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).
3. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.
27% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
USD/EUR

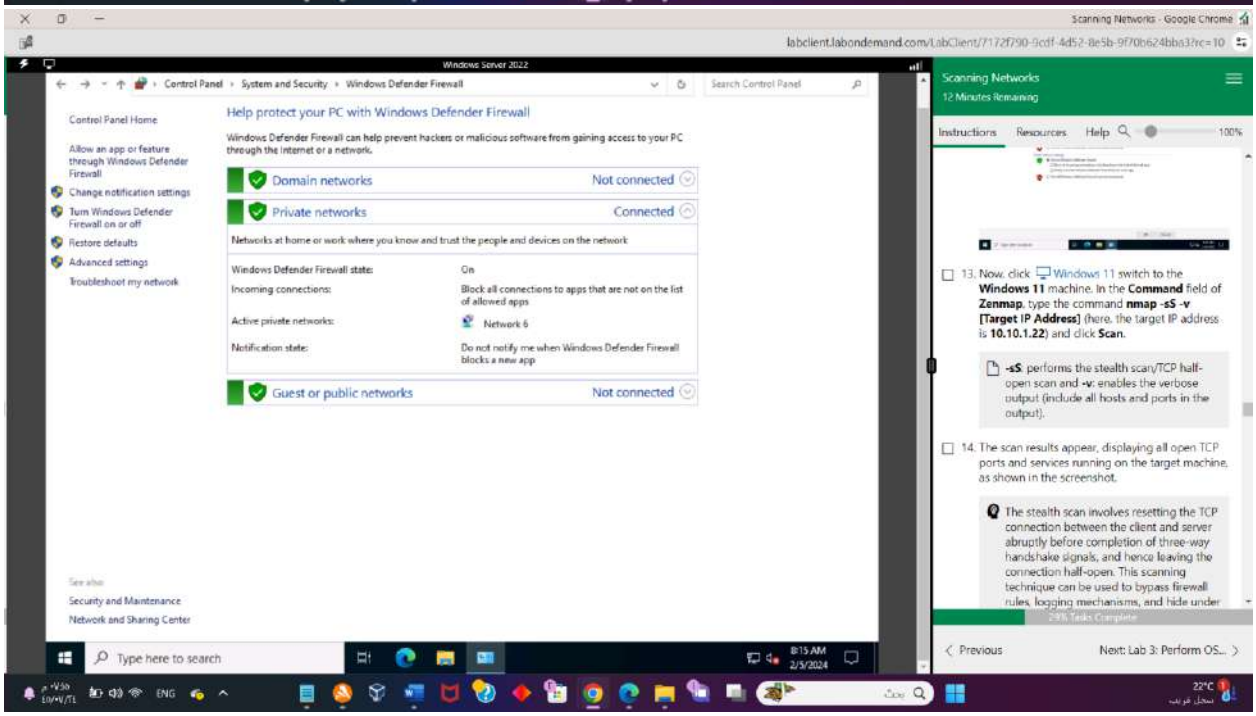

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
Status Command
Unsaved nmap -sT -v 10.10.1.22
Append Scan
Remove Scan
Cancel Scan
Filter Hosts
Scanning Networks
18 Minutes Remaining
Instructions
Resources
Help
100%
2. The Zenmap appears in the Command field, type the command nmap -sT -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sT: performs the TCP connect/full open scan and -v: enables the verbose output (include all hosts and ports in the output).
3. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.
27% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
USD/EUR

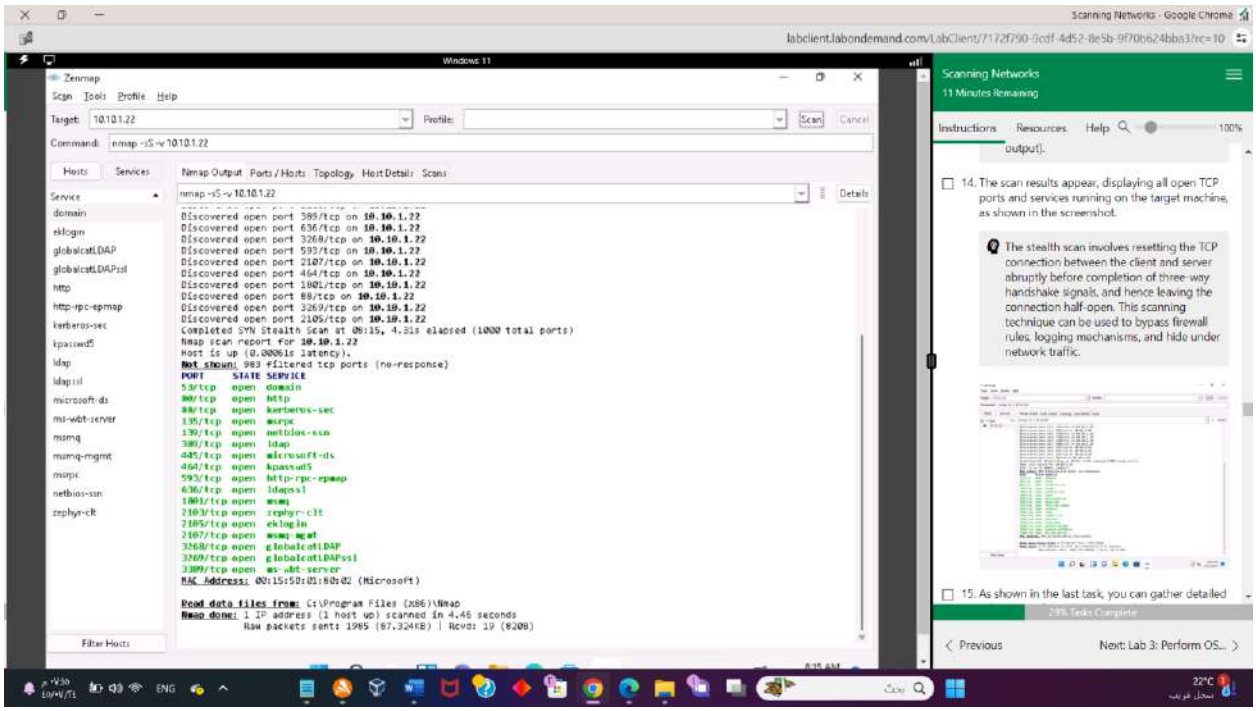

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
Service
domain
eklogin
globalcatLDAP
globalcatLDAPssl
http
http-rpc-epmap
kerberos-sec
kpasswd5
ldap
ldapssl
microsoft-ds
ms-wbt-server
msmq
msmq-mgmt
msrpc
netbios-ssn
zephyr-clt
Status Command
Unsaved nmap -sT -v 10.10.1.22
Append Scan
Remove Scan
Cancel Scan
Filter Hosts
Scanning Networks
17 Minutes Remaining
Instructions
Resources
Help
100%
You can use any of these services and their open ports to enter into the target network/host and establish a connection.
9. In this sub-task, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., Windows Server 2022) in order to observe the result. To do this, we need to enable Windows Firewall in the Windows Server 2022 machine.
10. Click Windows Server 2022 to switch to the Windows Server 2022 machine.
11. Click Ctrl+Alt+Delete to activate the machine. By default, CEH\Administrator user profile is selected, type PaSSw0rd to paste the password in the Password field and press Enter to login.
Alternatively, you can also click PaSSw0rd under Windows Server 2022 machine thumbnail in the Resources pane or Click Type Text | Type Password button under Commands (thunder icon) menu.
27% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
USD/EUR

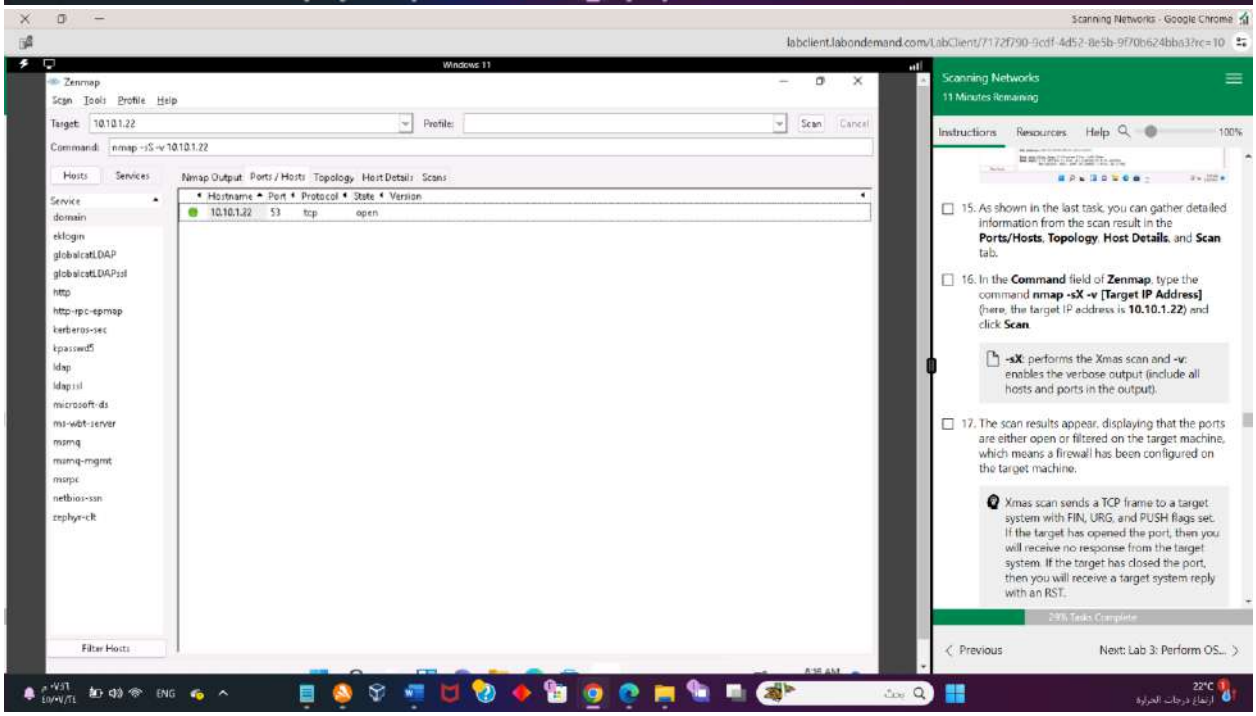

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows Server 2022
Networks
Network 6
Do you want to allow your PC to be discoverable by other PCs and devices on this network?
We recommend allowing this on your home and work networks, but not public ones.
Yes
No
Scanning Networks
16 Minutes Remaining
Instructions
Resources
Help
100%
CSH-Administrator
12. Navigate to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, enable Windows Firewall and click OK, as shown in the screenshot.
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...

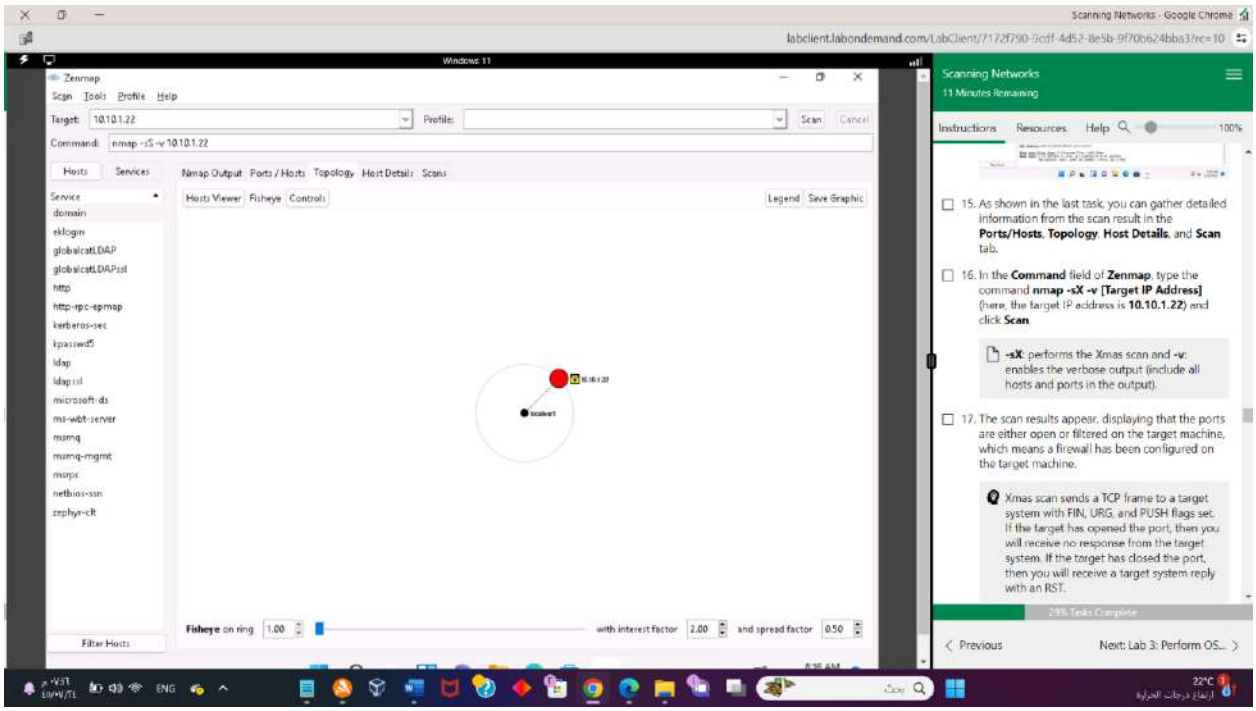

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows Server 2022
Control Panel > System and Security > Windows Defender Firewall > Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Domain network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel
Type here to search
8:14 AM
2/5/2024
Scanning Networks
12 Minutes Remaining
Instructions
Resources
Help
100%
CSH-Administrator
12. Navigate to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, enable Windows Firewall and click OK, as shown in the screenshot.
13. Now, click Windows 11 switch to the Windows 11 machine. In the Command field of Zenmap, type the command nmap -sS -v
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...

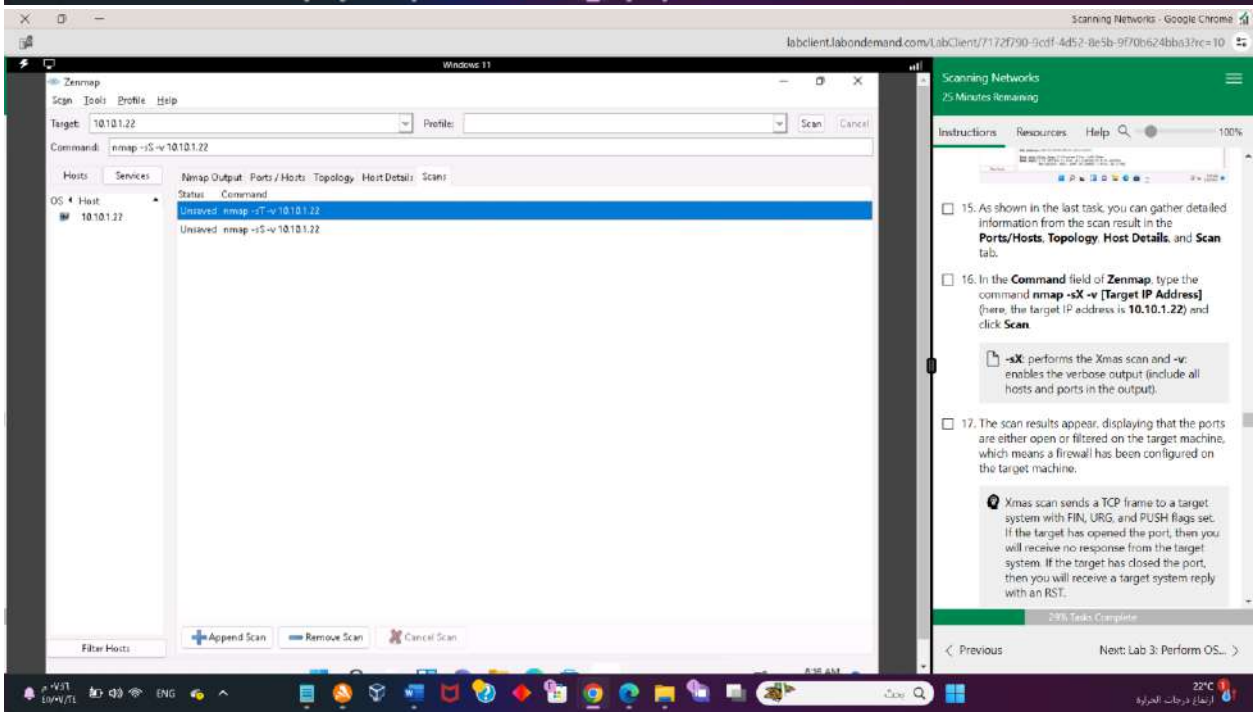

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows Server 2022
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Domain network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel
Type here to search
8:15 AM
2/5/2024
Scanning Networks
12 Minutes Remaining
Instructions
Resources
Help
100%
12. Navigate to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, enable Windows Firewall and click OK, as shown in the screenshot.
13. Now, click Windows 11 switch to the Windows 11 machine. In the Command field of Zenmap, type the command nmap -sS -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sS: performs the stealth scan/TCP half-
Previous
Next: Lab 3: Perform OS...
22°C

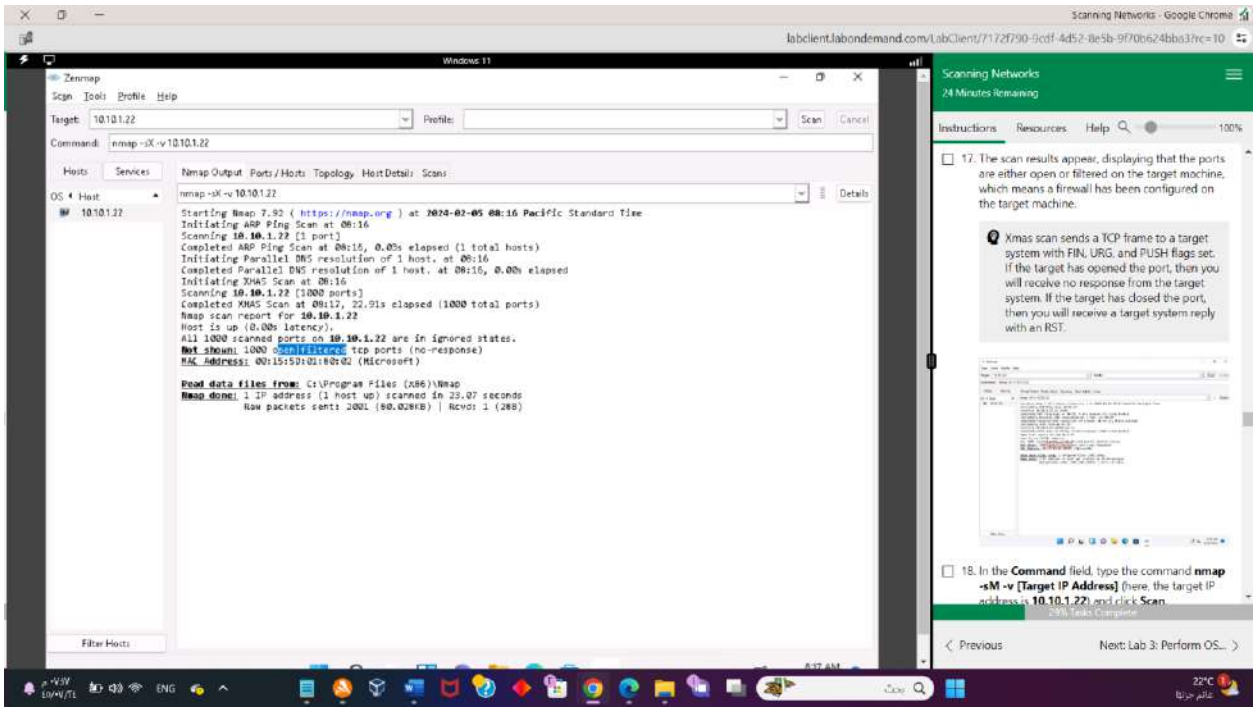

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows Server 2022
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Domain networks
Not connected
Private networks
Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Defender Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active private networks:
Network 6
Notification state:
Do not notify me when Windows Defender Firewall blocks a new app
Guest or public networks
Not connected
See also
Security and Maintenance
Network and Sharing Center
Type here to search
8:15 AM
2/5/2024
Scanning Networks
12 Minutes Remaining
Instructions
Resources
Help
100%
13. Now, click Windows 11 switch to the Windows 11 machine. In the Command field of Zenmap, type the command nmap -sS -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sS: performs the stealth scan/TCP half-open scan and -v: enables the verbose output (include all hosts and ports in the output).
14. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.
The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under
Previous
Next: Lab 3: Perform OS...
22°C

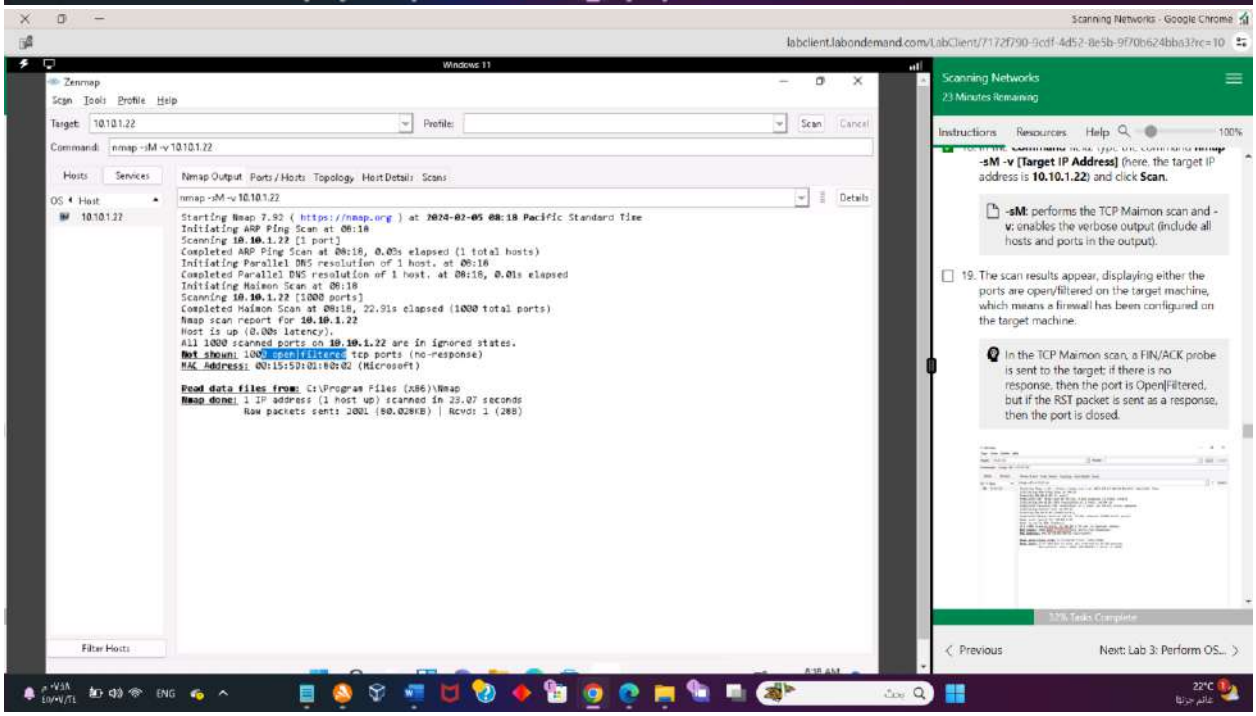

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -v 10.10.1.22
Details
Service
domain
eklogin
globalcatLDAP
globalcatLDAPssl
http
http-rpc-epmap
kerberos-sec
kpasswd5
ldap
ldapssl
microsoft-ds
ms-wbt-server
msmq
msmq-mgmt
msrpc
netbios-ssn
zephyr-clt
Discovered open port 389/tcp on 10.10.1.22
Discovered open port 636/tcp on 10.10.1.22
Discovered open port 3268/tcp on 10.10.1.22
Discovered open port 593/tcp on 10.10.1.22
Discovered open port 2107/tcp on 10.10.1.22
Discovered open port 464/tcp on 10.10.1.22
Discovered open port 1801/tcp on 10.10.1.22
Discovered open port 88/tcp on 10.10.1.22
Discovered open port 3269/tcp on 10.10.1.22
Discovered open port 2105/tcp on 10.10.1.22
Completed SYN Stealth Scan at 09:15, 4.81s elapsed (1000 total ports)
Nmap scan report for 10.10.1.22
Host is up (0.00061s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
Raw packets sent: 1985 (87.324KB) | Rcvd: 19 (820B)
Filter Hosts
Scanning Networks
11 Minutes Remaining
Instructions
Resources
Help
100%
output).
14. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.
The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.
15. As shown in the last task, you can gather detailed
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

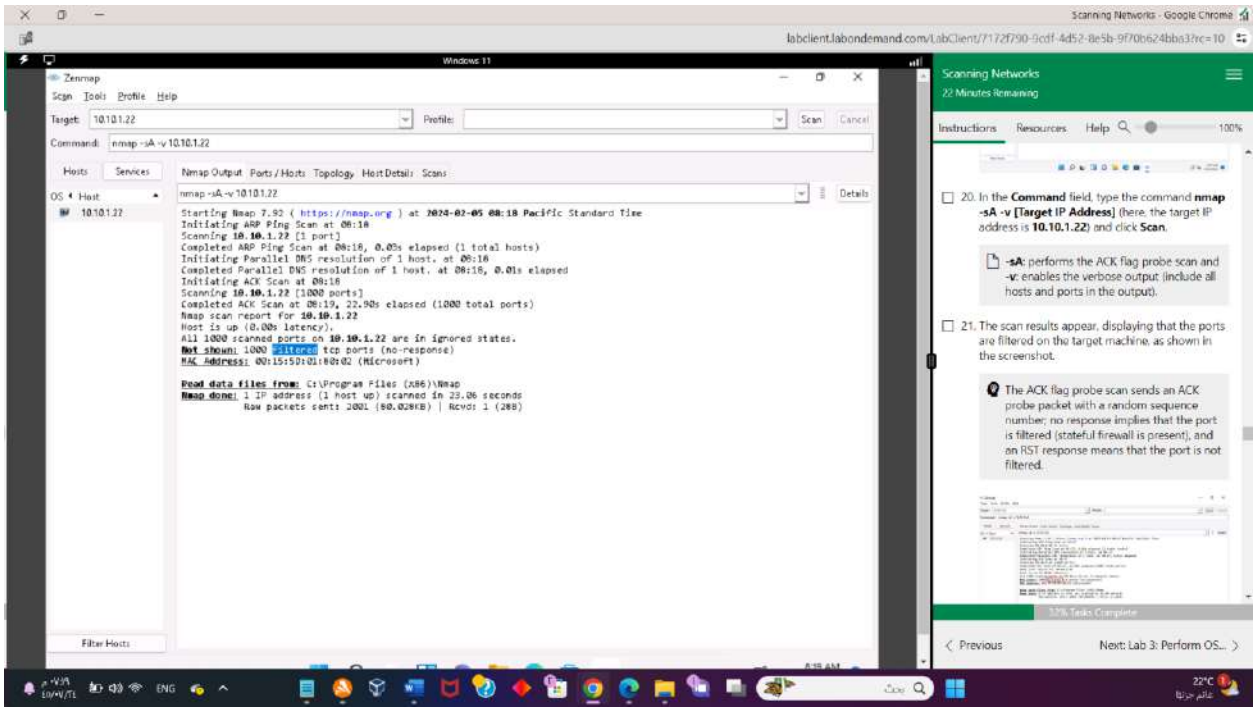

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hostname Port Protocol State Version
10.10.1.22 53 tcp open
Service
domain
eklogin
globalcatLDAP
globalcatLDAPssl
http
http-rpc-epmap
kerberos-sec
kpasswd5
ldap
ldapssl
microsoft-ds
ms-wbt-server
msmq
msmq-mgmt
msrpc
netbios-ssn
zephyr-clt
Filter Hosts
Scanning Networks
11 Minutes Remaining
Instructions
Resources
Help
100%
15. As shown in the last task, you can gather detailed information from the scan result in the Ports/Hosts, Topology, Host Details, and Scan tab.
16. In the Command field of Zenmap, type the command nmap -sX -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sX: performs the Xmas scan and -v: enables the verbose output (include all hosts and ports in the output).
17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.
Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

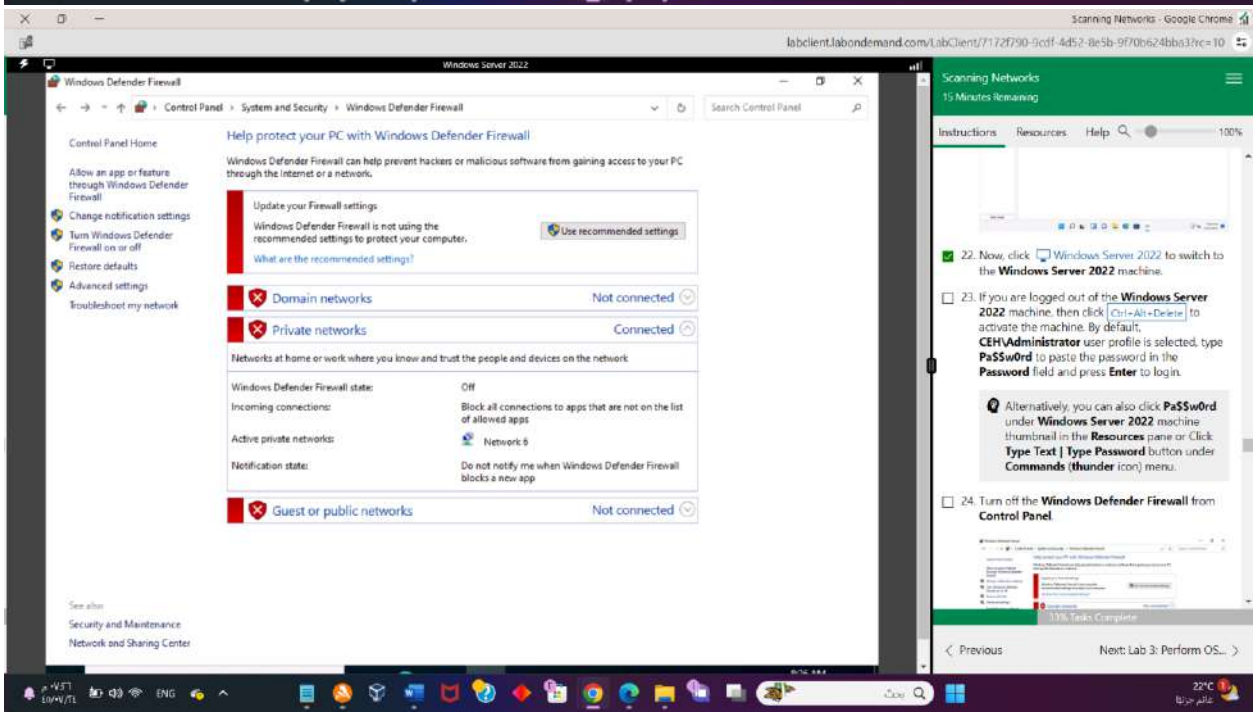

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
Service
domain
eklogin
globalcatLDAP
globalcatLDAPssl
http
http-rpc-epmap
kerberos-sec
kpasswd5
ldap
ldapssl
microsoft-ds
ms-wbt-server
msmq
msmq-mgmt
msrpc
netbios-ssn
zephyr-clt
Hosts Viewer Fisheye Controls
Legend Save Graphic
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50
Filter Hosts
Scanning Networks
11 Minutes Remaining
Instructions Resources Help 100%
15. As shown in the last task, you can gather detailed information from the scan result in the Ports/Hosts, Topology, Host Details, and Scan tab.
16. In the Command field of Zenmap, type the command nmap -sX -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sX: performs the Xmas scan and -v: enables the verbose output (include all hosts and ports in the output).
17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.
Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...
22°C

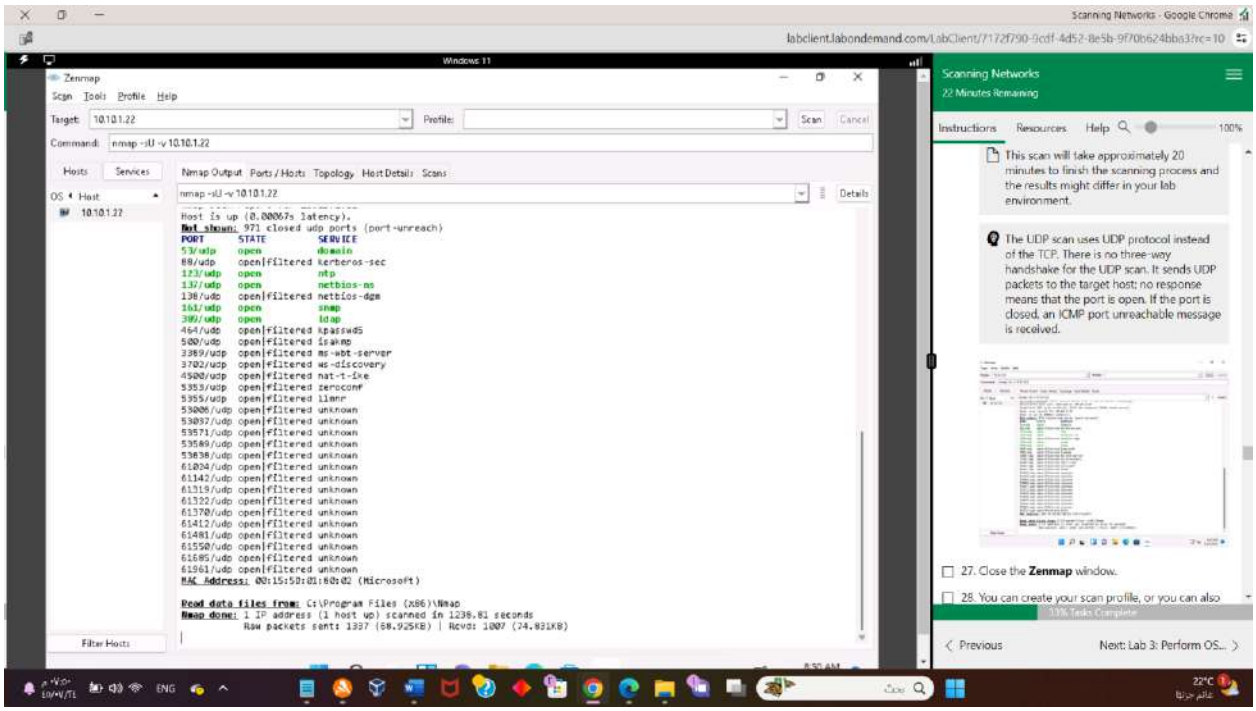

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
Status Command
Unsaved nmap -sT -v 10.10.1.22
Unsaved nmap -sS -v 10.10.1.22
Append Scan
Remove Scan
Cancel Scan
Filter Hosts
Scanning Networks
25 Minutes Remaining
Instructions Resources Help 100%
15. As shown in the last task, you can gather detailed information from the scan result in the Ports/Hosts, Topology, Host Details, and Scan tab.
16. In the Command field of Zenmap, type the command nmap -sX -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sX: performs the Xmas scan and -v: enables the verbose output (include all hosts and ports in the output).
17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.
Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...
22°C

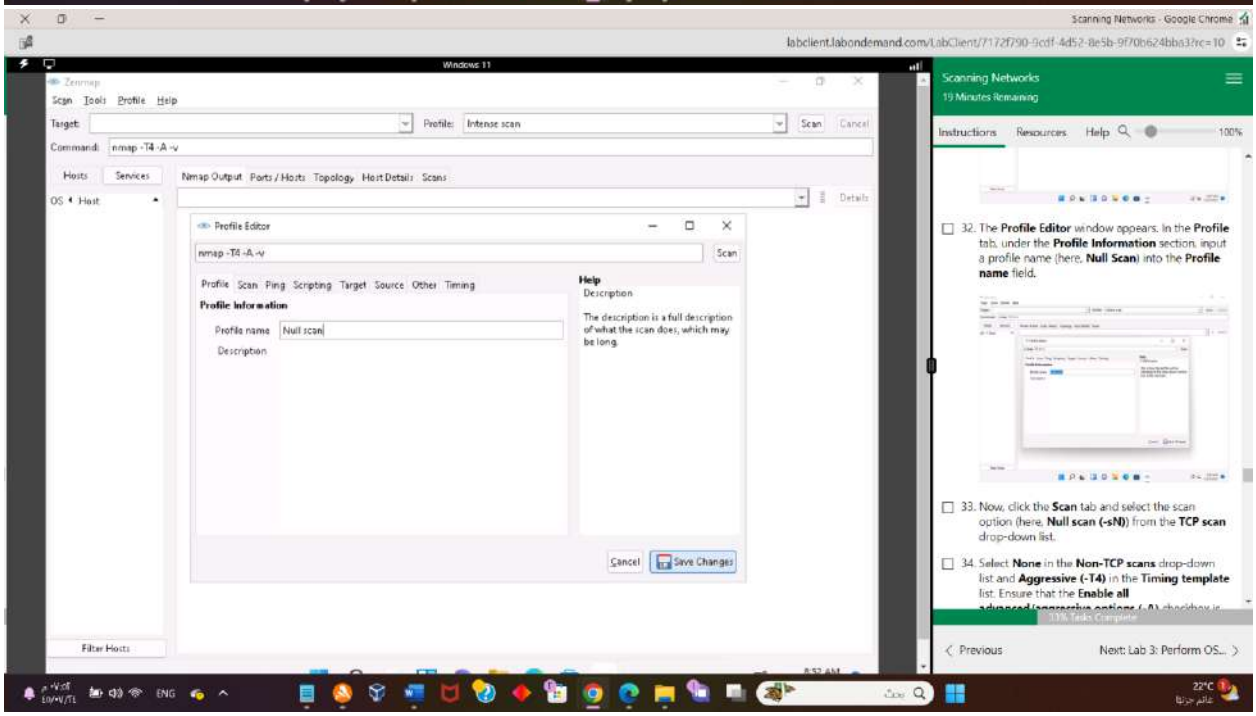

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sX -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
nmap -sX -v 10.10.1.22
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 08:16 Pacific Standard Time
Initiating ARP Ping Scan at 08:16
Scanning 10.10.1.22 [1 port]
Completed ARP Ping Scan at 08:16, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:16
Completed Parallel DNS resolution of 1 host. at 08:16, 0.00s elapsed
Initiating XMAS Scan at 08:16
Scanning 10.10.1.22 [1000 ports]
Completed XMAS Scan at 08:17, 22.91s elapsed (1000 total ports)
Nmap scan report for 10.10.1.22
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.1.22 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
Filter Hosts
Scanning Networks
24 Minutes Remaining
Instructions
Resources
Help
100%
17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.
Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.
18. In the Command field, type the command nmap -sM -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
29% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

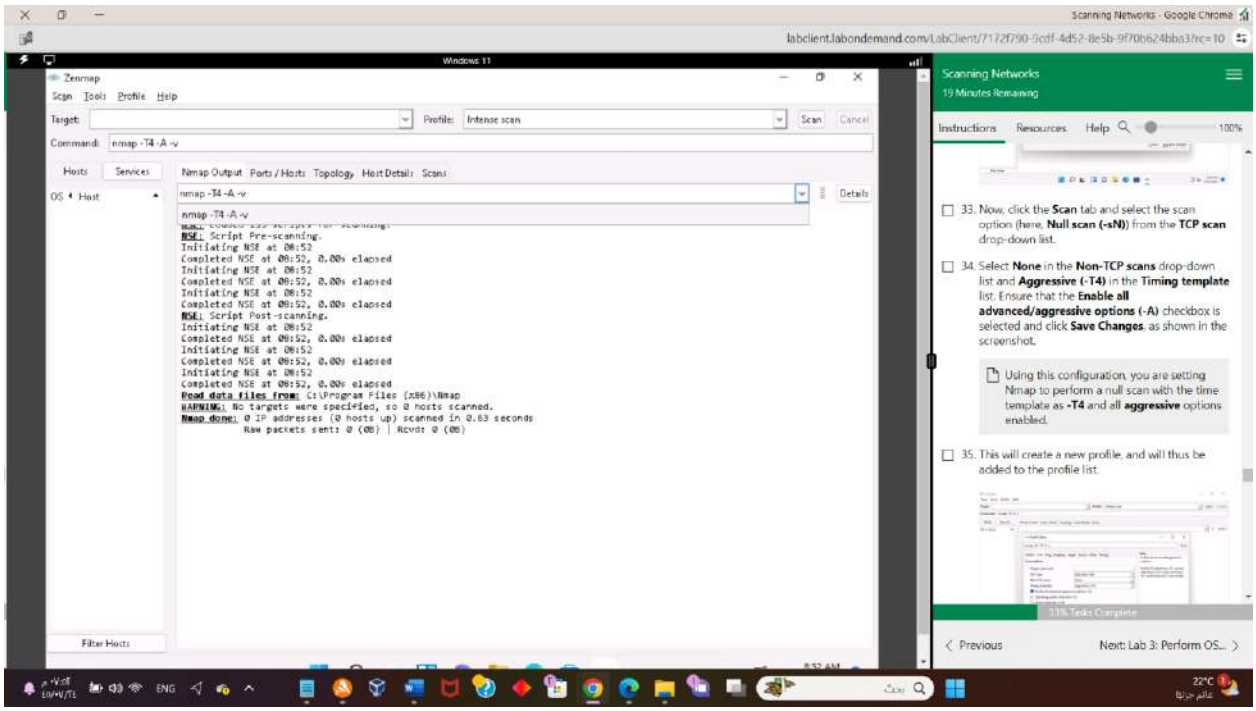

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sM -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
nmap -sM -v 10.10.1.22
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 08:18 Pacific Standard Time
Initiating ARP Ping Scan at 08:18
Scanning 10.10.1.22 [1 port]
Completed ARP Ping Scan at 08:18, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:18
Completed Parallel DNS resolution of 1 host. at 08:18, 0.01s elapsed
Initiating Maimon Scan at 08:18
Scanning 10.10.1.22 [1000 ports]
Completed Maimon Scan at 08:18, 22.91s elapsed (1000 total ports)
Nmap scan report for 10.10.1.22
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.1.22 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
Filter Hosts
Scanning Networks
23 Minutes Remaining
Instructions
Resources
Help
100%
-sM -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sM: performs the TCP Maimon scan and -v: enables the verbose output (include all hosts and ports in the output).
19. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.
In the TCP Maimon scan, a FIN/ACK probe is sent to the target: if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

