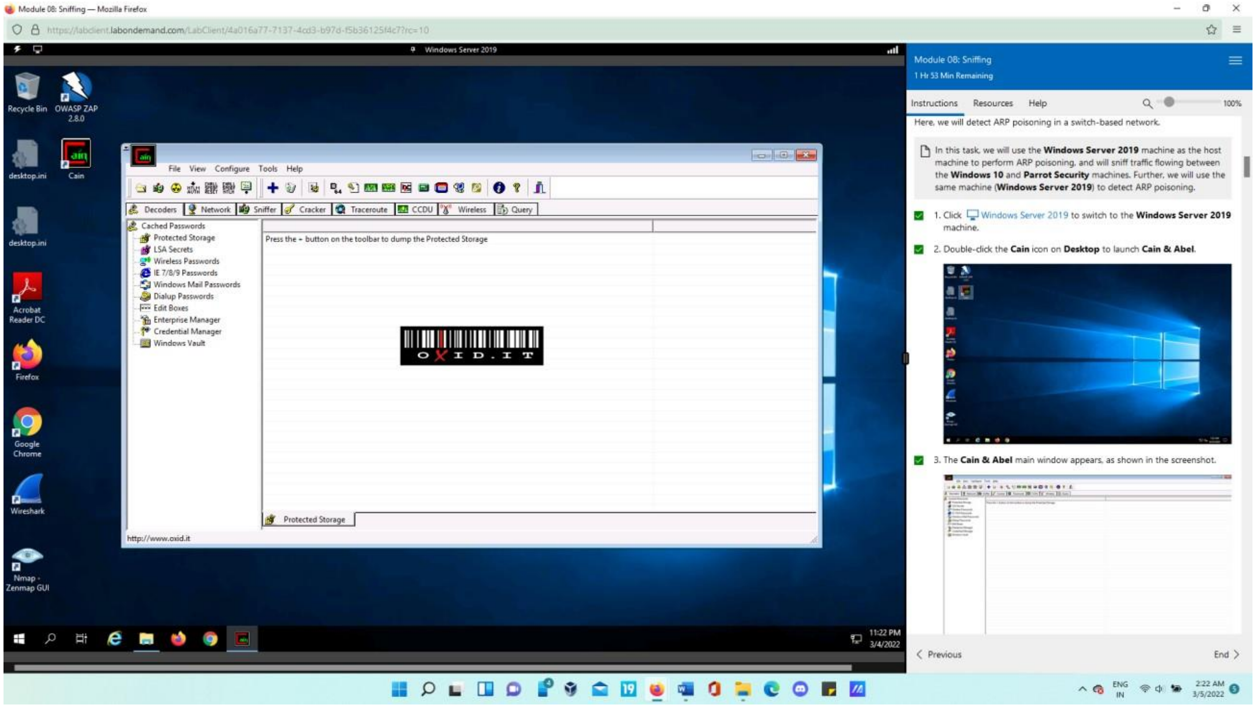
Lab 3: Detect Network Sniffing

Task 1: Detect ARP Poisoning in a Switch-Based Network

- Launch Cain & Abel in Windows server 2019.



Press the + button on the toolbar to dump the Protected Storage

Here, we will detect ARP poisoning in a switch-based network.

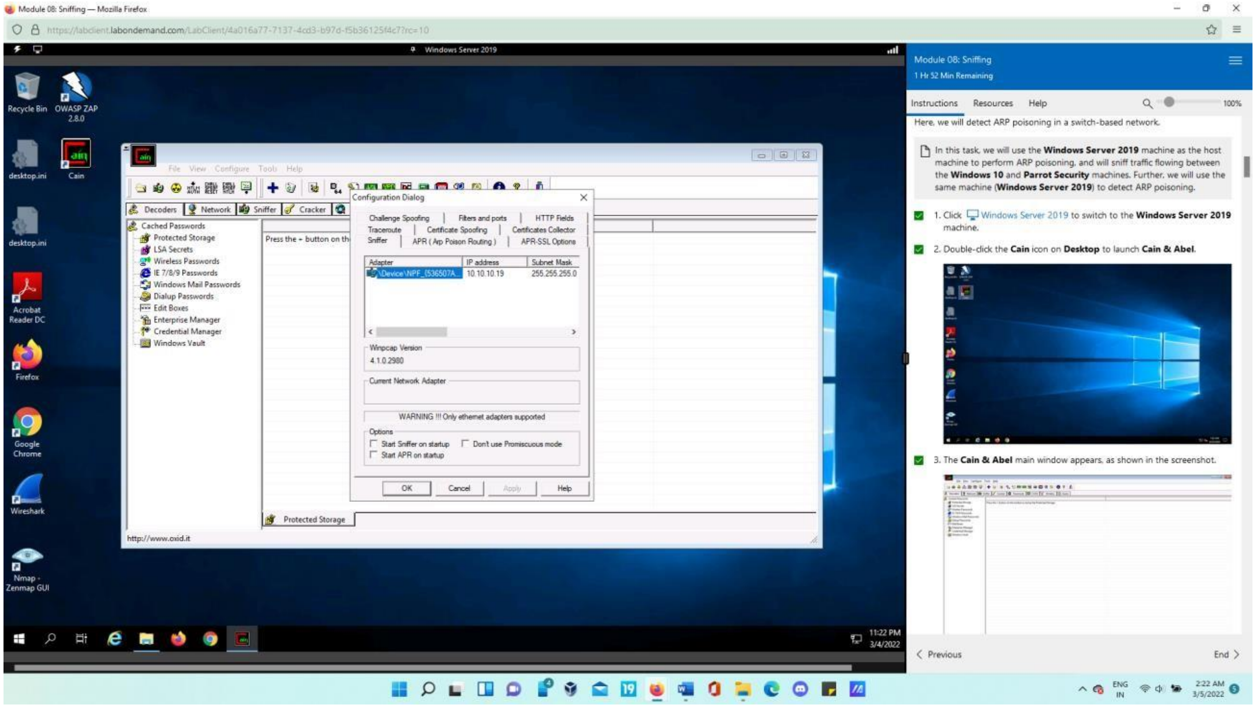
In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

☑ 1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.

☑ 2. Double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

☑ 3. The **Cain & Abel** main window appears, as shown in the screenshot.

- To configure an ethernet card, go to the menu bar and select Configure. In Configuration dialog box, Sniffer tab will be selected by default, we must make sure that Adapter linked with the IP Address of the machine is selected and press ok.



Configuration Dialog

Challenge Spoofing | Filters and ports | HTTP Fields
Traceroute | Certificate Spoofing | Certificates Collector
Sniffer | APR (Arp Poison Routing) | APR-SSL Options

Adapter	IP address	Subnet Mask
\Device\NPF_{536507A...	10.10.10.19	255.255.255.0

Winpcap Version: 4.1.0.2980

Current Network Adapter

WARNING !!! Only ethernet adapters supported

Options
☐ Start Sniffer on startup ☐ Don't use Promiscuous mode
☐ Start APR on startup

OK | Cancel | Apply | Help

Module 08: Sniffing
1 Hr 52 Min Remaining

Instructions Resources Help 100%

Here, we will detect ARP poisoning in a switch-based network.

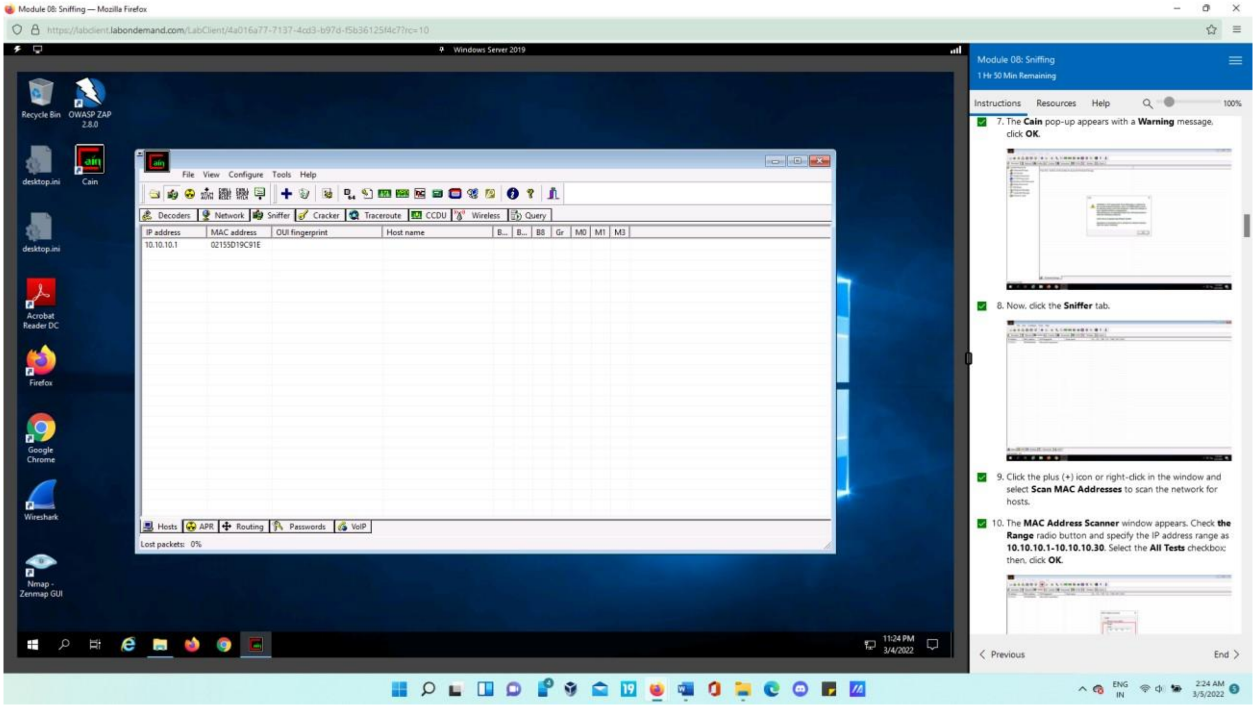
In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

☑ 1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.

☑ 2. Double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

☑ 3. The **Cain & Abel** main window appears, as shown in the screenshot.

- Start sniffing by pressing start button. In sniffer tab, press (+) icon and select Scan MAC Addresses to scan the network for hosts.