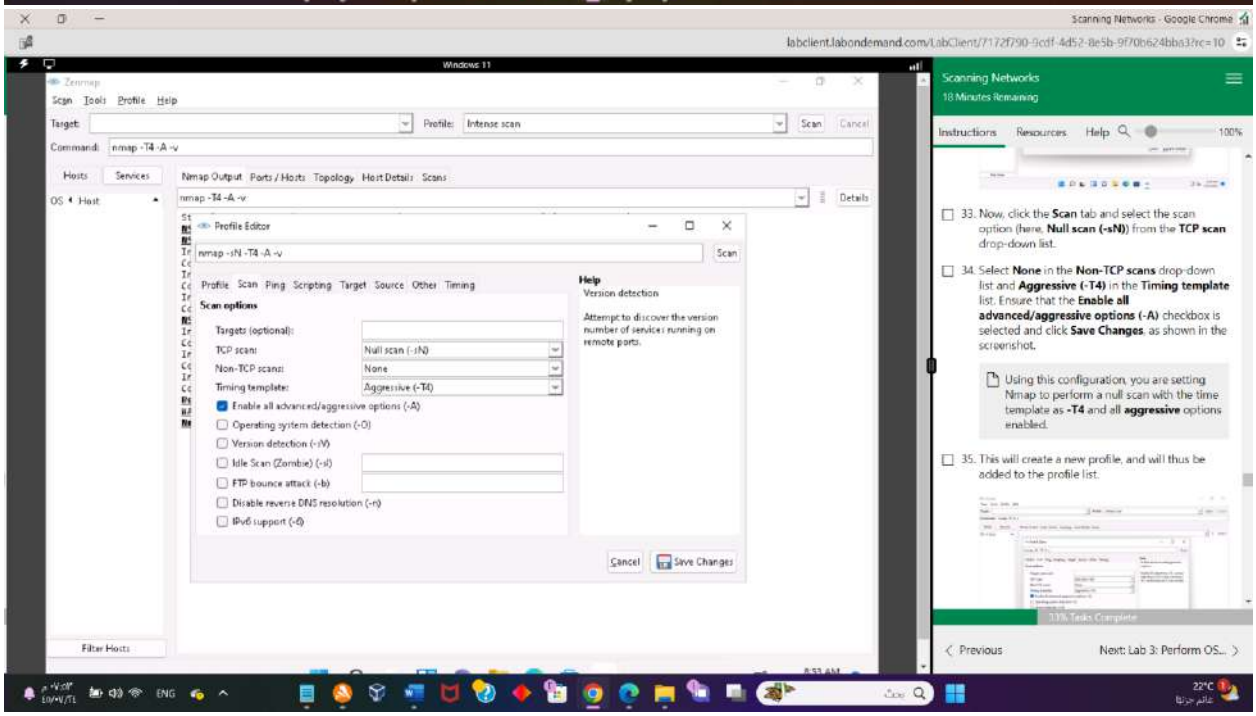

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sA -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 08:18 Pacific Standard Time
Initiating ARP Ping Scan at 08:18
Scanning 10.10.1.22 [1 port]
Completed ARP Ping Scan at 08:18, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:18
Completed Parallel DNS resolution of 1 host. at 08:18, 0.01s elapsed
Initiating ACK Scan at 08:18
Scanning 10.10.1.22 [1000 ports]
Completed ACK Scan at 08:19, 22.90s elapsed (1000 total ports)
Nmap scan report for 10.10.1.22
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.1.22 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.06 seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
Filter Hosts
Scanning Networks
22 Minutes Remaining
Instructions
Resources
Help
100%
20. In the Command field, type the command nmap -sA -v [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sA: performs the ACK flag probe scan and -v: enables the verbose output (include all hosts and ports in the output).
21. The scan results appear, displaying that the ports are filtered on the target machine, as shown in the screenshot.
The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

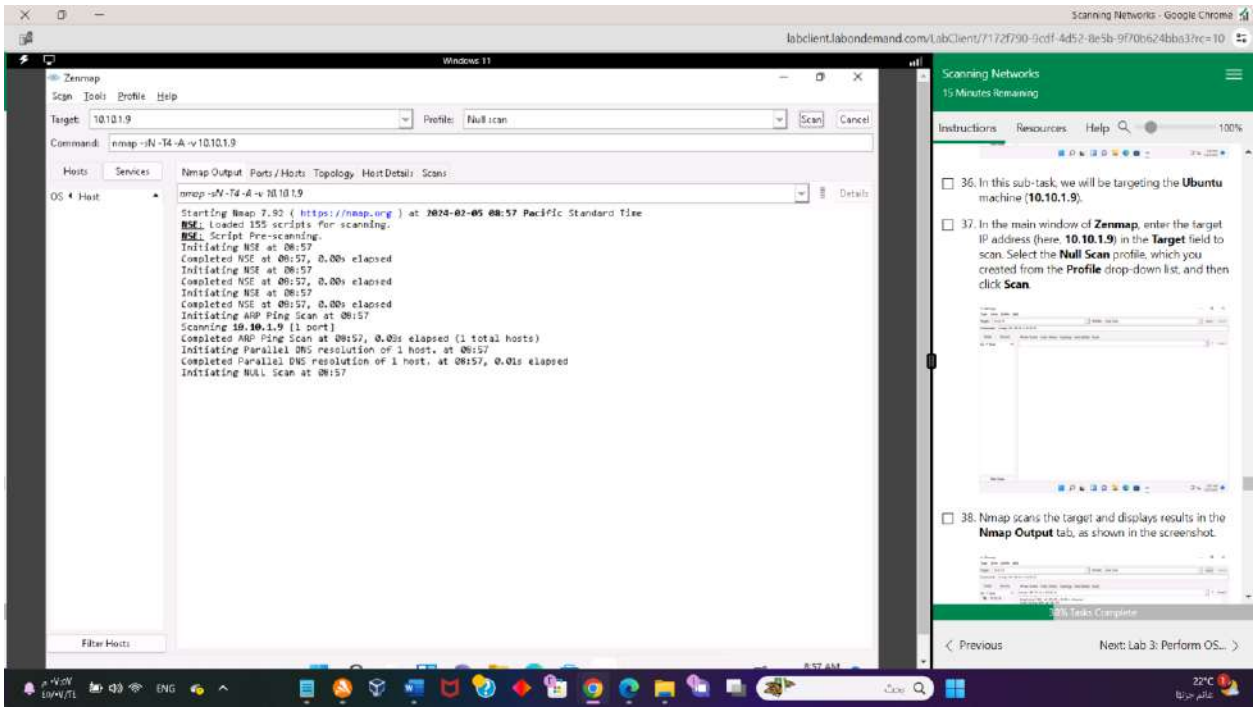

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows Server 2022
Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Defender Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Domain networks
Not connected
Private networks
Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Defender Firewall state: Off
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active private networks: Network 6
Notification state: Do not notify me when Windows Defender Firewall blocks a new app
Guest or public networks
Not connected
See also
Security and Maintenance
Network and Sharing Center
Scanning Networks
15 Minutes Remaining
Instructions
Resources
Help
100%
22. Now, click Windows Server 2022 to switch to the Windows Server 2022 machine.
23. If you are logged out of the Windows Server 2022 machine, then click Ctrl+Alt+Delete to activate the machine. By default, CEH\Administrator user profile is selected, type Pa$$w0rd to paste the password in the Password field and press Enter to login.
Alternatively, you can also click Pa$$w0rd under Windows Server 2022 machine thumbnail in the Resources pane or Click Type Text | Type Password button under Commands (thunder icon) menu.
24. Turn off the Windows Defender Firewall from Control Panel.
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

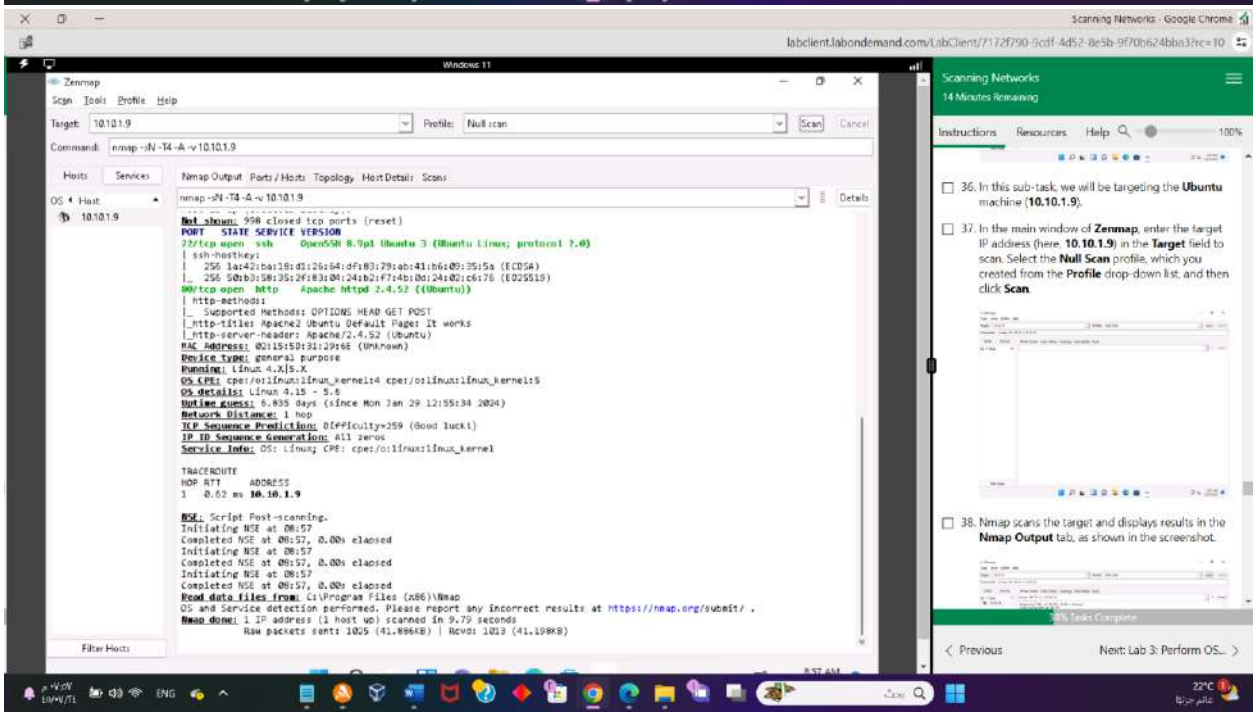

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan
Cancel
Command: nmap -sU -v 10.10.1.22
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.22
Details
Host is up (0.00067s latency).
Not shown: 971 closed udp ports (port-unreach)
PORT STATE SERVICE
53/udp open domain
88/udp open|filtered kerberos-sec
123/udp open ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
161/udp open snmp
389/udp open ldap
464/udp open|filtered kpasswd5
500/udp open|filtered isakmp
3389/udp open|filtered ms-wbt-server
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
53006/udp open|filtered unknown
53037/udp open|filtered unknown
53571/udp open|filtered unknown
53589/udp open|filtered unknown
53838/udp open|filtered unknown
61024/udp open|filtered unknown
61142/udp open|filtered unknown
61319/udp open|filtered unknown
61322/udp open|filtered unknown
61370/udp open|filtered unknown
61412/udp open|filtered unknown
61481/udp open|filtered unknown
61550/udp open|filtered unknown
61685/udp open|filtered unknown
61961/udp open|filtered unknown
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1238.81 seconds
Raw packets sent: 1337 (58.925KB) | Rcvd: 1007 (74.931KB)
Filter Hosts
Scanning Networks
22 Minutes Remaining
Instructions
Resources
Help
100%
This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.
The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.
27. Close the Zenmap window.
28. You can create your scan profile, or you can also
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

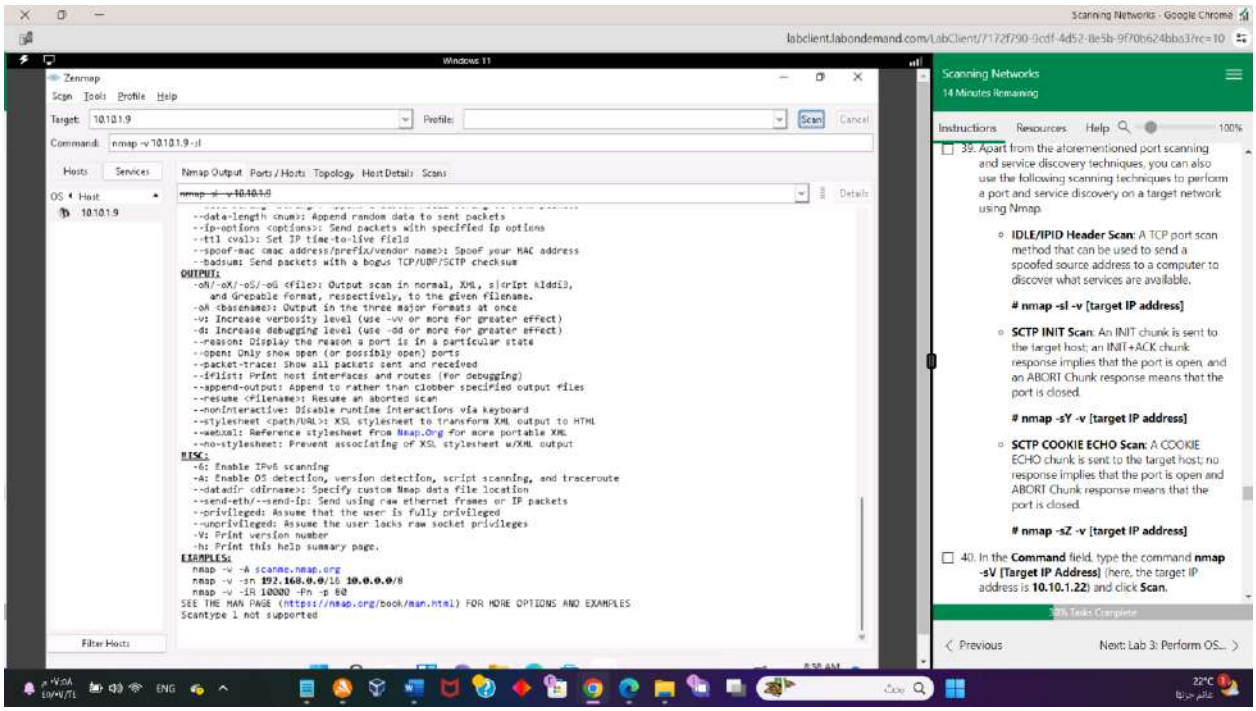

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Details
Profile Editor
nmap -T4 -A -v
Scan
Profile Scan Ping Scripting Target Source Other Timing
Profile Information
Profile name: Null scan
Description
Help
Description
The description is a full description of what the scan does, which may be long.
Cancel
Save Changes
Filter Hosts
Scanning Networks
19 Minutes Remaining
Instructions
Resources
Help
100%
32. The Profile Editor window appears. In the Profile tab, under the Profile Information section, input a profile name (here, Null Scan) into the Profile name field.
33. Now, click the Scan tab and select the scan option (here, Null scan (-sN)) from the TCP scan drop-down list.
34. Select None in the Non-TCP scans drop-down list and Aggressive (-T4) in the Timing template list. Ensure that the Enable all
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

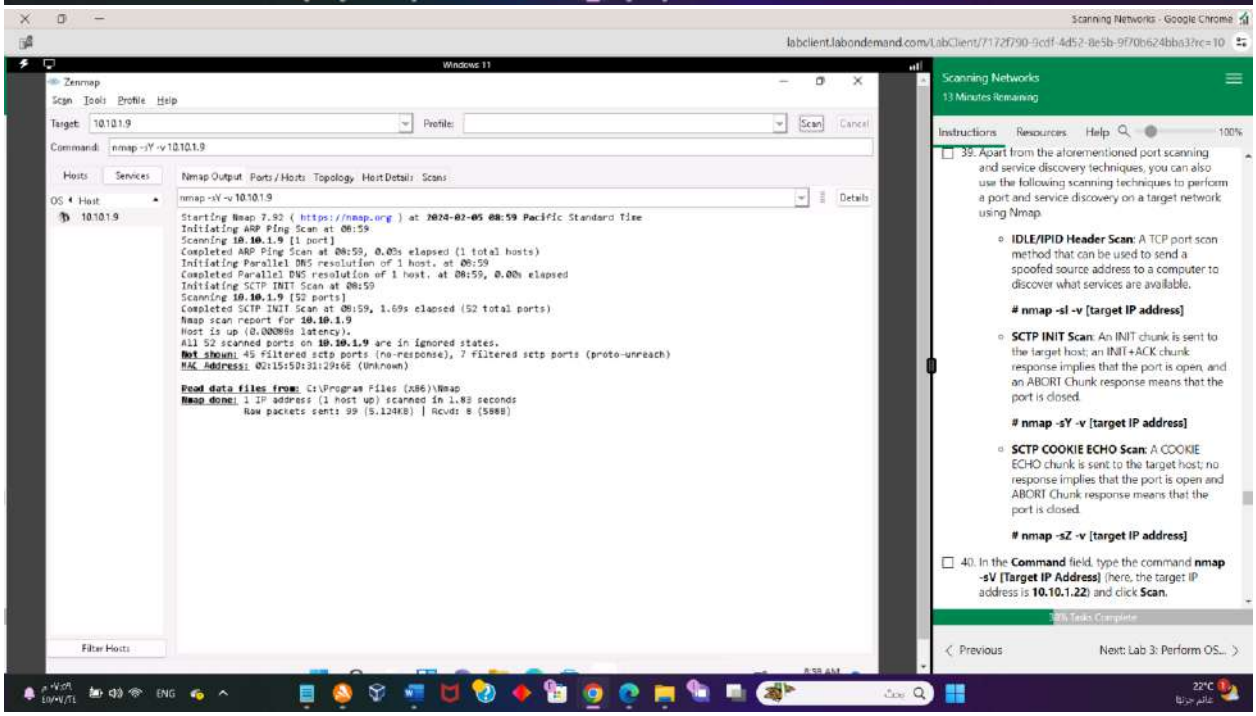

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
nmap -T4 -A -v
Details
NSE: Script Pre-scanning.
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
NSE: Script Post-scanning.
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
Initiating NSE at 08:52
Completed NSE at 08:52, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.63 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
Filter Hosts
Scanning Networks
19 Minutes Remaining
Instructions
Resources
Help
100%
33. Now, click the Scan tab and select the scan option (here, Null scan (-sN)) from the TCP scan drop-down list.
34. Select None in the Non-TCP scans drop-down list and Aggressive (-T4) in the Timing template list. Ensure that the Enable all advanced/aggressive options (-A) checkbox is selected and click Save Changes, as shown in the screenshot.
Using this configuration, you are setting Nmap to perform a null scan with the time template as -T4 and all aggressive options enabled.
35. This will create a new profile, and will thus be added to the profile list.
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

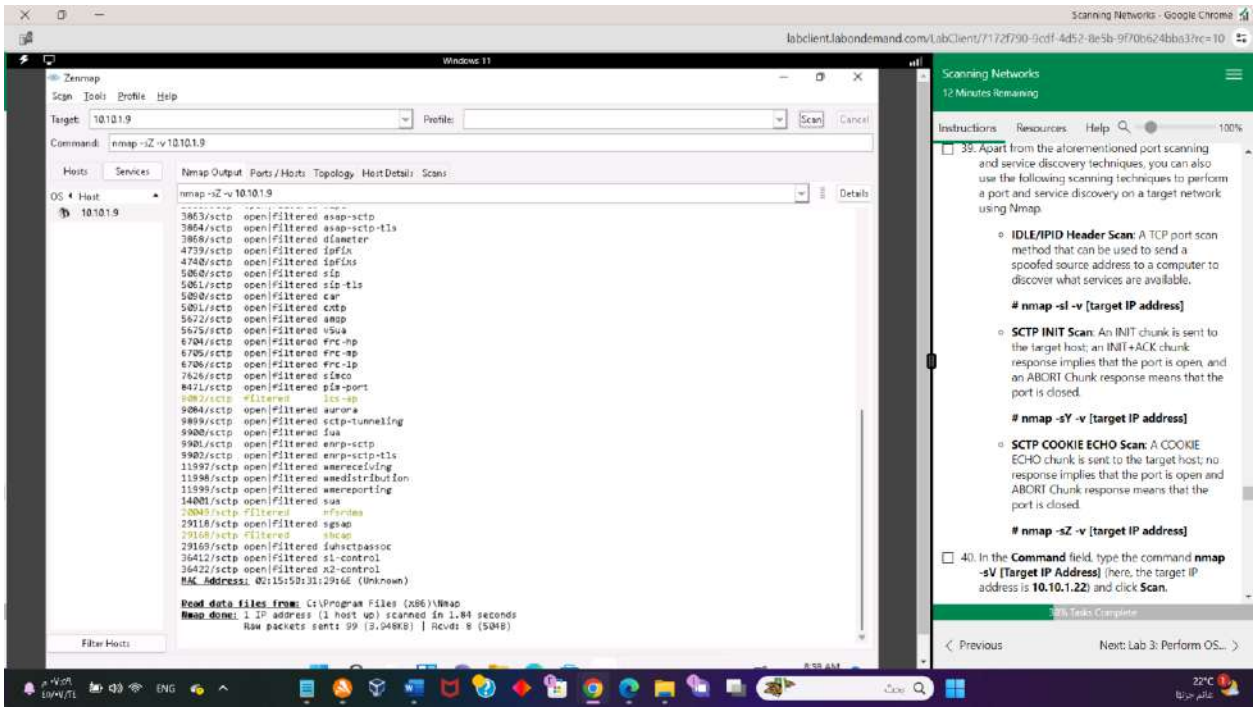

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
nmap -T4 -A -v
Details
Profile Editor
nmap -sN -T4 -A -v
Scan
Profile Scan Ping Scripting Target Source Other Timing
Scan options
Targets (optional):
TCP scan: Null scan (-sN)
Non-TCP scans: None
Timing template: Aggressive (-T4)
Enable all advanced/aggressive options (-A)
Operating system detection (-O)
Version detection (-sV)
Idle Scan (Zombie) (-sI)
FTP bounce attack (-b)
Disable reverse DNS resolution (-n)
IPv6 support (-6)
Help
Version detection
Attempt to discover the version number of services running on remote ports.
Cancel
Save Changes
Filter Hosts
Scanning Networks
18 Minutes Remaining
Instructions
Resources
Help
100%
33. Now, click the Scan tab and select the scan option (here, Null scan (-sN)) from the TCP scan drop-down list.
34. Select None in the Non-TCP scans drop-down list and Aggressive (-T4) in the Timing template list. Ensure that the Enable all advanced/aggressive options (-A) checkbox is selected and click Save Changes, as shown in the screenshot.
Using this configuration, you are setting Nmap to perform a null scan with the time template as -T4 and all aggressive options enabled.
35. This will create a new profile, and will thus be added to the profile list.
33% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

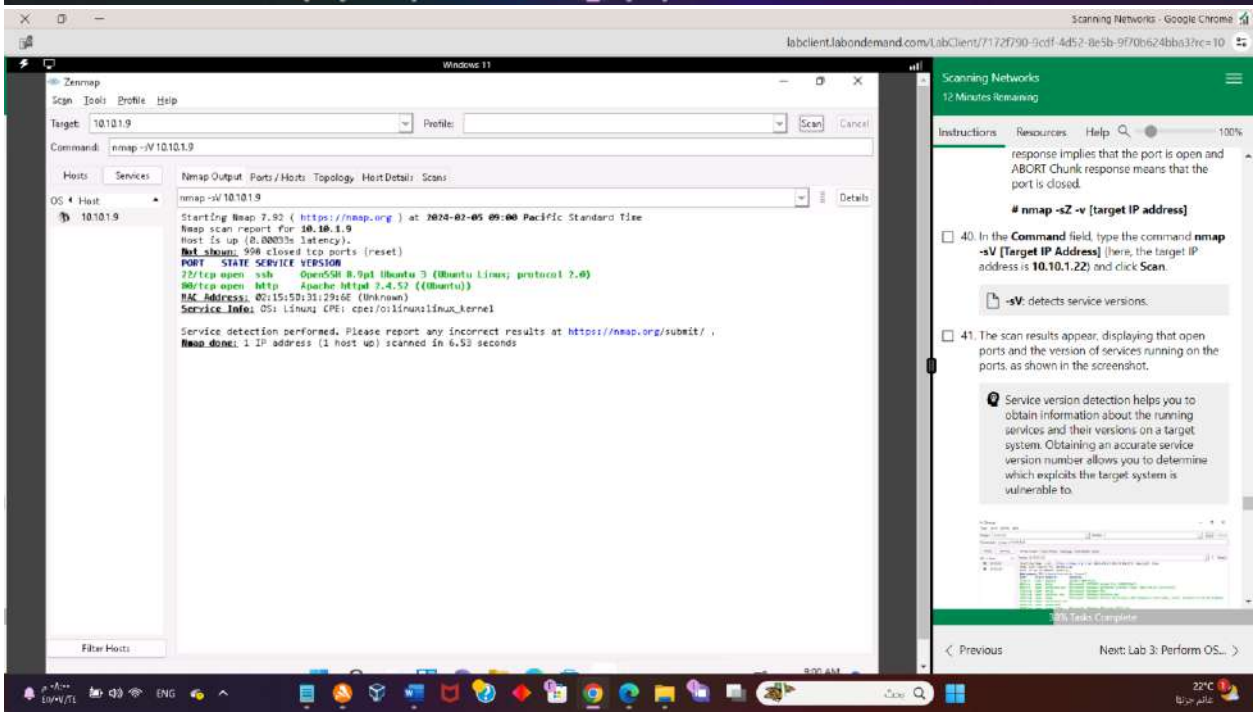

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile: Null scan
Scan
Cancel
Command: nmap -sN -T4 -A -v 10.10.1.9
Hosts
Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sN -T4 -A -v 10.10.1.9
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 08:57 Pacific Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Initiating ARP Ping Scan at 08:57
Scanning 10.10.1.9 [1 port]
Completed ARP Ping Scan at 08:57, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:57
Completed Parallel DNS resolution of 1 host. at 08:57, 0.01s elapsed
Initiating NULL Scan at 08:57
Filter Hosts
Scanning Networks
15 Minutes Remaining
Instructions
Resources
Help
100%
36. In this sub-task, we will be targeting the Ubuntu machine (10.10.1.9).
37. In the main window of Zenmap, enter the target IP address (here, 10.10.1.9) in the Target field to scan. Select the Null Scan profile, which you created from the Profile drop-down list, and then click Scan.
38. Nmap scans the target and displays results in the Nmap Output tab, as shown in the screenshot.
Previous
Next: Lab 3: Perform OS...
22°C

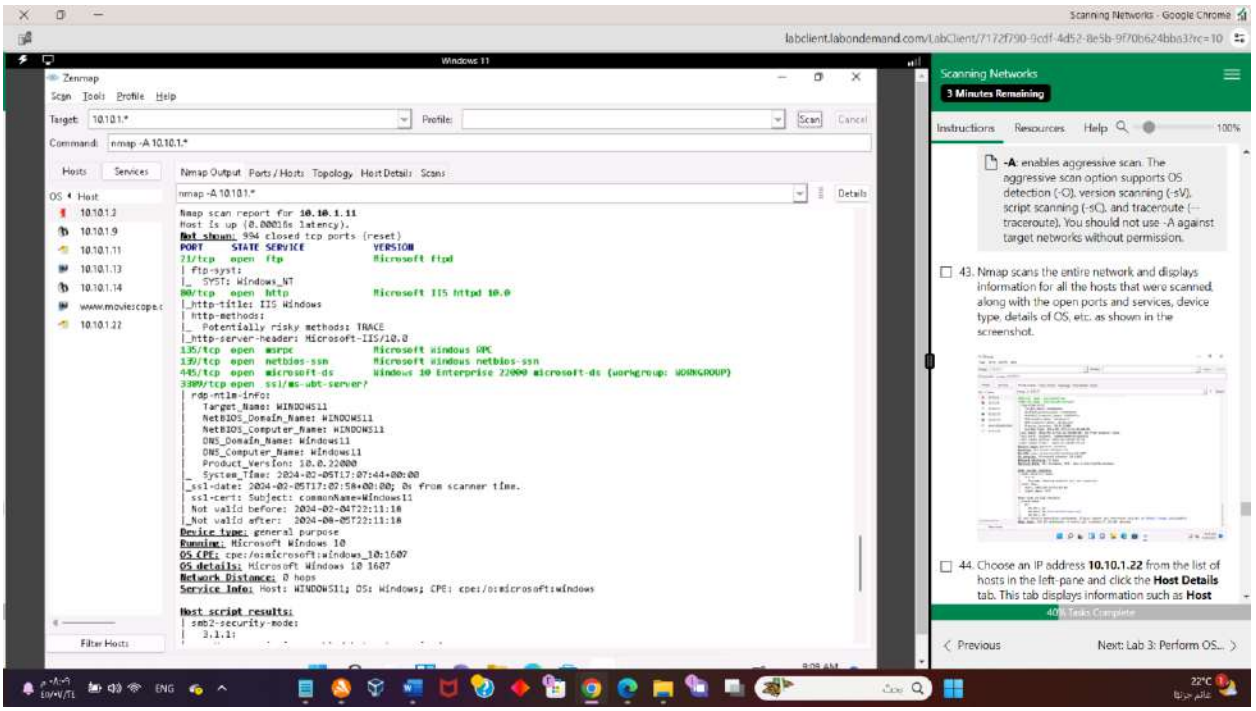

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile: Null scan
Scan
Cancel
Command: nmap -sN -T4 -A -v 10.10.1.9
Hosts
Services
OS Host
10.10.1.9
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sN -T4 -A -v 10.10.1.9
Details
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 1a:42:ba:18:d1:26:64:df:83:79:ab:41:b6:09:35:5a (ECDSA)
|_ 256 50:b3:58:35:2f:83:04:24:b2:f7:4b:0d:24:02:c6:76 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:15:5D:31:29:6E (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 6.835 days (since Mon Jan 29 12:55:34 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE
HOP RTT ADDRESS
1 0.62 ms 10.10.1.9
NSE: Script Post-scanning.
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Initiating NSE at 08:57
Completed NSE at 08:57, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
Raw packets sent: 1025 (41.886KB) | Rcvd: 1013 (41.198KB)
Filter Hosts
Scanning Networks
14 Minutes Remaining
Instructions
Resources
Help
100%
36. In this sub-task, we will be targeting the Ubuntu machine (10.10.1.9).
37. In the main window of Zenmap, enter the target IP address (here, 10.10.1.9) in the Target field to scan. Select the Null Scan profile, which you created from the Profile drop-down list, and then click Scan.
38. Nmap scans the target and displays results in the Nmap Output tab, as shown in the screenshot.
Previous
Next: Lab 3: Perform OS...
22°C

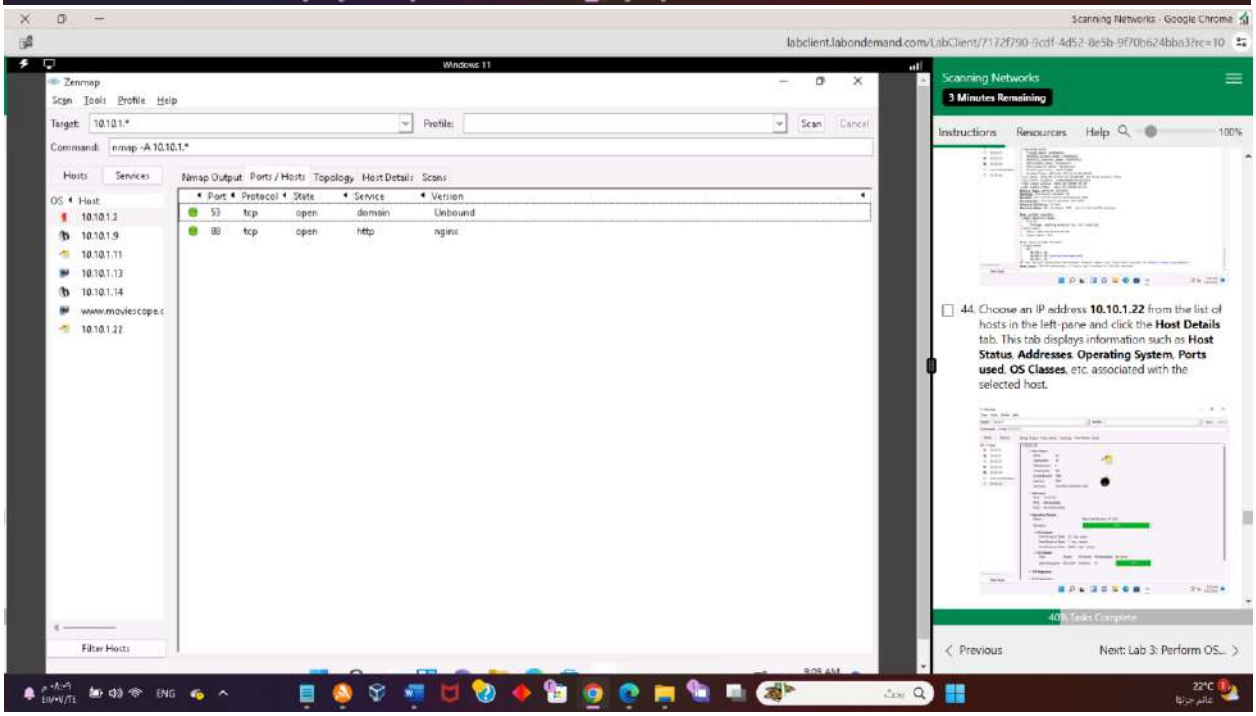

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile:
Scan
Cancel
Command: nmap -v 10.10.1.9 -sI
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.9
Details
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdd3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype 1 not supported
Filter Hosts
Scanning Networks
14 Minutes Remaining
Instructions
Resources
Help
100%
39. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.
IDLE/IPID Header Scan: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.
nmap -sI -v [target IP address]
SCTP INIT Scan: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.
nmap -sY -v [target IP address]
SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.
nmap -sZ -v [target IP address]
40. In the Command field, type the command nmap -sV [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
Previous
Next: Lab 3: Perform OS...
22°C

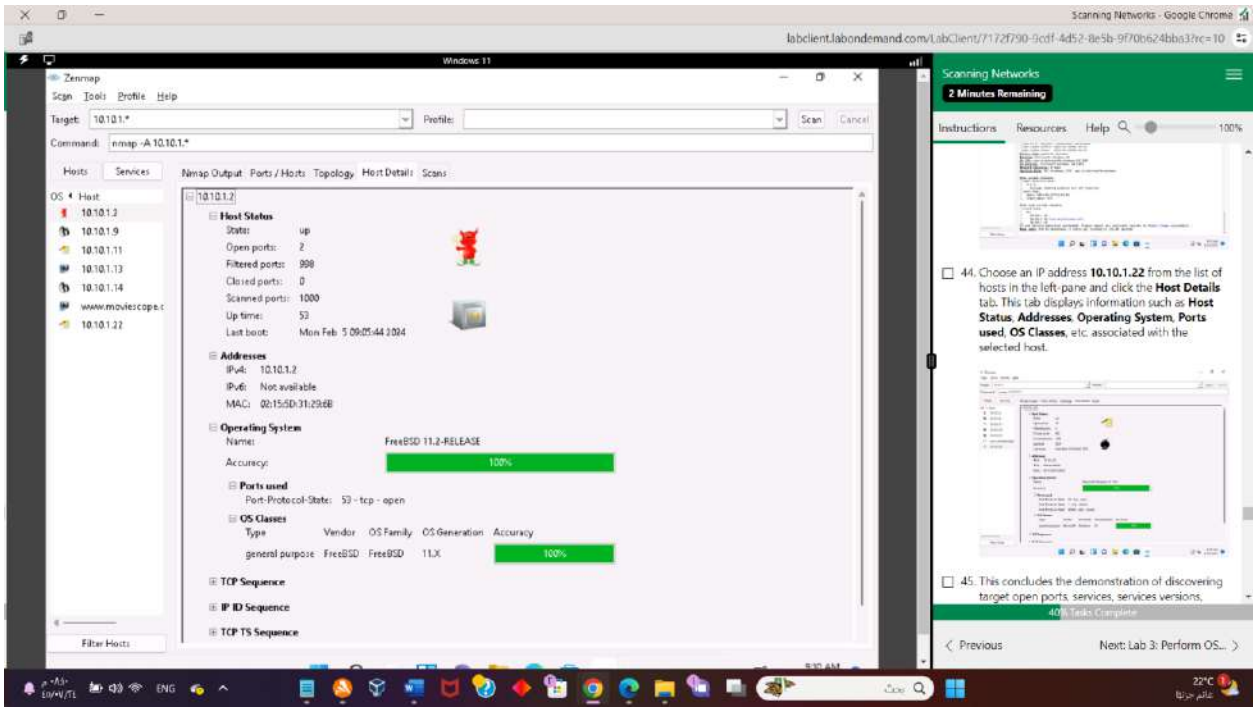

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile:
Scan
Cancel
Command: nmap -sY -v 10.10.1.9
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.9
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 08:59 Pacific Standard Time
Initiating ARP Ping Scan at 08:59
Scanning 10.10.1.9 [1 port]
Completed ARP Ping Scan at 08:59, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:59
Completed Parallel DNS resolution of 1 host. at 08:59, 0.00s elapsed
Initiating SCTP INIT Scan at 08:59
Scanning 10.10.1.9 [52 ports]
Completed SCTP INIT Scan at 08:59, 1.69s elapsed (52 total ports)
Nmap scan report for 10.10.1.9
Host is up (0.00086s latency).
All 52 scanned ports on 10.10.1.9 are in ignored states.
Not shown: 45 filtered sctp ports (no-response), 7 filtered sctp ports (proto-unreach)
MAC Address: 02:15:5D:31:29:6E (Unknown)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
Raw packets sent: 99 (5.124KB) | Rcvd: 8 (588B)
Filter Hosts
Scanning Networks
13 Minutes Remaining
Instructions
Resources
Help
100%
39. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.
IDLE/IPID Header Scan: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.
nmap -sI -v [target IP address]
SCTP INIT Scan: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.
nmap -sY -v [target IP address]
SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.
nmap -sZ -v [target IP address]
40. In the Command field, type the command nmap -sV [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
Previous
Next: Lab 3: Perform OS...
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile:
Scan
Cancel
Command: nmap -sZ -v 10.10.1.9
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.9
Details
3863/sctp open|filtered asap-sctp
3864/sctp open|filtered asap-sctp-tls
3868/sctp open|filtered diameter
4739/sctp open|filtered ipfix
4740/sctp open|filtered ipfixs
5060/sctp open|filtered sip
5061/sctp open|filtered sip-tls
5090/sctp open|filtered car
5091/sctp open|filtered cxtp
5672/sctp open|filtered amqp
5675/sctp open|filtered v5ua
6704/sctp open|filtered frc-hp
6705/sctp open|filtered frc-mp
6706/sctp open|filtered frc-lp
7626/sctp open|filtered simco
8471/sctp open|filtered pim-port
9084/sctp open|filtered aurora
9899/sctp open|filtered sctp-tunneling
9900/sctp open|filtered iua
9901/sctp open|filtered enrp-sctp
9902/sctp open|filtered enrp-sctp-tls
11997/sctp open|filtered wmereceiving
11998/sctp open|filtered wmedistribution
11999/sctp open|filtered wmereporting
14001/sctp open|filtered sua
29118/sctp open|filtered sgsap
29169/sctp open|filtered iuhsctpassoc
36412/sctp open|filtered s1-control
36422/sctp open|filtered x2-control
MAC Address: 02:15:5D:31:29:6E (Unknown)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
Raw packets sent: 99 (3.948KB) | Rcvd: 8 (504B)
Filter Hosts
Scanning Networks
12 Minutes Remaining
Instructions
Resources
Help
100%
39. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.
IDLE/IPID Header Scan: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.
nmap -sI -v [target IP address]
SCTP INIT Scan: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.
nmap -sY -v [target IP address]
SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.
nmap -sZ -v [target IP address]
40. In the Command field, type the command nmap -sV [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
Previous
Next: Lab 3: Perform OS...
22°C

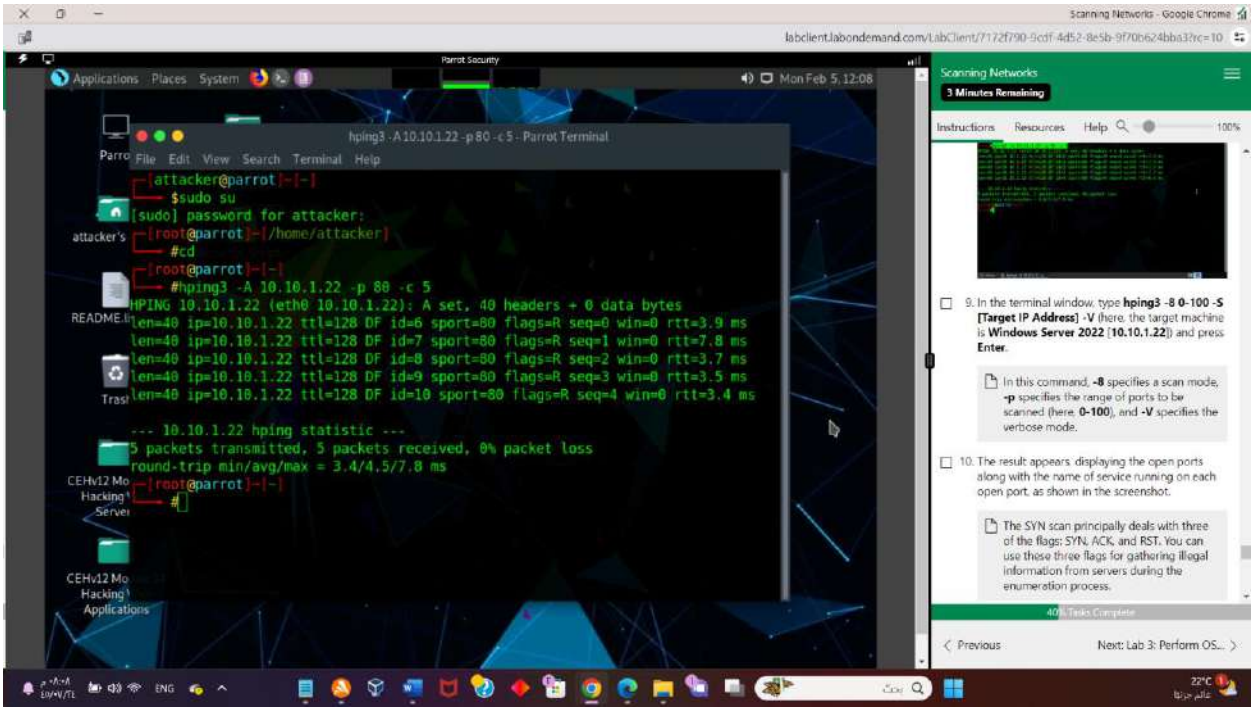

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.9
Profile:
Scan
Cancel
Command: nmap -sV 10.10.1.9
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.9
Details
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 09:00 Pacific Standard Time
Nmap scan report for 10.10.1.9
Host is up (0.00033s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 02:15:5D:31:29:6E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
Filter Hosts
Scanning Networks
12 Minutes Remaining
Instructions
Resources
Help
100%
response implies that the port is open and ABORT Chunk response means that the port is closed.
nmap -sZ -v [target IP address]
40. In the Command field, type the command nmap -sV [Target IP Address] (here, the target IP address is 10.10.1.22) and click Scan.
-sV: detects service versions.
41. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.
Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.
Previous
Next: Lab 3: Perform OS...
22°C

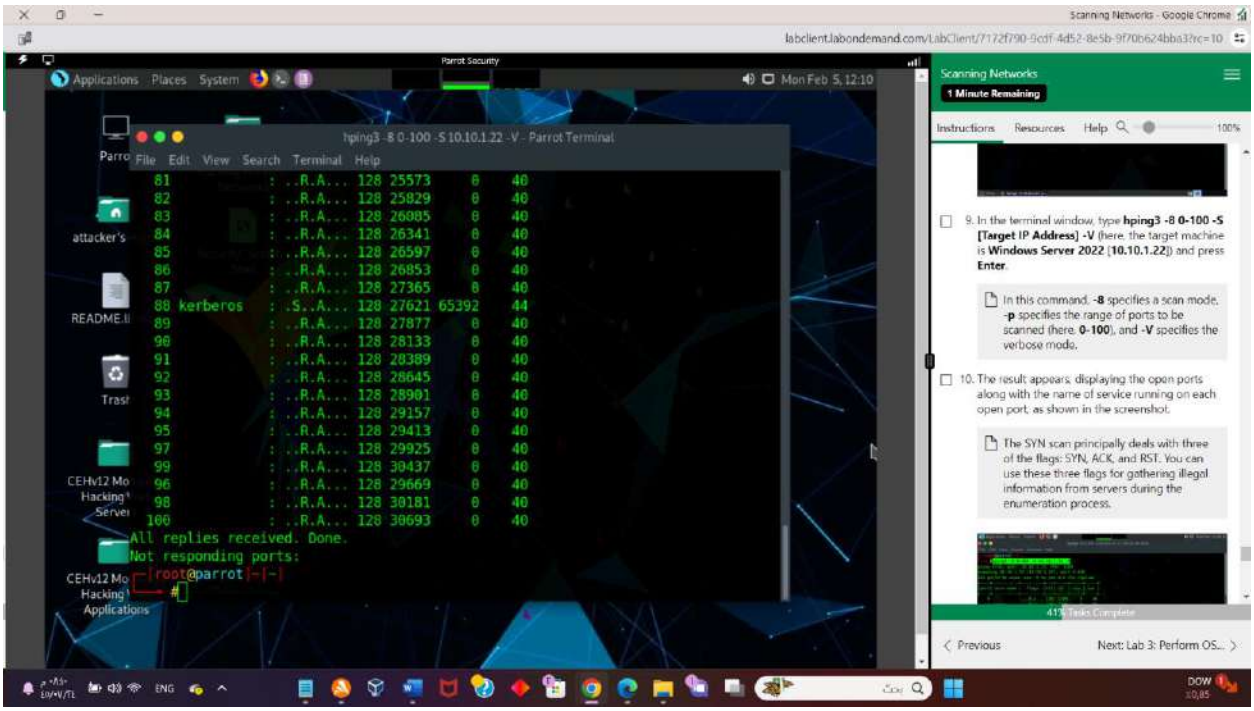

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.*
Profile:
Scan
Cancel
Command: nmap -A 10.10.1.*
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.10.1.3
10.10.1.9
10.10.1.11
10.10.1.13
10.10.1.14
www.moviescope.c
10.10.1.22
Filter Hosts
Nmap scan report for 10.10.1.11
Host is up (0.00016s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 10 Enterprise 22000 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open ssl/ms-wbt-server?
| rdp-ntlm-info:
| Target_Name: WINDOWS11
| NetBIOS_Domain_Name: WINDOWS11
| NetBIOS_Computer_Name: WINDOWS11
| DNS_Domain_Name: Windows11
| DNS_Computer_Name: Windows11
| Product_Version: 10.0.22000
|_ System_Time: 2024-02-05T17:07:44+00:00
|_ssl-date: 2024-02-05T17:07:58+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Windows11
| Not valid before: 2024-02-04T22:11:18
|_Not valid after: 2024-08-05T22:11:18
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops
Service Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3.1.1:
Details
Scanning Networks
3 Minutes Remaining
Instructions
Resources
Help
100%
-A: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.
43. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot.
44. Choose an IP address 10.10.1.22 from the list of hosts in the left-pane and click the Host Details tab. This tab displays information such as Host
40% Tasks Complete
Previous
Next: Lab 3: Perform OS...
22°C

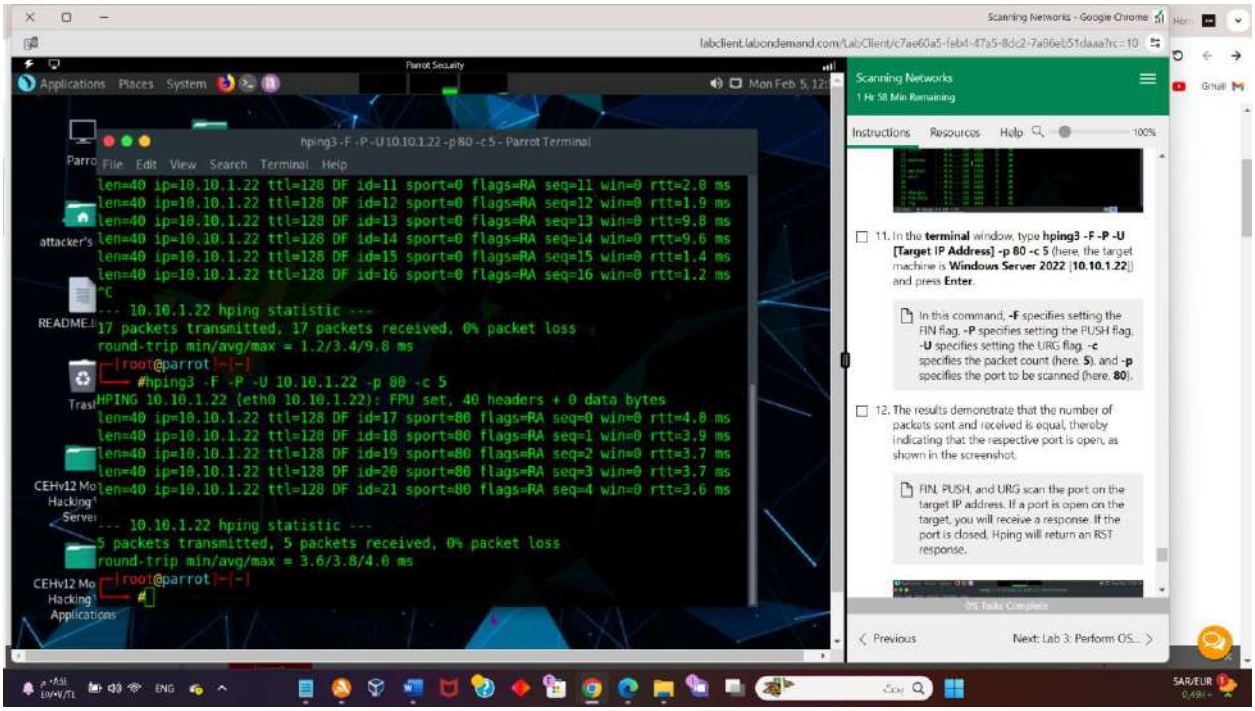

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.*
Profile:
Scan
Cancel
Command: nmap -A 10.10.1.*
Hosts
Services
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
53 tcp open domain Unbound
80 tcp open http nginx
OS Host
10.10.1.3
10.10.1.9
10.10.1.11
10.10.1.13
10.10.1.14
www.moviescope.c
10.10.1.22
Filter Hosts
Scanning Networks
3 Minutes Remaining
Instructions
Resources
Help
100%
44. Choose an IP address 10.10.1.22 from the list of hosts in the left-pane and click the Host Details tab. This tab displays information such as Host Status, Addresses, Operating System, Ports used, OS Classes, etc. associated with the selected host.
40% Tasks Complete
Previous
Next: Lab 3: Perform OS...
22°C

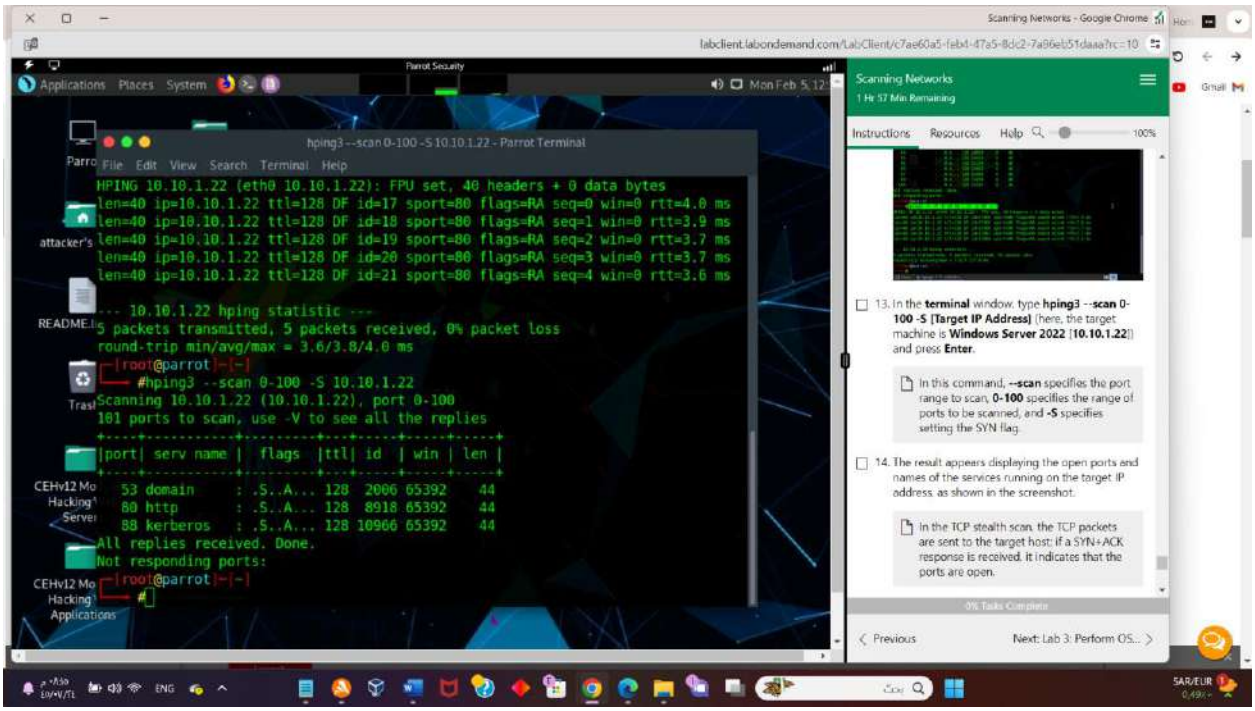


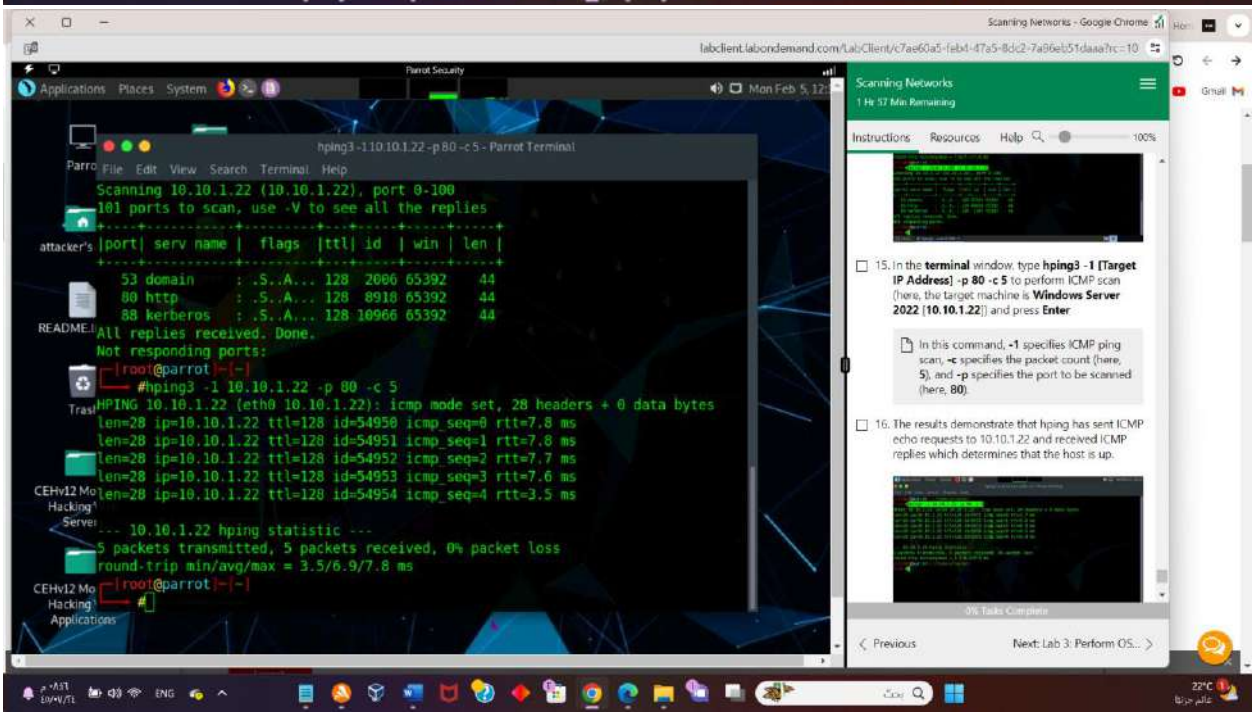
Lab 02 – Task 05

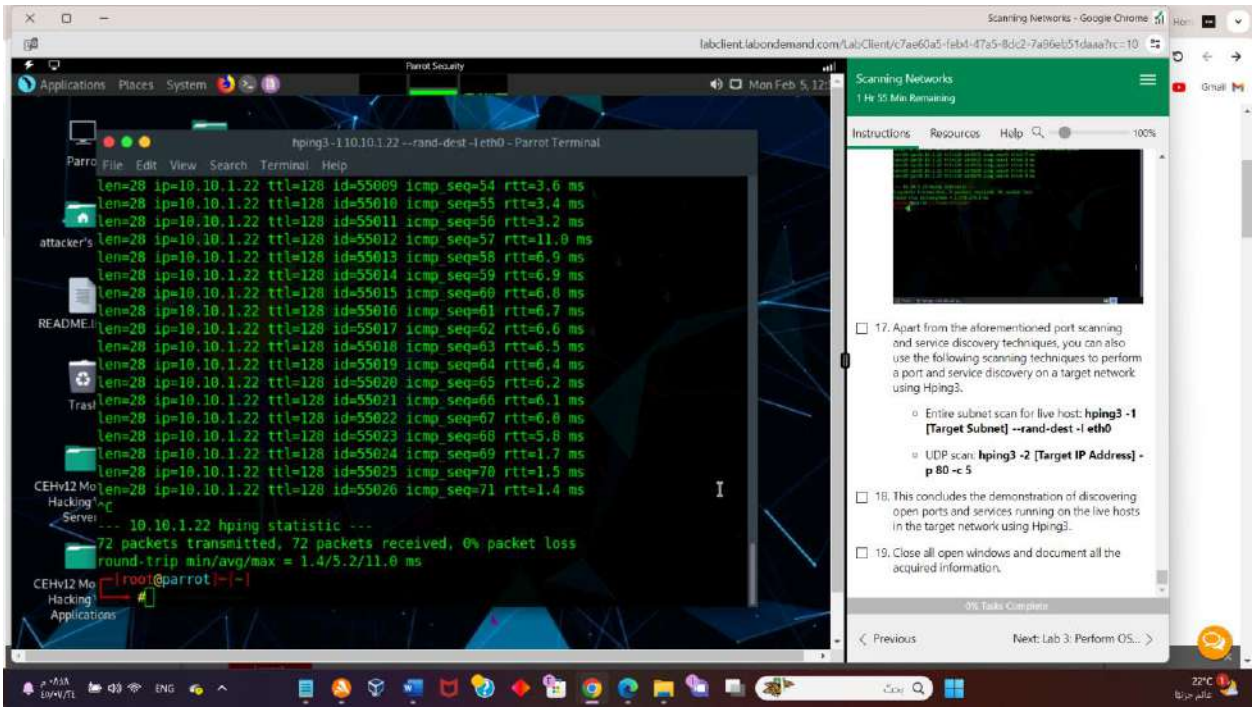


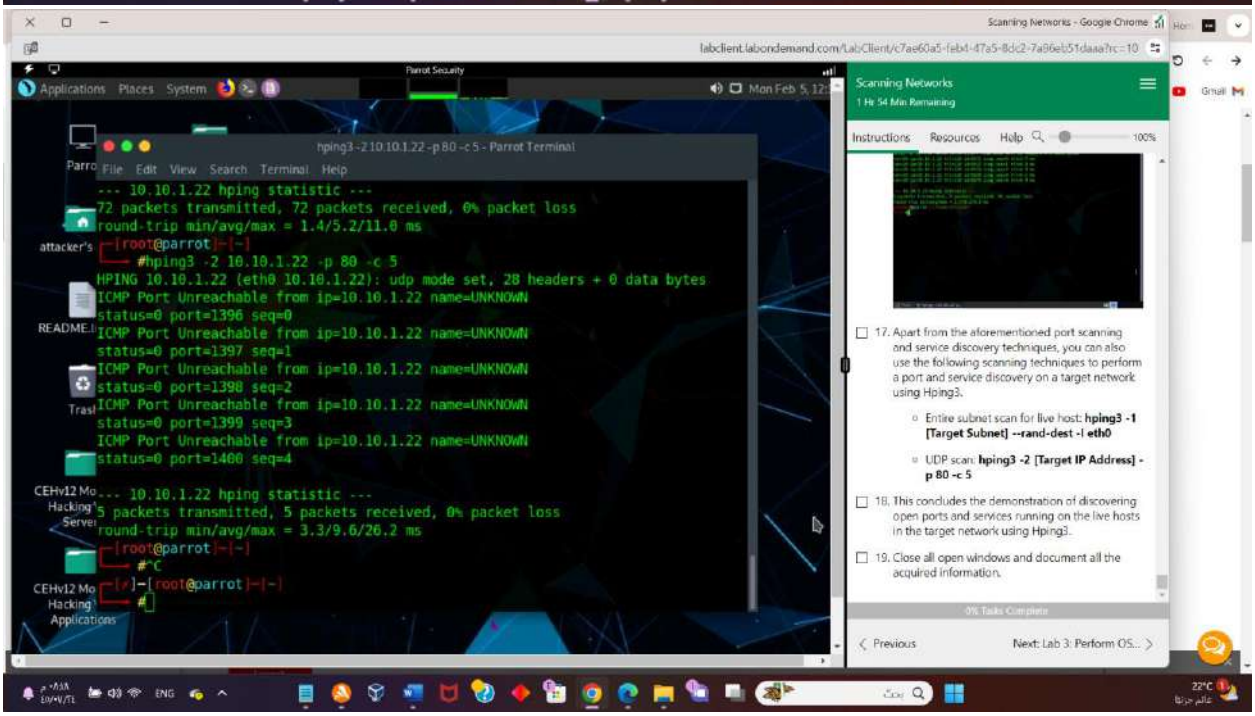

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 12:10
hping3 -8 0-100 -S 10.10.1.22 -V - Parrot Terminal
File Edit View Search Terminal Help
81 : ..R.A... 128 25573 0 40
82 : ..R.A... 128 25829 0 40
83 : ..R.A... 128 26085 0 40
84 : ..R.A... 128 26341 0 40
85 : ..R.A... 128 26597 0 40
86 : ..R.A... 128 26853 0 40
87 : ..R.A... 128 27365 0 40
88 kerberos : .S..A... 128 27621 65392 44
89 : ..R.A... 128 27877 0 40
90 : ..R.A... 128 28133 0 40
91 : ..R.A... 128 28389 0 40
92 : ..R.A... 128 28645 0 40
93 : ..R.A... 128 28901 0 40
94 : ..R.A... 128 29157 0 40
95 : ..R.A... 128 29413 0 40
97 : ..R.A... 128 29925 0 40
99 : ..R.A... 128 30437 0 40
96 : ..R.A... 128 29669 0 40
98 : ..R.A... 128 30181 0 40
100 : ..R.A... 128 30693 0 40
All replies received. Done.
Not responding ports:
root@parrot
#
Scanning Networks
1 Minute Remaining
Instructions Resources Help
9. In the terminal window, type hping3 -8 0-100 -S [Target IP Address] -V (here, the target machine is Windows Server 2022 (10.10.1.22)) and press Enter.
In this command, -8 specifies a scan mode, -p specifies the range of ports to be scanned (here, 0-100), and -V specifies the verbose mode.
10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.
The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.
41% Tasks Complete
Previous
Next: Lab 3: Perform OS...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/c7ae60a5-febd-47a5-8dc2-7a86eb51daaa?rc=10
Parrot Security
Applications Places System
hping3 -F -P -U 10.10.1.22 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
len=40 ip=10.10.1.22 ttl=128 DF id=11 sport=0 flags=RA seq=11 win=0 rtt=2.0 ms
len=40 ip=10.10.1.22 ttl=128 DF id=12 sport=0 flags=RA seq=12 win=0 rtt=1.9 ms
len=40 ip=10.10.1.22 ttl=128 DF id=13 sport=0 flags=RA seq=13 win=0 rtt=9.8 ms
len=40 ip=10.10.1.22 ttl=128 DF id=14 sport=0 flags=RA seq=14 win=0 rtt=9.6 ms
len=40 ip=10.10.1.22 ttl=128 DF id=15 sport=0 flags=RA seq=15 win=0 rtt=1.4 ms
len=40 ip=10.10.1.22 ttl=128 DF id=16 sport=0 flags=RA seq=16 win=0 rtt=1.2 ms
^C
--- 10.10.1.22 hping statistic ---
17 packets transmitted, 17 packets received, 0% packet loss
round-trip min/avg/max = 1.2/3.4/9.8 ms
root@parrot
#hping3 -F -P -U 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): FPU set, 40 headers + 0 data bytes
len=40 ip=10.10.1.22 ttl=128 DF id=17 sport=80 flags=RA seq=0 win=0 rtt=4.8 ms
len=40 ip=10.10.1.22 ttl=128 DF id=18 sport=80 flags=RA seq=1 win=0 rtt=3.9 ms
len=40 ip=10.10.1.22 ttl=128 DF id=19 sport=80 flags=RA seq=2 win=0 rtt=3.7 ms
len=40 ip=10.10.1.22 ttl=128 DF id=20 sport=80 flags=RA seq=3 win=0 rtt=3.7 ms
len=40 ip=10.10.1.22 ttl=128 DF id=21 sport=80 flags=RA seq=4 win=0 rtt=3.6 ms
--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.6/3.8/4.0 ms
root@parrot
#
Scanning Networks
1 Hr 58 Min Remaining
Instructions Resources Help
11. In the terminal window, type hping3 -F -P -U [Target IP Address] -p 80 -c 5 (here, the target machine is Windows Server 2022 (10.10.1.22)) and press Enter.
In this command, -F specifies setting the FIN flag, -P specifies setting the PUSH flag, -U specifies setting the URG flag, -c specifies the packet count (here, 5), and -p specifies the port to be scanned (here, 80).
12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.
FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will receive a response. If the port is closed, Hping will return an RST response.
0% Tasks Complete
Previous
Next: Lab 3: Perform OS...

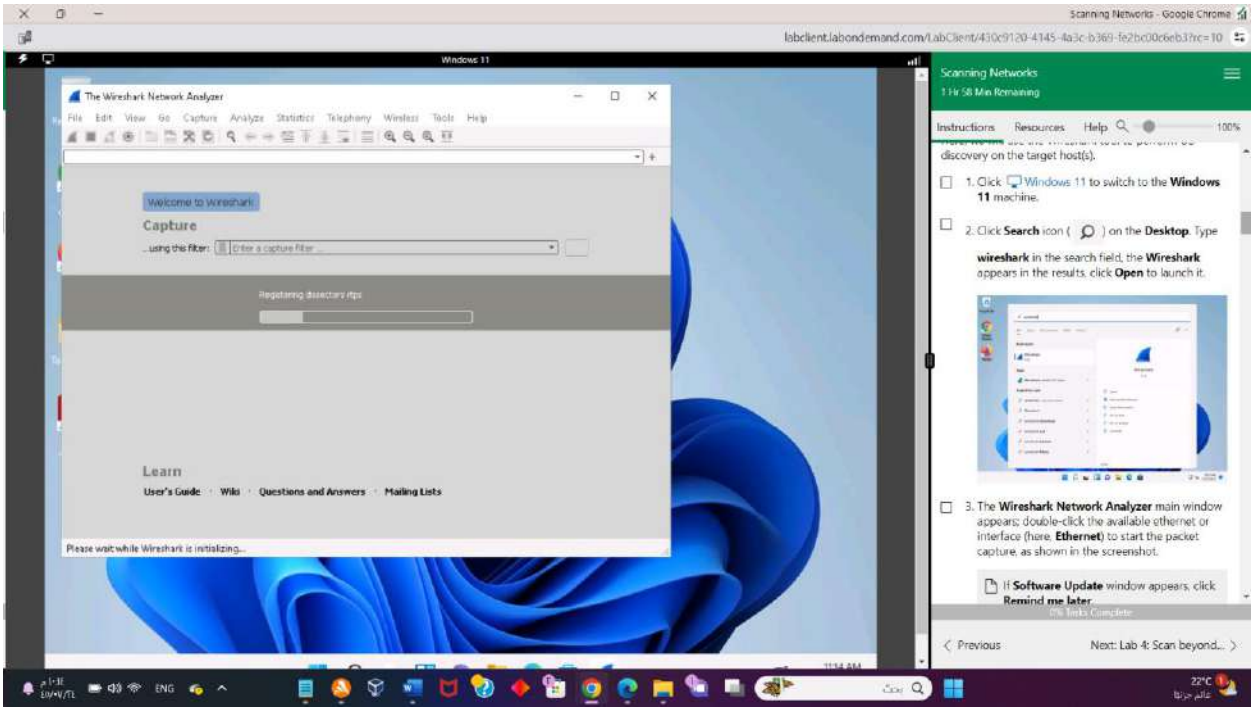

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/c7ae60a5-febd-47a5-8dc2-7a86eb51daaa?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 12:
hping3 --scan 0-100 -S 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
HPING 10.10.1.22 (eth0 10.10.1.22): FPU set, 40 headers + 0 data bytes
len=40 ip=10.10.1.22 ttl=128 DF id=17 sport=80 flags=RA seq=0 win=0 rtt=4.0 ms
len=40 ip=10.10.1.22 ttl=128 DF id=18 sport=80 flags=RA seq=1 win=0 rtt=3.9 ms
len=40 ip=10.10.1.22 ttl=128 DF id=19 sport=80 flags=RA seq=2 win=0 rtt=3.7 ms
len=40 ip=10.10.1.22 ttl=128 DF id=20 sport=80 flags=RA seq=3 win=0 rtt=3.7 ms
len=40 ip=10.10.1.22 ttl=128 DF id=21 sport=80 flags=RA seq=4 win=0 rtt=3.6 ms
--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.6/3.8/4.0 ms
[root@parrot]-[~]
#hping3 --scan 0-100 -S 10.10.1.22
Scanning 10.10.1.22 (10.10.1.22), port 0-100
101 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
53 domain : .S..A... 128 2006 65392 44
80 http : .S..A... 128 8918 65392 44
88 kerberos : .S..A... 128 10966 65392 44
All replies received. Done.
Not responding ports:
[root@parrot]-[~]
#
attacker's
README.
Trash
CEHv12 Mo
Hacking
Server
Applications
Scanning Networks
1 Hr 57 Min Remaining
Instructions Resources Help 100%
13. In the terminal window, type hping3 --scan 0-100 -S [Target IP Address] (here, the target machine is Windows Server 2022 [10.10.1.22]) and press Enter.
In this command, --scan specifies the port range to scan, 0-100 specifies the range of ports to be scanned, and -S specifies setting the SYN flag.
14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.
In the TCP stealth scan, the TCP packets are sent to the target host. If a SYN+ACK response is received, it indicates that the ports are open.
0% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
SAR/EUR

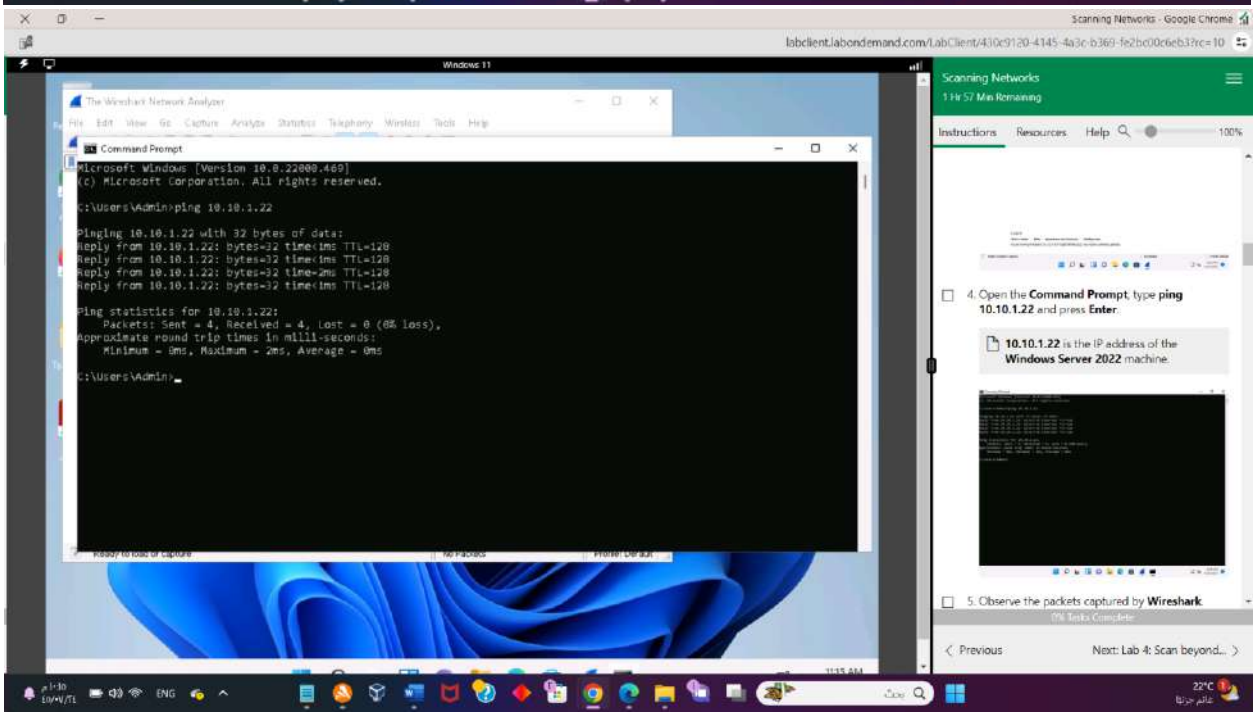

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/c7ae60a5-febd-47a5-8dc2-7a86eb51daaa?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 12:
hping3 -1 10.10.1.22 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
Scanning 10.10.1.22 (10.10.1.22), port 0-100
101 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
53 domain : .S..A... 128 2006 65392 44
80 http : .S..A... 128 8918 65392 44
88 kerberos : .S..A... 128 10966 65392 44
All replies received. Done.
Not responding ports:
[root@parrot]-[~]
#hping3 -1 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): icmp mode set, 28 headers + 0 data bytes
len=28 ip=10.10.1.22 ttl=128 id=54950 icmp_seq=0 rtt=7.8 ms
len=28 ip=10.10.1.22 ttl=128 id=54951 icmp_seq=1 rtt=7.8 ms
len=28 ip=10.10.1.22 ttl=128 id=54952 icmp_seq=2 rtt=7.7 ms
len=28 ip=10.10.1.22 ttl=128 id=54953 icmp_seq=3 rtt=7.6 ms
len=28 ip=10.10.1.22 ttl=128 id=54954 icmp_seq=4 rtt=3.5 ms
--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/6.9/7.8 ms
[root@parrot]-[~]
#
attacker's
README.
Trash
CEHv12 Mo
Hacking
Server
Applications
Scanning Networks
1 Hr 57 Min Remaining
Instructions Resources Help 100%
15. In the terminal window, type hping3 -1 [Target IP Address] -p 80 -c 5 to perform ICMP scan (here, the target machine is Windows Server 2022 [10.10.1.22]) and press Enter
In this command, -1 specifies ICMP ping scan, -c specifies the packet count (here, 5), and -p specifies the port to be scanned (here, 80).
16. The results demonstrate that hping has sent ICMP echo requests to 10.10.1.22 and received ICMP replies which determines that the host is up.
0% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

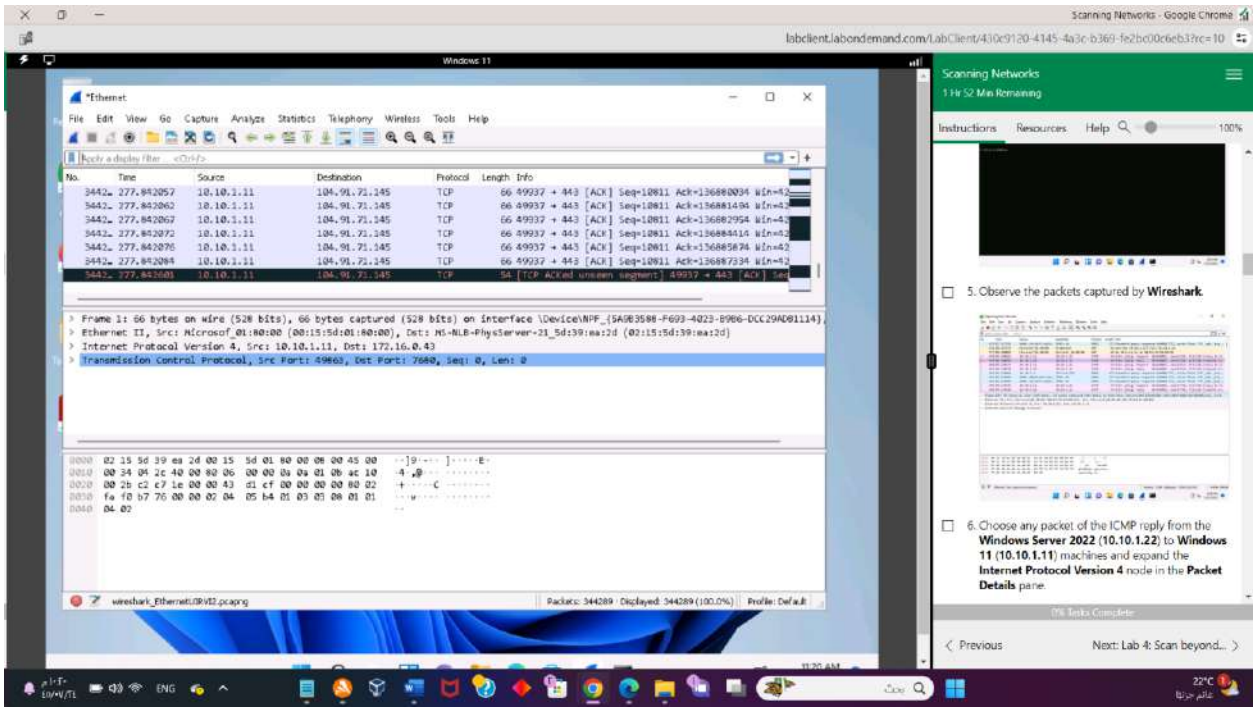

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/c7ae60a5-febd-47a5-8dc2-7a86eb51daaa?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 12:
hping3 -1 10.10.1.22 --rand-dest -I eth0 - Parrot Terminal
File Edit View Search Terminal Help
len=28 ip=10.10.1.22 ttl=128 id=55009 icmp_seq=54 rtt=3.6 ms
len=28 ip=10.10.1.22 ttl=128 id=55010 icmp_seq=55 rtt=3.4 ms
len=28 ip=10.10.1.22 ttl=128 id=55011 icmp_seq=56 rtt=3.2 ms
len=28 ip=10.10.1.22 ttl=128 id=55012 icmp_seq=57 rtt=11.0 ms
len=28 ip=10.10.1.22 ttl=128 id=55013 icmp_seq=58 rtt=6.9 ms
len=28 ip=10.10.1.22 ttl=128 id=55014 icmp_seq=59 rtt=6.9 ms
len=28 ip=10.10.1.22 ttl=128 id=55015 icmp_seq=60 rtt=6.8 ms
len=28 ip=10.10.1.22 ttl=128 id=55016 icmp_seq=61 rtt=6.7 ms
len=28 ip=10.10.1.22 ttl=128 id=55017 icmp_seq=62 rtt=6.6 ms
len=28 ip=10.10.1.22 ttl=128 id=55018 icmp_seq=63 rtt=6.5 ms
len=28 ip=10.10.1.22 ttl=128 id=55019 icmp_seq=64 rtt=6.4 ms
len=28 ip=10.10.1.22 ttl=128 id=55020 icmp_seq=65 rtt=6.2 ms
len=28 ip=10.10.1.22 ttl=128 id=55021 icmp_seq=66 rtt=6.1 ms
len=28 ip=10.10.1.22 ttl=128 id=55022 icmp_seq=67 rtt=6.0 ms
len=28 ip=10.10.1.22 ttl=128 id=55023 icmp_seq=68 rtt=5.8 ms
len=28 ip=10.10.1.22 ttl=128 id=55024 icmp_seq=69 rtt=1.7 ms
len=28 ip=10.10.1.22 ttl=128 id=55025 icmp_seq=70 rtt=1.5 ms
len=28 ip=10.10.1.22 ttl=128 id=55026 icmp_seq=71 rtt=1.4 ms
^C
--- 10.10.1.22 hping statistic ---
72 packets transmitted, 72 packets received, 0% packet loss
round-trip min/avg/max = 1.4/5.2/11.0 ms
[root@parrot]-[~]
#
attacker's
README.
Trash
CEHv12 Mo
Hacking
Server
CEHv12 Mo
Hacking
Applications
Scanning Networks
1 Hr 55 Min Remaining
Instructions
Resources
Help
100%
17. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.
Entire subnet scan for live host: hping3 -1 [Target Subnet] --rand-dest -I eth0
UDP scan: hping3 -2 [Target IP Address] -p 80 -c 5
18. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
19. Close all open windows and document all the acquired information.
0% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

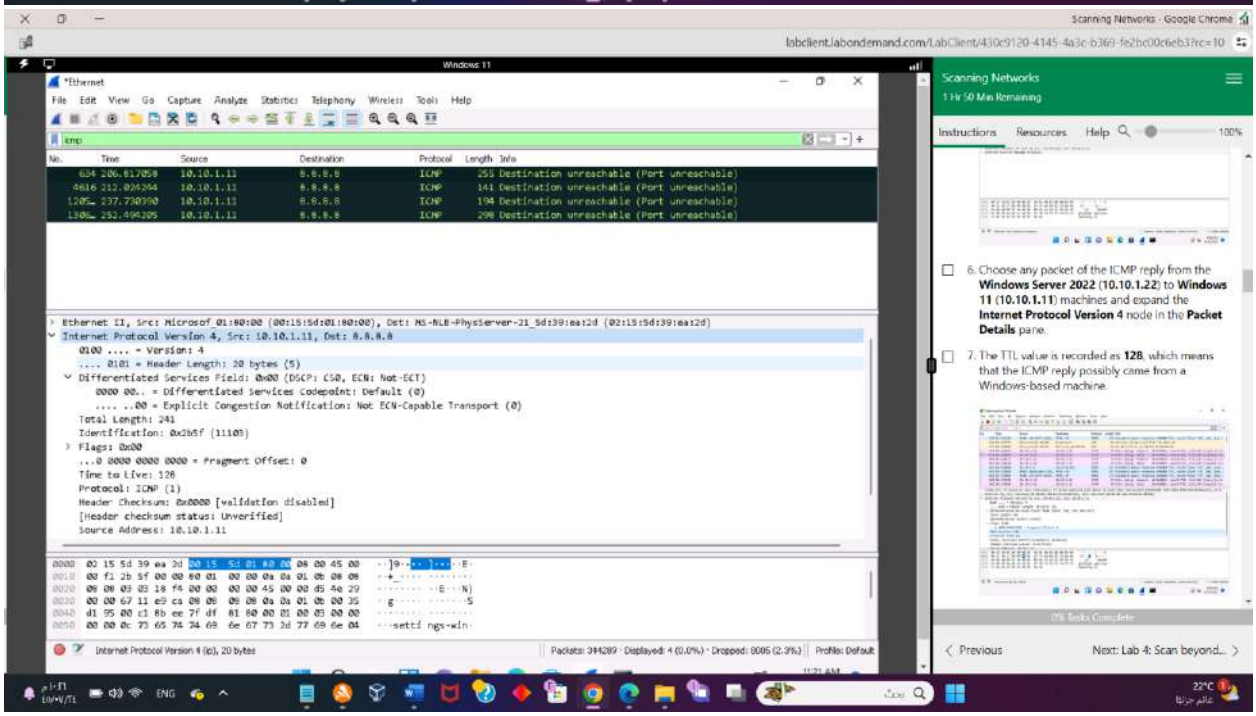

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/c7ae60a5-febd-47a5-8dc2-7a86eb51daaa?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 12:
hping3 -2 10.10.1.22 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
--- 10.10.1.22 hping statistic ---
72 packets transmitted, 72 packets received, 0% packet loss
round-trip min/avg/max = 1.4/5.2/11.0 ms
[root@parrot]-[~]
#hping3 -2 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=10.10.1.22 name=UNKNOWN
status=0 port=1396 seq=0
ICMP Port Unreachable from ip=10.10.1.22 name=UNKNOWN
status=0 port=1397 seq=1
ICMP Port Unreachable from ip=10.10.1.22 name=UNKNOWN
status=0 port=1398 seq=2
ICMP Port Unreachable from ip=10.10.1.22 name=UNKNOWN
status=0 port=1399 seq=3
ICMP Port Unreachable from ip=10.10.1.22 name=UNKNOWN
status=0 port=1400 seq=4
--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.3/9.6/26.2 ms
[root@parrot]-[~]
#^C
[root@parrot]-[~]
#
attacker's
README.
Trash
CEHv12 Mo
Hacking
Server
CEHv12 Mo
Hacking
Applications
Scanning Networks
1 Hr 54 Min Remaining
Instructions
Resources
Help
100%
17. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.
Entire subnet scan for live host: hping3 -1 [Target Subnet] --rand-dest -I eth0
UDP scan: hping3 -2 [Target IP Address] -p 80 -c 5
18. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
19. Close all open windows and document all the acquired information.
0% Tasks Complete
Previous
Next: Lab 3: Perform OS...
ENG
22°C