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.10.1	02155D19C91E									

Lost packets: 0%

Module 08: Sniffing
1 Hr 50 Min Remaining

Instructions Resources Help 100%

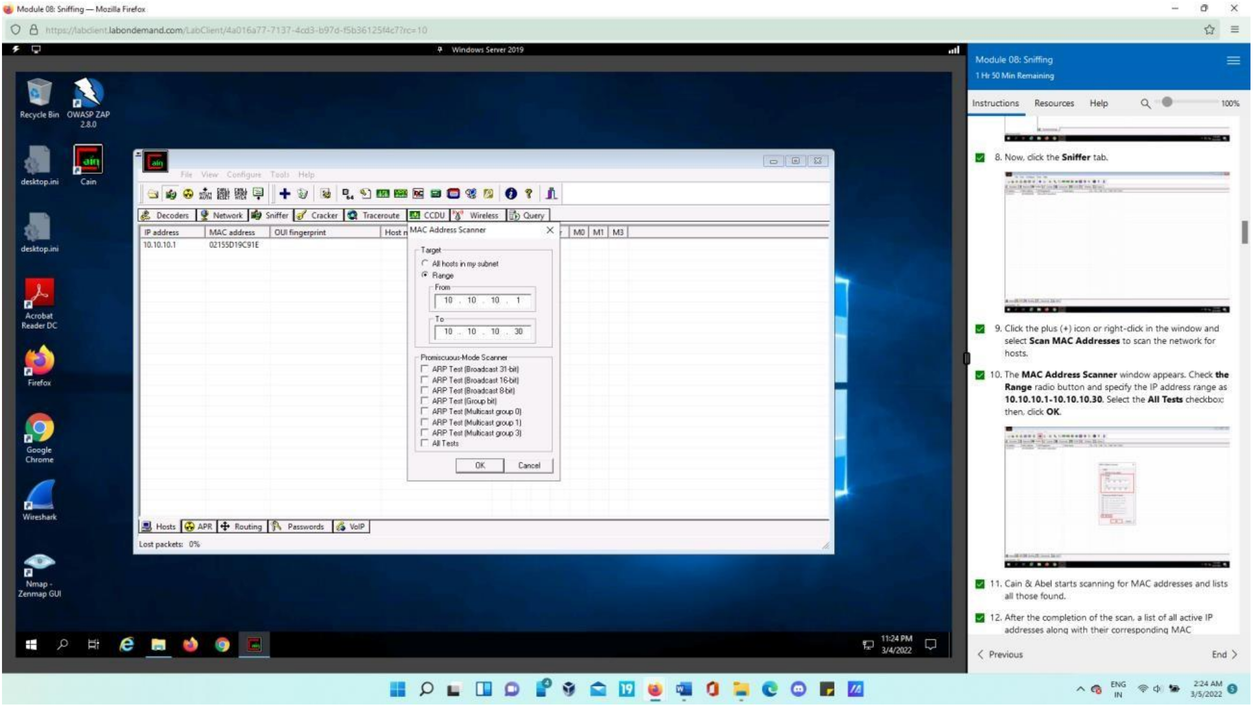
☑ 7. The **Cain** pop-up appears with a **Warning** message, click **OK**.

☑ 8. Now, click the **Sniffer** tab.

☑ 9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

☑ 10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

- In MAC address scanner window pop-up, select range radio and specify the address range of IP as 10.10.10.1-10.10.10.30 and select All test check box. Then the tool starts scanning for MAC addresses and it will list out whatever it has found.



Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10

Windows Server 2019

MAC Address Scanner

Target

○ All hosts in my subnet

● Range

From: 10 . 10 . 10 . 1

To: 10 . 10 . 10 . 30

Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)
□ ARP Test (Broadcast 16-bit)
□ ARP Test (Broadcast 8-bit)
□ ARP Test (Group bit)
□ ARP Test (Multicast group 0)
□ ARP Test (Multicast group 1)
□ ARP Test (Multicast group 3)
□ All Tests

IP address	MAC address	OUI fingerprint
10.10.10.1	02155D19C91E	

Lost packets: 0%

Module 08: Sniffing

1 Hr 50 Min Remaining

8. Now, click the **Sniffer** tab.

9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

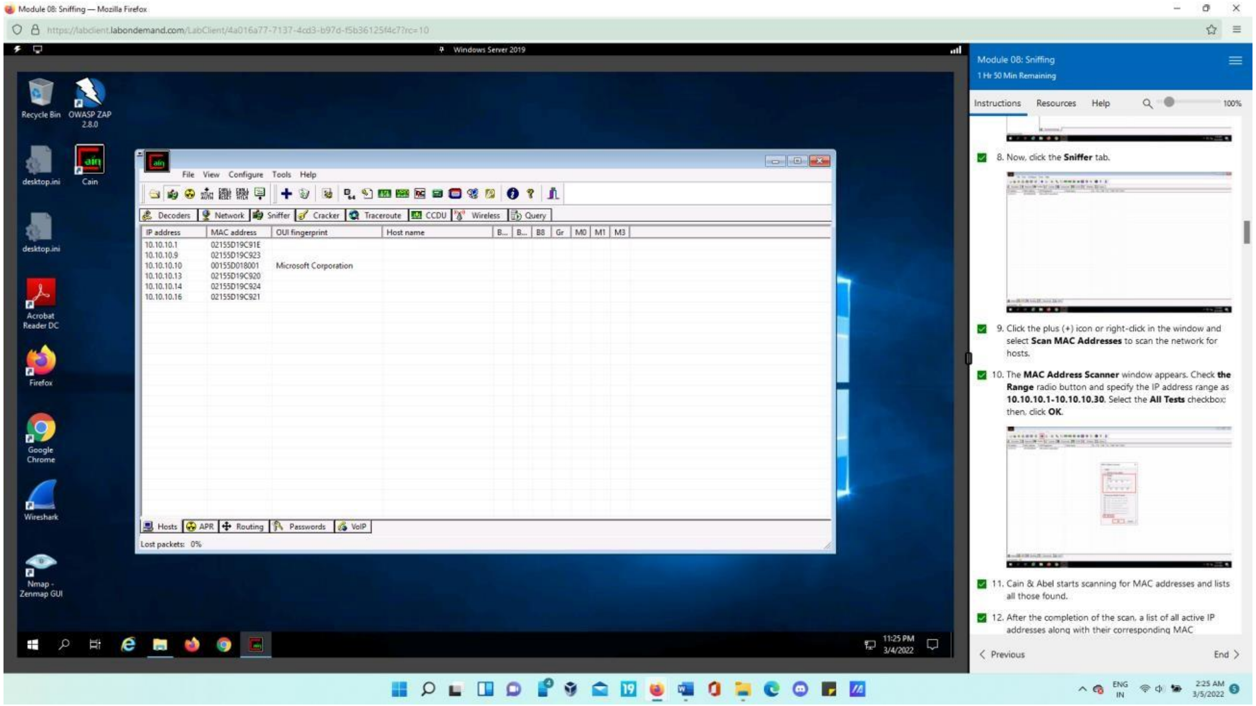
10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

11. Cain & Abel starts scanning for MAC addresses and lists all those found.

12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC

.

After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.



Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10

Windows Server 2019

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.10.1	02155D19C91E									
10.10.10.9	02155D19C923									
10.10.10.10	00155D018001	Microsoft Corporation								
10.10.10.13	02155D19C920									
10.10.10.14	02155D19C924									
10.10.10.16	02155D19C921									

Lost packets: 0%

Module 08: Sniffing

1 Hr 50 Min Remaining

8. Now, click the **Sniffer** tab.

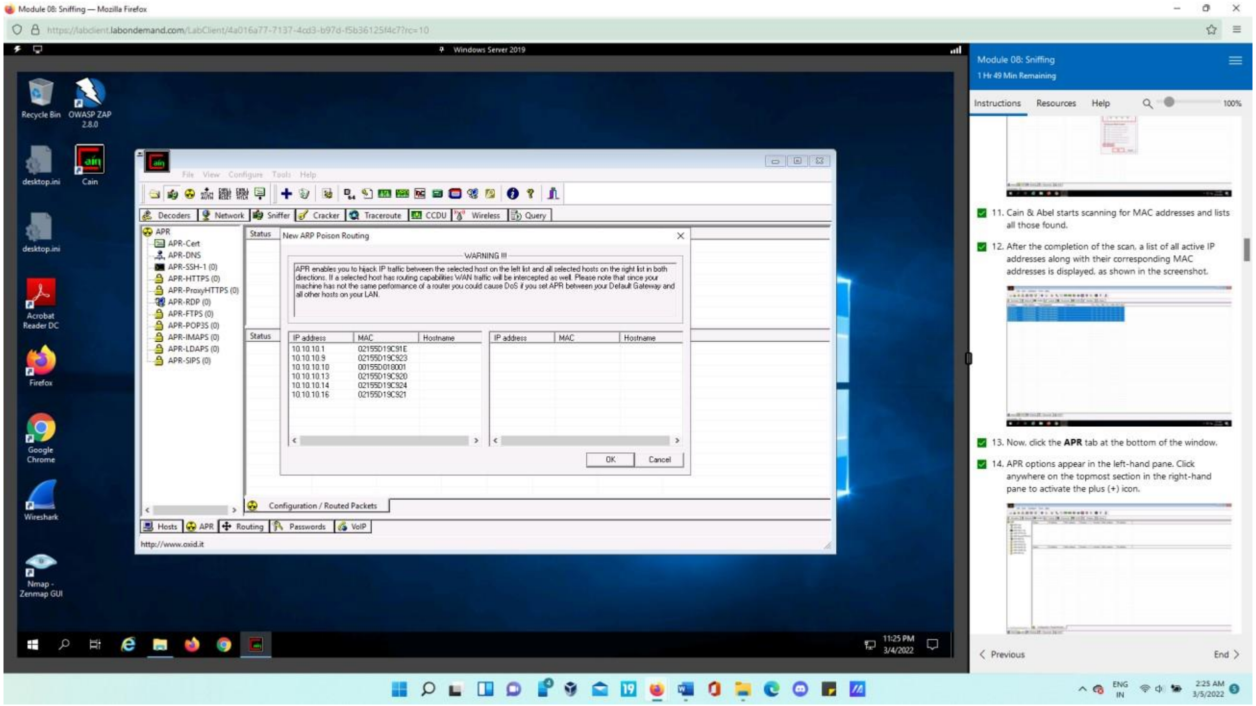
9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

10. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

11. Cain & Abel starts scanning for MAC addresses and lists all those found.

12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC

- At the bottom of the window, click the APR tab.



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.10.10.1	02155D19C91E	
10.10.10.9	02155D19C923	
10.10.10.10	00155D018001	
10.10.10.13	02155D19C920	
10.10.10.14	02155D19C924	
10.10.10.16	02155D19C921	

IP address	MAC	Hostname

OK Cancel

☑ 11. Cain & Abel starts scanning for MAC addresses and lists all those found.

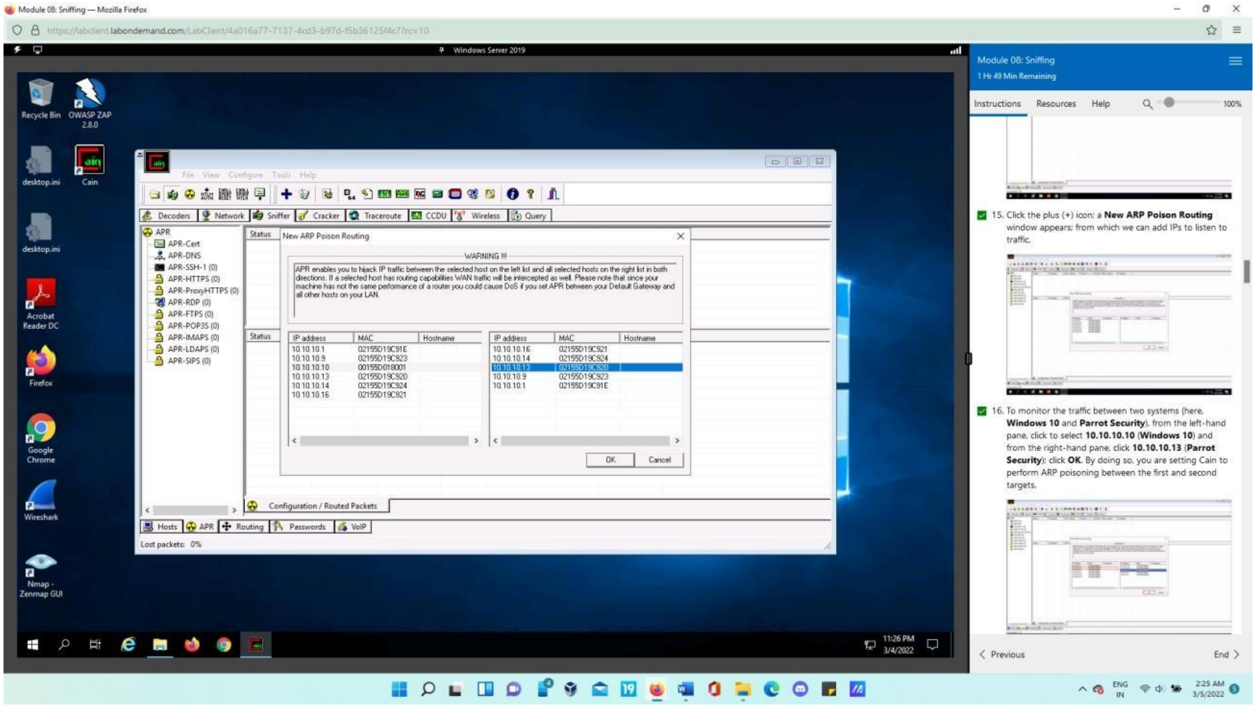
☑ 12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

☑ 13. Now, click the **APR** tab at the bottom of the window.

☑ 14. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

•

Here, now add IPs to listen to traffic in ARP poisoning window. For observing traffic between ParrotOS and Windows10. Select 10.10.10.13 from right-pane and select 10.10.10.10 from leftpane of the window. This informs Cain to execute ARP poisoning between the two targets.



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.10.10.1	02155D19C91E	
10.10.10.9	02155D19C923	
10.10.10.10	00155D018001	
10.10.10.13	02155D19C920	
10.10.10.14	02155D19C924	
10.10.10.16	02155D19C921	

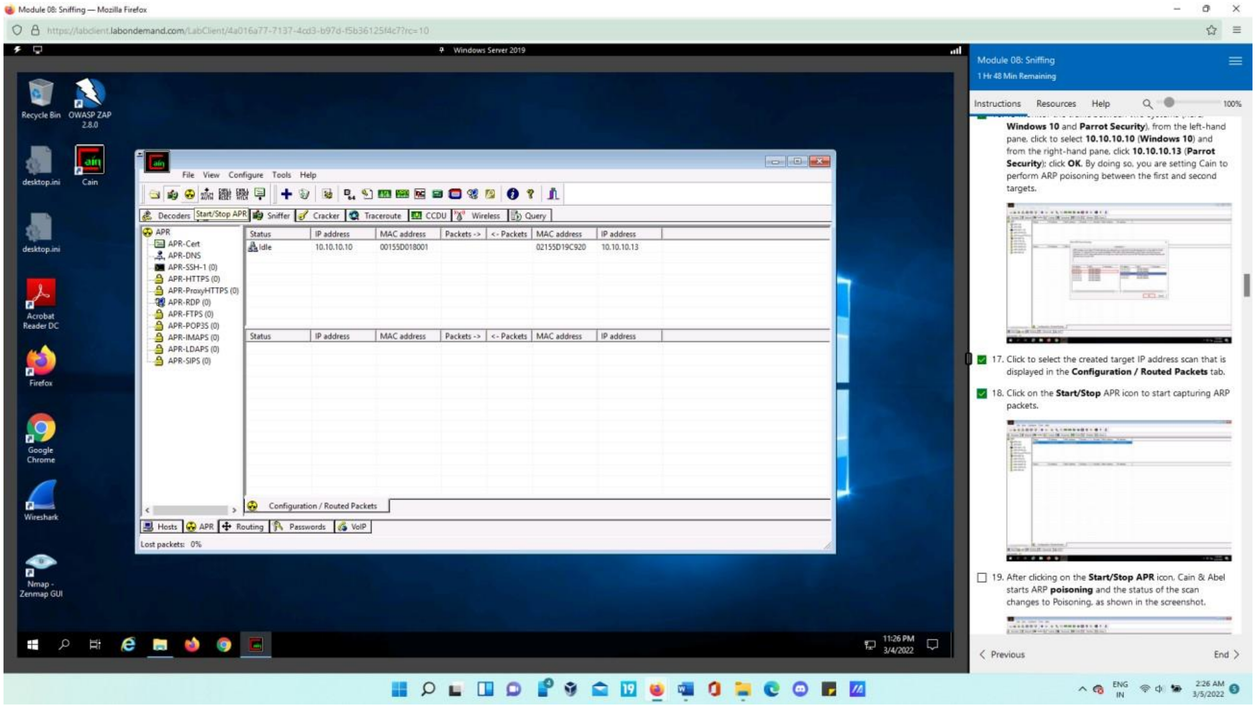
IP address	MAC	Hostname
10.10.10.16	02155D19C921	
10.10.10.14	02155D19C924	
10.10.10.13	02155D19C920	
10.10.10.9	02155D19C923	
10.10.10.1	02155D19C91E	

OK Cancel

☑ 15. Click the plus (+) icon: a **New ARP Poison Routing** window appears: from which we can add IPs to listen to traffic.

☑ 16. To monitor the traffic between two systems (here, **Windows 10** and **Parrot Security**), from the left-hand pane, click to select **10.10.10.10** (**Windows 10**) and from the right-hand pane, click **10.10.10.13** (**Parrot Security**): click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

- Now start capturing ARP packets.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.10.10.10	00155D018001			02155D19C920	10.10.10.13

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

Windows 10 and **Parrot Security**), from the left-hand pane, click to select **10.10.10.10** (**Windows 10**) and from the right-hand pane, click **10.10.10.13** (**Parrot Security**): click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

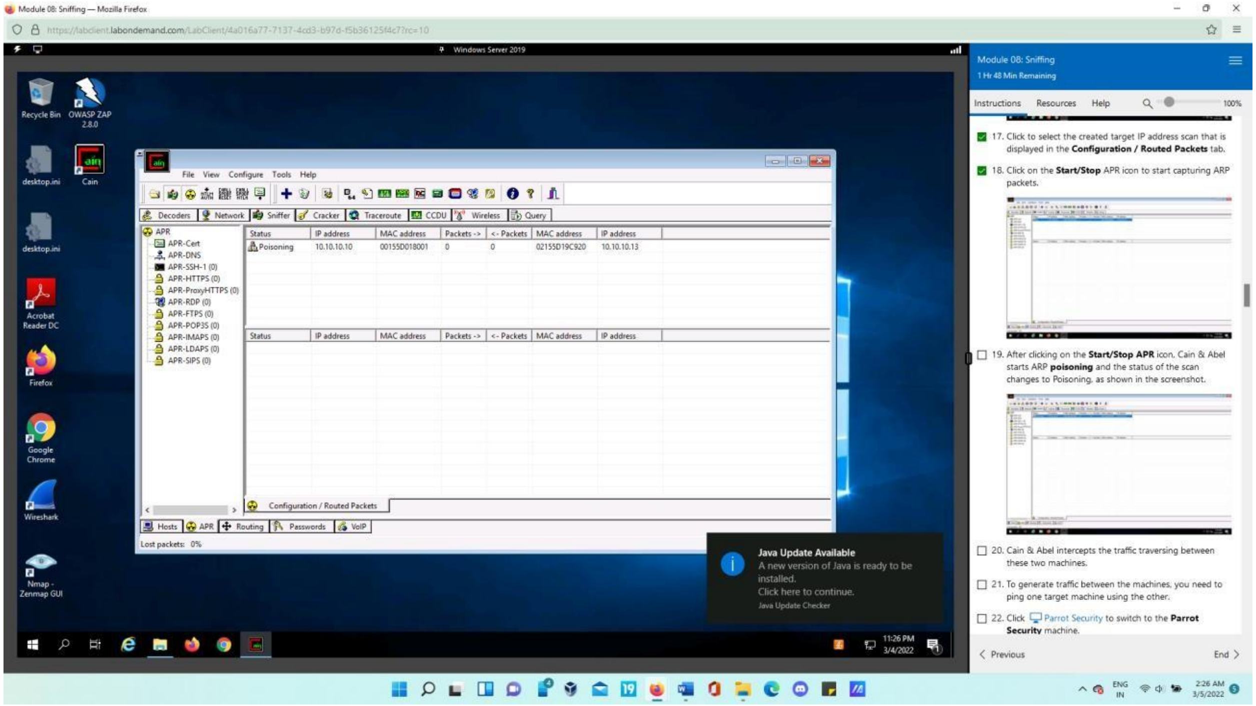
☑ 17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

☑ 18. Click on the **Start/Stop** APR icon to start capturing ARP packets.

☐ 19. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP **poisoning** and the status of the scan changes to Poisoning, as shown in the screenshot.

-

Cain starts ARP poisoning, as also we can see the status of scan to poisoning. The traffic between these two machines is intercepted by Cain & Abel. You must ping one target machine using the other to generate traffic between the devices.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.10.10.10	00155D018001	0	0	02155D19C920	10.10.10.13

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

Lost packets: 0%

Java Update Available
A new version of Java is ready to be installed.
Click here to continue.
Java Update Checker

☑ 17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

☑ 18. Click on the **Start/Stop** APR icon to start capturing ARP packets.

□ 19. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP **poisoning** and the status of the scan changes to Poisoning, as shown in the screenshot.

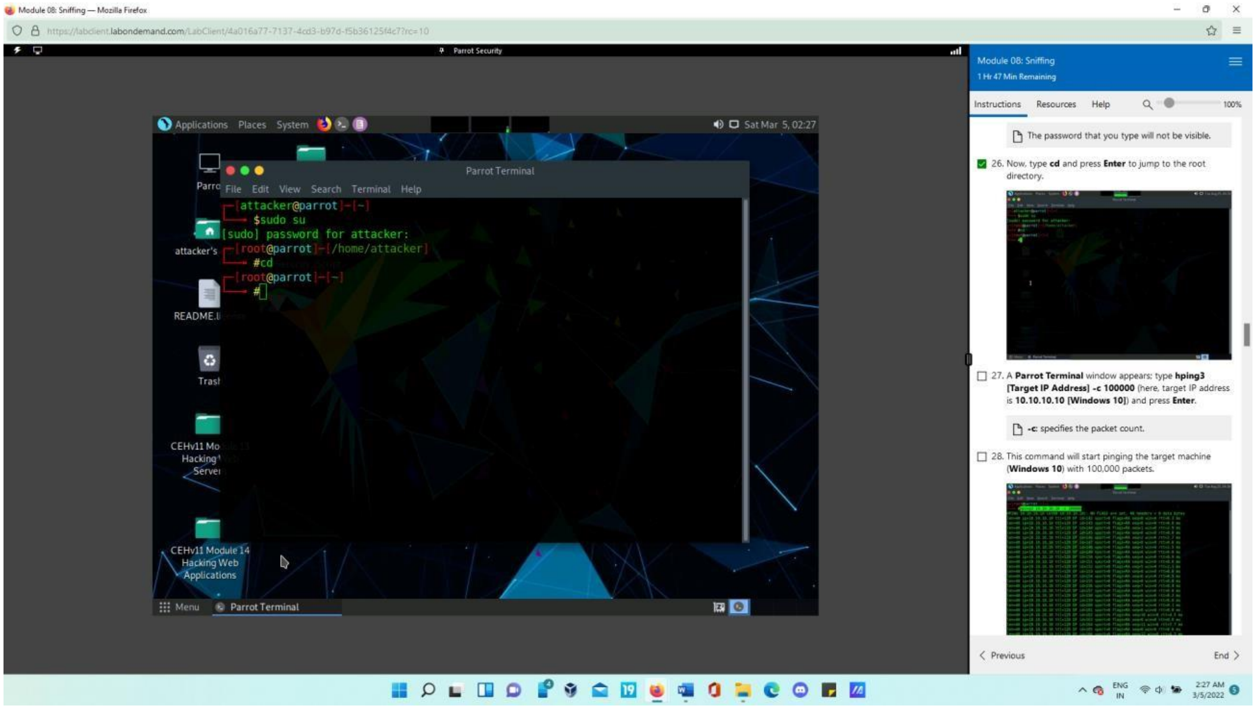
□ 20. Cain & Abel intercepts the traffic traversing between these two machines.