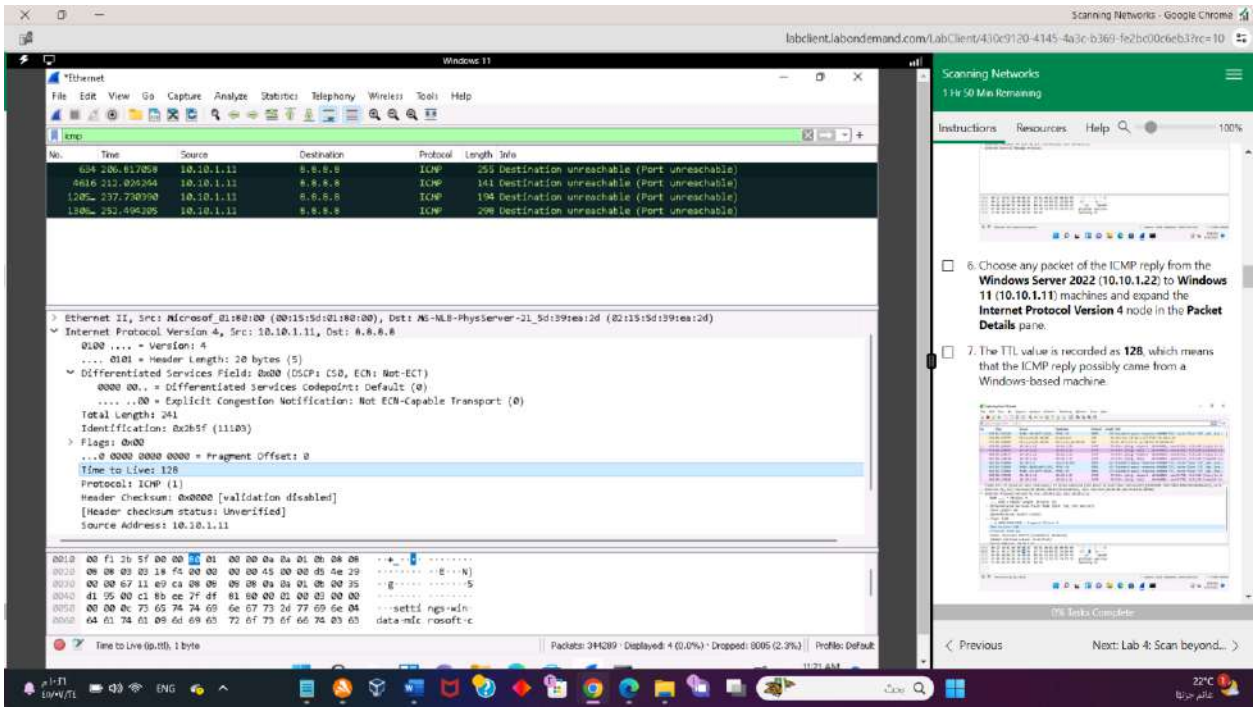
Lab 03 – Task 01

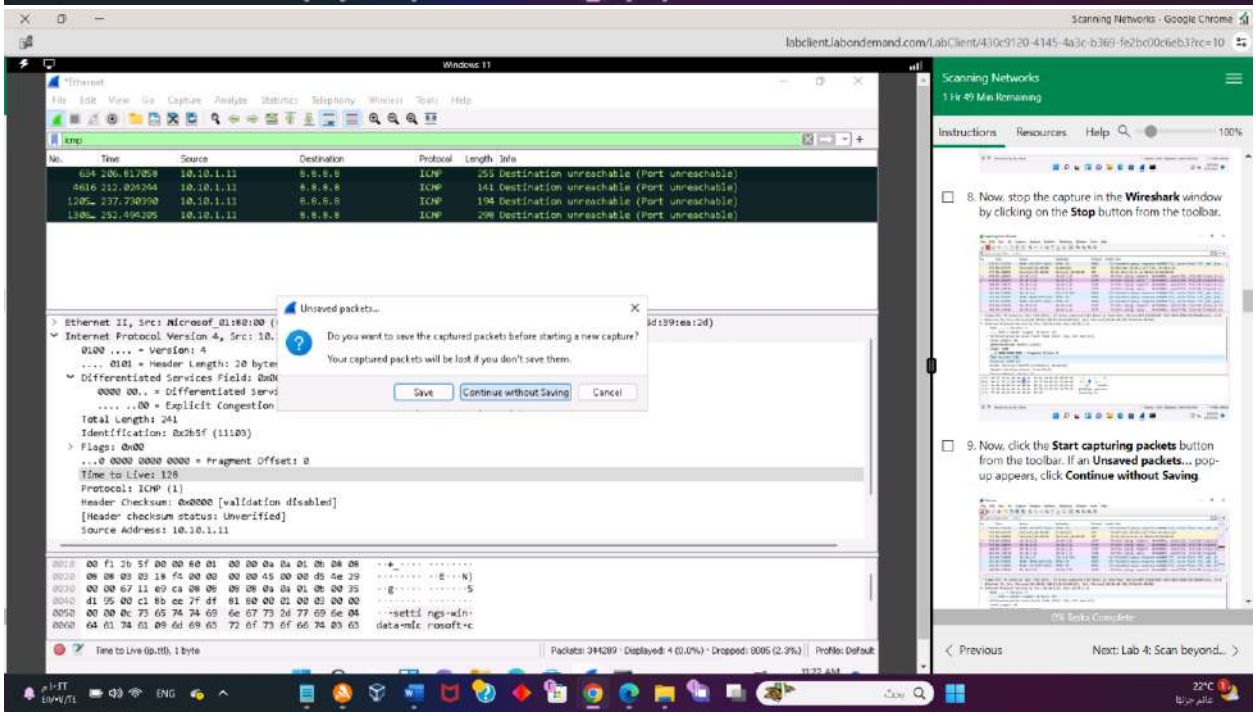


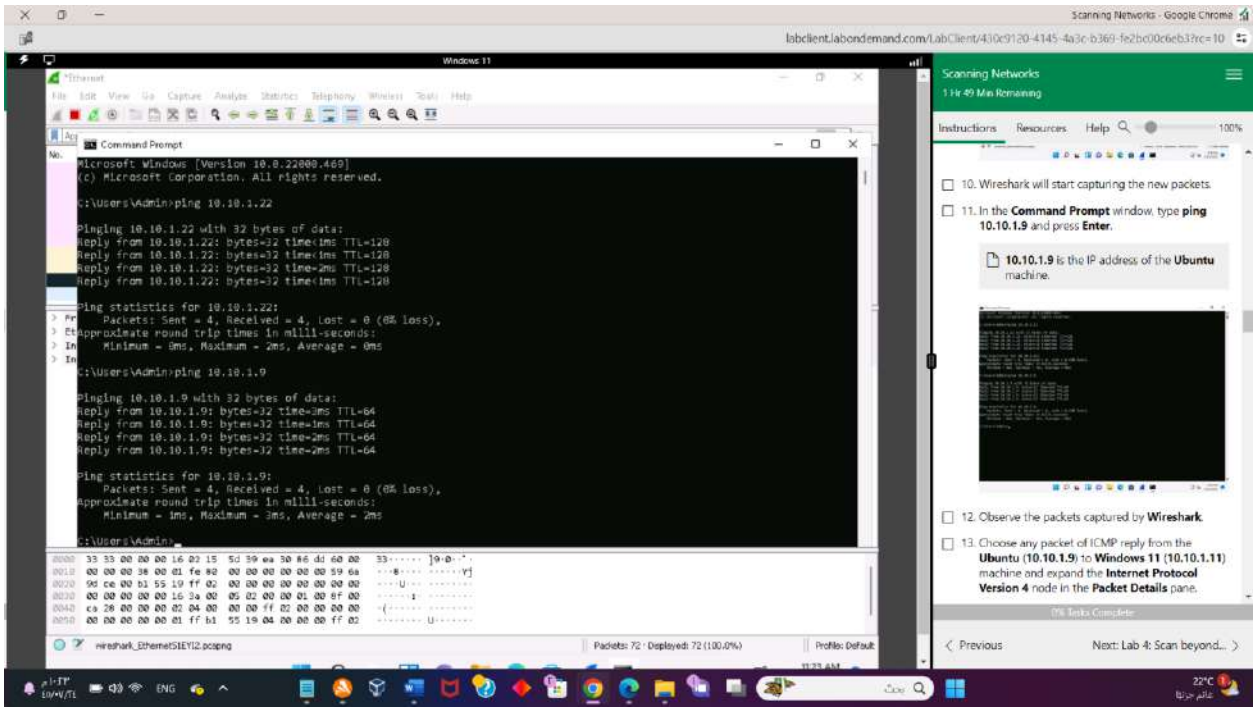


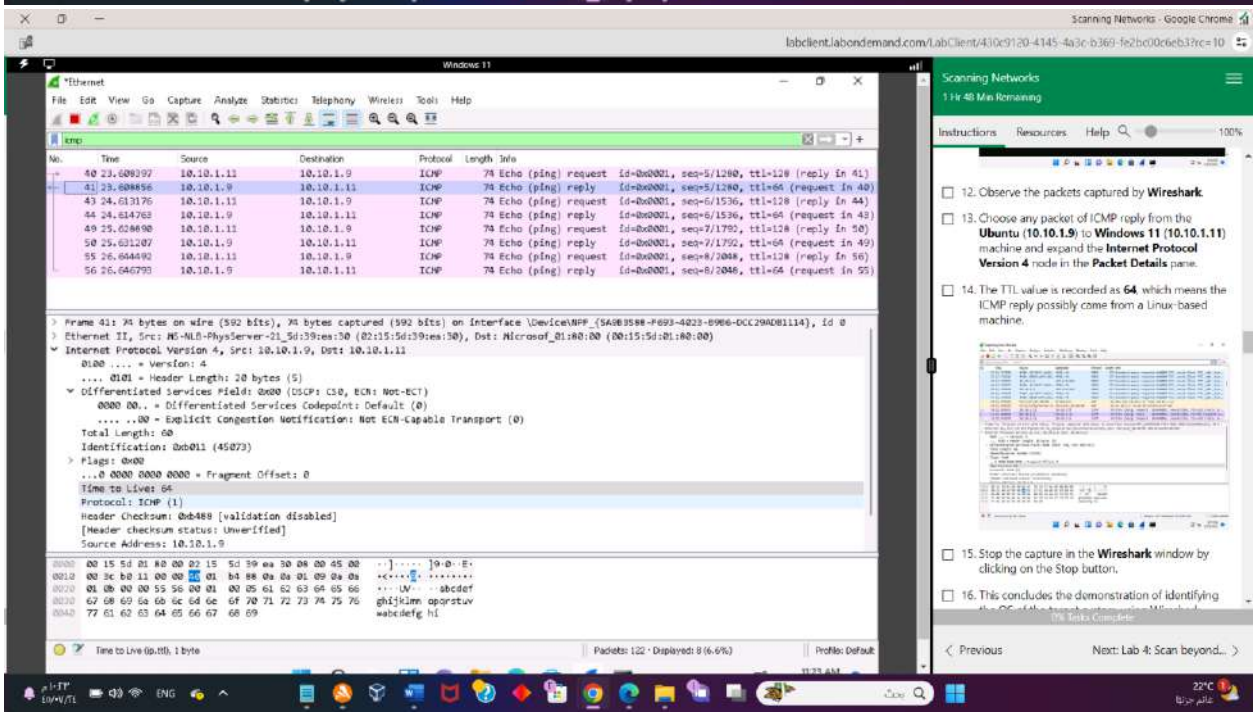

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/4d0c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
3442… 277.842057 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136880094 Win=62
3442… 277.842062 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136881494 Win=62
3442… 277.842067 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136882954 Win=62
3442… 277.842072 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136884414 Win=62
3442… 277.842076 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136885874 Win=62
3442… 277.842084 10.10.1.11 104.91.71.145 TCP 66 49937 → 443 [ACK] Seq=10811 Ack=136887334 Win=62
3442… 277.842601 10.10.1.11 104.91.71.145 TCP 54 [TCP ACKed unseen segment] 49937 → 443 [ACK] Seq
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{5A0B3588-F693-4023-B9B6-DCC29AD81114}
Ethernet II, Src: Microsof_01:80:00 (00:15:5d:01:80:00), Dst: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d)
Internet Protocol Version 4, Src: 10.10.1.11, Dst: 172.16.0.43
Transmission Control Protocol, Src Port: 49663, Dst Port: 7680, Seq: 0, Len: 0
wireshark_EthernetUSRV12.pcapng
Packets: 344289 · Displayed: 344289 (100.0%)
Profile: Default
Scanning Networks
1 Hr 52 Min Remaining
Instructions Resources Help 100%
5. Observe the packets captured by Wireshark.
6. Choose any packet of the ICMP reply from the Windows Server 2022 (10.10.1.22) to Windows 11 (10.10.1.11) machines and expand the Internet Protocol Version 4 node in the Packet Details pane.
0% Tasks Complete
Previous
Next: Lab 4: Scan beyond...
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/4d0c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
634 206.617058 10.10.1.11 8.8.8.8 ICMP 255 Destination unreachable (Port unreachable)
4616 212.026244 10.10.1.11 8.8.8.8 ICMP 141 Destination unreachable (Port unreachable)
1205… 237.730990 10.10.1.11 8.8.8.8 ICMP 194 Destination unreachable (Port unreachable)
1305… 252.496205 10.10.1.11 8.8.8.8 ICMP 298 Destination unreachable (Port unreachable)
Ethernet II, Src: Microsof_01:80:00 (00:15:5d:01:80:00), Dst: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d)
Internet Protocol Version 4, Src: 10.10.1.11, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 241
Identification: 0x2b5f (11103)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.10.1.11
Internet Protocol Version 4 (ip), 20 bytes
Packets: 344289 · Displayed: 4 (0.0%) · Dropped: 8005 (2.3%)
Profile: Default
Scanning Networks
1 Hr 50 Min Remaining
Instructions Resources Help 100%
6. Choose any packet of the ICMP reply from the Windows Server 2022 (10.10.1.22) to Windows 11 (10.10.1.11) machines and expand the Internet Protocol Version 4 node in the Packet Details pane.
7. The TTL value is recorded as 128, which means that the ICMP reply possibly came from a Windows-based machine.
0% Tasks Complete
Previous
Next: Lab 4: Scan beyond...
22°C

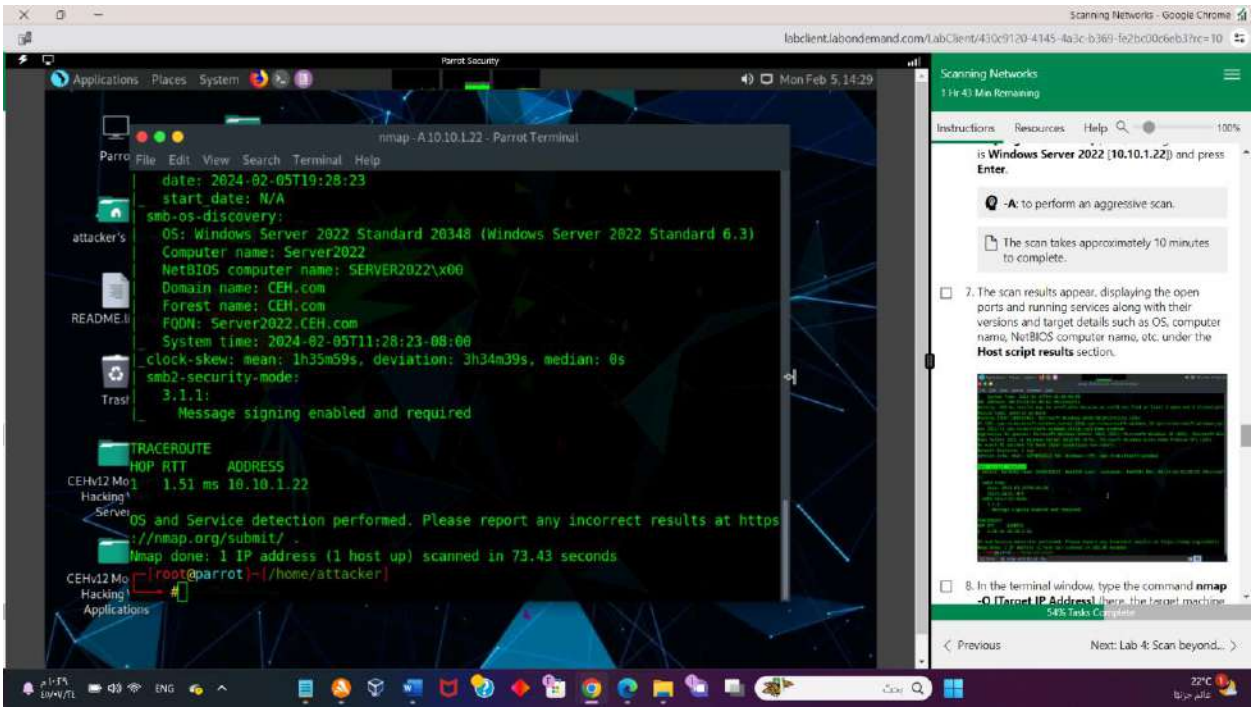

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/4d0c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
634 206.617058 10.10.1.11 8.8.8.8 ICMP 255 Destination unreachable (Port unreachable)
4616 212.026264 10.10.1.11 8.8.8.8 ICMP 141 Destination unreachable (Port unreachable)
12852 237.730990 10.10.1.11 8.8.8.8 ICMP 194 Destination unreachable (Port unreachable)
13806 252.496205 10.10.1.11 8.8.8.8 ICMP 298 Destination unreachable (Port unreachable)
Ethernet II, Src: Microsof_01:80:00 (00:15:5d:01:80:00), Dst: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d)
Internet Protocol Version 4, Src: 10.10.1.11, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 241
Identification: 0x2b5f (11103)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.10.1.11
Time to Live (ip.ttl), 1 byte
Packets: 344289 · Displayed: 4 (0.0%) · Dropped: 8005 (2.3%)
Profile: Default
Scanning Networks
1 Hr 50 Min Remaining
Instructions Resources Help 100%
6. Choose any packet of the ICMP reply from the Windows Server 2022 (10.10.1.22) to Windows 11 (10.10.1.11) machines and expand the Internet Protocol Version 4 node in the Packet Details pane.
7. The TTL value is recorded as 128, which means that the ICMP reply possibly came from a Windows-based machine.
0% Tasks Complete
Previous
Next: Lab 4: Scan beyond...

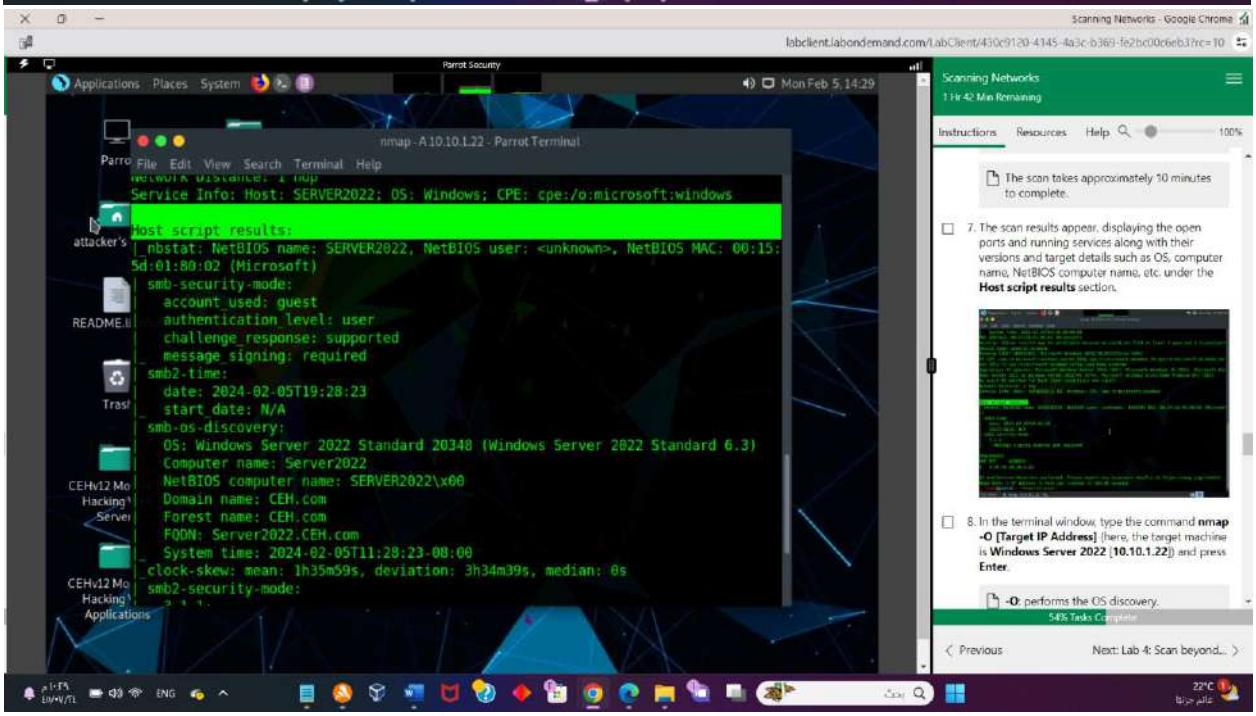

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/4d0c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Unsaved packets...
Do you want to save the captured packets before starting a new capture?
Your captured packets will be lost if you don't save them.
Save
Continue without Saving
Cancel
Scanning Networks
1 Hr 49 Min Remaining
Instructions Resources Help 100%
8. Now, stop the capture in the Wireshark window by clicking on the Stop button from the toolbar.
9. Now, click the Start capturing packets button from the toolbar. If an Unsaved packets... pop-up appears, click Continue without Saving.
0% Tasks Complete
Previous
Next: Lab 4: Scan beyond...

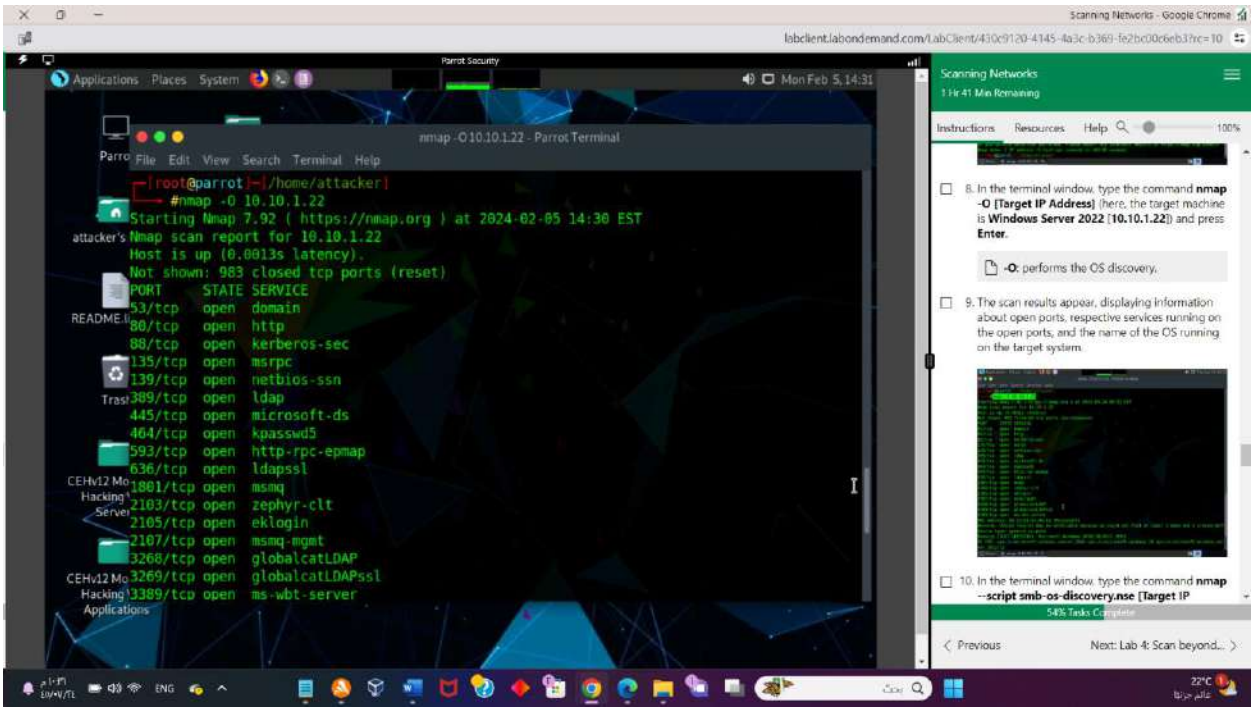


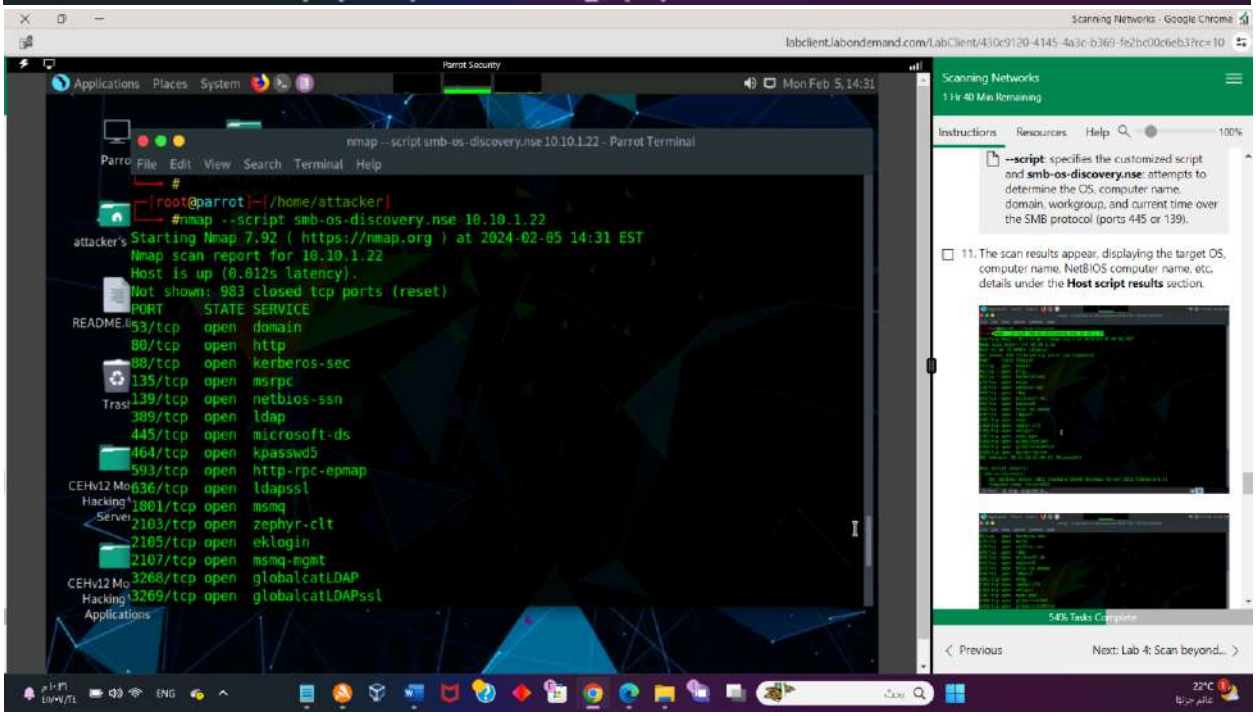


Lab 03 – Task 02

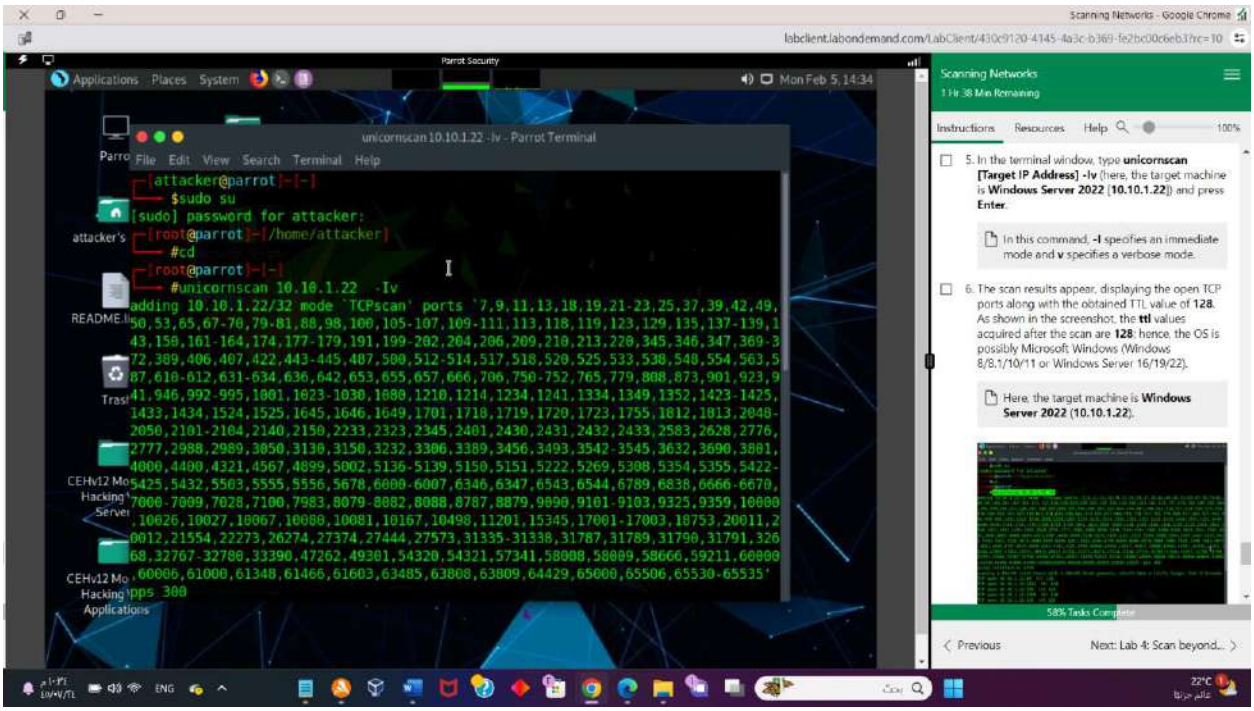

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:29
nmap -A 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
date: 2024-02-05T19:28:23
start_date: N/A
smb-os-discovery:
OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
Computer name: Server2022
NetBIOS computer name: SERVER2022\x00
Domain name: CEH.com
Forest name: CEH.com
FQDN: Server2022.CEH.com
System time: 2024-02-05T11:28:23-08:00
clock-skew: mean: 1h35m59s, deviation: 3h34m39s, median: 0s
smb2-security-mode:
3.1.1:
Message signing enabled and required
TRACEROUTE
HOP RTT ADDRESS
1 1.51 ms 10.10.1.22
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.43 seconds
root@parrot /home/attacker
#
Scanning Networks
1 Hr 43 Min Remaining
Instructions Resources Help 100%
is Windows Server 2022 (10.10.1.22)) and press Enter.
-A: to perform an aggressive scan.
The scan takes approximately 10 minutes to complete.
7. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the Host script results section.
8. In the terminal window, type the command nmap -O [Target IP Address] (here, the target machine
54% Tasks Complete
Previous
Next: Lab 4: Scan beyond...

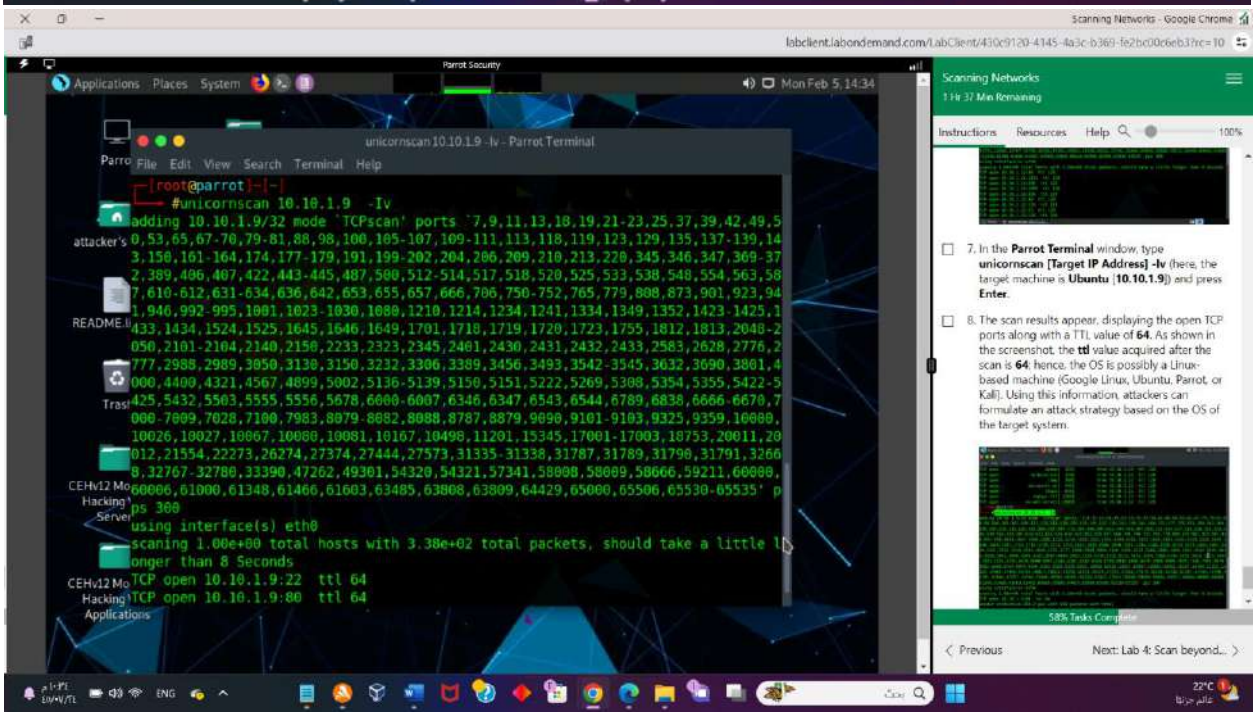

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:29
nmap -A 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microsoft)
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: required
smb2-time:
date: 2024-02-05T19:28:23
start_date: N/A
smb-os-discovery:
OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
Computer name: Server2022
NetBIOS computer name: SERVER2022\x00
Domain name: CEH.com
Forest name: CEH.com
FQDN: Server2022.CEH.com
System time: 2024-02-05T11:28:23-08:00
clock-skew: mean: 1h35m59s, deviation: 3h34m39s, median: 0s
smb2-security-mode:
Scanning Networks
1 Hr 42 Min Remaining
Instructions Resources Help 100%
The scan takes approximately 10 minutes to complete.
7. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the Host script results section.
8. In the terminal window, type the command nmap -O [Target IP Address] (here, the target machine is Windows Server 2022 (10.10.1.22)) and press Enter.
-O: performs the OS discovery.
54% Tasks Complete
Previous
Next: Lab 4: Scan beyond...



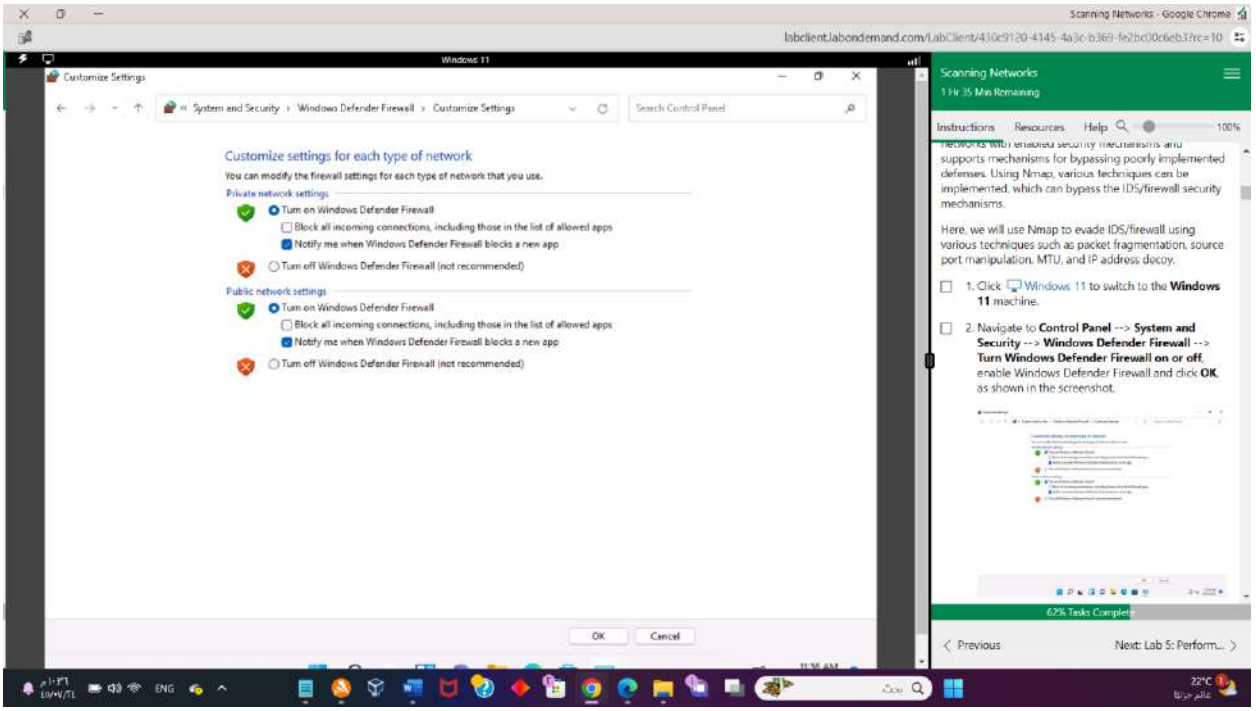


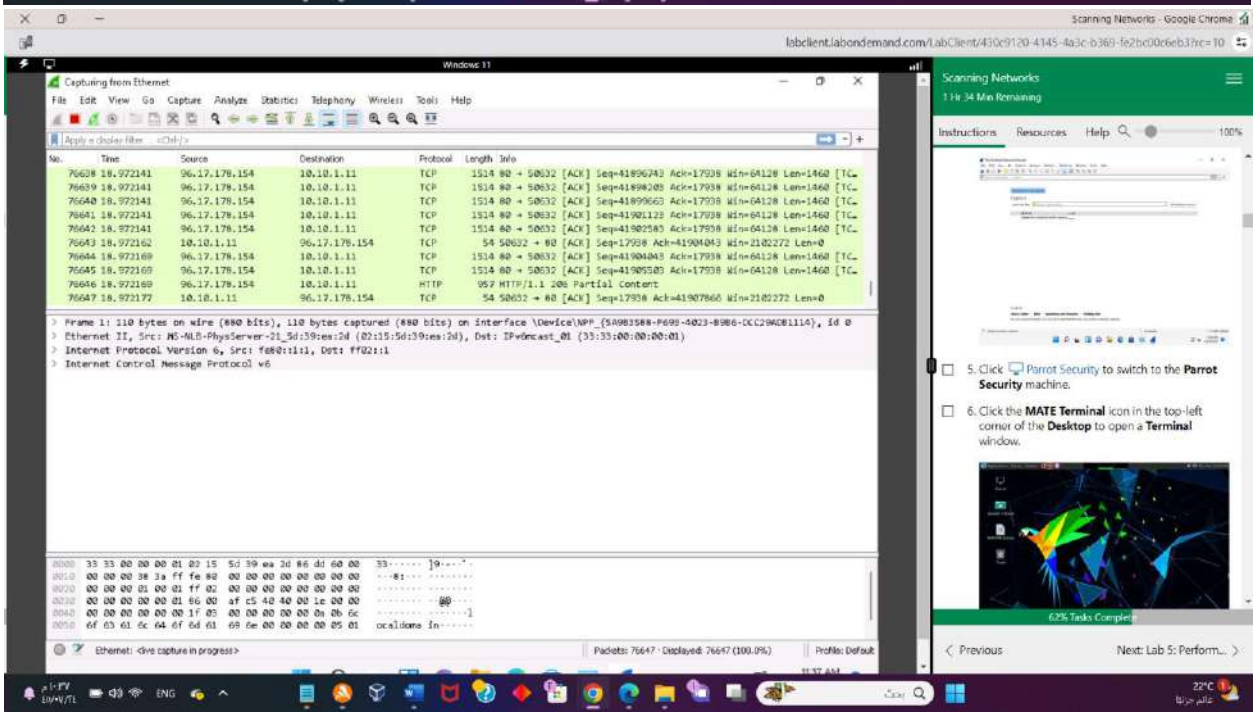
Lab 03 – Task 03

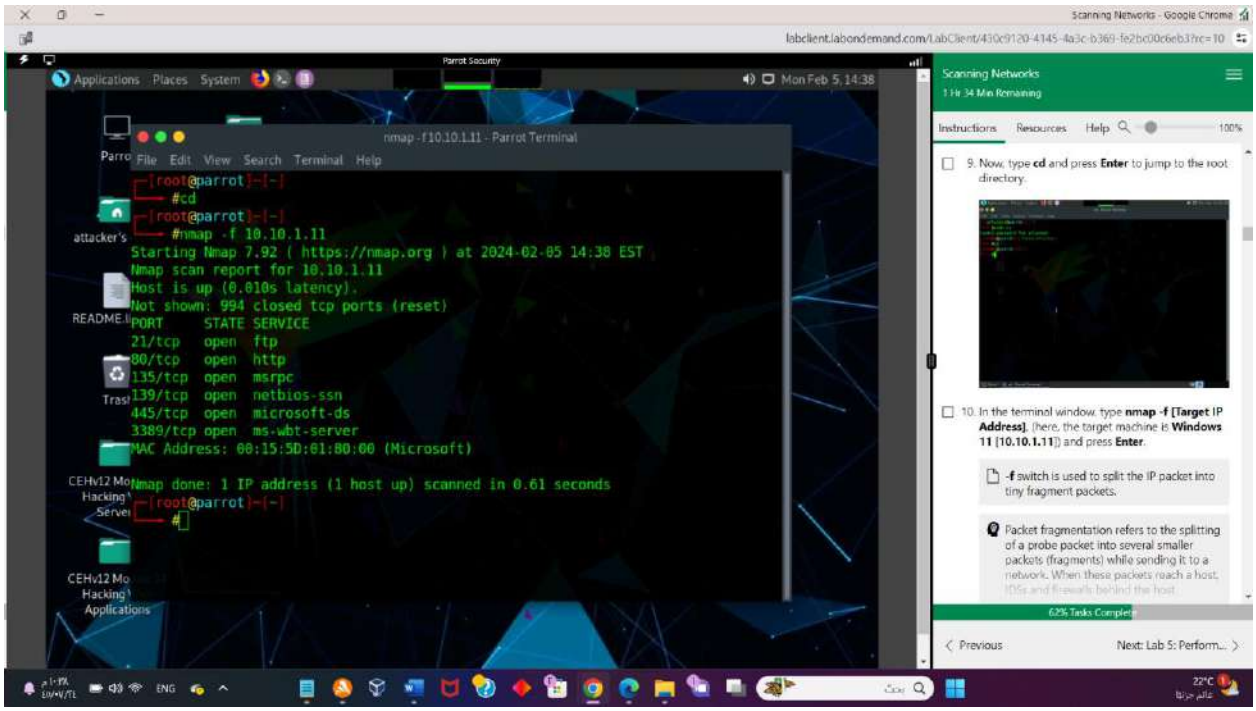

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:34
unicornscan 10.10.1.22 -Iv - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#unicornscan 10.10.1.22 -Iv
adding 10.10.1.22/32 mode 'TCPscan' ports '7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,158,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
Scanning Networks
1 Hr 38 Min Remaining
Instructions Resources Help 100%
5. In the terminal window, type unicornscan [Target IP Address] -Iv (here, the target machine is Windows Server 2022 (10.10.1.22)) and press Enter.
In this command, -I specifies an immediate mode and v specifies a verbose mode.
6. The scan results appear, displaying the open TCP ports along with the obtained TTL value of 128. As shown in the screenshot, the ttl values acquired after the scan are 128; hence, the OS is possibly Microsoft Windows (Windows 8/8.1/10/11 or Windows Server 16/19/22).
Here, the target machine is Windows Server 2022 (10.10.1.22).
58% Tasks Complete
Previous
Next: Lab 4: Scan beyond...

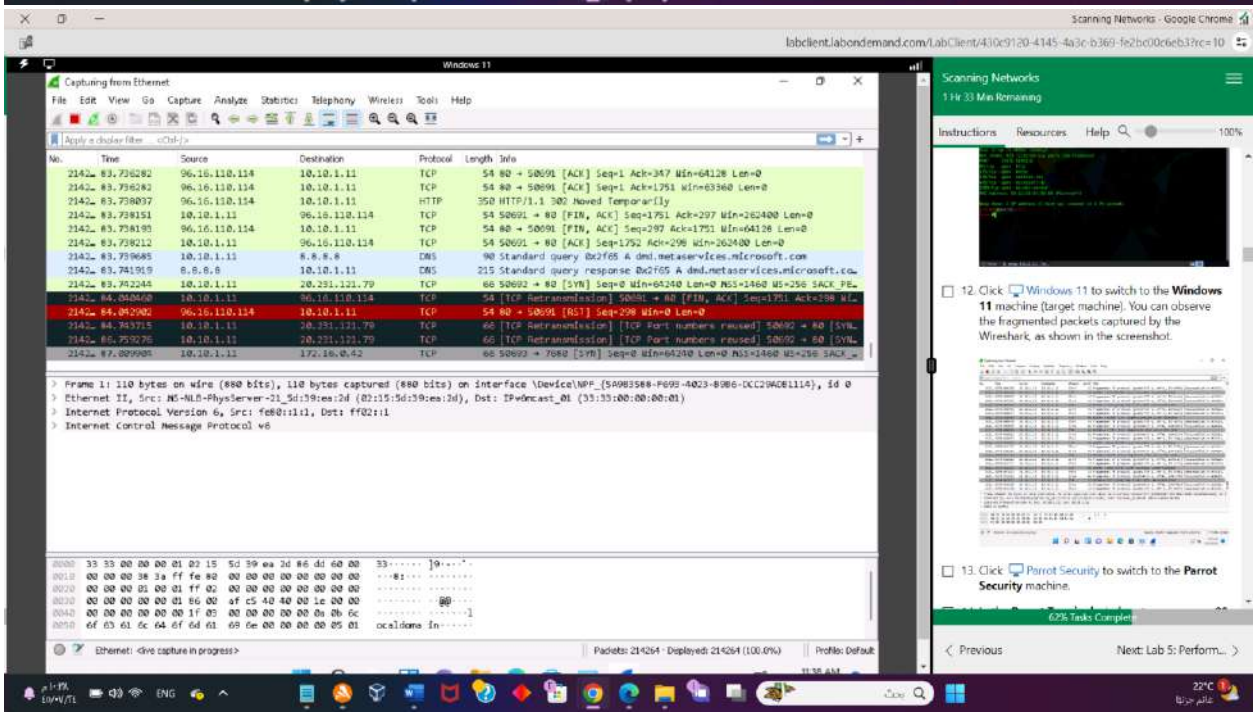

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:34
unicornscan 10.10.1.9 -Iv - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#unicornscan 10.10.1.9 -Iv
adding 10.10.1.9/32 mode 'TCPscan' ports '7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,158,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
TCP open 10.10.1.9:22 ttl 64
TCP open 10.10.1.9:80 ttl 64
Scanning Networks
1 Hr 37 Min Remaining
Instructions Resources Help 100%
7. In the Parrot Terminal window, type unicornscan [Target IP Address] -Iv (here, the target machine is Ubuntu (10.10.1.9)) and press Enter.
8. The scan results appear, displaying the open TCP ports along with a TTL value of 64. As shown in the screenshot, the ttl value acquired after the scan is 64; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali). Using this information, attackers can formulate an attack strategy based on the OS of the target system.
58% Tasks Complete
Previous
Next: Lab 4: Scan beyond...