□ 21. To generate traffic between the machines, you need to ping one target machine using the other.

□ 22. Click Parrot Security to switch to the **Parrot Security** machine.

- Now, open terminal window in ParrotOS. Escalate privileges to root and navigate to root directory.

-


Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Parrot Security
Applications Places System
Sat Mar 5, 02:27
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
Module 08: Sniffing
1 Hr 47 Min Remaining
Instructions Resources Help
100%
Previous
End
2:27 AM
3/5/2022

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

The password that you type will not be visible.

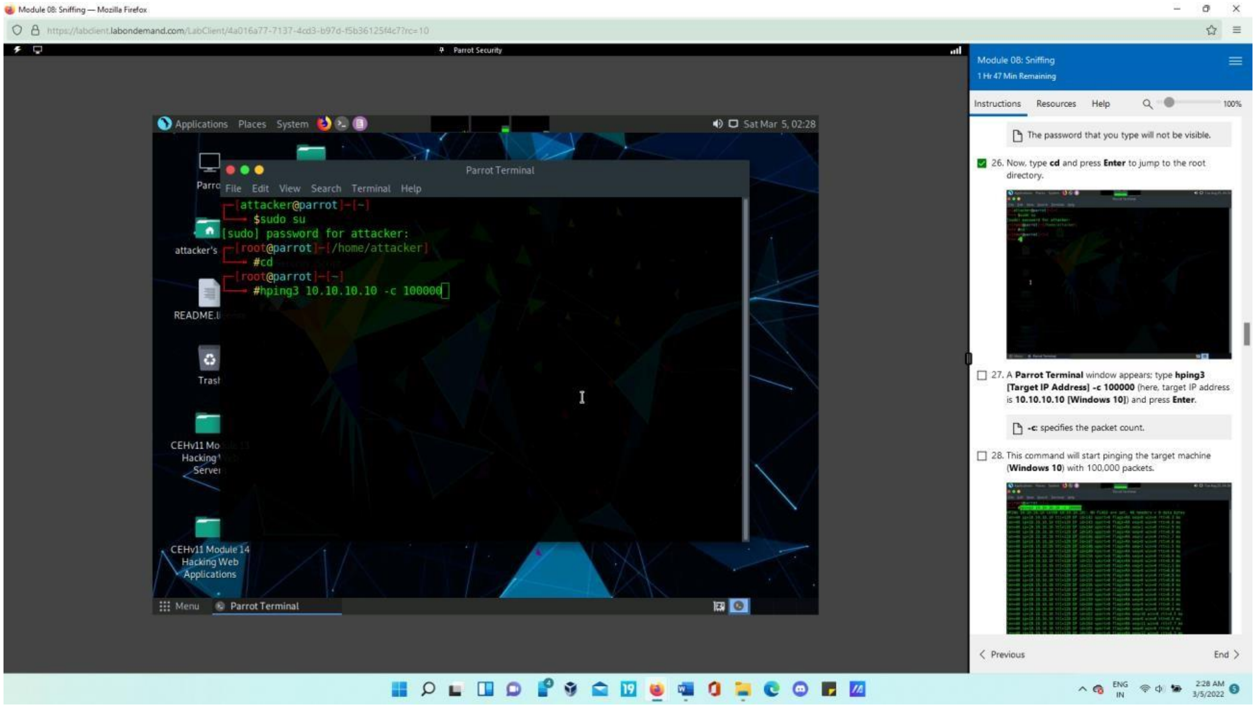
☑ 26. Now, type **cd** and press **Enter** to jump to the root directory.

□ 27. A **Parrot Terminal** window appears; type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.10.10 [Windows 10]**) and press **Enter**.

-c: specifies the packet count.

□ 28. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.

Execute the command hping3 10.10.10.10 -c 100000


Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Parrot Security
Applications Places System
Sat Mar 5, 02:28
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
Module 08: Sniffing
1 Hr 47 Min Remaining
Instructions Resources Help
100%
Previous
End
2:28 AM
3/5/2022

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #hping3 10.10.10.10 -c 100000
```

The password that you type will not be visible.

☑ 26. Now, type **cd** and press **Enter** to jump to the root directory.

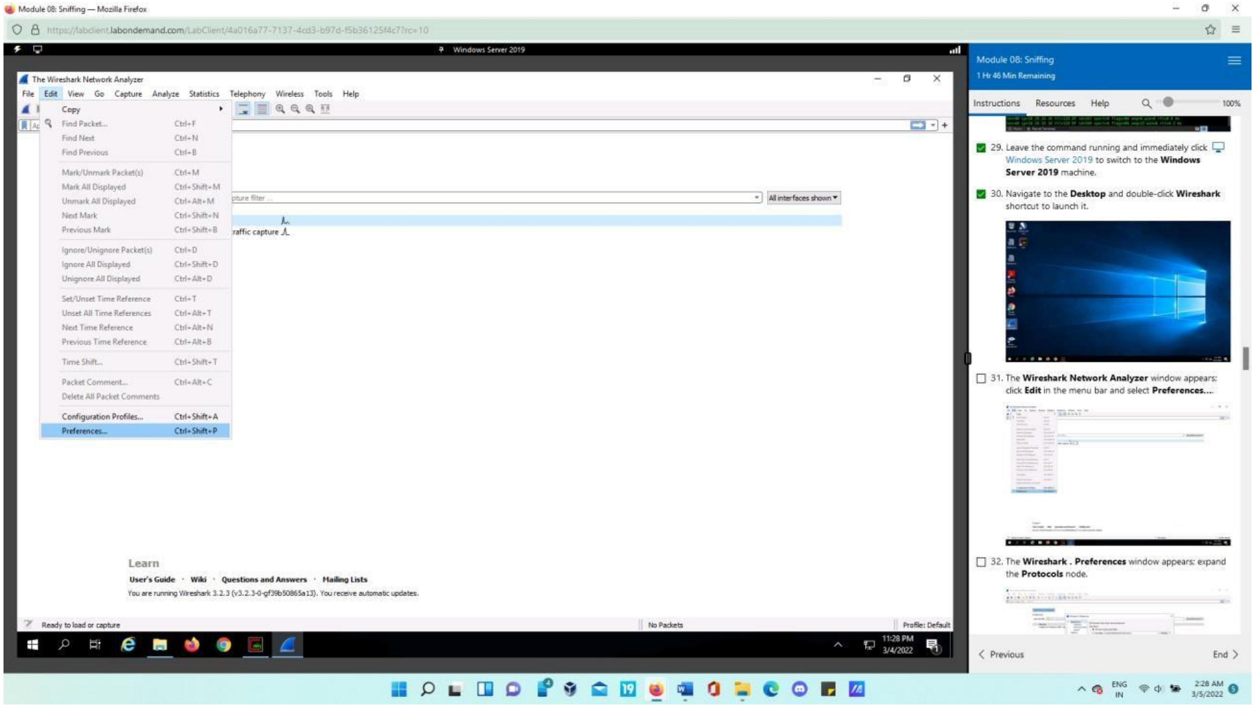
□ 27. A **Parrot Terminal** window appears; type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.10.10 [Windows 10]**) and press **Enter**.

-c: specifies the packet count.

□ 28. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.

-

- Open Wireshark and navigate to Edit > Preferences


Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default
11:28 PM
3/4/2022
Module 08: Sniffing
1 Hr 46 Min Remaining
Instructions
Resources
Help
100%
Previous
End
ENG
IN
2:28 AM
3/5/2022

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

☑ 29. Leave the command running and immediately click Windows Server 2019 to switch to the **Windows Server 2019** machine.

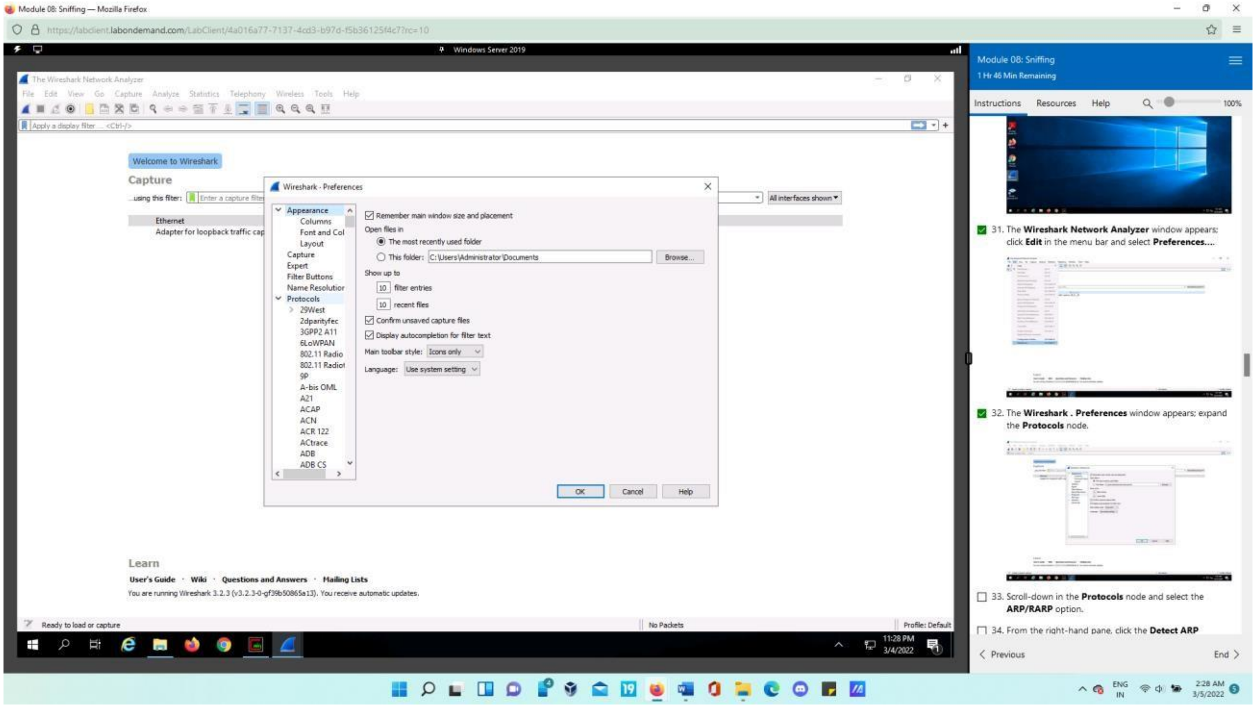
☑ 30. Navigate to the **Desktop** and double-click **Wireshark** shortcut to launch it.

□ 31. The **Wireshark Network Analyzer** window appears: click **Edit** in the menu bar and select **Preferences...**.

□ 32. The **Wireshark . Preferences** window appears: expand the **Protocols** node.

Expand Protocols > select ARP/RARP

-



☑ Remember main window size and placement

Open files in

● The most recently used folder

○ This folder: C:\Users\Administrator\Documents

Show up to

10 filter entries

10 recent files

☑ Confirm unsaved capture files

☑ Display autocompletion for filter text

Main toolbar style: Icons only

Language: Use system setting

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

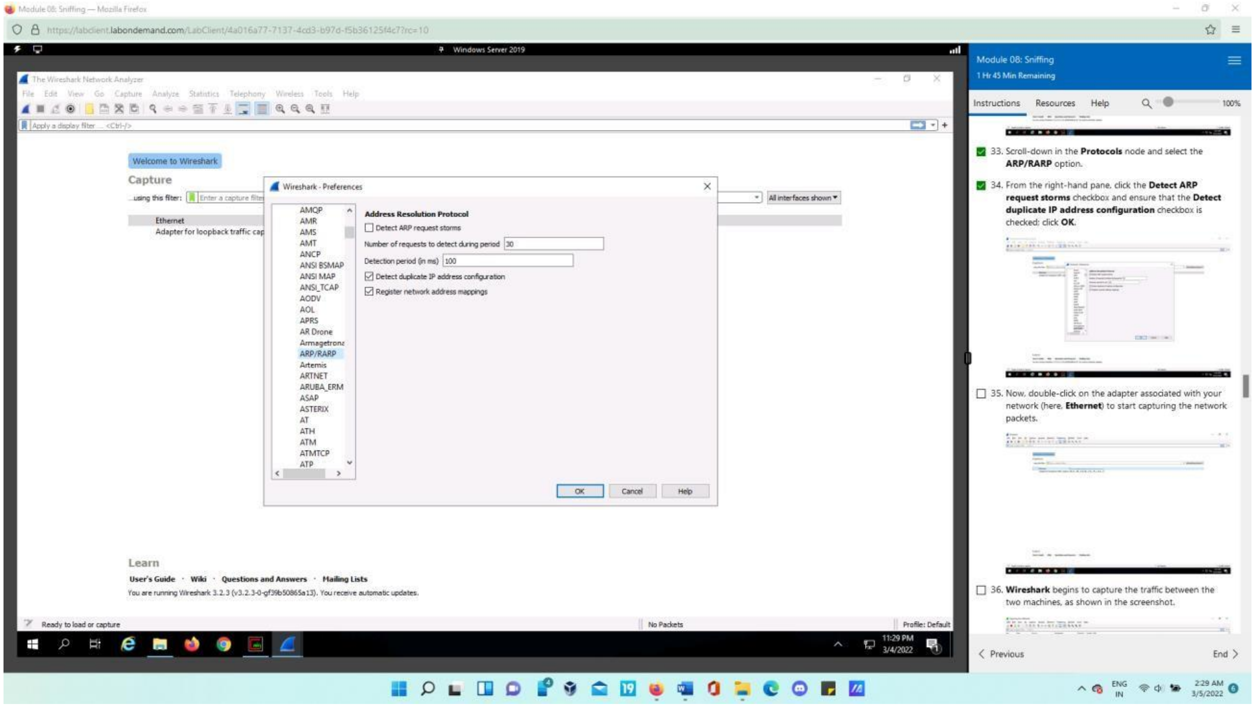
☑ 31. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences....**

☑ 32. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

☐ 33. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

☐ 34. From the right-hand pane, click the **Detect ARP**

- Select the Detect ARP request storms checkbox and make sure to also check Detect duplicate IP address configuration.



Address Resolution Protocol

☐ Detect ARP request storms

Number of requests to detect during period 30

Detection period (in ms) 100

☑ Detect duplicate IP address configuration

☑ Register network address mappings

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

☑ 33. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

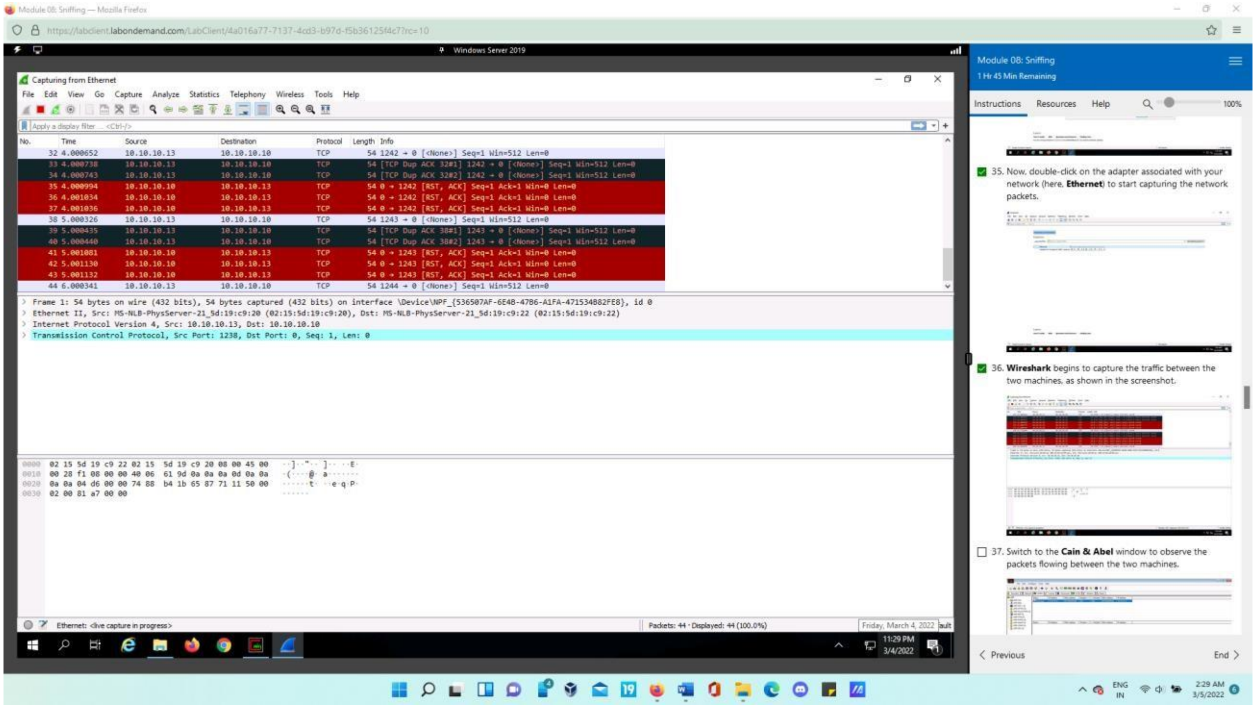
☑ 34. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.

☐ 35. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.

☐ 36. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.

-

Select the relevant network adapter to start capturing network packets.



Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source        Destination   Protocol Length Info
   32 4.000652   10.10.10.13   10.10.10.10   TCP      54 1242 → 0 [<None>] Seq=1 Win=512 Len=0
   33 4.000738   10.10.10.13   10.10.10.10   TCP      54 [TCP Dup ACK 32#1] 1242 → 0 [<None>] Seq=1 Win=512 Len=0
   34 4.000743   10.10.10.13   10.10.10.10   TCP      54 [TCP Dup ACK 32#2] 1242 → 0 [<None>] Seq=1 Win=512 Len=0
   35 4.000994   10.10.10.10   10.10.10.13   TCP      54 0 → 1242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   36 4.001034   10.10.10.10   10.10.10.13   TCP      54 0 → 1242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   37 4.001036   10.10.10.10   10.10.10.13   TCP      54 0 → 1242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   38 5.000326   10.10.10.13   10.10.10.10   TCP      54 1243 → 0 [<None>] Seq=1 Win=512 Len=0
   39 5.000435   10.10.10.13   10.10.10.10   TCP      54 [TCP Dup ACK 38#1] 1243 → 0 [<None>] Seq=1 Win=512 Len=0
   40 5.000440   10.10.10.13   10.10.10.10   TCP      54 [TCP Dup ACK 38#2] 1243 → 0 [<None>] Seq=1 Win=512 Len=0
   41 5.001081   10.10.10.10   10.10.10.13   TCP      54 0 → 1243 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   42 5.001130   10.10.10.10   10.10.10.13   TCP      54 0 → 1243 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   43 5.001132   10.10.10.10   10.10.10.13   TCP      54 0 → 1243 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   44 6.000341   10.10.10.13   10.10.10.10   TCP      54 1244 → 0 [<None>] Seq=1 Win=512 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{536507AF-6E4B-47B6-A1FA-471534882FE8}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:c9:20 (02:15:5d:19:c9:20), Dst: MS-NLB-PhysServer-21_5d:19:c9:22 (02:15:5d:19:c9:22)
> Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
> Transmission Control Protocol, Src Port: 1238, Dst Port: 0, Seq: 1, Len: 0

0000  02 15 5d 19 c9 22 02 15  5d 19 c9 20 08 00 45 00   ··]··"·· ]·· ··E·
0010  00 28 f1 08 00 00 40 06  61 9d 0a 0a 0a 0d 0a 0a   ·(····@· a·······
0020  0a 0a 04 d6 00 00 74 88  b4 1b 65 87 71 11 50 00   ······t· ··e·q·P·
0030  02 00 81 a7 00 00                                  ······
```