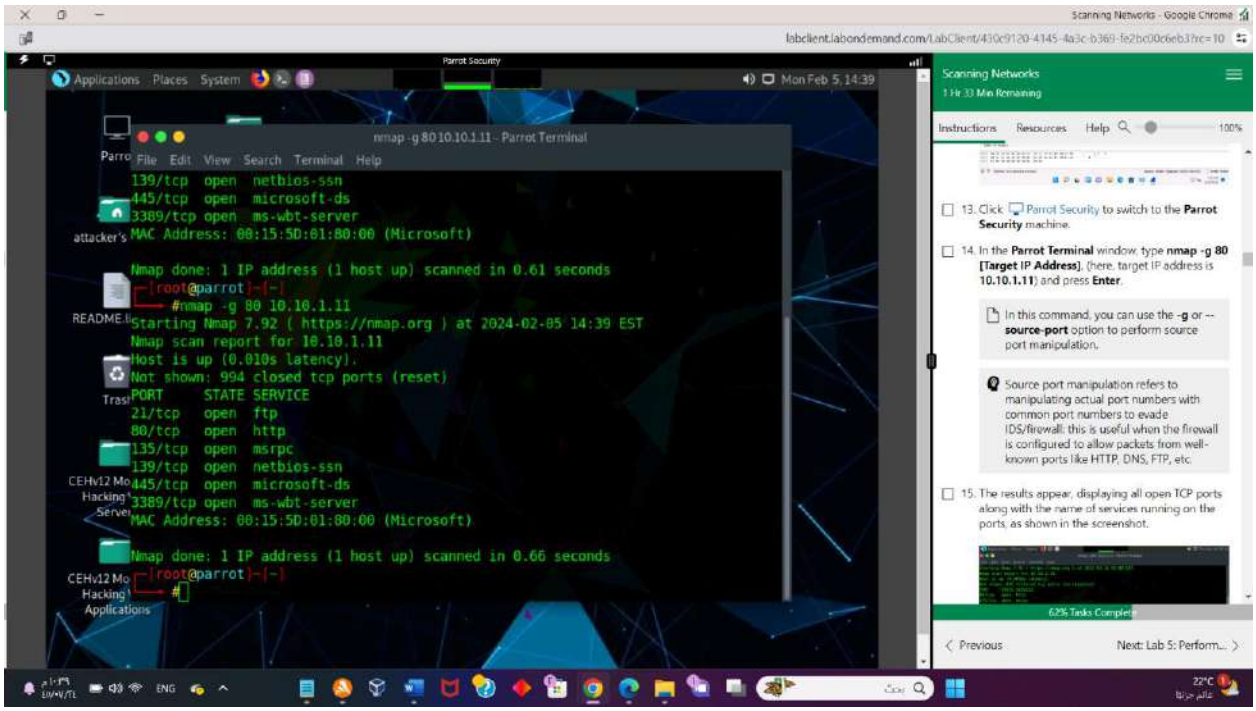
Lab 04 – Task 01

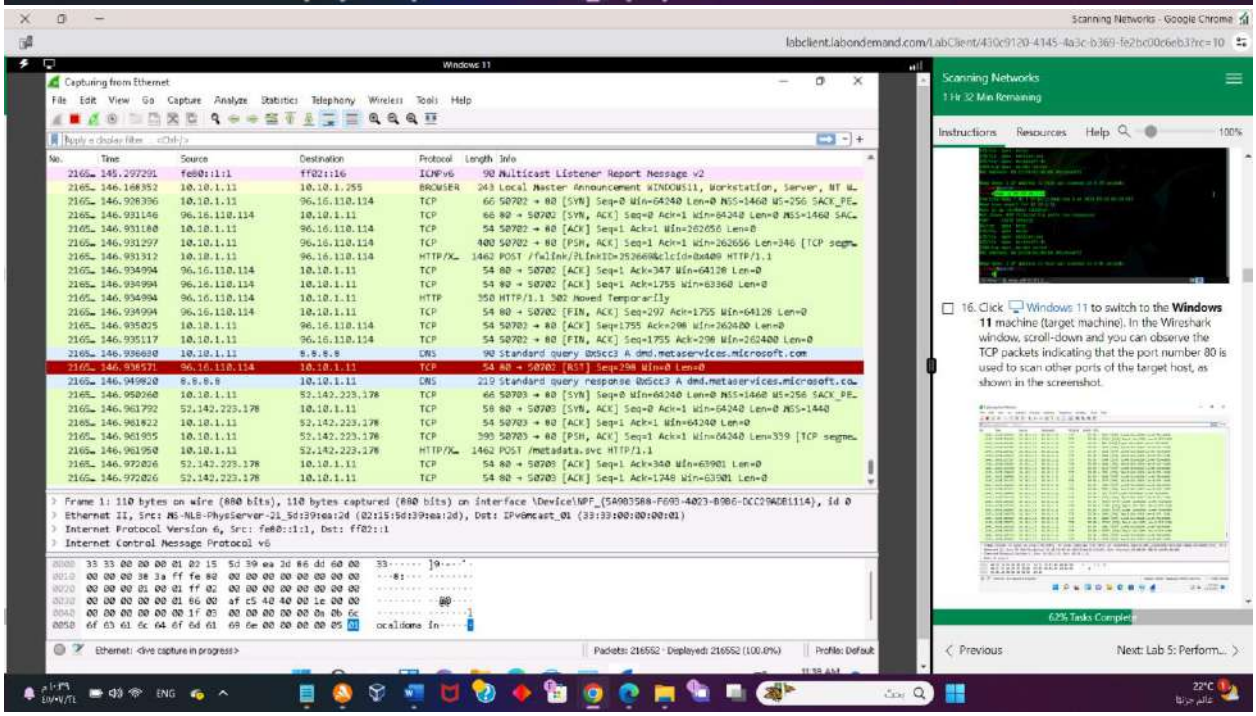


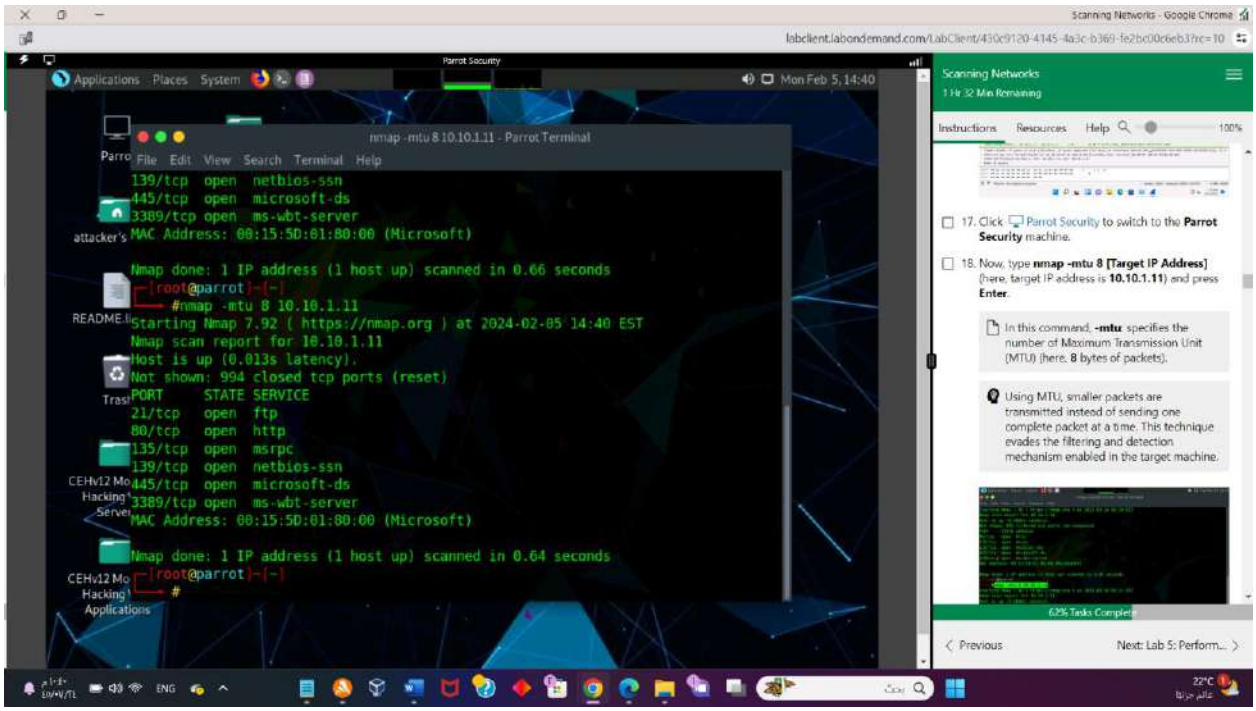


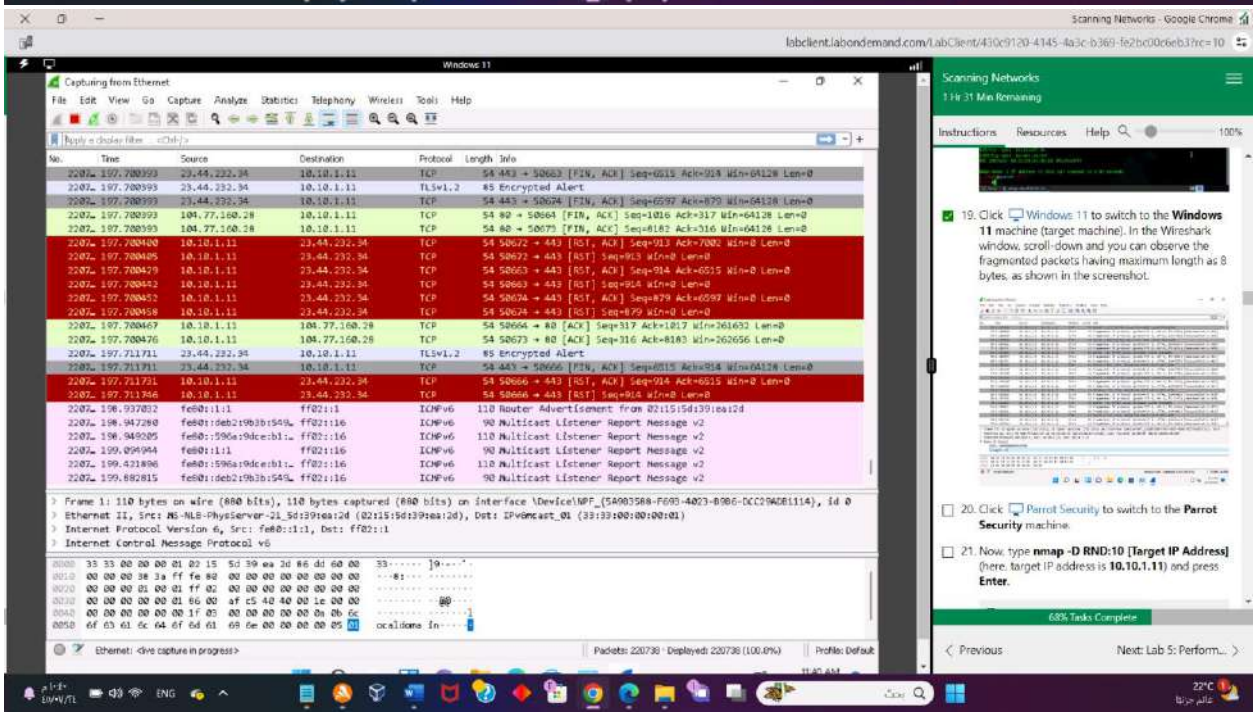

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:38
nmap -f10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#cd
[root@parrot]~[~]
#nmap -f 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 14:38 EST
Nmap scan report for 10.10.1.11
Host is up (0.010s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
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: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
[root@parrot]~[~]
#
Scanning Networks
1 Hr 34 Min Remaining
Instructions Resources Help
100%
9. Now, type cd and press Enter to jump to the root directory.
10. In the terminal window, type nmap -f [Target IP Address], (here, the target machine is Windows 11 [10.10.1.11]) and press Enter.
-f switch is used to split the IP packet into tiny fragment packets.
Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host
62% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

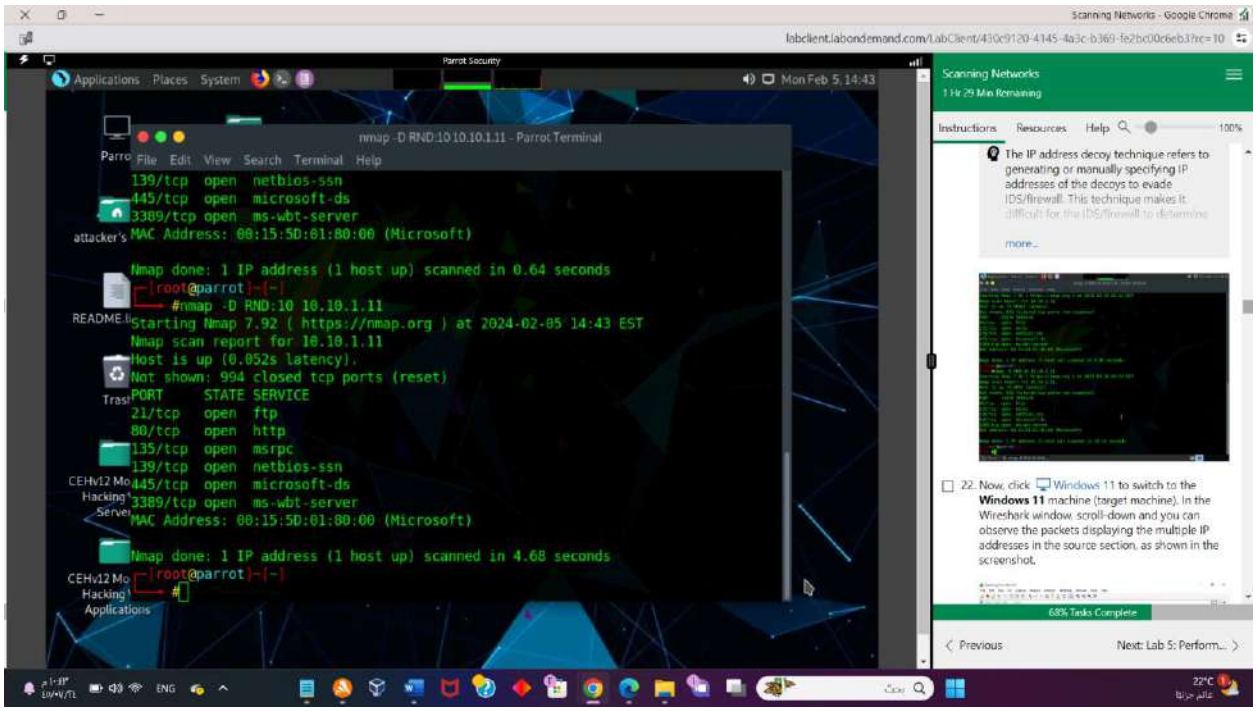

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
2142... 83.736282 96.16.110.114 10.10.1.11 TCP 54 80 → 50691 [ACK] Seq=1 Ack=357 Win=64128 Len=0
2142... 83.736282 96.16.110.114 10.10.1.11 TCP 54 80 → 50691 [ACK] Seq=1 Ack=1751 Win=63360 Len=0
2142... 83.738037 96.16.110.114 10.10.1.11 HTTP 350 HTTP/1.1 302 Moved Temporarily
2142... 83.738151 10.10.1.11 96.16.110.114 TCP 54 50691 → 80 [FIN, ACK] Seq=1751 Ack=297 Win=262400 Len=0
2142... 83.738195 96.16.110.114 10.10.1.11 TCP 54 80 → 50691 [FIN, ACK] Seq=297 Ack=1751 Win=64128 Len=0
2142... 83.738212 10.10.1.11 96.16.110.114 TCP 54 50691 → 80 [ACK] Seq=1752 Ack=298 Win=262400 Len=0
2142... 83.739685 10.10.1.11 8.8.8.8 DNS 90 Standard query 0x2f65 A dmd.metaservices.microsoft.com
2142... 83.741919 8.8.8.8 10.10.1.11 DNS 215 Standard query response 0x2f65 A dmd.metaservices.microsoft.co...
2142... 83.742244 10.10.1.11 20.231.121.79 TCP 66 50692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE...
2142... 84.040460 10.10.1.11 96.16.110.114 TCP 54 [TCP Retransmission] 50691 → 80 [FIN, ACK] Seq=1751 Ack=298 Wi...
2142... 84.042902 96.16.110.114 10.10.1.11 TCP 54 80 → 50691 [RST] Seq=298 Win=0 Len=0
2142... 84.343715 10.10.1.11 20.231.121.79 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 50692 → 80 [SYN...
2142... 86.759276 10.10.1.11 20.231.121.79 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 50692 → 80 [SYN...
2142... 87.009905 10.10.1.11 172.16.0.42 TCP 66 50693 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_...
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{5A9B3588-F098-4023-B9B6-DCC29ADE1114}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:59:ea:2d (02:15:5d:59:ea:2d), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
Internet Control Message Protocol v6
Ethernet: <live capture in progress>
Packets: 214264 · Displayed: 214264 (100.0%)
Profile: Default
Scanning Networks
1 Hr 33 Min Remaining
Instructions Resources Help
100%
12. Click Windows 11 to switch to the Windows 11 machine (target machine). You can observe the fragmented packets captured by the Wireshark, as shown in the screenshot.
13. Click Parrot Security to switch to the Parrot Security machine.
62% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

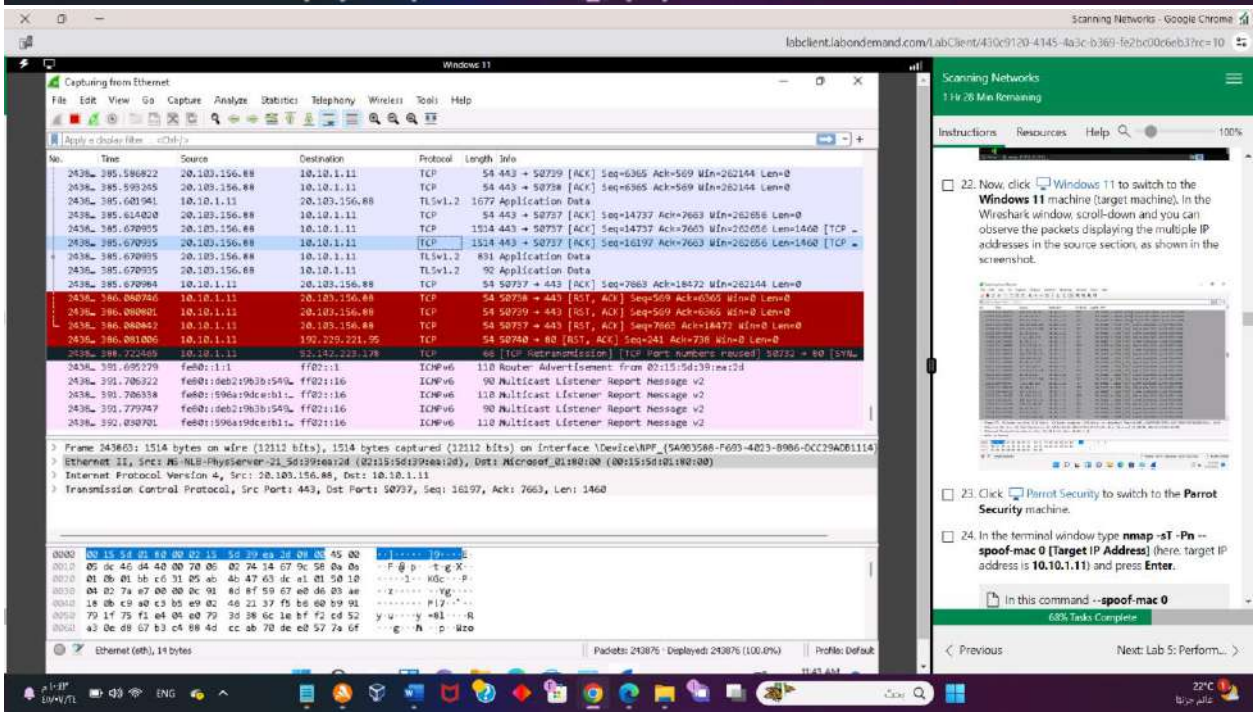

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:39
nmap -g 80 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
┌[root@parrot]-[~]
└─# nmap -g 80 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 14:39 EST
Nmap scan report for 10.10.1.11
Host is up (0.010s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
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: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
┌[root@parrot]-[~]
└─#
attacker's
README.li
Trash
CEHv12 Mo Hacking Server
CEHv12 Mo Hacking Applications
Scanning Networks
1 Hr 33 Min Remaining
Instructions Resources Help 100%
13. Click Parrot Security to switch to the Parrot Security machine.
14. In the Parrot Terminal window, type nmap -g 80 [Target IP Address], (here, target IP address is 10.10.1.11) and press Enter.
In this command, you can use the -g or --source-port option to perform source port manipulation.
Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall; this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.
15. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.
62% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

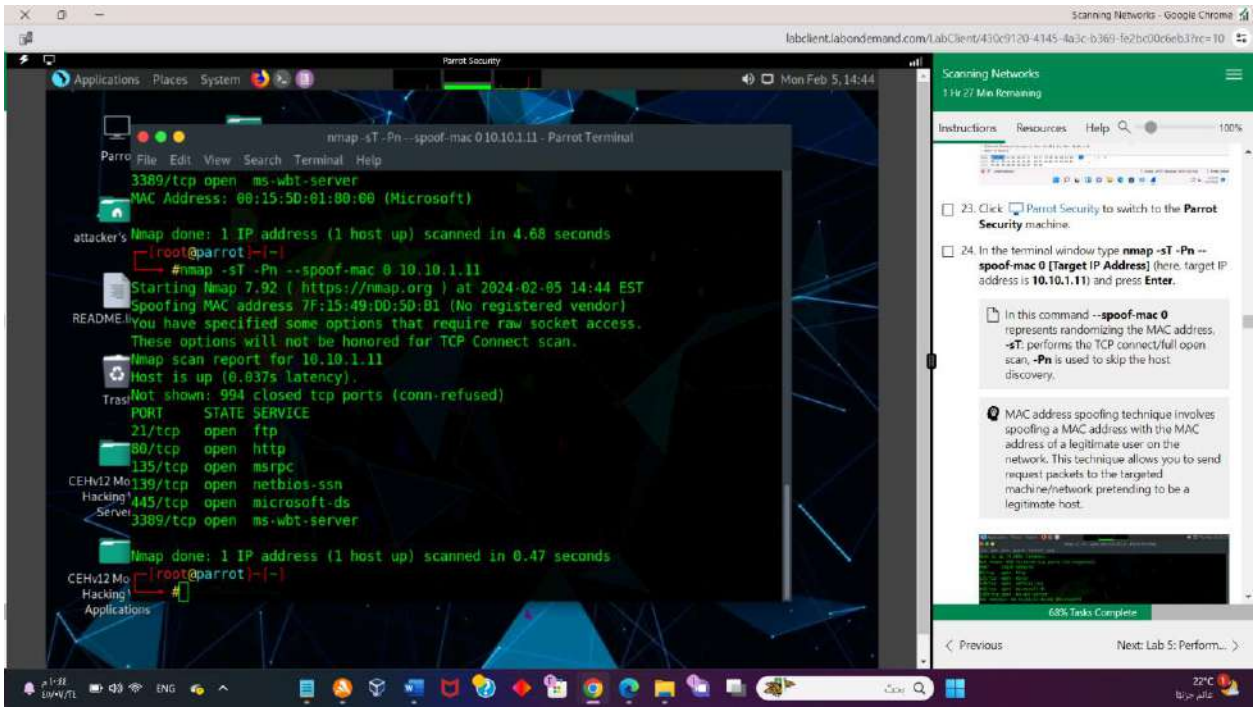

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
2165… 145.297291 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
2165… 146.168352 10.10.1.11 10.10.1.255 BROWSER 243 Local Master Announcement WINDOWS11, Workstation, Server, NT W…
2165… 146.928396 10.10.1.11 96.16.110.114 TCP 66 50702 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE…
2165… 146.931146 96.16.110.114 10.10.1.11 TCP 66 80 → 50702 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SAC…
2165… 146.931180 10.10.1.11 96.16.110.114 TCP 54 50702 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2165… 146.931297 10.10.1.11 96.16.110.114 TCP 400 50702 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=346 [TCP segm…
2165… 146.931312 10.10.1.11 96.16.110.114 HTTP/X… 1462 POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1
2165… 146.934994 96.16.110.114 10.10.1.11 TCP 54 80 → 50702 [ACK] Seq=1 Ack=347 Win=64128 Len=0
2165… 146.934994 96.16.110.114 10.10.1.11 TCP 54 80 → 50702 [ACK] Seq=1 Ack=1755 Win=63360 Len=0
2165… 146.934994 96.16.110.114 10.10.1.11 HTTP 350 HTTP/1.1 302 Moved Temporarily
2165… 146.934994 96.16.110.114 10.10.1.11 TCP 54 80 → 50702 [FIN, ACK] Seq=297 Ack=1755 Win=64128 Len=0
2165… 146.935025 10.10.1.11 96.16.110.114 TCP 54 50702 → 80 [ACK] Seq=1755 Ack=298 Win=262400 Len=0
2165… 146.935117 10.10.1.11 96.16.110.114 TCP 54 50702 → 80 [FIN, ACK] Seq=1755 Ack=298 Win=262400 Len=0
2165… 146.936030 10.10.1.11 8.8.8.8 DNS 90 Standard query 0x5cc3 A dmd.metaservices.microsoft.com
2165… 146.936571 96.16.110.114 10.10.1.11 TCP 54 80 → 50702 [RST] Seq=298 Win=0 Len=0
2165… 146.949920 8.8.8.8 10.10.1.11 DNS 219 Standard query response 0x5cc3 A dmd.metaservices.microsoft.co…
2165… 146.950260 10.10.1.11 52.142.223.178 TCP 66 50703 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE…
2165… 146.961792 52.142.223.178 10.10.1.11 TCP 58 80 → 50703 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440
2165… 146.961822 10.10.1.11 52.142.223.178 TCP 54 50703 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2165… 146.961955 10.10.1.11 52.142.223.178 TCP 390 50703 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=339 [TCP segme…
2165… 146.961950 10.10.1.11 52.142.223.178 HTTP/X… 1462 POST /metadata.svc HTTP/1.1
2165… 146.972026 52.142.223.178 10.10.1.11 TCP 54 80 → 50703 [ACK] Seq=1 Ack=340 Win=63901 Len=0
2165… 146.972026 52.142.223.178 10.10.1.11 TCP 54 80 → 50703 [ACK] Seq=1 Ack=1748 Win=63901 Len=0
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{5A903588-F695-4023-B9B6-DCC29ADB1114}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
Internet Control Message Protocol v6
Ethernet: <live capture in progress>
Packets: 216552 · Displayed: 216552 (100.0%)
Profile: Default
Scanning Networks
1 Hr 32 Min Remaining
Instructions Resources Help 100%
16. Click Windows 11 to switch to the Windows 11 machine (target machine). In the Wireshark window, scroll-down and you can observe the TCP packets indicating that the port number 80 is used to scan other ports of the target host, as shown in the screenshot.
62% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

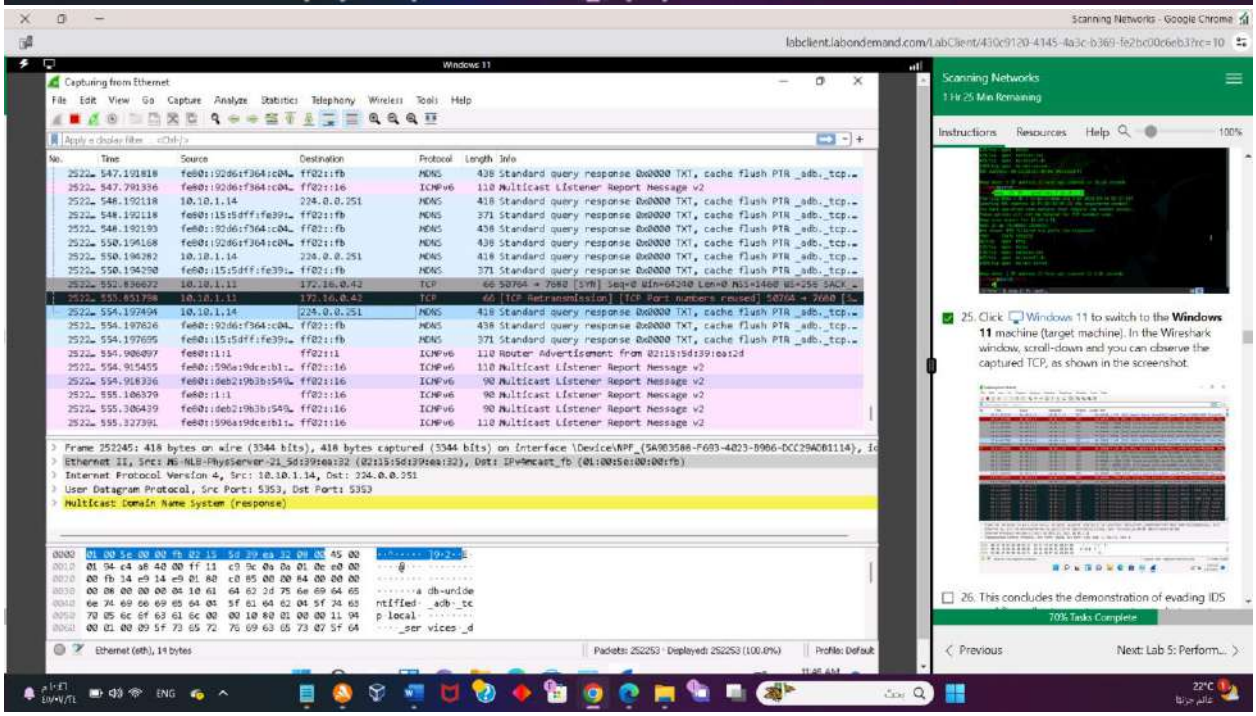

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:40
nmap -mtu 8 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
[root@parrot]-[~]
#nmap -mtu 8 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 14:40 EST
Nmap scan report for 10.10.1.11
Host is up (0.013s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
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: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
[root@parrot]-[~]
#
Scanning Networks
1 Hr 32 Min Remaining
Instructions Resources Help 100%
17. Click Parrot Security to switch to the Parrot Security machine.
18. Now, type nmap -mtu 8 [Target IP Address] (here, target IP address is 10.10.1.11) and press Enter.
In this command, -mtu specifies the number of Maximum Transmission Unit (MTU) (here, 8 bytes of packets).
Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.
62% Tasks Complete
Previous
Next: Lab 5: Perform...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{5A903588-F695-4023-B9B6-DCC29ADB1114}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
Internet Control Message Protocol v6
Ethernet: <live capture in progress>
Packets: 220738 · Displayed: 220738 (100.0%)
Profile: Default
Scanning Networks
1 Hr 31 Min Remaining
Instructions Resources Help 100%
19. Click Windows 11 to switch to the Windows 11 machine (target machine). In the Wireshark window, scroll-down and you can observe the fragmented packets having maximum length as 8 bytes, as shown in the screenshot.
20. Click Parrot Security to switch to the Parrot Security machine.
21. Now, type nmap -D RND:10 [Target IP Address] (here, target IP address is 10.10.1.11) and press Enter.
68% Tasks Complete
Previous
Next: Lab 5: Perform...

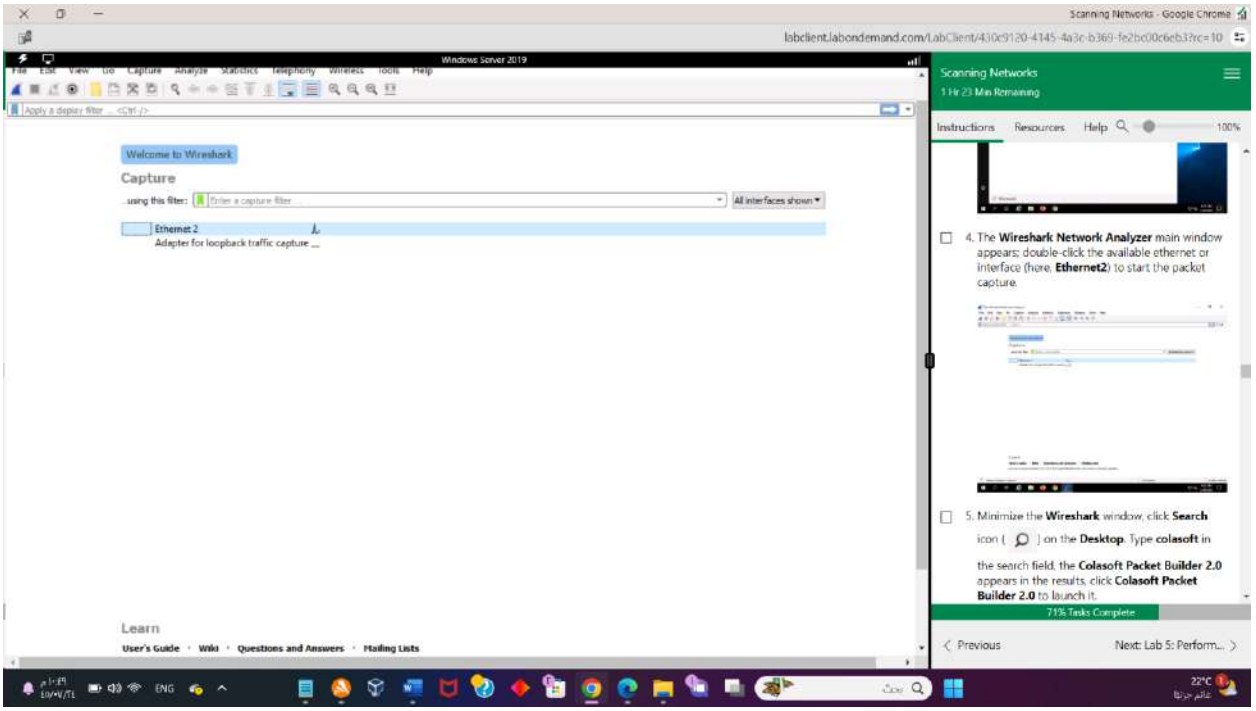

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:43
nmap -D RND:10 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
[root@parrot]-[~]
#nmap -D RND:10 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 14:43 EST
Nmap scan report for 10.10.1.11
Host is up (0.052s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
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: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
[root@parrot]-[~]
#
Scanning Networks
1 Hr 29 Min Remaining
Instructions Resources Help 100%
The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine
more...
22. Now, click Windows 11 to switch to the Windows 11 machine (target machine). In the Wireshark window, scroll-down and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.
68% Tasks Complete
Previous
Next: Lab 5: Perform...

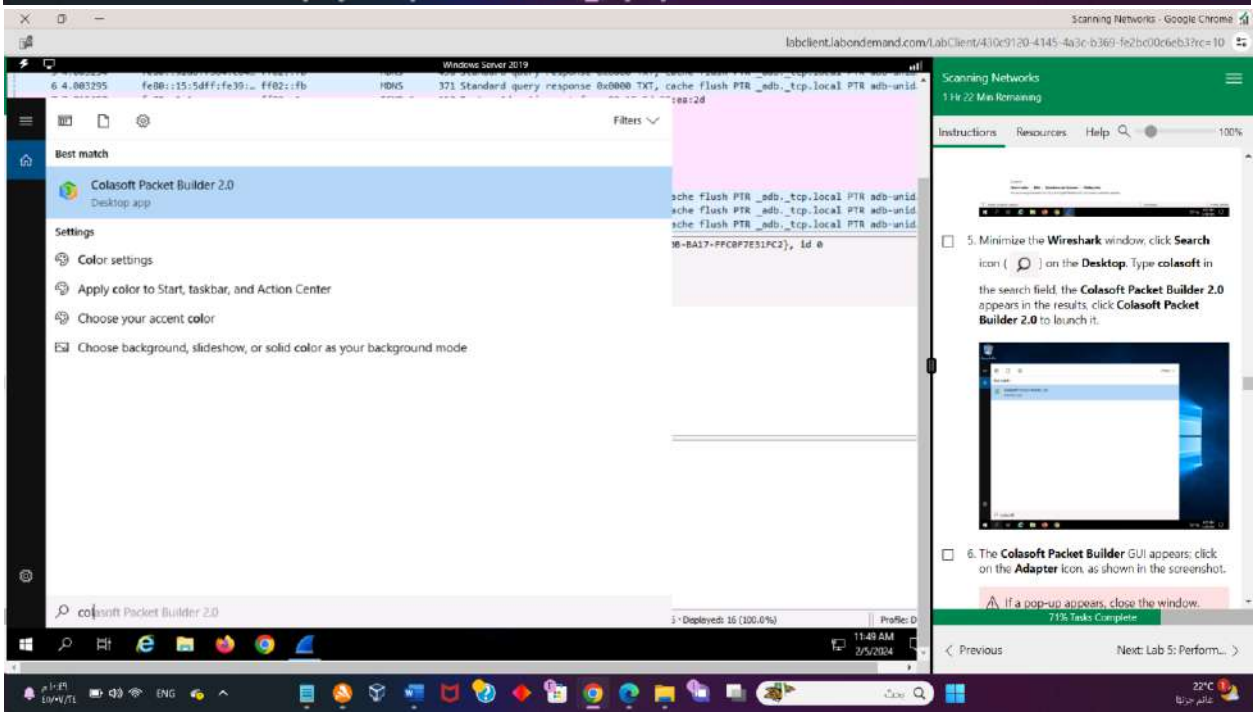

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame 243663: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{5A903588-F693-4023-B986-DCC29AOB1114}
Ethernet II, Src: MS-NLB-PhysServer-21_5d:39:ea:2d (02:15:5d:39:ea:2d), Dst: Microsof_01:80:00 (00:15:5d:01:80:00)
Internet Protocol Version 4, Src: 20.103.156.88, Dst: 10.10.1.11
Transmission Control Protocol, Src Port: 443, Dst Port: 50737, Seq: 16197, Ack: 7663, Len: 1460
Scanning Networks
1 Hr 28 Min Remaining
Instructions Resources Help 100%
22. Now, click Windows 11 to switch to the Windows 11 machine (target machine). In the Wireshark window, scroll-down and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.
23. Click Parrot Security to switch to the Parrot Security machine.
24. In the terminal window type nmap -sT -Pn --spoof-mac 0 [Target IP Address] (here, target IP address is 10.10.1.11) and press Enter.
In this command --spoof-mac 0
68% Tasks Complete
Previous
Next: Lab 5: Perform...

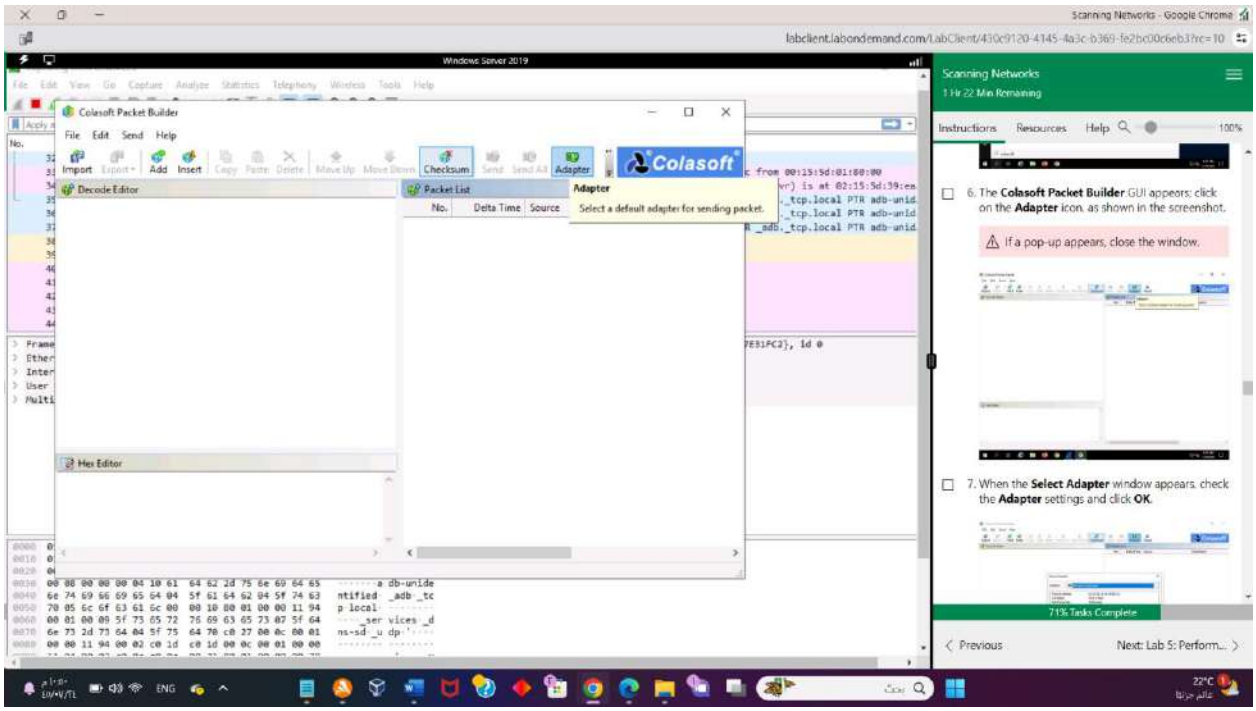

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:44
nmap -sT -Pn --spoof-mac 0 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
[root@parrot]-[~]
#nmap -sT -Pn --spoof-mac 0 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2024-02-05 14:44 EST
Spoofing MAC address 7F:15:49:DD:5D:B1 (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 10.10.1.11
Host is up (0.037s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
[root@parrot]-[~]
#
Scanning Networks
1 Hr 27 Min Remaining
Instructions Resources Help 100%
23. Click Parrot Security to switch to the Parrot Security machine.
24. In the terminal window type nmap -sT -Pn --spoof-mac 0 [Target IP Address] (here, target IP address is 10.10.1.11) and press Enter.
In this command --spoof-mac 0 represents randomizing the MAC address. -sT: performs the TCP connect/full open scan, -Pn is used to skip the host discovery.
MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.
68% Tasks Complete
Previous
Next: Lab 5: Perform...