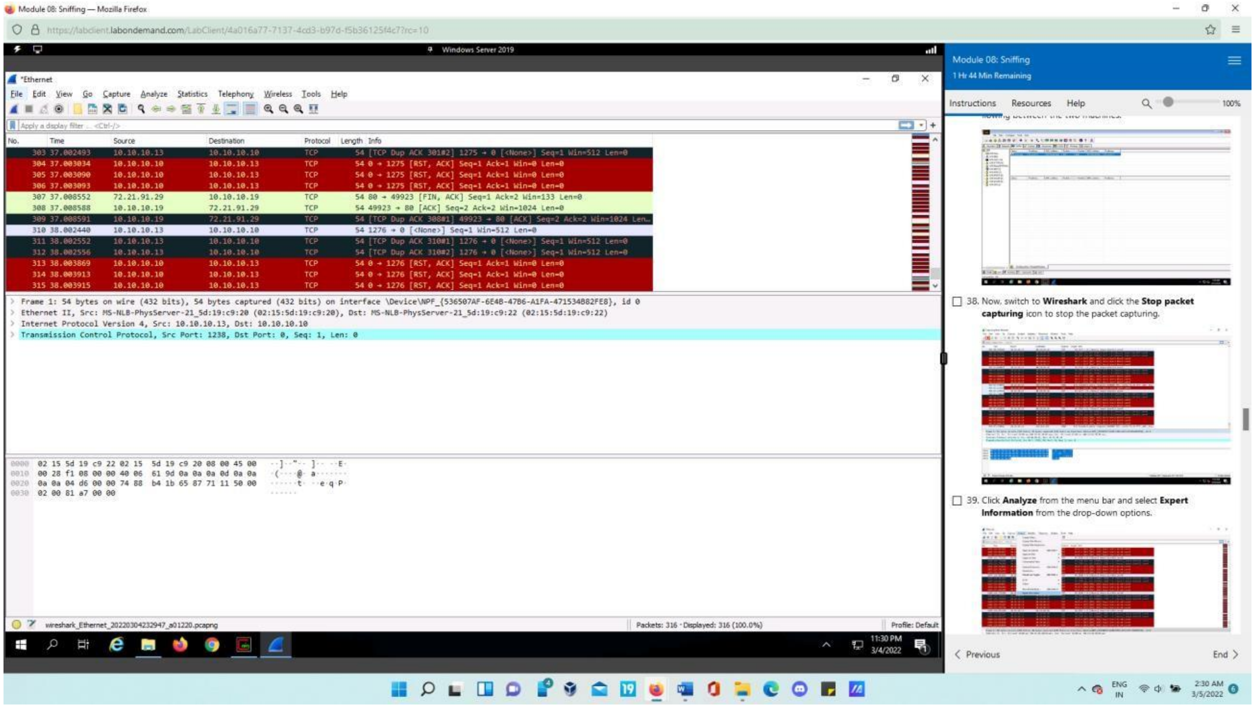
☑ 35. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.

☑ 36. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.

☐ 37. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.

- Go to Cain and Able to observe traffic flowing between these two machines, then go to Wireshark and stop the packet capture.

-



Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

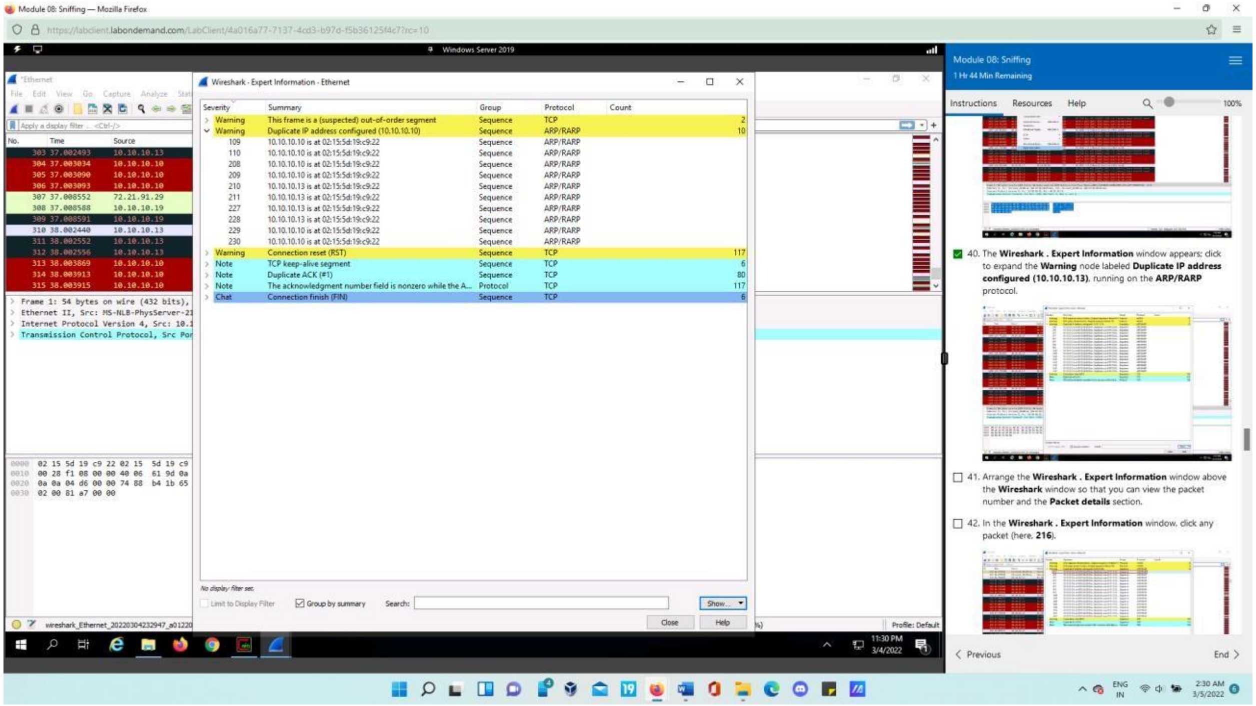
```
No.   Time       Source       Destination  Protocol Length Info
  303 37.002493  10.10.10.13  10.10.10.10  TCP      54 [TCP Dup ACK 301#2] 1275 → 0 [<None>] Seq=1 Win=512 Len=0
  304 37.003034  10.10.10.10  10.10.10.13  TCP      54 0 → 1275 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  305 37.003090  10.10.10.10  10.10.10.13  TCP      54 0 → 1275 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  306 37.003093  10.10.10.10  10.10.10.13  TCP      54 0 → 1275 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  307 37.008552  72.21.91.29  10.10.10.19  TCP      54 80 → 49923 [FIN, ACK] Seq=1 Ack=2 Win=133 Len=0
  308 37.008588  10.10.10.19  72.21.91.29  TCP      54 49923 → 80 [ACK] Seq=2 Ack=2 Win=1024 Len=0
  309 37.008591  10.10.10.19  72.21.91.29  TCP      54 [TCP Dup ACK 308#1] 49923 → 80 [ACK] Seq=2 Ack=2 Win=1024 Len…
  310 38.002440  10.10.10.13  10.10.10.10  TCP      54 1276 → 0 [<None>] Seq=1 Win=512 Len=0
  311 38.002552  10.10.10.13  10.10.10.10  TCP      54 [TCP Dup ACK 310#1] 1276 → 0 [<None>] Seq=1 Win=512 Len=0
  312 38.002556  10.10.10.13  10.10.10.10  TCP      54 [TCP Dup ACK 310#2] 1276 → 0 [<None>] Seq=1 Win=512 Len=0
  313 38.003869  10.10.10.10  10.10.10.13  TCP      54 0 → 1276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  314 38.003913  10.10.10.10  10.10.10.13  TCP      54 0 → 1276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  315 38.003915  10.10.10.10  10.10.10.13  TCP      54 0 → 1276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{536507AF-6E4B-47B6-A1FA-471534882FE8}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:c9:20 (02:15:5d:19:c9:20), Dst: MS-NLB-PhysServer-21_5d:19:c9:22 (02:15:5d:19:c9:22)
> Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
> Transmission Control Protocol, Src Port: 1238, Dst Port: 0, Seq: 1, Len: 0

0000  02 15 5d 19 c9 22 02 15  5d 19 c9 20 08 00 45 00   ··]··"·· ]·· ··E·
0010  00 28 f1 08 00 00 40 06  61 9d 0a 0a 0a 0d 0a 0a   ·(····@· a·······
0020  0a 0a 04 d6 00 00 74 88  b4 1b 65 87 71 11 50 00   ······t· ··e·q·P·
0030  02 00 81 a7 00 00                                  ······

wireshark_Ethernet_20220304232947_a01220.pcapng    Packets: 316 · Displayed: 316 (100.0%)    Profile: Default
```

□ 38. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.

□ 39. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.

Select from menu bar Analyze > Expert information. Expect Information windows pops up and expand Warning node with Duplicate IP address configured (10.10.10.13), which is running on ARP/RARP protocol.

-



Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
*Ethernet
File Edit View Go Capture Analyze Stat
Apply a display filter ... <Ctrl-/>
Wireshark · Expert Information · Ethernet
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help
wireshark_Ethernet_20220304232947_a01220
Profile: Default
11:30 PM
3/4/2022
Module 08: Sniffing
1 Hr 44 Min Remaining
Instructions
Resources
Help
100%
Previous
End
2:30 AM
3/5/2022
ENG
IN

```
No.   Time        Source
  303 37.002493   10.10.10.13
  304 37.003034   10.10.10.10
  305 37.003090   10.10.10.10
  306 37.003093   10.10.10.10
  307 37.008552   72.21.91.29
  308 37.008588   10.10.10.19
  309 37.008591   10.10.10.19
  310 38.002440   10.10.10.13
  311 38.002552   10.10.10.13
  312 38.002556   10.10.10.13
  313 38.003869   10.10.10.10
  314 38.003913   10.10.10.10
  315 38.003915   10.10.10.10

> Frame 1: 54 bytes on wire (432 bits),
> Ethernet II, Src: MS-NLB-PhysServer-21
> Internet Protocol Version 4, Src: 10.1
> Transmission Control Protocol, Src Por

0000  02 15 5d 19 c9 22 02 15  5d 19 c9
0010  00 28 f1 08 00 00 40 06  61 9d 0a
0020  0a 0a 04 d6 00 00 74 88  b4 1b 65
0030  02 00 81 a7 00 00
```

Severity	Summary	Group	Protocol	Count
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	2
˅ Warning	Duplicate IP address configured (10.10.10.10)	Sequence	ARP/RARP	10
109	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
110	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
208	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
209	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
210	10.10.10.13 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
211	10.10.10.13 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
227	10.10.10.13 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
228	10.10.10.13 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
229	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
230	10.10.10.10 is at 02:15:5d:19:c9:22	Sequence	ARP/RARP	
> Warning	Connection reset (RST)	Sequence	TCP	117
> Note	TCP keep-alive segment	Sequence	TCP	6
> Note	Duplicate ACK (#1)	Sequence	TCP	80
> Note	The acknowledgment number field is nonzero while the A...	Protocol	TCP	117
> Chat	Connection finish (FIN)	Sequence	TCP	6