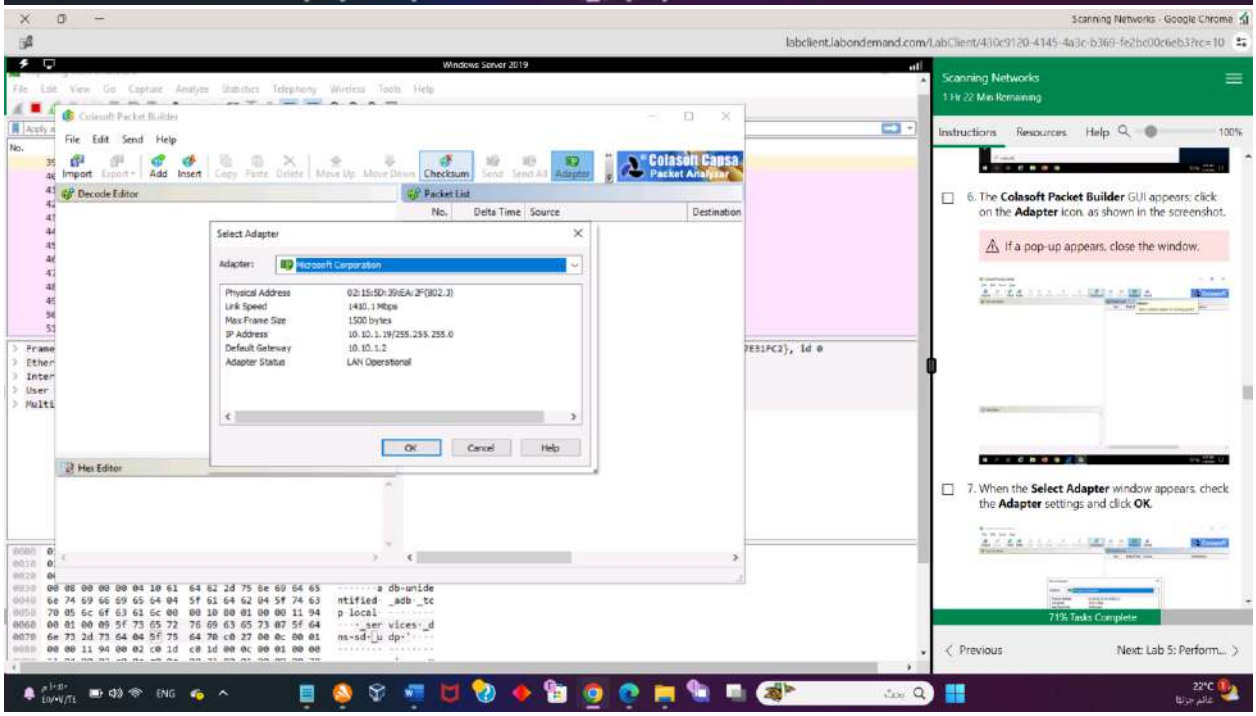

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame 252245: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF_{5A983588-F693-4823-B986-DCC29AC81114}, id
Ethernet II, Src: MS-NLB-PhysServer-21_5d:39:ea:32 (02:15:5d:39:ea:32), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 10.10.1.14, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)
Scanning Networks
1 Hr 25 Min Remaining
Instructions Resources Help 100%
25. Click Windows 11 to switch to the Windows 11 machine (target machine). In the Wireshark window, scroll-down and you can observe the captured TCP, as shown in the screenshot.
26. This concludes the demonstration of evading IDS
70% Tasks Complete
Previous
Next: Lab 5: Perform...

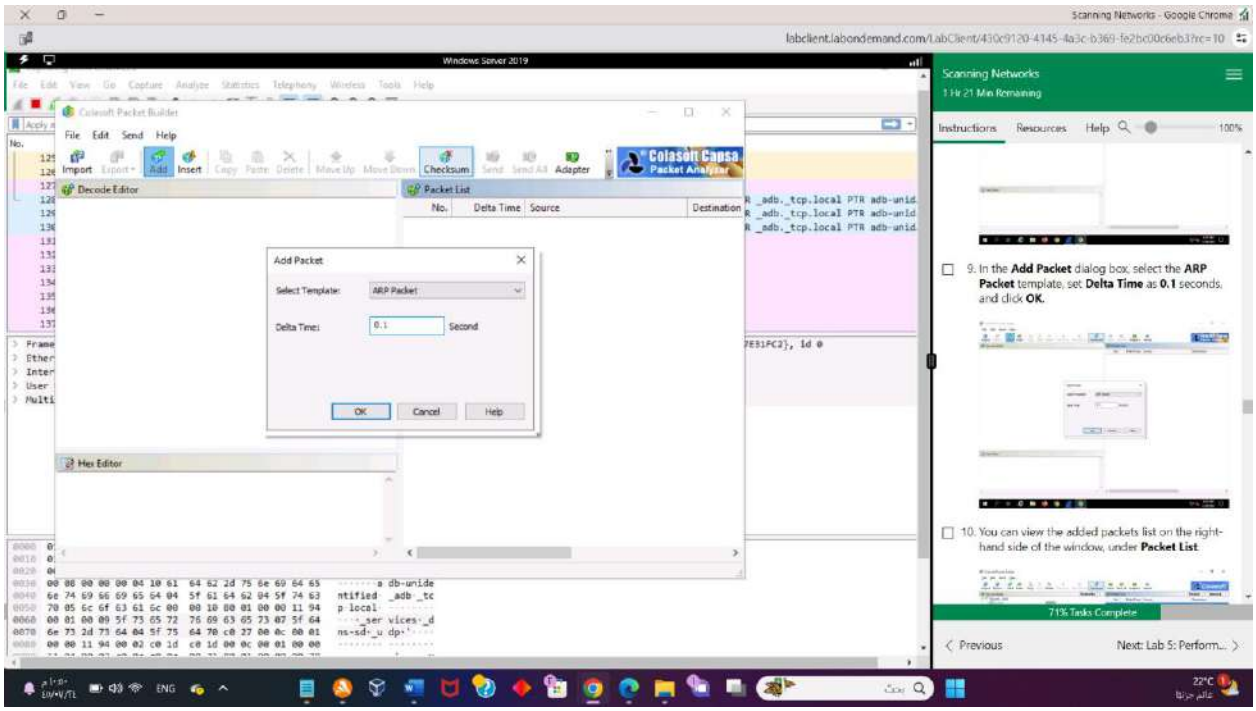
Lab 04 – Task 02

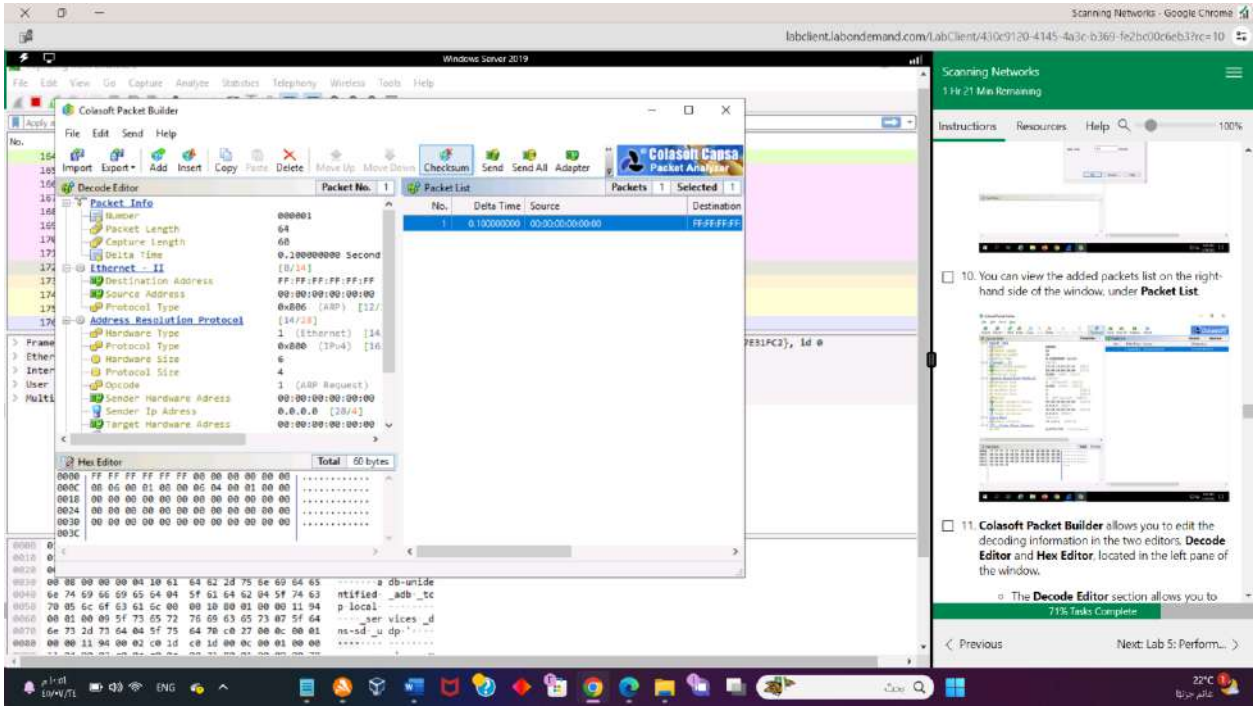


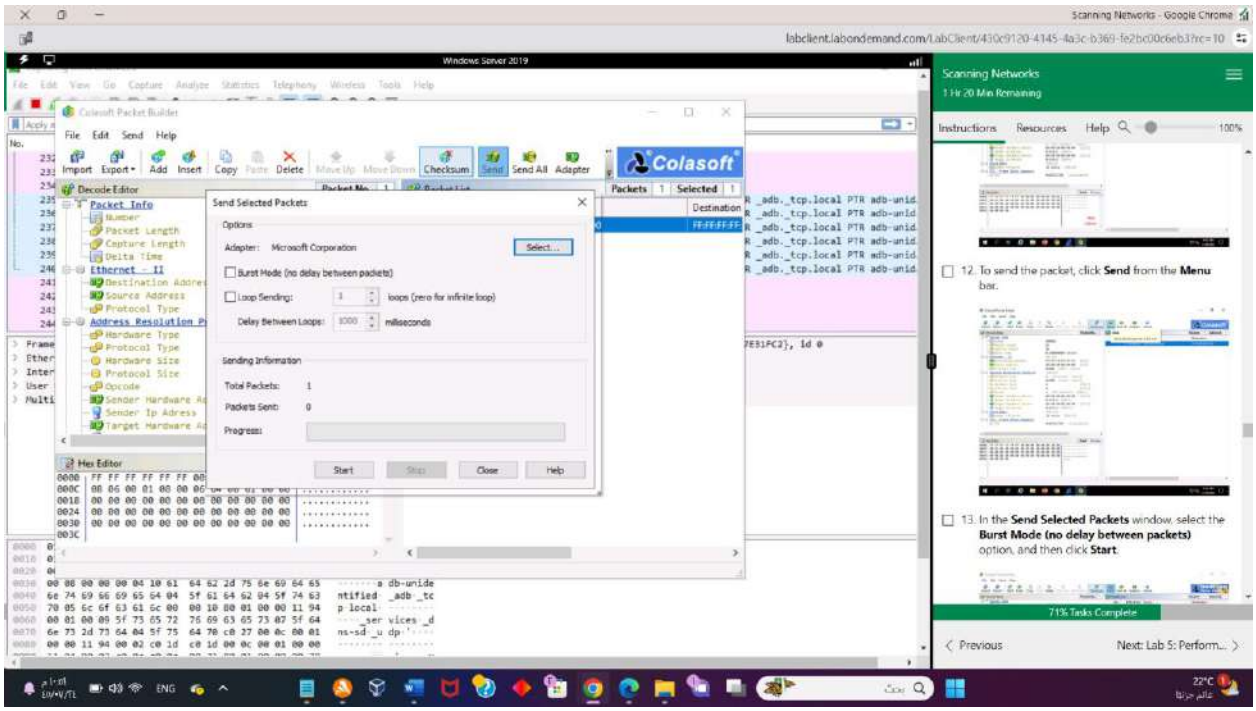


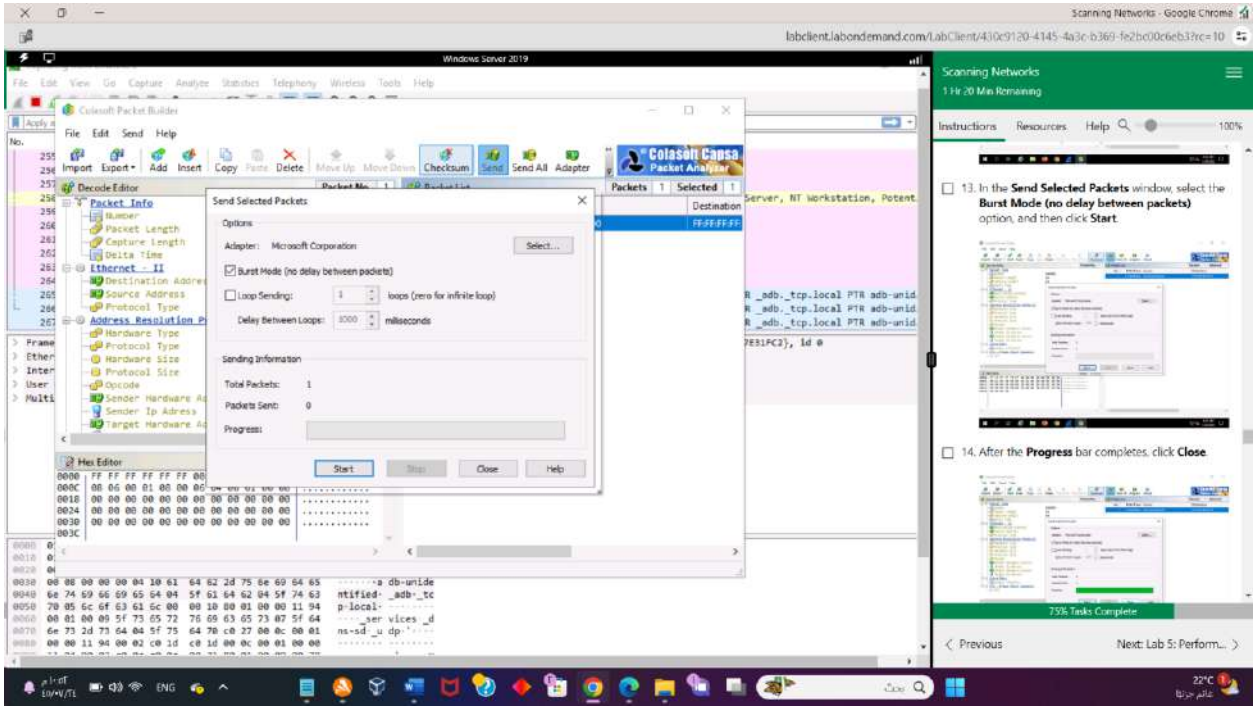

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter
Colasoft
Decode Editor
Packet List
No. Delta Time Source
Adapter
Select a default adapter for sending packet.
Hex Editor
Scanning Networks
1 Hr 22 Min Remaining
Instructions Resources Help 100%
6. The Colasoft Packet Builder GUI appears; click on the Adapter icon, as shown in the screenshot.
If a pop-up appears, close the window.
7. When the Select Adapter window appears, check the Adapter settings and click OK.
71% Tasks Complete
Previous
Next: Lab 5: Perform...

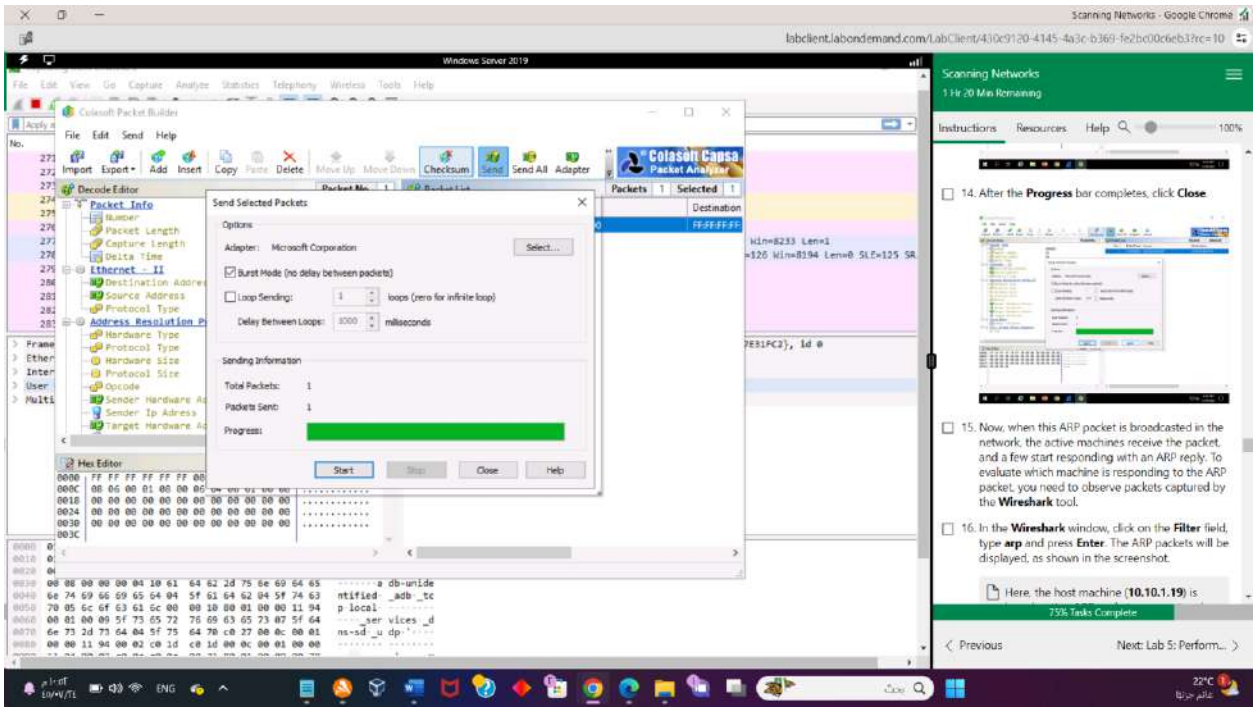

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter
Colasoft Capsa Packet Analyzer
Decode Editor
Packet List
No. Delta Time Source Destination
Select Adapter
Adapter: Microsoft Corporation
Physical Address 02:15:5D:39:EA:2F(802.3)
Link Speed 1410.1 Mbps
Max Frame Size 1500 bytes
IP Address 10.10.1.19/255.255.255.0
Default Gateway 10.10.1.2
Adapter Status LAN Operational
OK Cancel Help
Hex Editor
Scanning Networks
1 Hr 22 Min Remaining
Instructions Resources Help 100%
6. The Colasoft Packet Builder GUI appears; click on the Adapter icon, as shown in the screenshot.
If a pop-up appears, close the window.
7. When the Select Adapter window appears, check the Adapter settings and click OK.
71% Tasks Complete
Previous
Next: Lab 5: Perform...

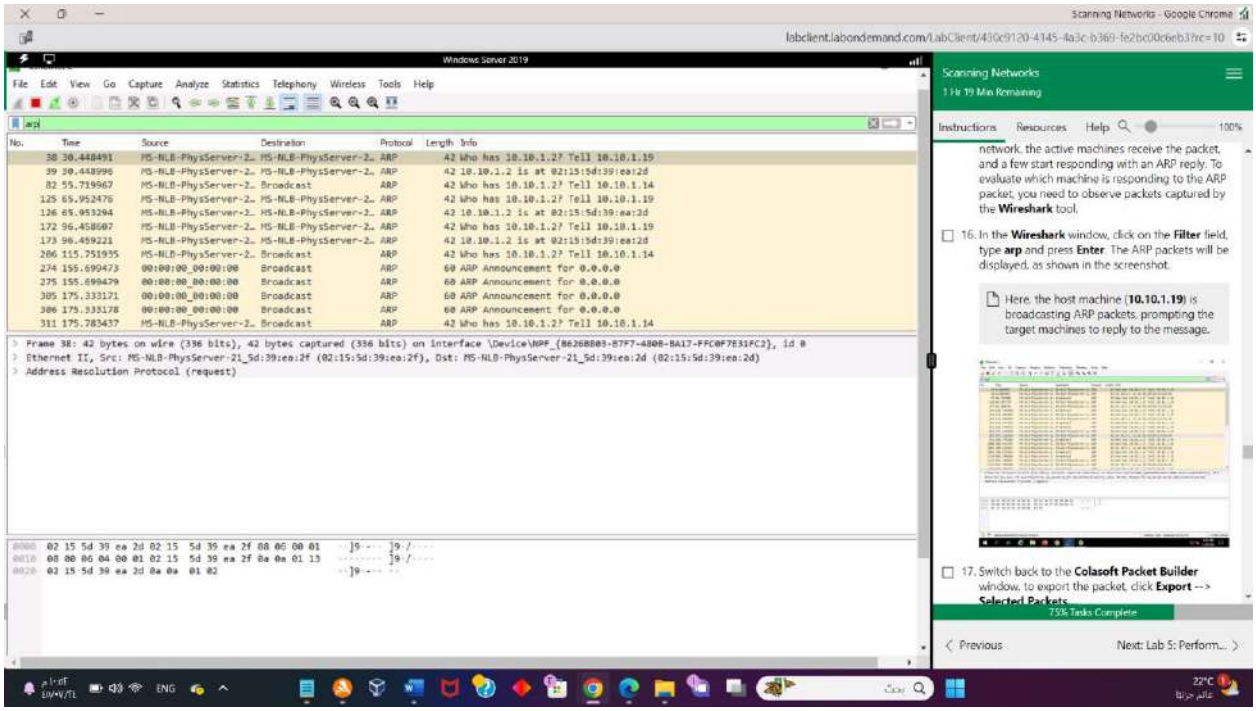

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter
Colasoft Capsa Packet Analyzer
Decode Editor
Packet List
No. Delta Time Source Destination
Add Packet
Select Template: ARP Packet
Delta Time: 0.1 Second
OK Cancel Help
Hex Editor
Scanning Networks
1 Hr 21 Min Remaining
Instructions Resources Help 100%
9. In the Add Packet dialog box, select the ARP Packet template, set Delta Time as 0.1 seconds, and click OK.
10. You can view the added packets list on the right-hand side of the window, under Packet List.
71% Tasks Complete
Previous
Next: Lab 5: Perform...

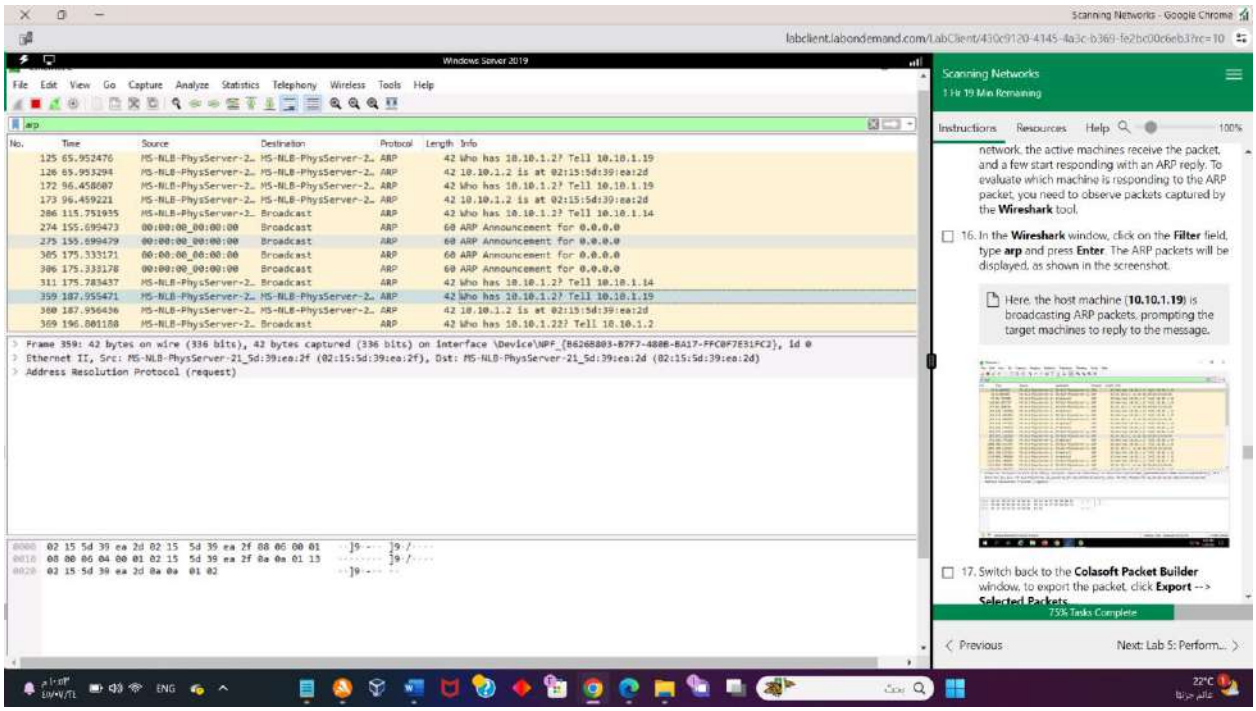

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
File Edit Send Help
Import Export Add Insert Copy Delete Checksum Send Send All Adapter
Colasoft Capsa Packet Analyzer
Decode Editor Packet No. 1
Packet List Packets 1 Selected 1
No. Delta Time Source Destination
Packet Info
Number 000001
Packet Length 64
Capture Length 60
Delta Time 0.100000000 Second
Ethernet - II
Destination Address FF:FF:FF:FF:FF:FF
Source Address 00:00:00:00:00:00
Protocol Type 0x806 (ARP)
Address Resolution Protocol
Hardware Type 1 (Ethernet)
Protocol Type 0x800 (IPv4)
Hardware Size 6
Protocol Size 4
Opcode 1 (ARP Request)
Sender Hardware Adress 00:00:00:00:00:00
Sender Ip Adress 0.0.0.0
Target Hardware Adress 00:00:00:00:00:00
Hex Editor Total 60 bytes
Scanning Networks
1 Hr 21 Min Remaining
Instructions Resources Help 100%
10. You can view the added packets list on the right-hand side of the window, under Packet List.
11. Colasoft Packet Builder allows you to edit the decoding information in the two editors. Decode Editor and Hex Editor, located in the left pane of the window.
The Decode Editor section allows you to
71% Tasks Complete
Previous
Next: Lab 5: Perform...

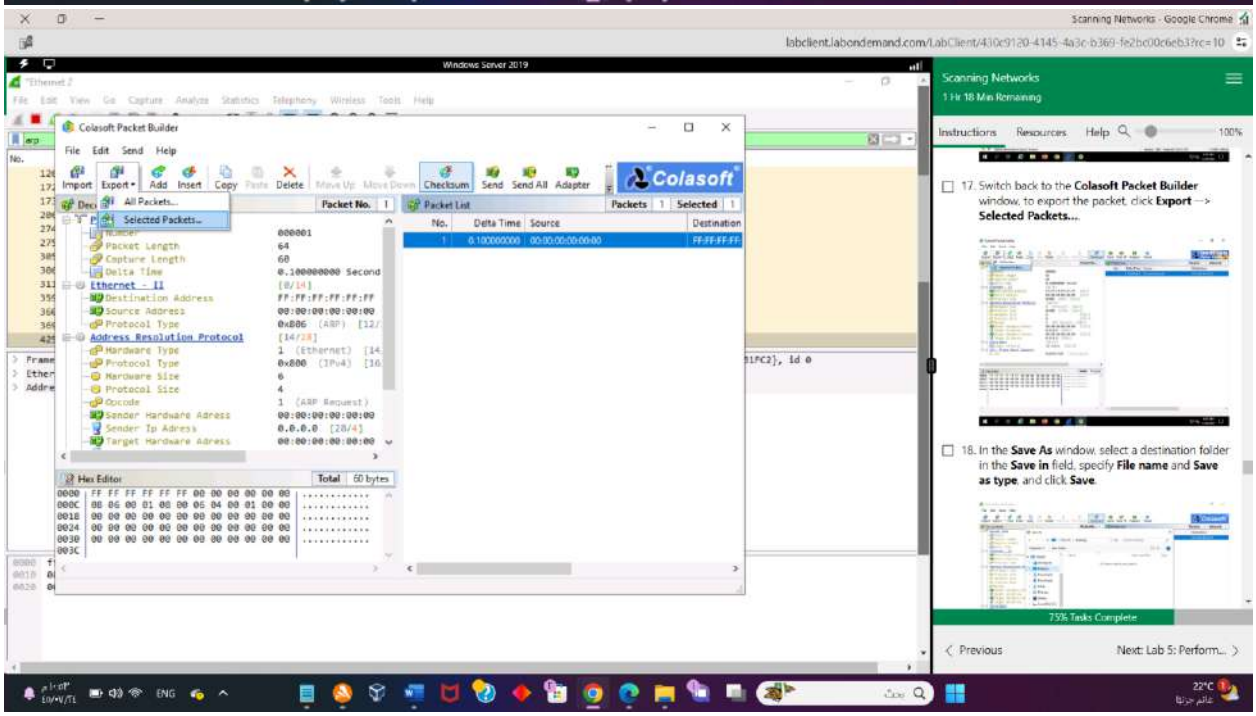

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
Send Selected Packets
Scanning Networks
1 Hr 20 Min Remaining
Instructions
Resources
Help
12. To send the packet, click Send from the Menu bar.
13. In the Send Selected Packets window, select the Burst Mode (no delay between packets) option, and then click Start.
71% Tasks Complete
Previous
Next: Lab 5: Perform...

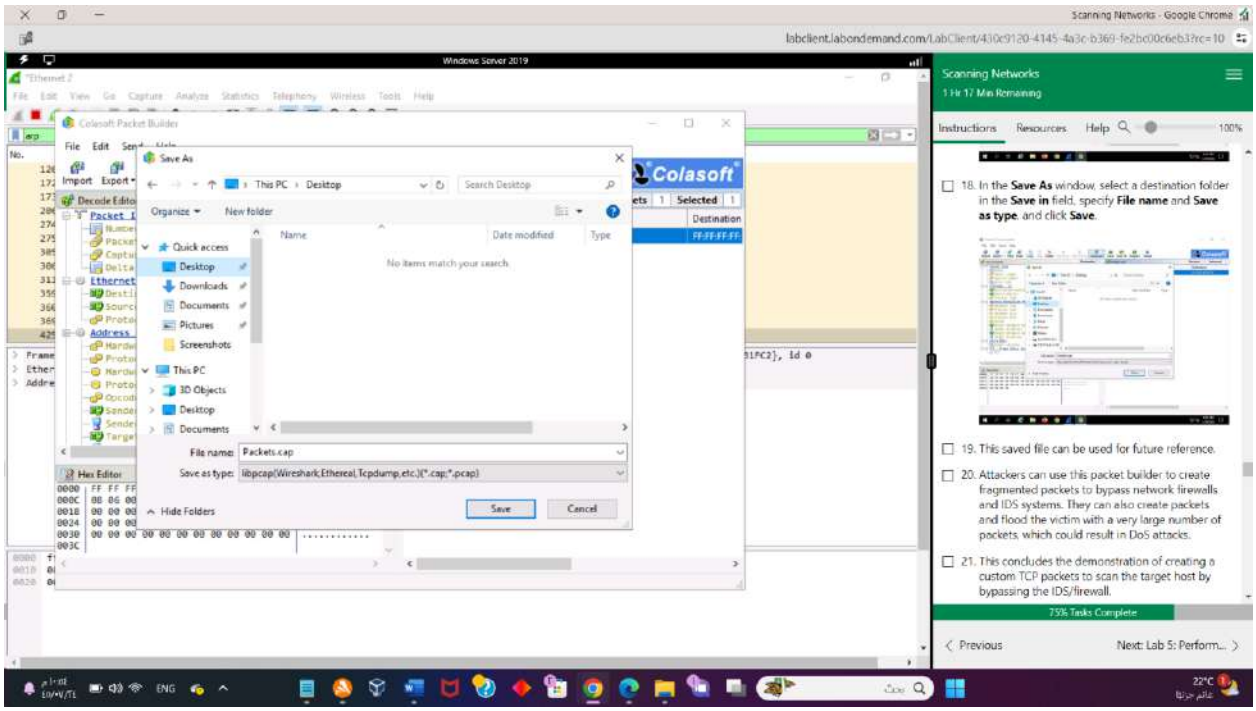

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
Send Selected Packets
Scanning Networks
1 Hr 20 Min Remaining
Instructions
Resources
Help
13. In the Send Selected Packets window, select the Burst Mode (no delay between packets) option, and then click Start.
14. After the Progress bar completes, click Close.
75% Tasks Complete
Previous
Next: Lab 5: Perform...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
Send Selected Packets
Scanning Networks
1 Hr 20 Min Remaining
Instructions
Resources
Help
14. After the Progress bar completes, click Close.
15. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the Wireshark tool.
16. In the Wireshark window, click on the Filter field, type arp and press Enter. The ARP packets will be displayed, as shown in the screenshot.
Here, the host machine (10.10.1.19) is
75% Tasks Complete
Previous
Next: Lab 5: Perform...

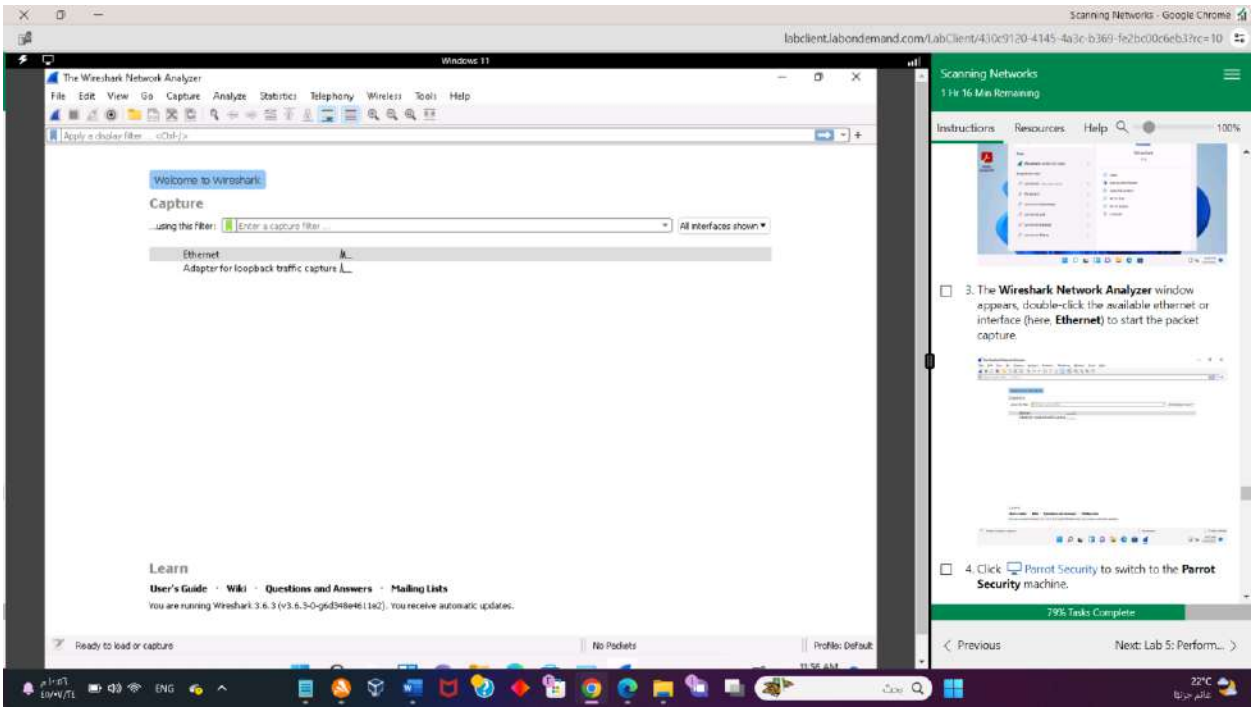

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Scanning Networks
1 Hr 19 Min Remaining
Instructions
Resources
Help
network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the Wireshark tool.
16. In the Wireshark window, click on the Filter field, type arp and press Enter. The ARP packets will be displayed, as shown in the screenshot.
Here, the host machine (10.10.1.19) is broadcasting ARP packets, prompting the target machines to reply to the message.
17. Switch back to the Colasoft Packet Builder window, to export the packet, click Export --> Selected Packets.
75% Tasks Complete
Previous
Next: Lab 5: Perform...

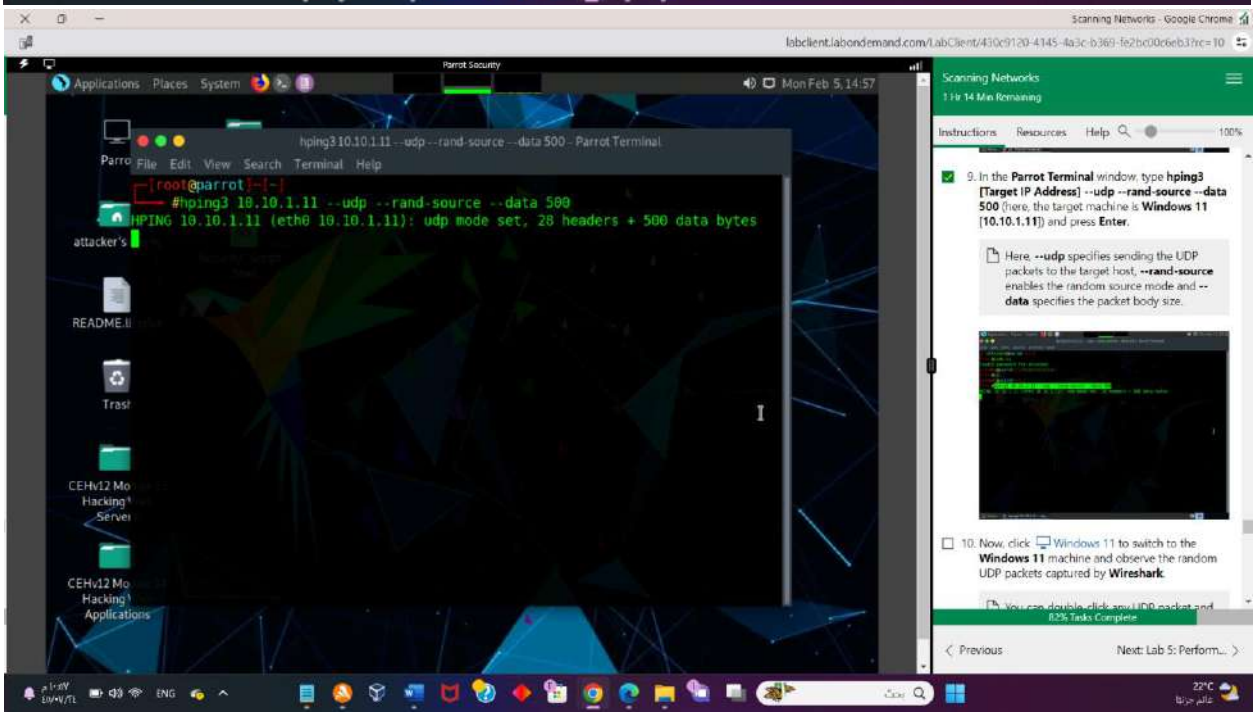

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Scanning Networks
1 Hr 19 Min Remaining
Instructions
Resources
Help
100%
network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the Wireshark tool.
16. In the Wireshark window, click on the Filter field, type arp and press Enter. The ARP packets will be displayed, as shown in the screenshot.
Here, the host machine (10.10.1.19) is broadcasting ARP packets, prompting the target machines to reply to the message.
17. Switch back to the Colasoft Packet Builder window, to export the packet, click Export --> Selected Packets...
75% Tasks Complete
Previous
Next: Lab 5: Perform...

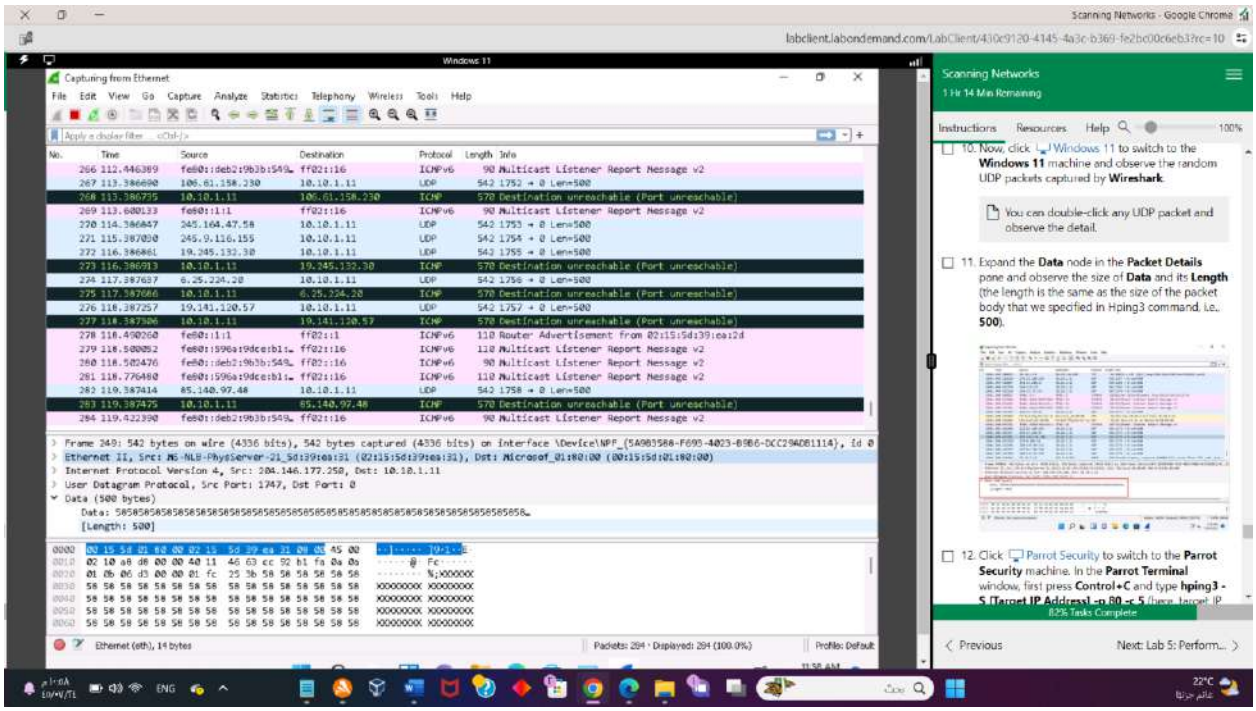

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows Server 2019
Colasoft Packet Builder
Scanning Networks
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
17. Switch back to the Colasoft Packet Builder window, to export the packet, click Export --> Selected Packets...
18. In the Save As window, select a destination folder in the Save in field, specify File name and Save as type, and click Save.
75% Tasks Complete
Previous
Next: Lab 5: Perform...