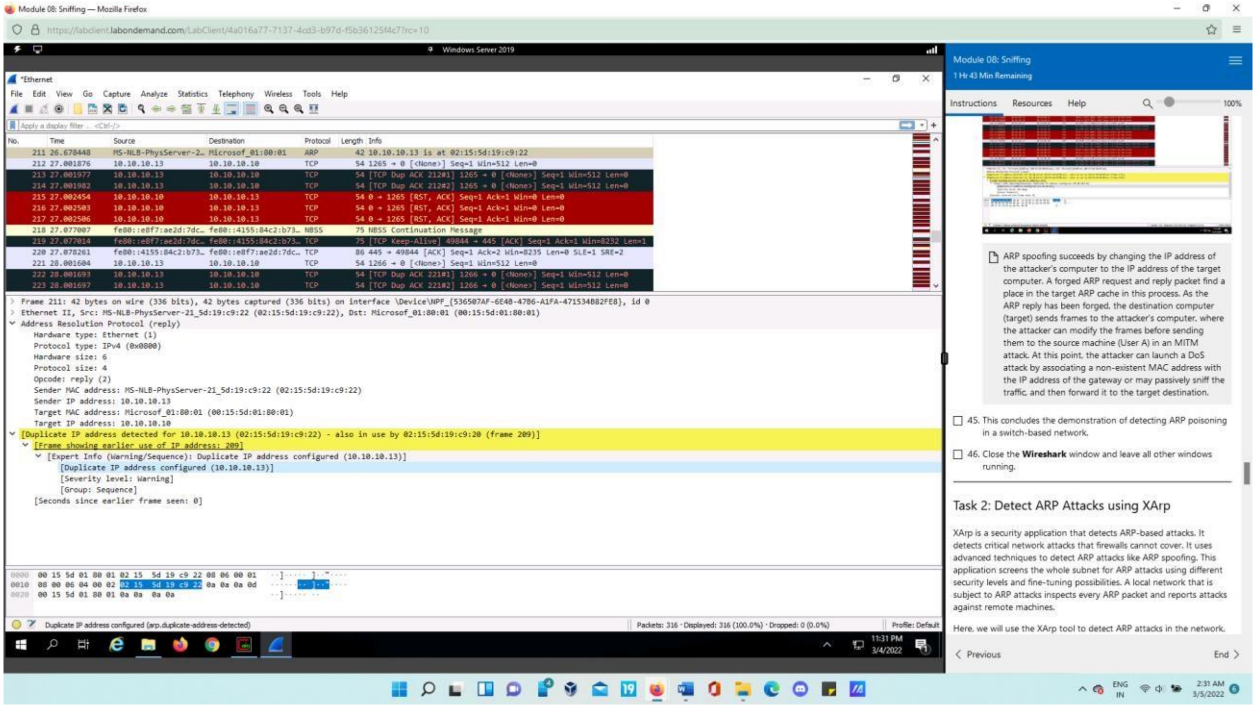
☑ 40. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.10.13)**, running on the **ARP/RARP** protocol.

☐ 41. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

☐ 42. In the **Wireshark . Expert Information** window, click any packet (here, **216**).

- Position the Wireshark Expert Information window above the Wireshark window so that the packet number and the Packet details section are visible. Select any packet in the Wireshark Expert Information window (here, 216). Wireshark highlights the packet when you choose the packet number, and the packet's related information is presented in the packet details section.
  The Wireshark Expert Information window should now be closed.

-



Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows Server 2019
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Module 08: Sniffing
1 Hr 43 Min Remaining
Instructions Resources Help
100%

```
No.   Time        Source                  Destination             Protocol Length Info
  211 26.678448   MS-NLB-PhysServer-2…    Microsof_01:80:01       ARP        42 10.10.10.13 is at 02:15:5d:19:c9:22
  212 27.001876   10.10.10.13             10.10.10.10             TCP        54 1265 → 0 [<None>] Seq=1 Win=512 Len=0
  213 27.001977   10.10.10.13             10.10.10.10             TCP        54 [TCP Dup ACK 212#1] 1265 → 0 [<None>] Seq=1 Win=512 Len=0
  214 27.001982   10.10.10.13             10.10.10.10             TCP        54 [TCP Dup ACK 212#2] 1265 → 0 [<None>] Seq=1 Win=512 Len=0
  215 27.002454   10.10.10.10             10.10.10.13             TCP        54 0 → 1265 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  216 27.002503   10.10.10.10             10.10.10.13             TCP        54 0 → 1265 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  217 27.002506   10.10.10.10             10.10.10.13             TCP        54 0 → 1265 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  218 27.077007   fe80::e8f7:ae2d:7dc…    fe80::4155:84c2:b73…    NBSS       75 NBSS Continuation Message
  219 27.077014   fe80::e8f7:ae2d:7dc…    fe80::4155:84c2:b73…    TCP        75 [TCP Keep-Alive] 49844 → 445 [ACK] Seq=1 Ack=1 Win=8232 Len=1
  220 27.078261   fe80::4155:84c2:b73…    fe80::e8f7:ae2d:7dc…    TCP        86 445 → 49844 [ACK] Seq=1 Ack=2 Win=8235 Len=0 SLE=1 SRE=2
  221 28.001604   10.10.10.13             10.10.10.10             TCP        54 1266 → 0 [<None>] Seq=1 Win=512 Len=0
  222 28.001693   10.10.10.13             10.10.10.10             TCP        54 [TCP Dup ACK 221#1] 1266 → 0 [<None>] Seq=1 Win=512 Len=0
  223 28.001697   10.10.10.13             10.10.10.10             TCP        54 [TCP Dup ACK 221#2] 1266 → 0 [<None>] Seq=1 Win=512 Len=0

> Frame 211: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{536507AF-6E48-4786-A1FA-471534B82FE8}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:c9:22 (02:15:5d:19:c9:22), Dst: Microsof_01:80:01 (00:15:5d:01:80:01)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: MS-NLB-PhysServer-21_5d:19:c9:22 (02:15:5d:19:c9:22)
    Sender IP address: 10.10.10.13
    Target MAC address: Microsof_01:80:01 (00:15:5d:01:80:01)
    Target IP address: 10.10.10.10
v [Duplicate IP address detected for 10.10.10.13 (02:15:5d:19:c9:22) - also in use by 02:15:5d:19:c9:20 (frame 209)]
  v [Frame showing earlier use of IP address: 209]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (10.10.10.13)]
        [Duplicate IP address configured (10.10.10.13)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 0]

0000  00 15 5d 01 80 01 02 15  5d 19 c9 22 08 06 00 01   ··]·····]··"····
0010  08 00 06 04 00 02 02 15  5d 19 c9 22 0a 0a 0a 0d   ········]··"····
0020  00 15 5d 01 80 01 0a 0a  0a 0a                     ··]·······

Duplicate IP address configured (arp.duplicate-address-detected)    Packets: 316 · Displayed: 316 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

□ 45. This concludes the demonstration of detecting ARP poisoning in a switch-based network.

□ 46. Close the **Wireshark** window and leave all other windows running.

Task 2: Detect ARP Attacks using XArp

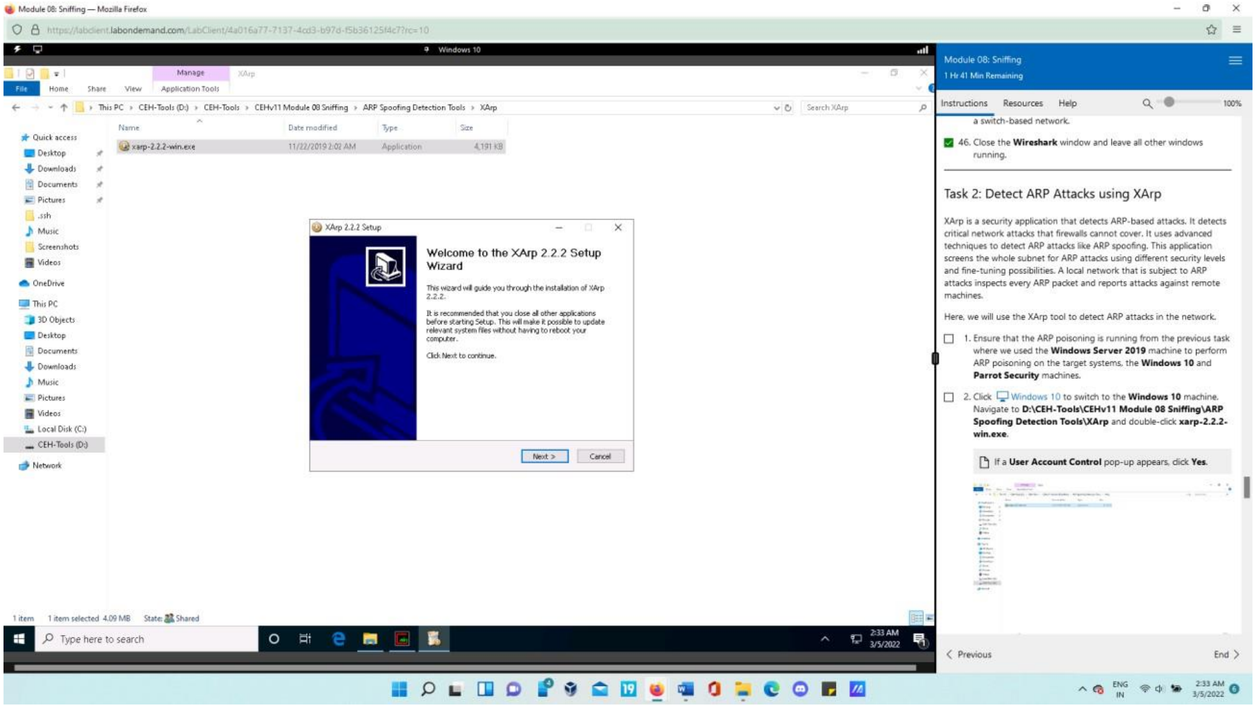
XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

Here, we will use the XArp tool to detect ARP attacks in the network.

Duplicate IP addresses have been found at one MAC address, as indicated by the yellow highlighted section.

Task 2: Detect ARP Attacks using XArp

- In Windows10 navigate to D:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp and execute the file xarp-2.2.2-win.exe.


Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows 10
This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 08 Sniffing › ARP Spoofing Detection Tools › XArp
Name
Date modified
Type
Size
xarp-2.2.2-win.exe
11/22/2019 2:02 AM
Application
4,191 KB
1 item 1 item selected 4.09 MB State: Shared
Type here to search
2:33 AM
3/5/2022
Module 08: Sniffing
1 Hr 41 Min Remaining
Instructions
Resources
Help
100%
Previous
End

XArp 2.2.2 Setup

Welcome to the XArp 2.2.2 Setup Wizard

This wizard will guide you through the installation of XArp 2.2.2.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Next > Cancel

a switch-based network.

☑ 46. Close the **Wireshark** window and leave all other windows running.

Task 2: Detect ARP Attacks using XArp

XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

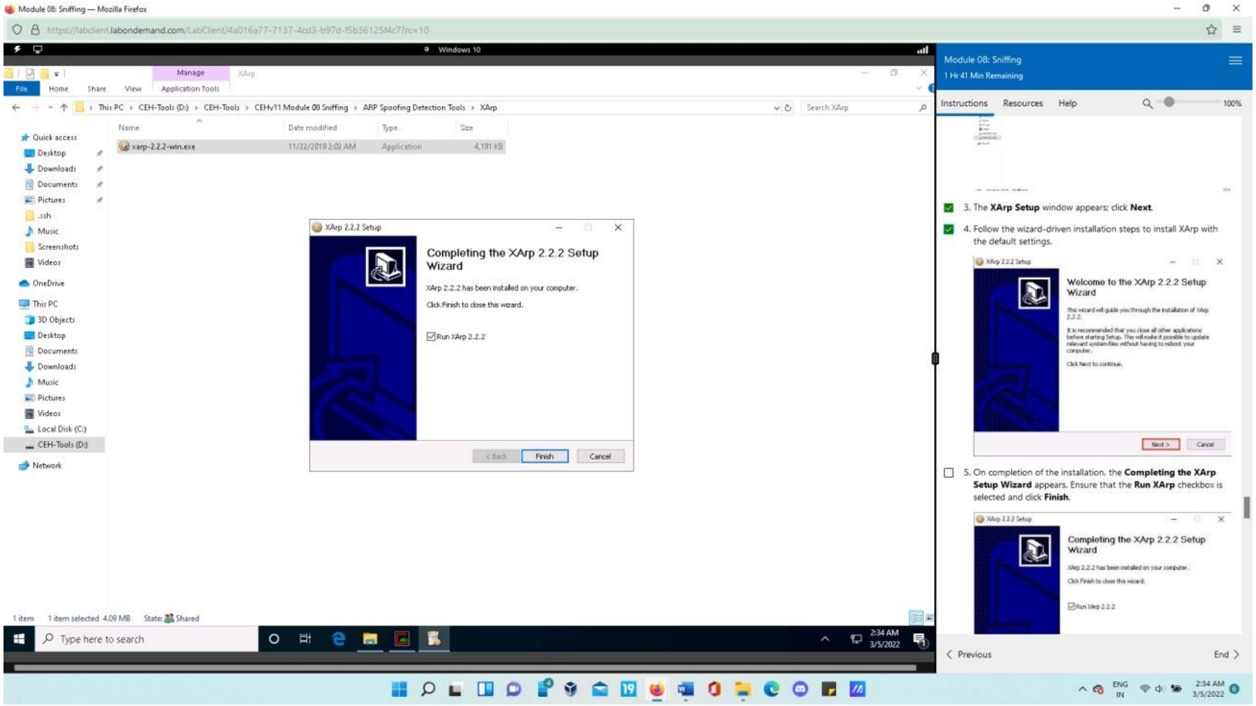
Here, we will use the XArp tool to detect ARP attacks in the network.

□ 1. Ensure that the ARP poisoning is running from the previous task where we used the **Windows Server 2019** machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** machines.

□ 2. Click Windows 10 to switch to the **Windows 10** machine. Navigate to **D:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp** and double-click **xarp-2.2.2-win.exe**.

If a **User Account Control** pop-up appears, click **Yes**.

- Run the setup and launch the XArp.


Module 08: Sniffing — Mozilla Firefox
https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10
Windows 10
This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 08 Sniffing › ARP Spoofing Detection Tools › XArp
xarp-2.2.2-win.exe
11/22/2019 2:02 AM
Application
4,191 KB
Type here to search
2:34 AM
3/5/2022
Module 08: Sniffing
1 Hr 41 Min Remaining
Instructions
Resources
Help
Previous
End

XArp 2.2.2 Setup

Completing the XArp 2.2.2 Setup Wizard

XArp 2.2.2 has been installed on your computer.

Click Finish to close this wizard.

☑ Run XArp 2.2.2

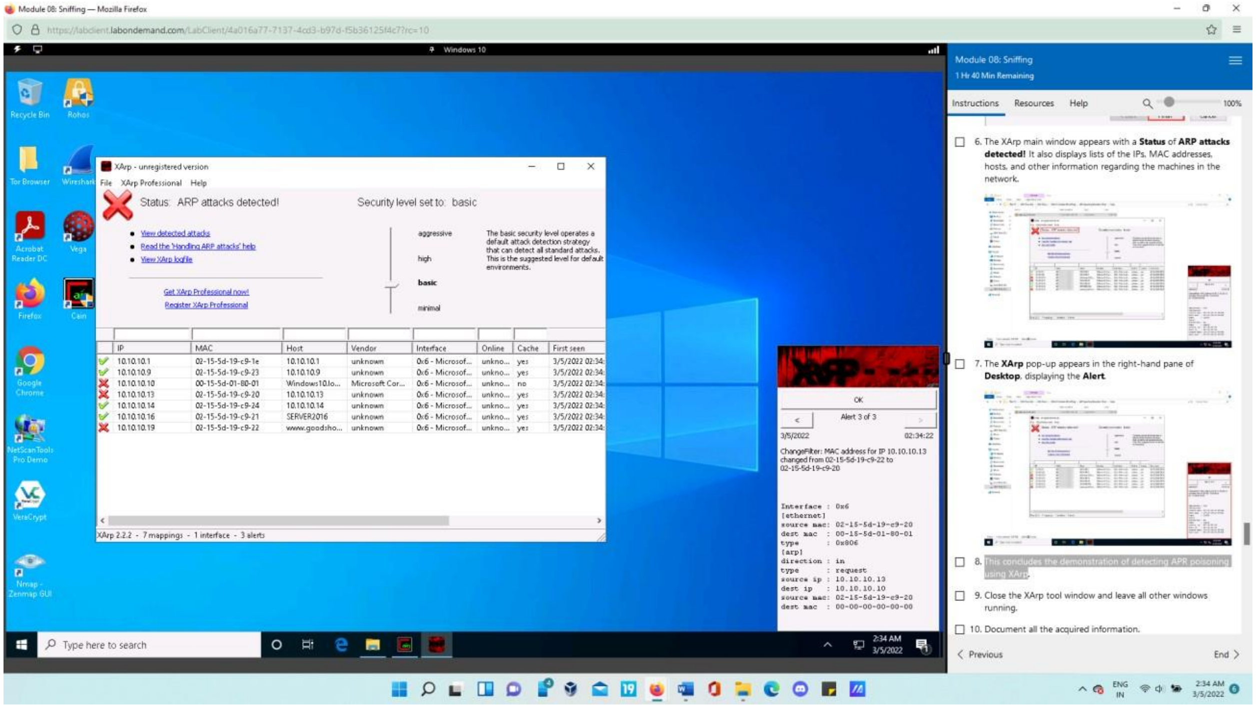
< Back Finish Cancel

☑ 3. The **XArp Setup** window appears; click **Next**.

☑ 4. Follow the wizard-driven installation steps to install XArp with the default settings.

□ 5. On completion of the installation, the **Completing the XArp Setup Wizard** appears. Ensure that the **Run XArp** checkbox is selected and click **Finish**.

Detected ARP attacks are showed on the XArp main pane. It also shows IP addresses, MAC addresses, hosts, and other details about the machines on the network. The Alert is displayed in the XArp pop-up on the right-hand pane of Desktop.



Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
✓	10.10.10.1	02-15-5d-19-c9-1e	10.10.10.1	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:
✓	10.10.10.9	02-15-5d-19-c9-23	10.10.10.9	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:
✗	10.10.10.10	00-15-5d-01-80-01	Windows10.lo...	Microsoft Cor...	0x6 - Microsof...	unkno...	no	3/5/2022 02:34:
✗	10.10.10.13	02-15-5d-19-c9-20	10.10.10.13	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:
✓	10.10.10.14	02-15-5d-19-c9-24	10.10.10.14	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:
✓	10.10.10.16	02-15-5d-19-c9-21	SERVER2016	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:
✗	10.10.10.19	02-15-5d-19-c9-22	www.goodsho...	unknown	0x6 - Microsof...	unkno...	yes	3/5/2022 02:34:

XArp 2.2.2 - 7 mappings - 1 interface - 3 alerts

Alert 3 of 3

3/5/2022 02:34:22

ChangeFilter: MAC address for IP 10.10.10.13 changed from 02-15-5d-19-c9-22 to 02-15-5d-19-c9-20