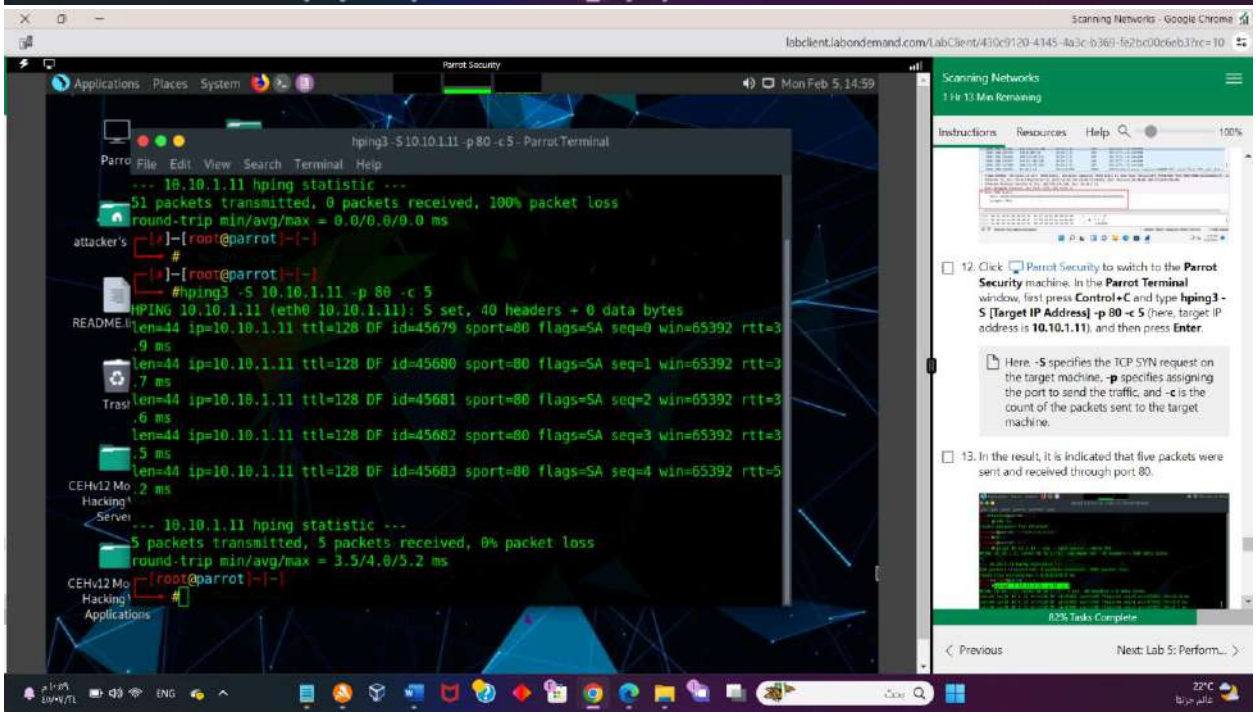


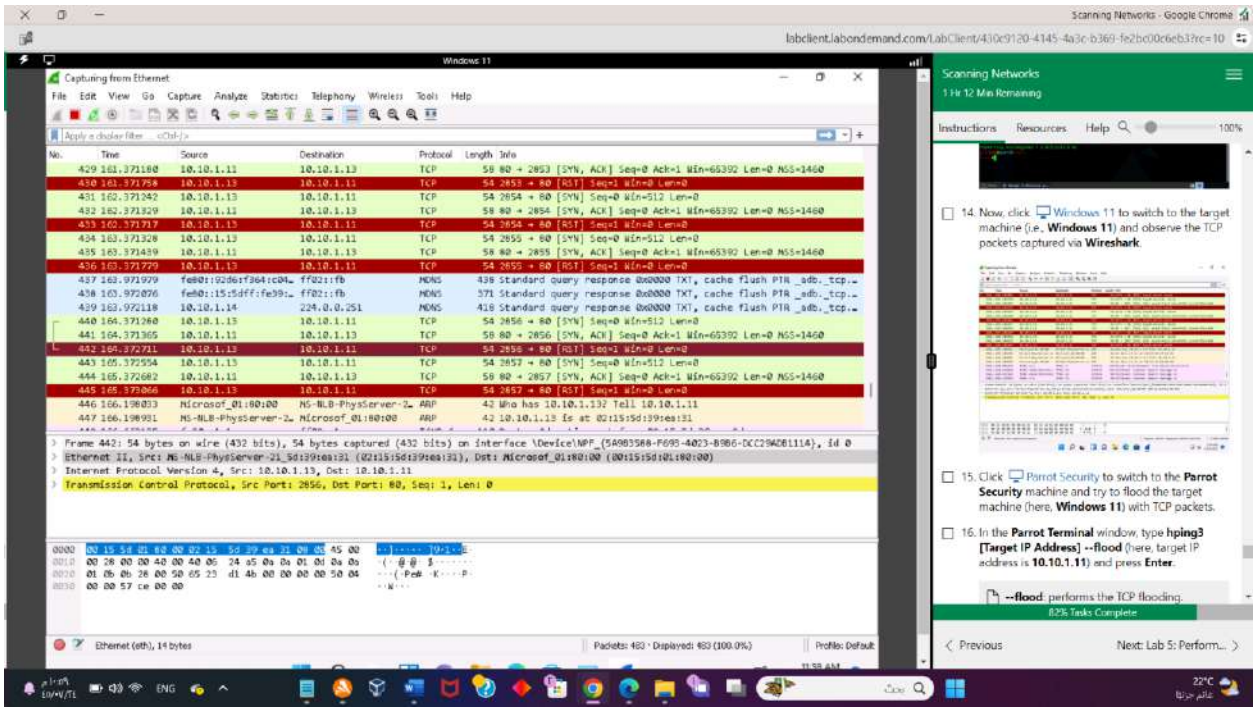
Lab 04 – Task 03

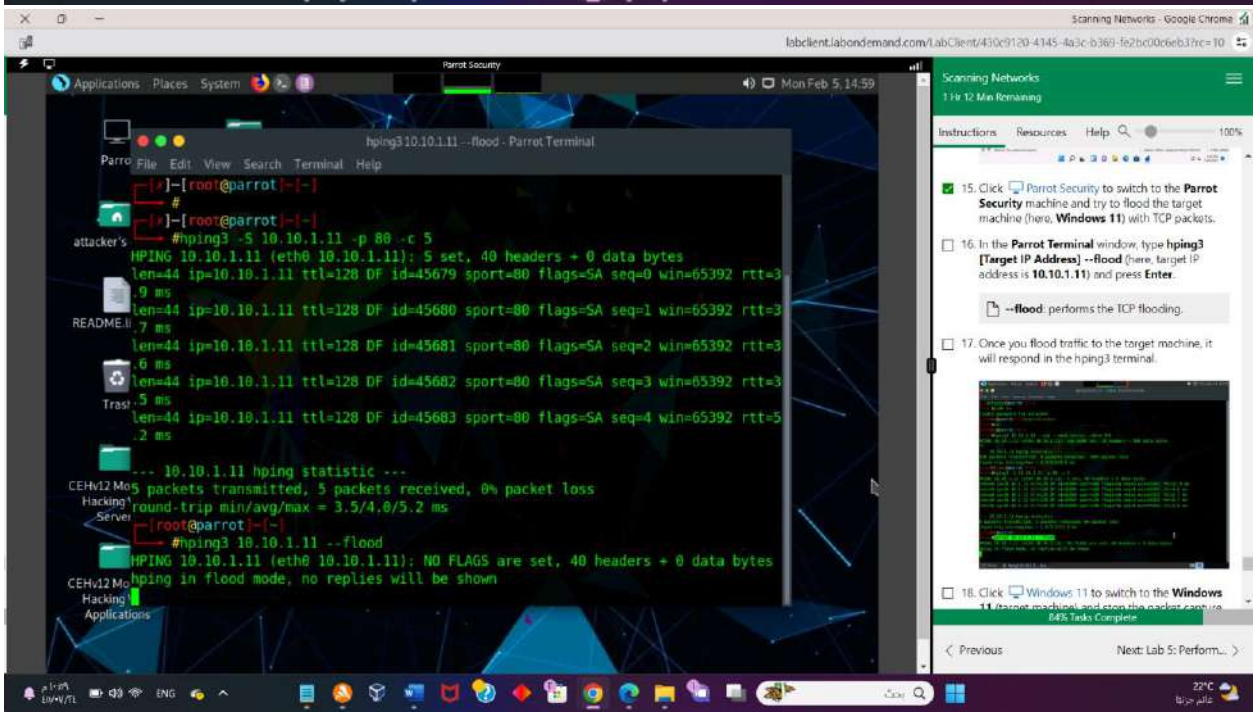

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ... All interfaces shown
Ethernet
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e61be2). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
Scanning Networks
1 Hr 16 Min Remaining
Instructions
Resources
Help
100%
3. The Wireshark Network Analyzer window appears, double-click the available ethernet or interface (here, Ethernet) to start the packet capture.
4. Click Parrot Security to switch to the Parrot Security machine.
79% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

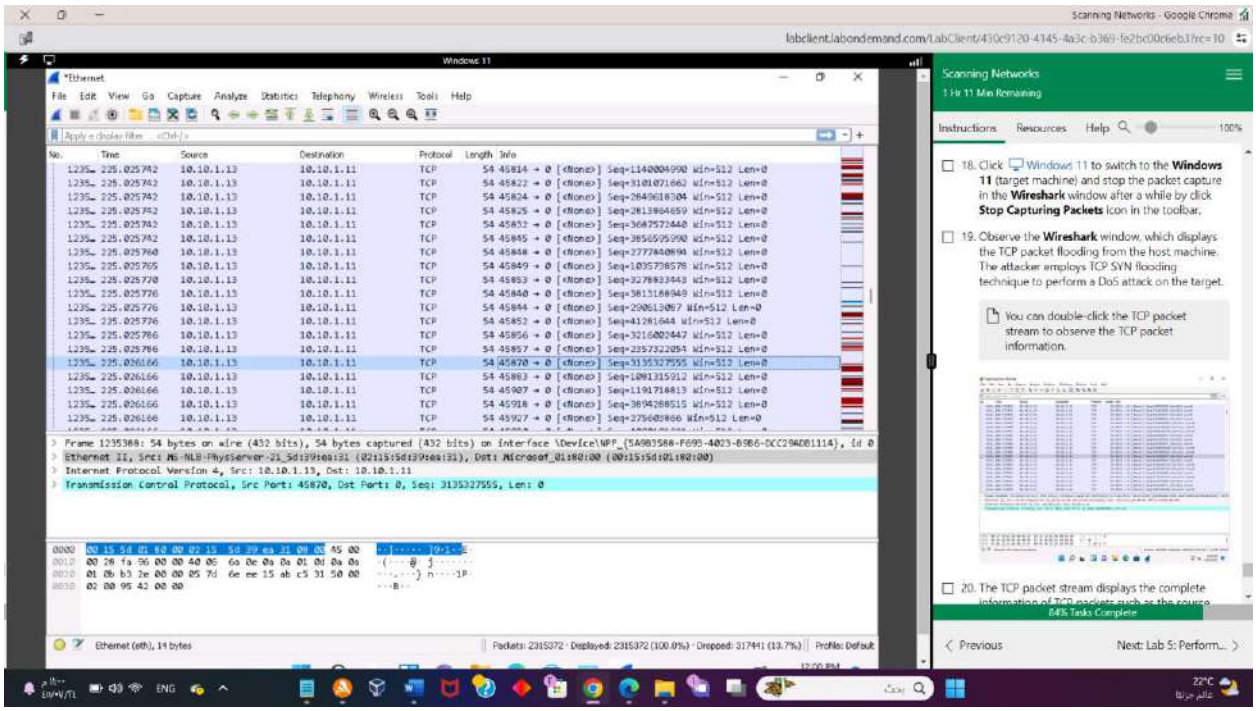

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:57
hping3 10.10.1.11 --udp --rand-source --data 500 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#hping3 10.10.1.11 --udp --rand-source --data 500
HPING 10.10.1.11 (eth0 10.10.1.11): udp mode set, 28 headers + 500 data bytes
attacker's
README.li
Trash
CEHv12 Mo
Hacking
Server
CEHv12 Mo
Hacking
Applications
Scanning Networks
1 Hr 14 Min Remaining
Instructions
Resources
Help
100%
9. In the Parrot Terminal window, type hping3 [Target IP Address] --udp --rand-source --data 500 (here, the target machine is Windows 11 [10.10.1.11]) and press Enter.
Here, --udp specifies sending the UDP packets to the target host, --rand-source enables the random source mode and --data specifies the packet body size.
10. Now, click Windows 11 to switch to the Windows 11 machine and observe the random UDP packets captured by Wireshark.
82% Tasks Complete
Previous
Next: Lab 5: Perform...
ENG
22°C

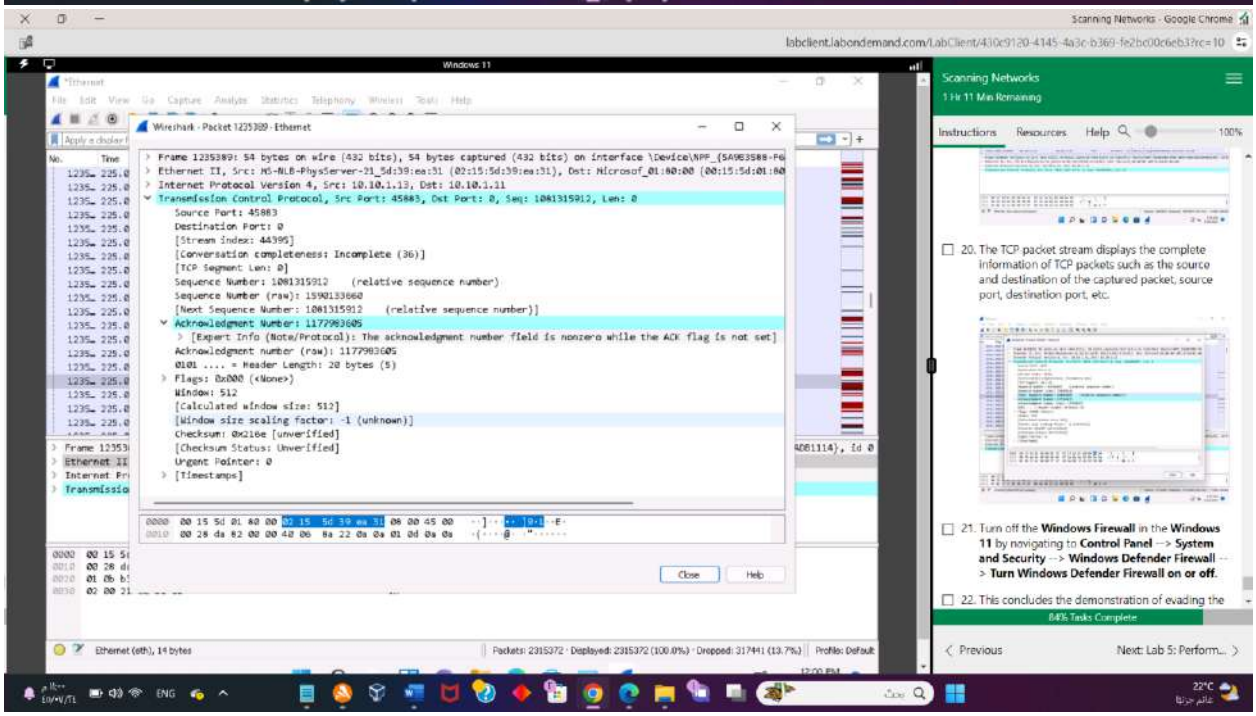

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Scanning Networks
1 Hr 14 Min Remaining
Instructions Resources Help 100%
10. Now, click Windows 11 to switch to the Windows 11 machine and observe the random UDP packets captured by Wireshark.
You can double-click any UDP packet and observe the detail.
11. Expand the Data node in the Packet Details pane and observe the size of Data and its Length (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., 500).
12. Click Parrot Security to switch to the Parrot Security machine. In the Parrot Terminal window, first press Control+C and type hping3 - S [Target IP Address] -p 80 -c 5 (here, target IP
82% Tasks Complete
Previous
Next: Lab 5: Perform...

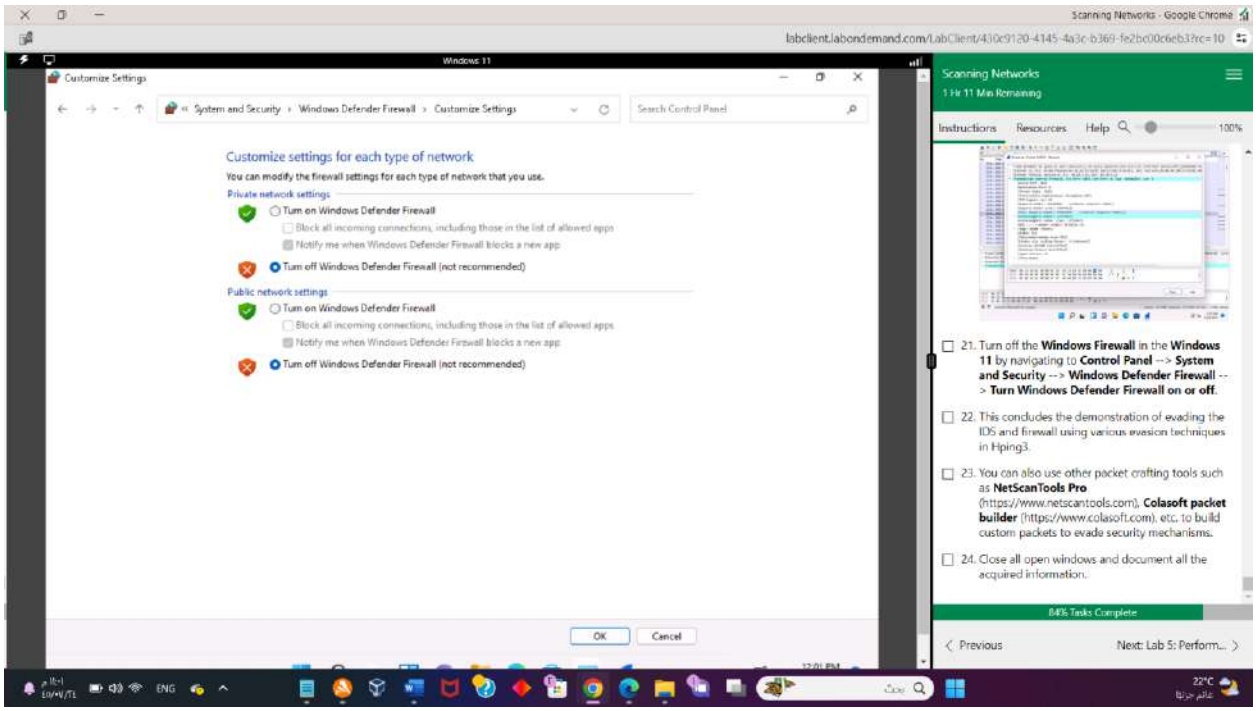

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 14:59
hping3 -S 10.10.1.11 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
--- 10.10.1.11 hping statistic ---
51 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@parrot]~[~]
#
[root@parrot]~[~]
#hping3 -S 10.10.1.11 -p 80 -c 5
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
len=44 ip=10.10.1.11 ttl=128 DF id=45679 sport=80 flags=SA seq=0 win=65392 rtt=3.9 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45680 sport=80 flags=SA seq=1 win=65392 rtt=3.7 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45681 sport=80 flags=SA seq=2 win=65392 rtt=3.6 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45682 sport=80 flags=SA seq=3 win=65392 rtt=3.5 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45683 sport=80 flags=SA seq=4 win=65392 rtt=5.2 ms
--- 10.10.1.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/4.0/5.2 ms
[root@parrot]~[~]
#
Scanning Networks
1 Hr 13 Min Remaining
Instructions Resources Help 100%
12. Click Parrot Security to switch to the Parrot Security machine. In the Parrot Terminal window, first press Control+C and type hping3 - S [Target IP Address] -p 80 -c 5 (here, target IP address is 10.10.1.11), and then press Enter.
Here, -S specifies the TCP SYN request on the target machine, -p specifies assigning the port to send the traffic, and -c is the count of the packets sent to the target machine.
13. In the result, it is indicated that five packets were sent and received through port 80.
82% Tasks Complete
Previous
Next: Lab 5: Perform...


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Scanning Networks
1 Hr 12 Min Remaining
Instructions Resources Help 100%
14. Now, click Windows 11 to switch to the target machine (i.e., Windows 11) and observe the TCP packets captured via Wireshark.
15. Click Parrot Security to switch to the Parrot Security machine and try to flood the target machine (here, Windows 11) with TCP packets.
16. In the Parrot Terminal window, type hping3 [Target IP Address] --flood (here, target IP address is 10.10.1.11) and press Enter.
--flood: performs the TCP flooding.
82% Tasks Complete
Previous
Next: Lab 5: Perform...

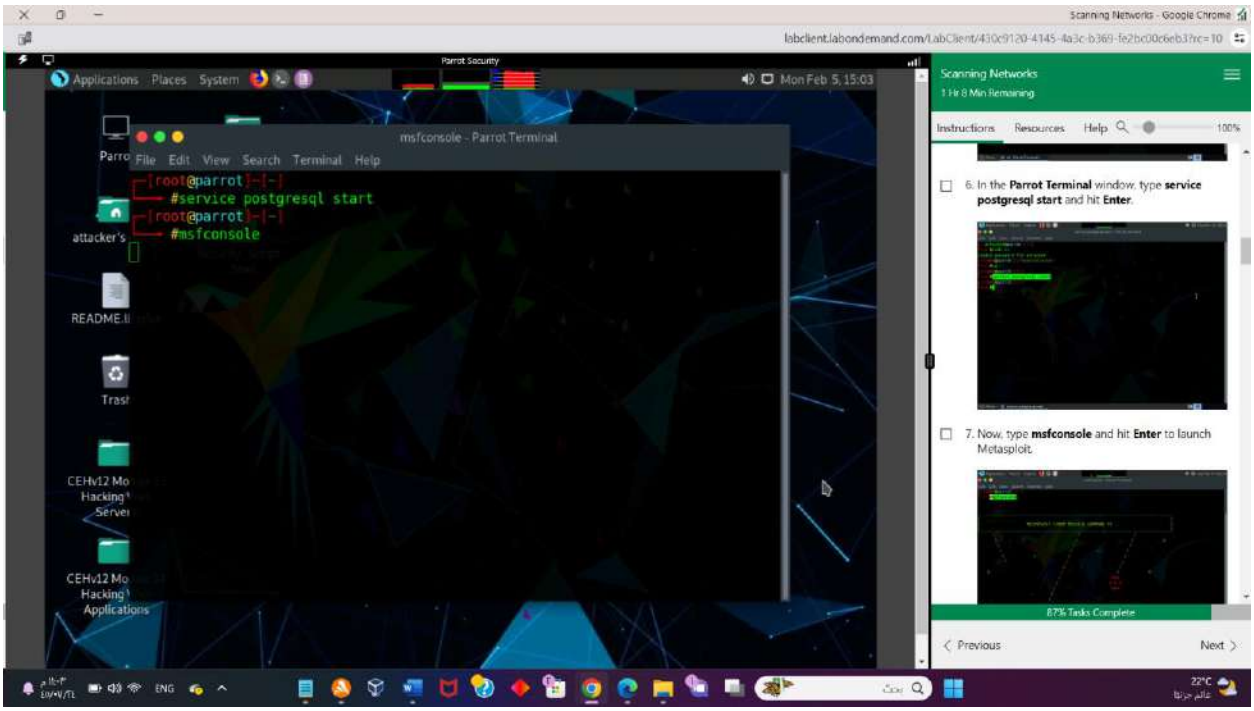

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System Mon Feb 5, 14:59
hping3 10.10.1.11 --flood - Parrot Terminal
File Edit View Search Terminal Help
#hping3 -S 10.10.1.11 -p 80 -c 5
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
--- 10.10.1.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/4.0/5.2 ms
#hping3 10.10.1.11 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
Scanning Networks
1 Hr 12 Min Remaining
Instructions Resources Help 100%
15. Click Parrot Security to switch to the Parrot Security machine and try to flood the target machine (here, Windows 11) with TCP packets.
16. In the Parrot Terminal window, type hping3 [Target IP Address] --flood (here, target IP address is 10.10.1.11) and press Enter.
--flood: performs the TCP flooding.
17. Once you flood traffic to the target machine, it will respond in the hping3 terminal.
18. Click Windows 11 to switch to the Windows
84% Tasks Complete
Previous
Next: Lab 5: Perform...

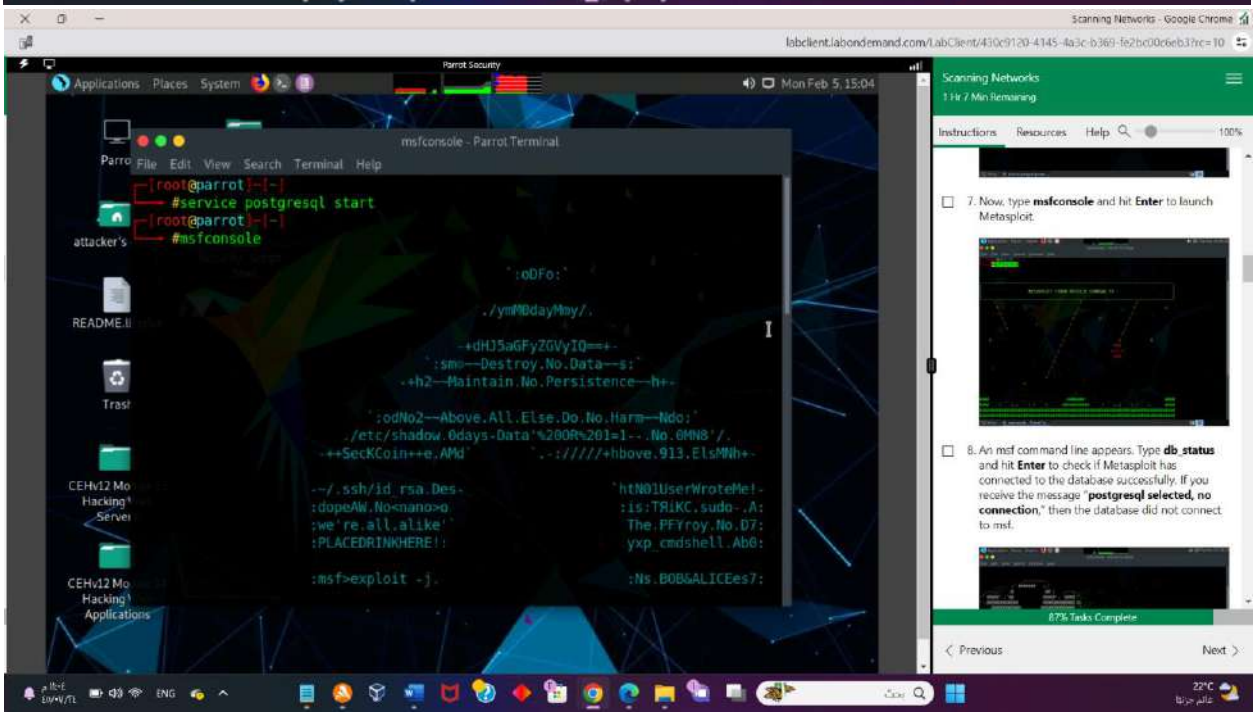

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Scanning Networks
1 Hr 11 Min Remaining
Instructions Resources Help 100%
18. Click Windows 11 to switch to the Windows 11 (target machine) and stop the packet capture in the Wireshark window after a while by click Stop Capturing Packets icon in the toolbar.
19. Observe the Wireshark window, which displays the TCP packet flooding from the host machine. The attacker employs TCP SYN flooding technique to perform a DoS attack on the target.
You can double-click the TCP packet stream to observe the TCP packet information.
20. The TCP packet stream displays the complete
84% Tasks Complete
Previous
Next: Lab 5: Perform...
Ethernet (eth), 14 bytes
Packets: 2315372 · Displayed: 2315372 (100.0%) · Dropped: 317441 (13.7%)
Profile: Default
ENG
22°C

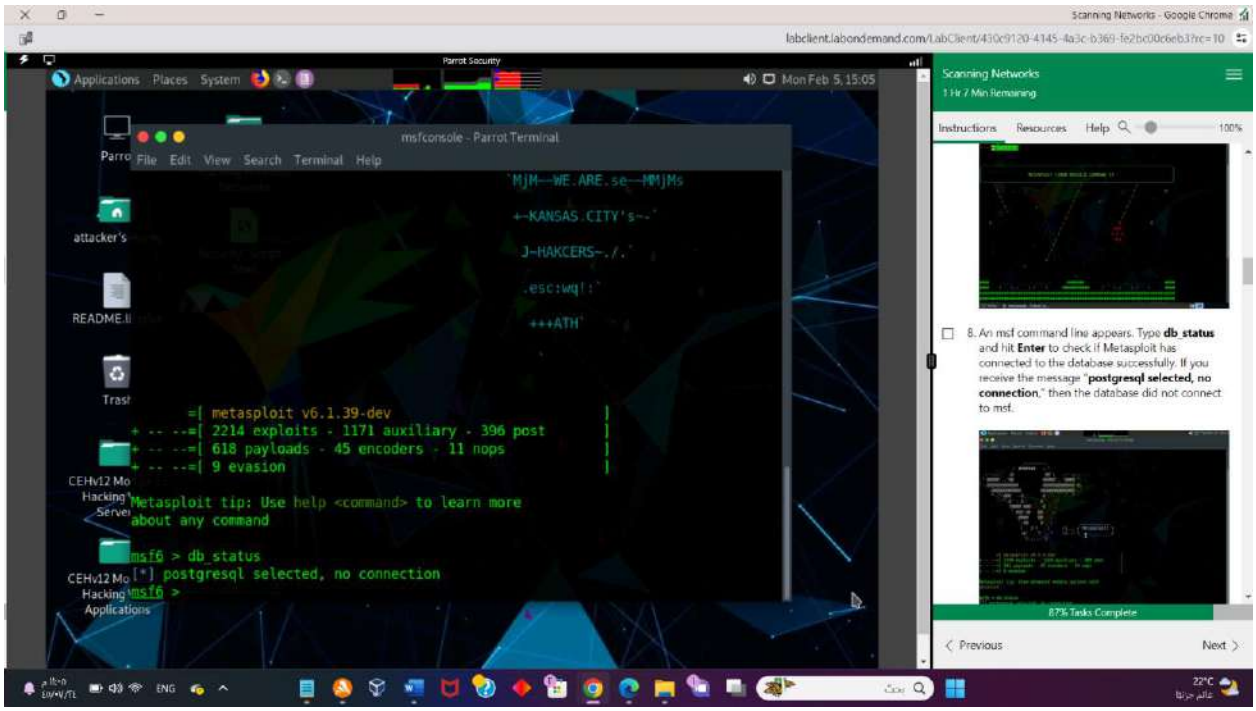

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Windows 11
Wireshark · Packet 1235389 · Ethernet
Frame 1235389: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{5A983588-F6
Ethernet II, Src: MS-NLB-PhysServer-21_5d:39:ea:31 (02:15:5d:39:ea:31), Dst: Microsof_01:80:00 (00:15:5d:01:80
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.11
Transmission Control Protocol, Src Port: 45883, Dst Port: 0, Seq: 1081315912, Len: 0
Source Port: 45883
Destination Port: 0
[Stream index: 44395]
[Conversation completeness: Incomplete (36)]
[TCP Segment Len: 0]
Sequence Number: 1081315912 (relative sequence number)
Sequence Number (raw): 1590133660
[Next Sequence Number: 1081315912 (relative sequence number)]
Acknowledgment Number: 1177983605
[Expert Info (Note/Protocol): The acknowledgment number field is nonzero while the ACK flag is not set]
Acknowledgment number (raw): 1177983605
0101 .... = Header Length: 20 bytes (5)
Flags: 0x000 (<None>)
Window: 512
[Calculated window size: 512]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x216e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
Close
Help
Scanning Networks
1 Hr 11 Min Remaining
Instructions Resources Help 100%
20. The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.
21. Turn off the Windows Firewall in the Windows 11 by navigating to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off.
22. This concludes the demonstration of evading the
84% Tasks Complete
Previous
Next: Lab 5: Perform...
Ethernet (eth), 14 bytes
Packets: 2315372 · Displayed: 2315372 (100.0%) · Dropped: 317441 (13.7%)
Profile: Default
ENG
22°C

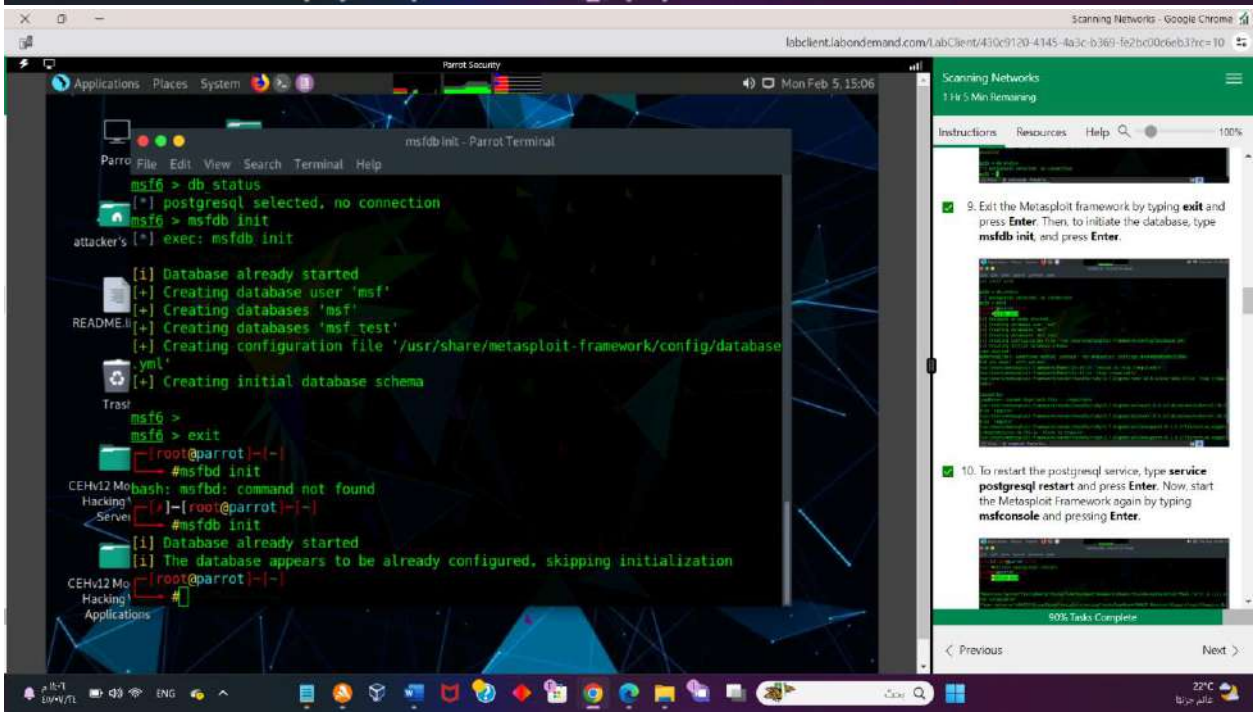


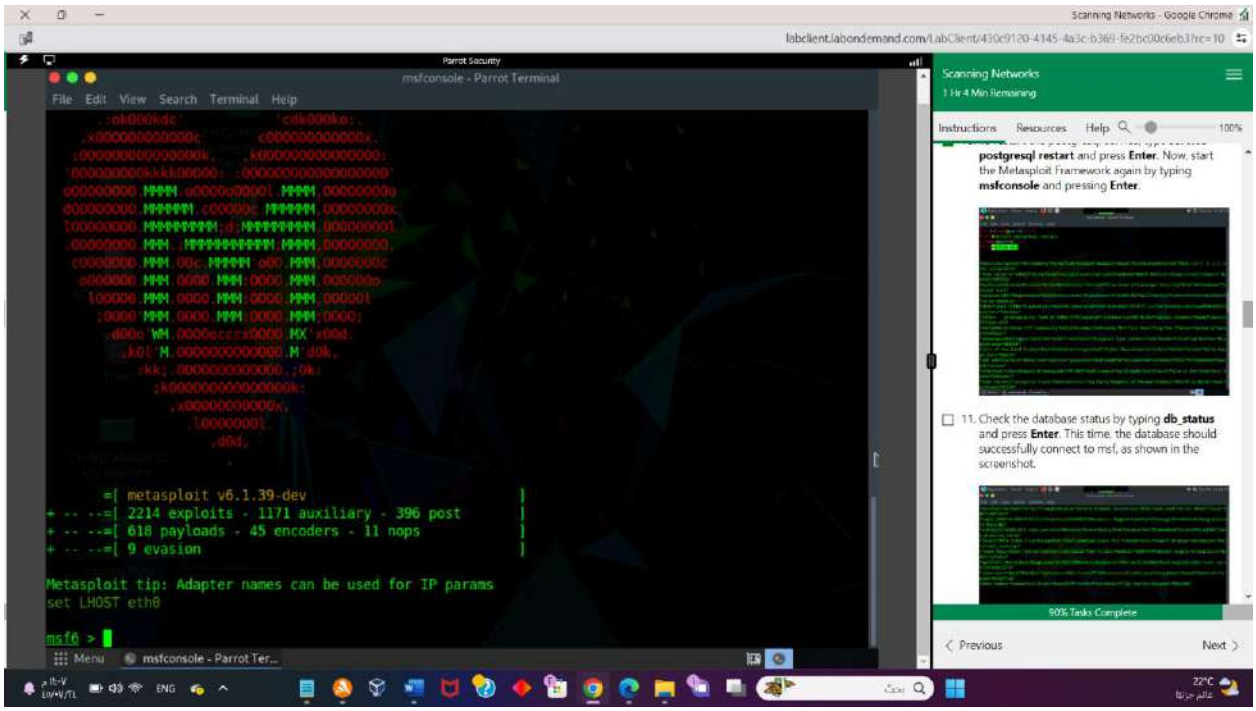
Lab 05 – Task 01

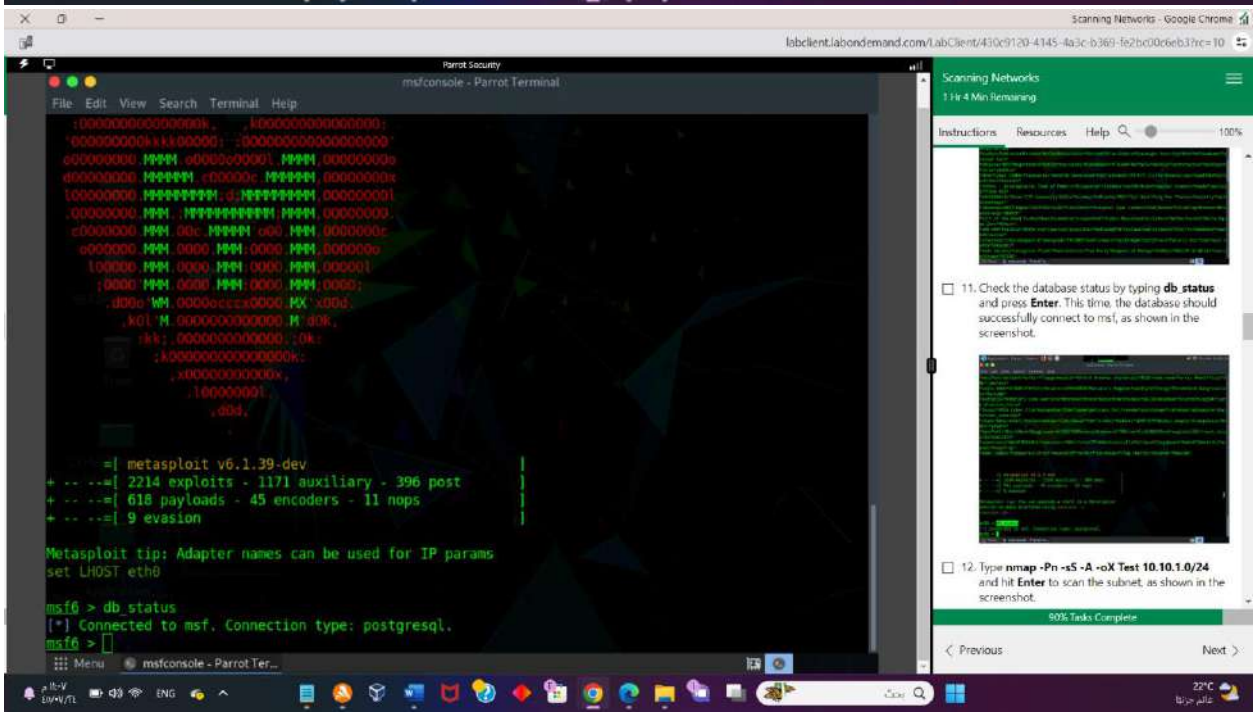

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 15:03
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#service postgresql start
[root@parrot]~[~]
#msfconsole
attacker's
README.li
Trash
CEHv12 Mo Hacking Server
CEHv12 Mo Hacking Applications
Scanning Networks
1 Hr 8 Min Remaining
Instructions
Resources
Help
100%
6. In the Parrot Terminal window, type service postgresql start and hit Enter.
7. Now, type msfconsole and hit Enter to launch Metasploit.
87% Tasks Complete
Previous
Next
ENG
22°C

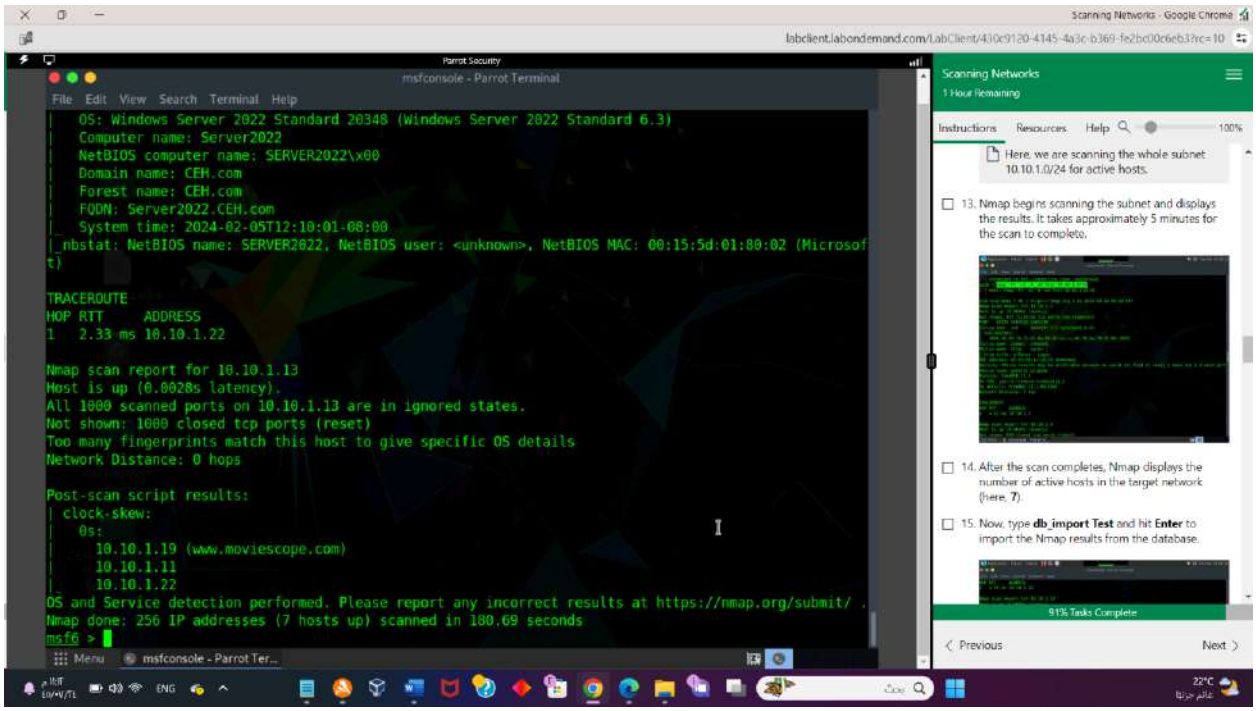

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 15:04
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#service postgresql start
[root@parrot]~[~]
#msfconsole
:oDFo:`
./ymM0dayMmy/.
-+dHJ5aGFyZGVyIQ==+-
`:sm⏓Destroy.No.Data—s:`
-+h2—Maintain.No.Persistence—h+-
':odNo2—Above.All.Else.Do.No.Harm—Ndo:'
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
-++SecKCoin++e.AMd` `.-://///+hbove.913.ElsMNh+-
~/.ssh/id_rsa.Des- 'htN01UserWroteMe!-
:dopeAW.No<nano>o :is:TRiKC.sudo-.A:
;we're.all.alike' The.PFYroy.No.D7:
:PLACEDRINKHERE!! yxp_cmdshell.Ab0:
:msf>exploit -j. :Ns.BOB&ALICEes7:
Scanning Networks
1 Hr 7 Min Remaining
Instructions
Resources
Help
100%
7. Now, type msfconsole and hit Enter to launch Metasploit.
8. An msf command line appears. Type db_status and hit Enter to check if Metasploit has connected to the database successfully. If you receive the message "postgresql selected, no connection," then the database did not connect to msf.
87% Tasks Complete
Previous
Next
ENG
22°C

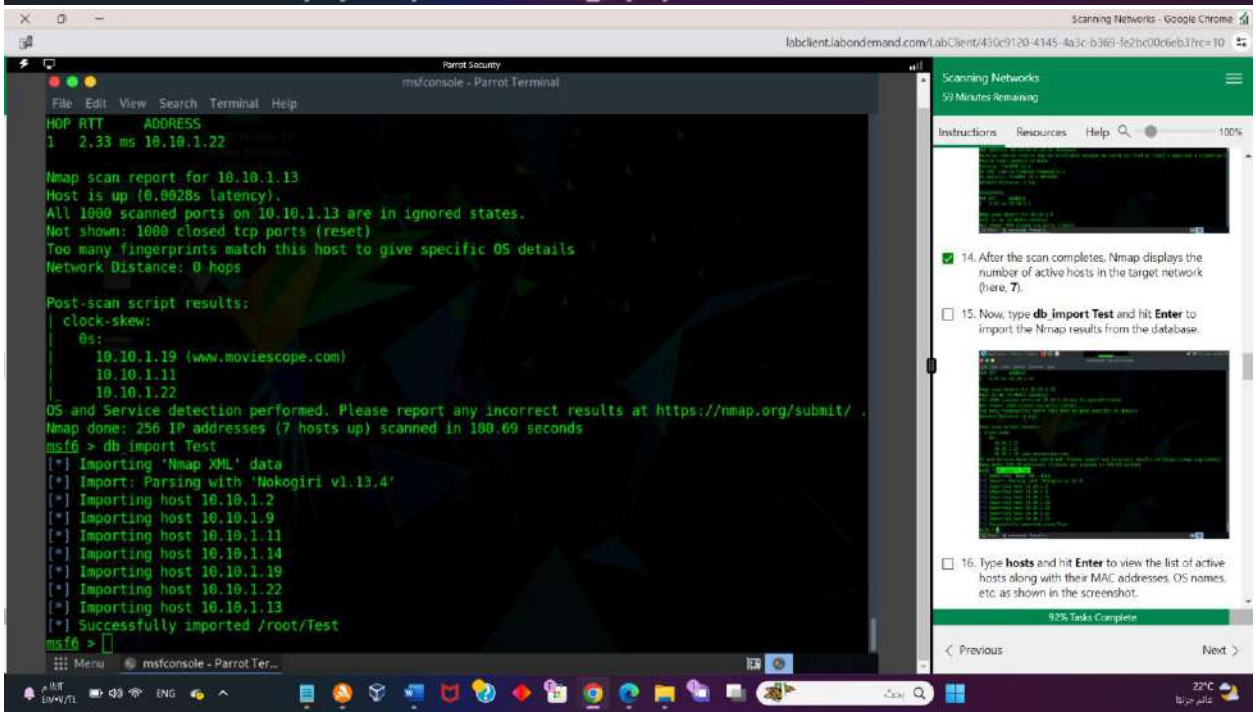

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 15:05
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.1.39-dev]
+ -- --=[2214 exploits - 1171 auxiliary - 396 post]
+ -- --=[618 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use help <command> to learn more about any command
msf6 > db_status
[*] postgresql selected, no connection
msf6 >
Scanning Networks
1 Hr 7 Min Remaining
Instructions Resources Help 100%
8. An msf command line appears. Type db_status and hit Enter to check if Metasploit has connected to the database successfully. If you receive the message "postgresql selected, no connection," then the database did not connect to msf.
87% Tasks Complete
Previous
Next
22°C

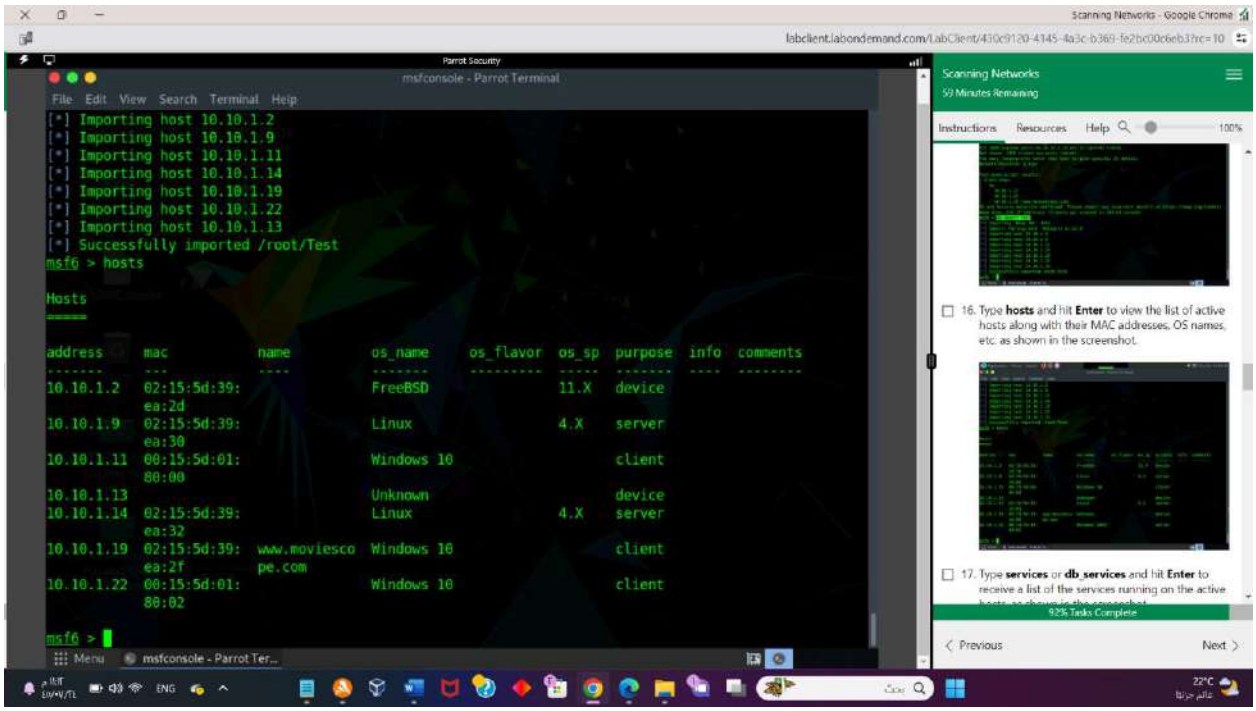

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
Applications Places System
Mon Feb 5, 15:06
msfdb init - Parrot Terminal
File Edit View Search Terminal Help
msf6 > db_status
[*] postgresql selected, no connection
msf6 > msfdb init
[*] exec: msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
msf6 >
msf6 > exit
#msfbd init
bash: msfbd: command not found
#msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Scanning Networks
1 Hr 5 Min Remaining
Instructions Resources Help 100%
9. Exit the Metasploit framework by typing exit and press Enter. Then, to initiate the database, type msfdb init, and press Enter.
10. To restart the postgresql service, type service postgresql restart and press Enter. Now, start the Metasploit Framework again by typing msfconsole and pressing Enter.
90% Tasks Complete
Previous
Next
22°C

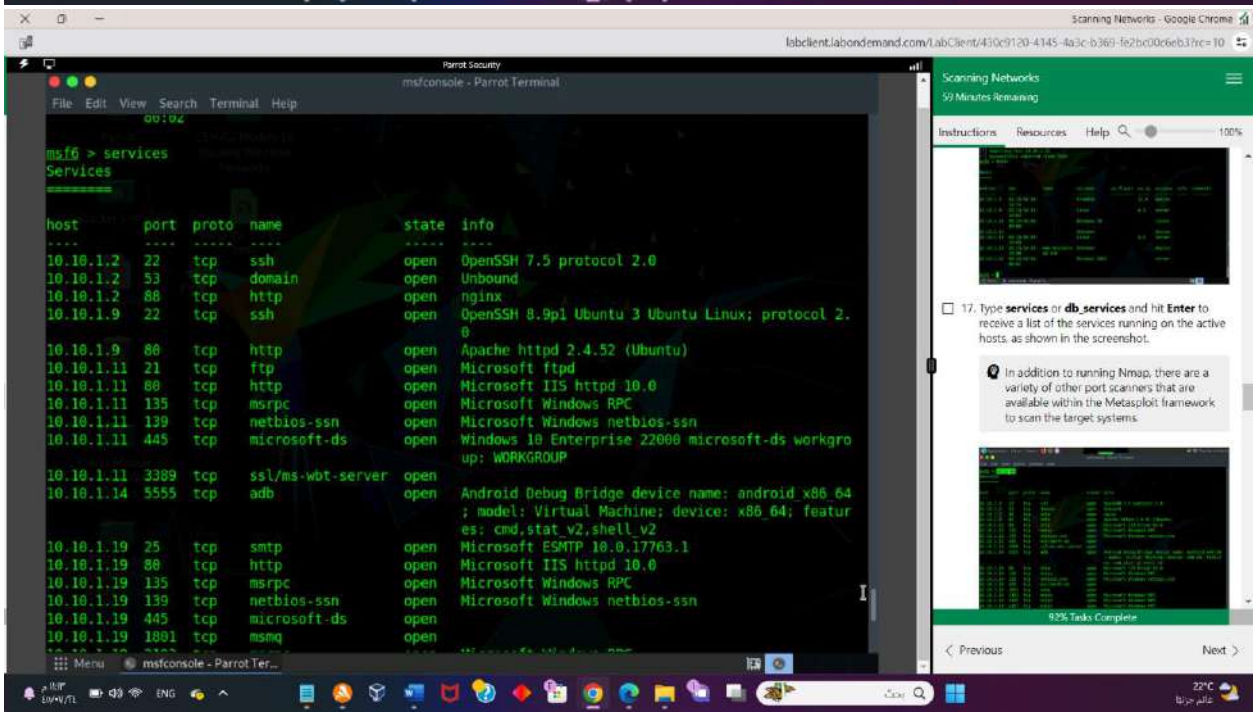

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.1.39-dev
+ -- --=[2214 exploits - 1171 auxiliary - 396 post
+ -- --=[618 payloads - 45 encoders - 11 nops
+ -- --=[9 evasion
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
msf6 >
Menu
msfconsole - Parrot Ter...
Scanning Networks
1 Hr 4 Min Remaining
Instructions
Resources
Help
100%
postgresql restart and press Enter. Now, start the Metasploit Framework again by typing msfconsole and pressing Enter.
11. Check the database status by typing db_status and press Enter. This time, the database should successfully connect to msf, as shown in the screenshot.
90% Tasks Complete
Previous
Next
22°C

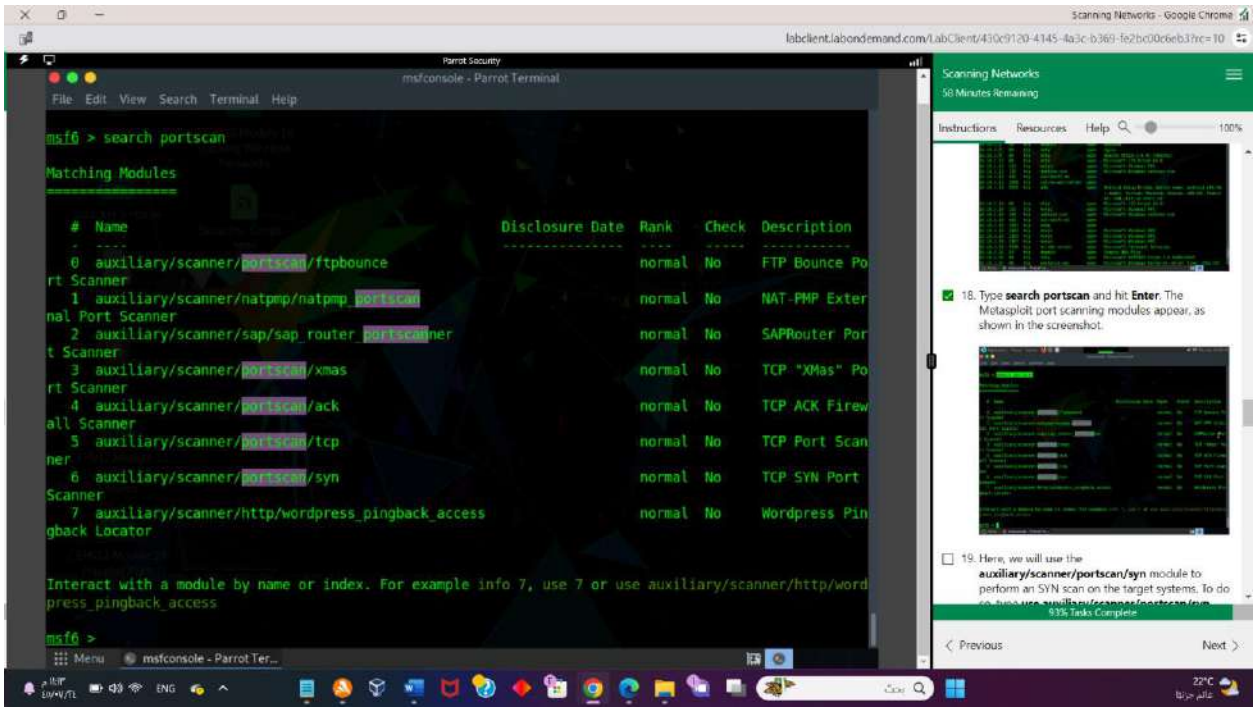

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.1.39-dev
+ -- --=[2214 exploits - 1171 auxiliary - 396 post
+ -- --=[618 payloads - 45 encoders - 11 nops
+ -- --=[9 evasion
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
Menu
msfconsole - Parrot Ter...
Scanning Networks
1 Hr 4 Min Remaining
Instructions
Resources
Help
100%
11. Check the database status by typing db_status and press Enter. This time, the database should successfully connect to msf, as shown in the screenshot.
12. Type nmap -Pn -sS -A -oX Test 10.10.1.0/24 and hit Enter to scan the subnet, as shown in the screenshot.
90% Tasks Complete
Previous
Next
22°C

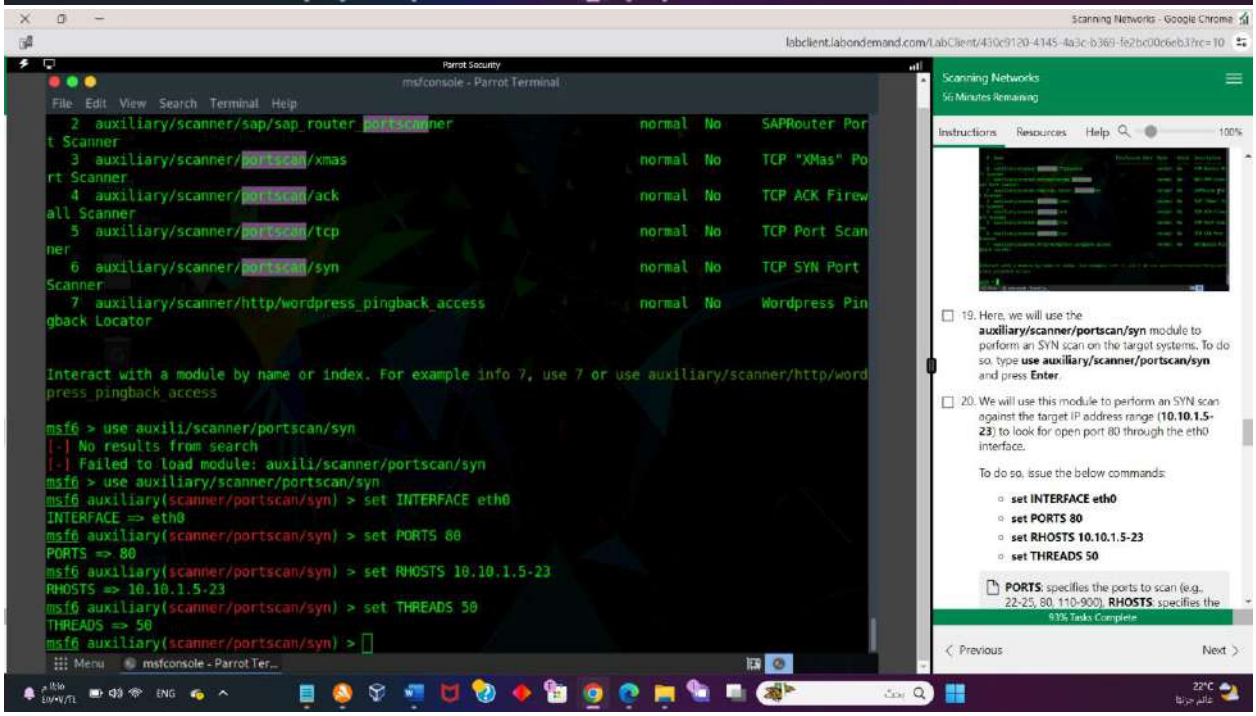

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
| OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
| Computer name: Server2022
| NetBIOS computer name: SERVER2022\x00
| Domain name: CEH.com
| Forest name: CEH.com
| FQDN: Server2022.CEH.com
|_ System time: 2024-02-05T12:10:01-08:00
|_nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microsoft)
TRACEROUTE
HOP RTT ADDRESS
1 2.33 ms 10.10.1.22
Nmap scan report for 10.10.1.13
Host is up (0.0028s latency).
All 1000 scanned ports on 10.10.1.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
Post-scan script results:
| clock-skew:
| 0s:
| 10.10.1.19 (www.moviescope.com)
| 10.10.1.11
|_ 10.10.1.22
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 180.69 seconds
msf6 >
Menu
msfconsole - Parrot Ter...
Scanning Networks
1 Hour Remaining
Instructions
Resources
Help
100%
Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.
13. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.
14. After the scan completes, Nmap displays the number of active hosts in the target network (here, 7).
15. Now, type db_import Test and hit Enter to import the Nmap results from the database.
91% Tasks Complete
Previous
Next
ENG
22°C

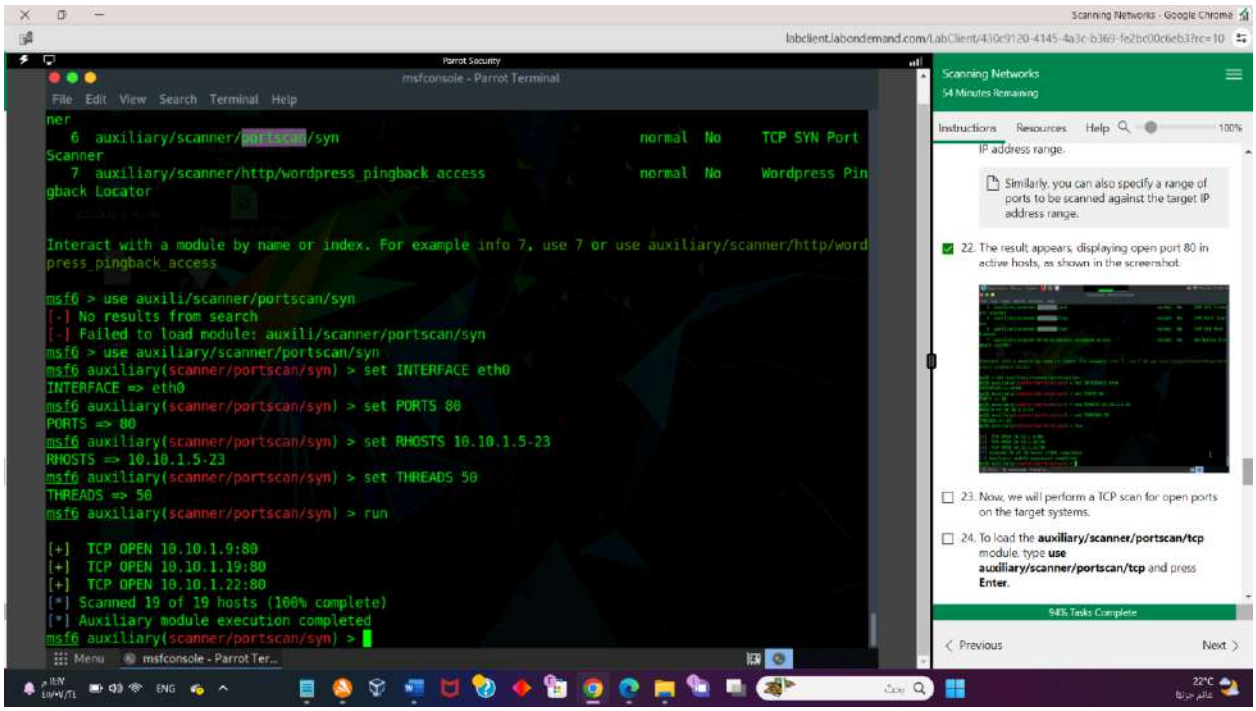

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
HOP RTT ADDRESS
1 2.33 ms 10.10.1.22
Nmap scan report for 10.10.1.13
Host is up (0.0028s latency).
All 1000 scanned ports on 10.10.1.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
Post-scan script results:
| clock-skew:
| 0s:
| 10.10.1.19 (www.moviescope.com)
| 10.10.1.11
|_ 10.10.1.22
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 180.69 seconds
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.4'
[*] Importing host 10.10.1.2
[*] Importing host 10.10.1.9
[*] Importing host 10.10.1.11
[*] Importing host 10.10.1.14
[*] Importing host 10.10.1.19
[*] Importing host 10.10.1.22
[*] Importing host 10.10.1.13
[*] Successfully imported /root/Test
msf6 >
Menu
msfconsole - Parrot Ter...
Scanning Networks
59 Minutes Remaining
Instructions
Resources
Help
100%
14. After the scan completes, Nmap displays the number of active hosts in the target network (here, 7).
15. Now, type db_import Test and hit Enter to import the Nmap results from the database.
16. Type hosts and hit Enter to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.
92% Tasks Complete
Previous
Next
ENG
22°C

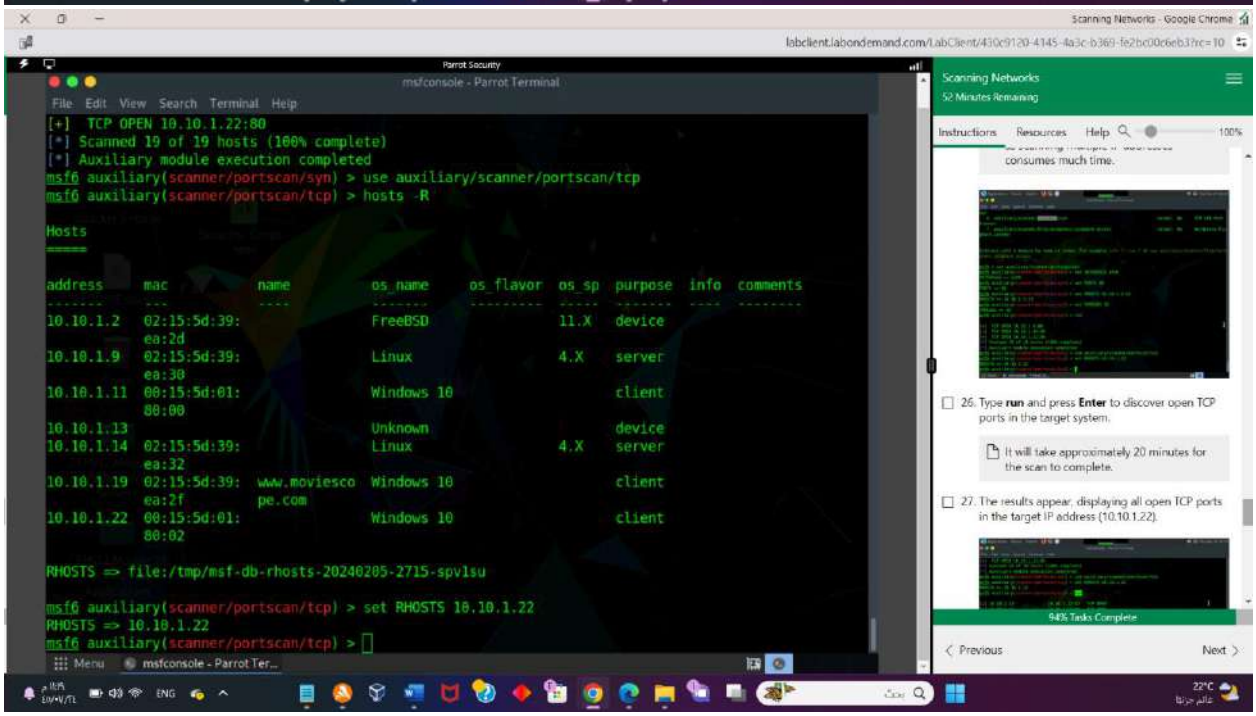

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Importing host 10.10.1.2
[*] Importing host 10.10.1.9
[*] Importing host 10.10.1.11
[*] Importing host 10.10.1.14
[*] Importing host 10.10.1.19
[*] Importing host 10.10.1.22
[*] Importing host 10.10.1.13
[*] Successfully imported /root/Test
msf6 > hosts
Hosts
address mac name os_name os_flavor os_sp purpose info comments
10.10.1.2 02:15:5d:39:ea:2d FreeBSD 11.X device
10.10.1.9 02:15:5d:39:ea:30 Linux 4.X server
10.10.1.11 00:15:5d:01:80:00 Windows 10 client
10.10.1.13 Unknown device
10.10.1.14 02:15:5d:39:ea:32 Linux 4.X server
10.10.1.19 02:15:5d:39:ea:2f www.moviescope.com Windows 10 client
10.10.1.22 00:15:5d:01:80:02 Windows 10 client
msf6 >
Menu
msfconsole - Parrot Ter...
Scanning Networks
59 Minutes Remaining
Instructions
Resources
Help
100%
16. Type hosts and hit Enter to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.
17. Type services or db_services and hit Enter to receive a list of the services running on the active
92% Tasks Complete
Previous
Next
22°C

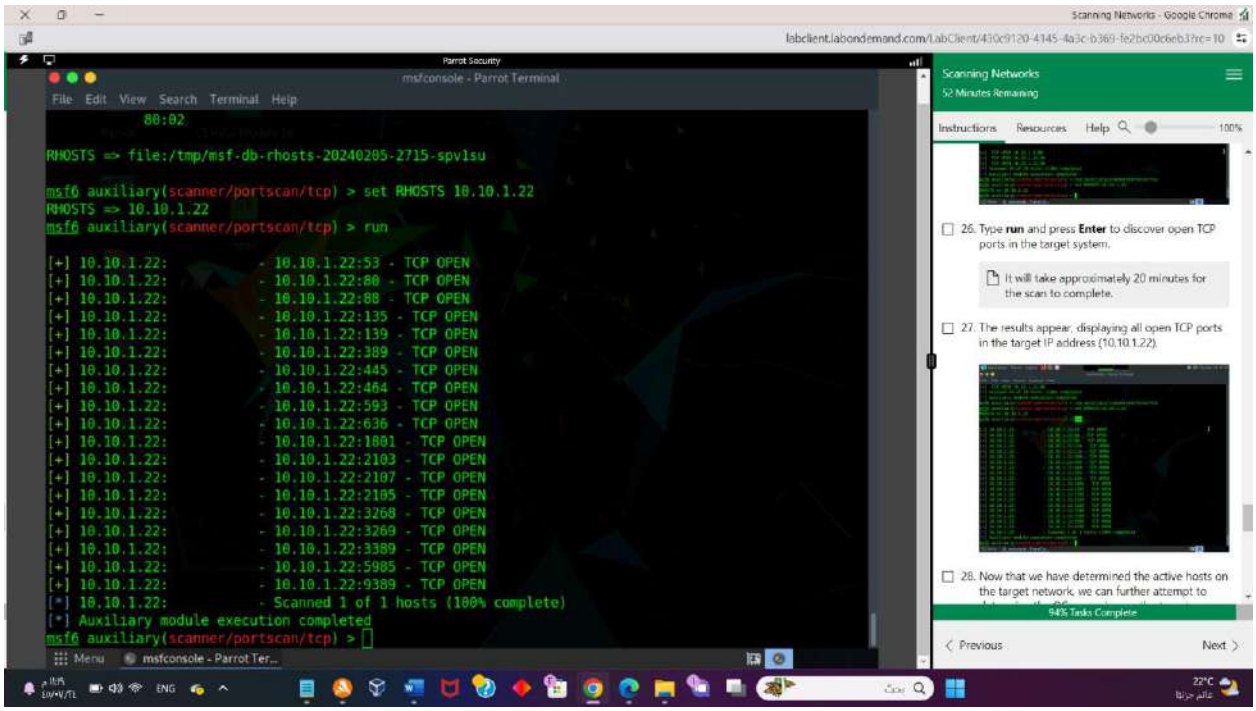

Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
msf6 > services
Services
host port proto name state info
10.10.1.2 22 tcp ssh open OpenSSH 7.5 protocol 2.0
10.10.1.2 53 tcp domain open Unbound
10.10.1.2 80 tcp http open nginx
10.10.1.9 22 tcp ssh open OpenSSH 8.9p1 Ubuntu 3 Ubuntu Linux; protocol 2.0
10.10.1.9 80 tcp http open Apache httpd 2.4.52 (Ubuntu)
10.10.1.11 21 tcp ftp open Microsoft ftpd
10.10.1.11 80 tcp http open Microsoft IIS httpd 10.0
10.10.1.11 135 tcp msrpc open Microsoft Windows RPC
10.10.1.11 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.1.11 445 tcp microsoft-ds open Windows 10 Enterprise 22000 microsoft-ds workgroup: WORKGROUP
10.10.1.11 3389 tcp ssl/ms-wbt-server open
10.10.1.14 5555 tcp adb open Android Debug Bridge device name: android_x86_64; model: Virtual Machine; device: x86_64; features: cmd,stat_v2,shell_v2
10.10.1.19 25 tcp smtp open Microsoft ESMTP 10.0.17763.1
10.10.1.19 80 tcp http open Microsoft IIS httpd 10.0
10.10.1.19 135 tcp msrpc open Microsoft Windows RPC
10.10.1.19 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.1.19 445 tcp microsoft-ds open
10.10.1.19 1801 tcp msmq open
Menu
msfconsole - Parrot Ter...
Scanning Networks
59 Minutes Remaining
Instructions
Resources
Help
100%
17. Type services or db_services and hit Enter to receive a list of the services running on the active hosts, as shown in the screenshot.
In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.
92% Tasks Complete
Previous
Next
22°C

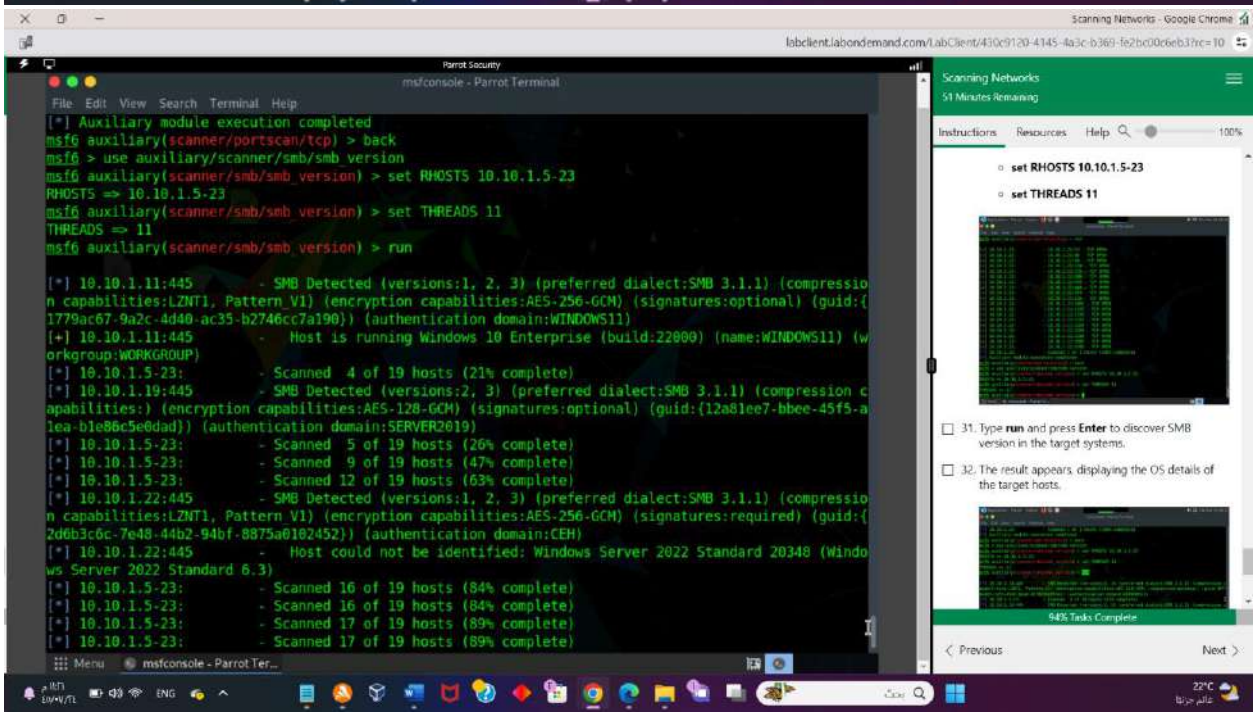

Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
msf6 > search portscan
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
1 auxiliary/scanner/natpmp/natpmp_portscan normal No NAT-PMP External Port Scanner
2 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner
3 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
4 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locator
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access
msf6 >
Menu msfconsole - Parrot Ter...
Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Scanning Networks
58 Minutes Remaining
Instructions Resources Help 100%
18. Type search portscan and hit Enter. The Metasploit port scanning modules appear, as shown in the screenshot.
19. Here, we will use the auxiliary/scanner/portscan/syn module to perform an SYN scan on the target systems. To do
93% Tasks Complete
Previous Next
22°C

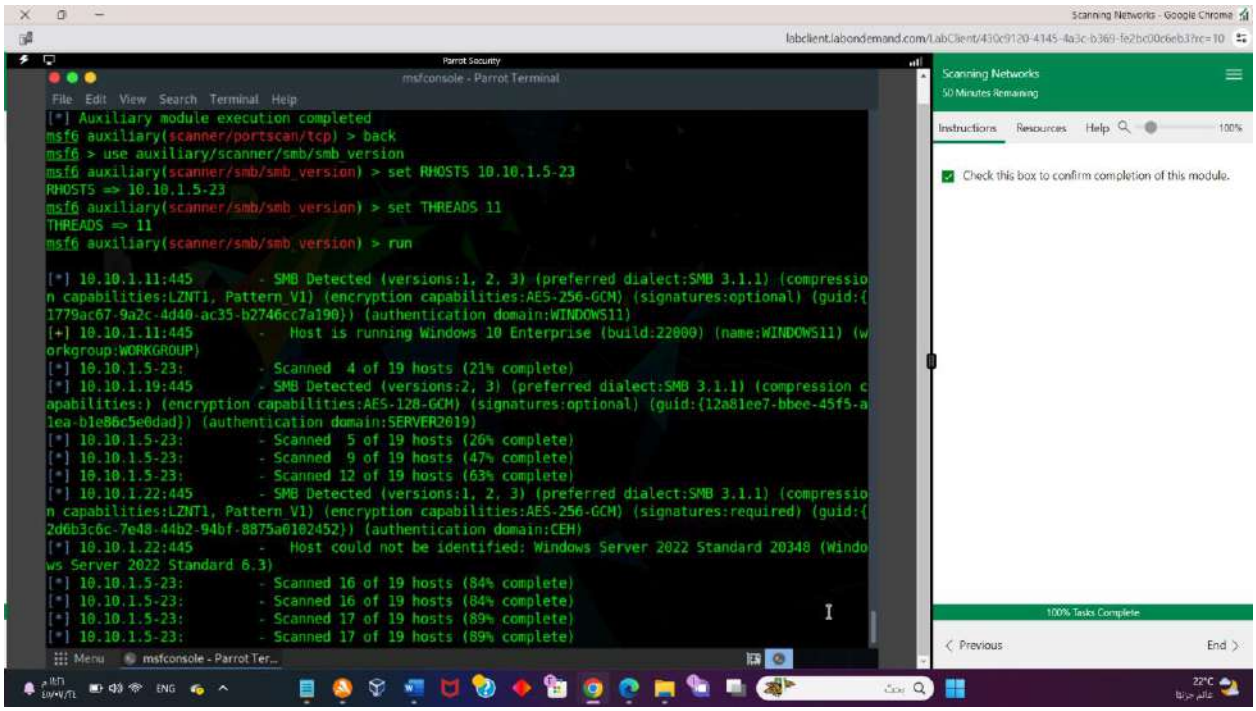

Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
2 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner
3 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
4 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locator
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access
msf6 > use auxili/scanner/portscan/syn
[-] No results from search
[-] Failed to load module: auxili/scanner/portscan/syn
msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) >
Menu msfconsole - Parrot Ter...
Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Scanning Networks
56 Minutes Remaining
Instructions Resources Help 100%
19. Here, we will use the auxiliary/scanner/portscan/syn module to perform an SYN scan on the target systems. To do so, type use auxiliary/scanner/portscan/syn and press Enter.
20. We will use this module to perform an SYN scan against the target IP address range (10.10.1.5-23) to look for open port 80 through the eth0 interface.
To do so, issue the below commands:
set INTERFACE eth0
set PORTS 80
set RHOSTS 10.10.1.5-23
set THREADS 50
PORTS: specifies the ports to scan (e.g., 22-25, 80, 110-900). RHOSTS: specifies the
93% Tasks Complete
Previous Next
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
ner
6 auxiliary/scanner/portscan/syn normal No TCP SYN Port
Scanner
7 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pin
gback Locator
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/word
press_pingback_access
msf6 > use auxili/scanner/portscan/syn
[-] No results from search
[-] Failed to load module: auxili/scanner/portscan/syn
msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) > run
[+] TCP OPEN 10.10.1.9:80
[+] TCP OPEN 10.10.1.19:80
[+] TCP OPEN 10.10.1.22:80
[*] Scanned 19 of 19 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) >
Menu
msfconsole - Parrot Ter...
Scanning Networks
54 Minutes Remaining
Instructions
Resources
Help
100%
IP address range.
Similarly, you can also specify a range of ports to be scanned against the target IP address range.
22. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.
23. Now, we will perform a TCP scan for open ports on the target systems.
24. To load the auxiliary/scanner/portscan/tcp module, type use auxiliary/scanner/portscan/tcp and press Enter.
94% Tasks Complete
Previous
Next
ENG
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[+] TCP OPEN 10.10.1.22:80
[*] Scanned 19 of 19 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > hosts -R
Hosts
address mac name os_name os_flavor os_sp purpose info comments
10.10.1.2 02:15:5d:39:ea:2d FreeBSD 11.X device
10.10.1.9 02:15:5d:39:ea:30 Linux 4.X server
10.10.1.11 00:15:5d:01:80:00 Windows 10 client
10.10.1.13 Unknown device
10.10.1.14 02:15:5d:39:ea:32 Linux 4.X server
10.10.1.19 02:15:5d:39:ea:2f www.moviesco pe.com Windows 10 client
10.10.1.22 00:15:5d:01:80:02 Windows 10 client
RHOSTS => file:/tmp/msf-db-rhosts-20240205-2715-spv1su
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.1.22
RHOSTS => 10.10.1.22
msf6 auxiliary(scanner/portscan/tcp) >
Menu
msfconsole - Parrot Ter...
Scanning Networks
52 Minutes Remaining
Instructions
Resources
Help
100%
consumes much time.
26. Type run and press Enter to discover open TCP ports in the target system.
It will take approximately 20 minutes for the scan to complete.
27. The results appear, displaying all open TCP ports in the target IP address (10.10.1.22).
94% Tasks Complete
Previous
Next
ENG
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
80:02
RHOSTS => file:/tmp/msf-db-rhosts-20240205-2715-spv1su
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.1.22
RHOSTS => 10.10.1.22
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 10.10.1.22: - 10.10.1.22:53 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:80 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:88 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:135 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:139 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:389 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:445 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:464 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:593 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:636 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:1801 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2103 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2107 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2105 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3268 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3269 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3389 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:5985 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:9389 - TCP OPEN
[*] 10.10.1.22: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
Menu
msfconsole - Parrot Ter...
Scanning Networks
52 Minutes Remaining
Instructions
Resources
Help
100%
26. Type run and press Enter to discover open TCP ports in the target system.
It will take approximately 20 minutes for the scan to complete.
27. The results appear, displaying all open TCP ports in the target IP address (10.10.1.22).
28. Now that we have determined the active hosts on the target network, we can further attempt to
94% Tasks Complete
Previous
Next
ENG
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.10.1.11:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compressio
n capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{
1779ac67-9a2c-4d40-ac35-b2746cc7a190}) (authentication domain:WINDOWS11)
[+] 10.10.1.11:445 - Host is running Windows 10 Enterprise (build:22000) (name:WINDOWS11) (w
orkgroup:WORKGROUP)
[*] 10.10.1.5-23: - Scanned 4 of 19 hosts (21% complete)
[*] 10.10.1.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression c
apabilities:) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{12a81ee7-bbee-45f5-a
1ea-b1e86c5e0dad}) (authentication domain:SERVER2019)
[*] 10.10.1.5-23: - Scanned 5 of 19 hosts (26% complete)
[*] 10.10.1.5-23: - Scanned 9 of 19 hosts (47% complete)
[*] 10.10.1.5-23: - Scanned 12 of 19 hosts (63% complete)
[*] 10.10.1.22:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compressio
n capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:required) (guid:{
2d6b3c6c-7e48-44b2-94bf-8875a0102452}) (authentication domain:CEH)
[*] 10.10.1.22:445 - Host could not be identified: Windows Server 2022 Standard 20348 (Windo
ws Server 2022 Standard 6.3)
[*] 10.10.1.5-23: - Scanned 16 of 19 hosts (84% complete)
[*] 10.10.1.5-23: - Scanned 16 of 19 hosts (84% complete)
[*] 10.10.1.5-23: - Scanned 17 of 19 hosts (89% complete)
[*] 10.10.1.5-23: - Scanned 17 of 19 hosts (89% complete)
Menu
msfconsole - Parrot Ter...
Scanning Networks
51 Minutes Remaining
Instructions
Resources
Help
100%
set RHOSTS 10.10.1.5-23
set THREADS 11
31. Type run and press Enter to discover SMB version in the target systems.
32. The result appears, displaying the OS details of the target hosts.
94% Tasks Complete
Previous
Next
ENG
22°C


Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/410c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10
Parrot Security
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.10.1.11:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compressio
n capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{
1779ac67-9a2c-4d40-ac35-b2746cc7a190}) (authentication domain:WINDOWS11)
[+] 10.10.1.11:445 - Host is running Windows 10 Enterprise (build:22000) (name:WINDOWS11) (w
orkgroup:WORKGROUP)
[*] 10.10.1.5-23: - Scanned 4 of 19 hosts (21% complete)
[*] 10.10.1.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression c
apabilities:) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{12a81ee7-bbee-45f5-a
1ea-b1e86c5e0dad}) (authentication domain:SERVER2019)
[*] 10.10.1.5-23: - Scanned 5 of 19 hosts (26% complete)
[*] 10.10.1.5-23: - Scanned 9 of 19 hosts (47% complete)
[*] 10.10.1.5-23: - Scanned 12 of 19 hosts (63% complete)
[*] 10.10.1.22:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compressio
n capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:required) (guid:{
2d0b3c0c-7e48-44b2-94bf-8875a0102452}) (authentication domain:CEH)
[*] 10.10.1.22:445 - Host could not be identified: Windows Server 2022 Standard 20348 (Windo
ws Server 2022 Standard 6.3)
[*] 10.10.1.5-23: - Scanned 16 of 19 hosts (84% complete)
[*] 10.10.1.5-23: - Scanned 16 of 19 hosts (84% complete)
[*] 10.10.1.5-23: - Scanned 17 of 19 hosts (89% complete)
[*] 10.10.1.5-23: - Scanned 17 of 19 hosts (89% complete)
Menu
msfconsole - Parrot Ter...
Scanning Networks
50 Minutes Remaining
Instructions
Resources
Help
100%
Check this box to confirm completion of this module.
100% Tasks Complete
Previous
End
ENG
22°C