```
Interface : 0x6
[ethernet]
source mac: 02-15-5d-19-c9-20
dest mac  : 00-15-5d-01-80-01
type      : 0x806
[arp]
direction : in
type      : request
source ip : 10.10.10.13
dest ip   : 10.10.10.10
source mac: 02-15-5d-19-c9-20
dest mac  : 00-00-00-00-00-00
```

Module 08: Sniffing

1 Hr 40 Min Remaining

□ 6. The XArp main window appears with a **Status** of **ARP attacks detected!** It also displays lists of the IPs, MAC addresses, hosts, and other information regarding the machines in the network.

□ 7. The **XArp** pop-up appears in the right-hand pane of **Desktop**, displaying the **Alert**.

□ 8. This concludes the demonstration of detecting APR poisoning using XArp.

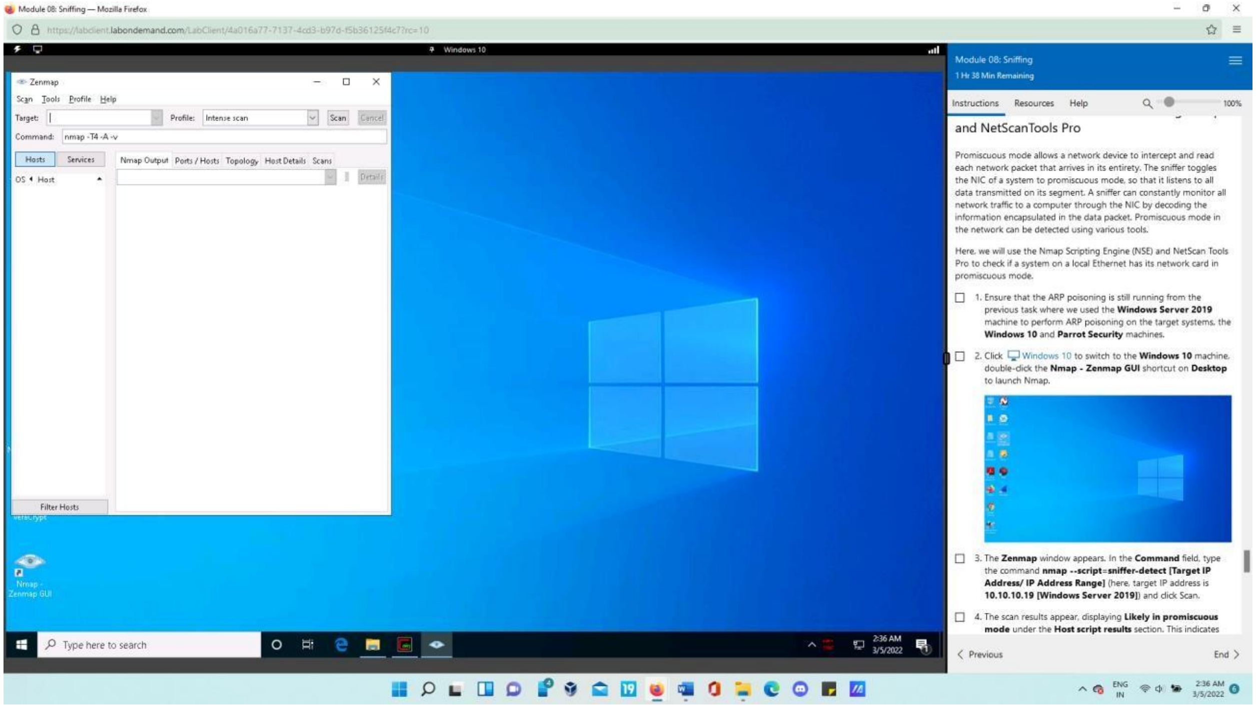
□ 9. Close the XArp tool window and leave all other windows running.

□ 10. Document all the acquired information.

This completes the XArp-based detection of APR poisoning exercise.

Task 3: Detect Promiscuous Mode using Nmap and NetScanTools Pro

- Use Windows10 and launch Nmap GUI version.



Target:

Profile: Intense scan

Command: nmap -T4 -A -v

and NetScanTools Pro

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

Here, we will use the Nmap Scripting Engine (NSE) and NetScan Tools Pro to check if a system on a local Ethernet has its network card in promiscuous mode.

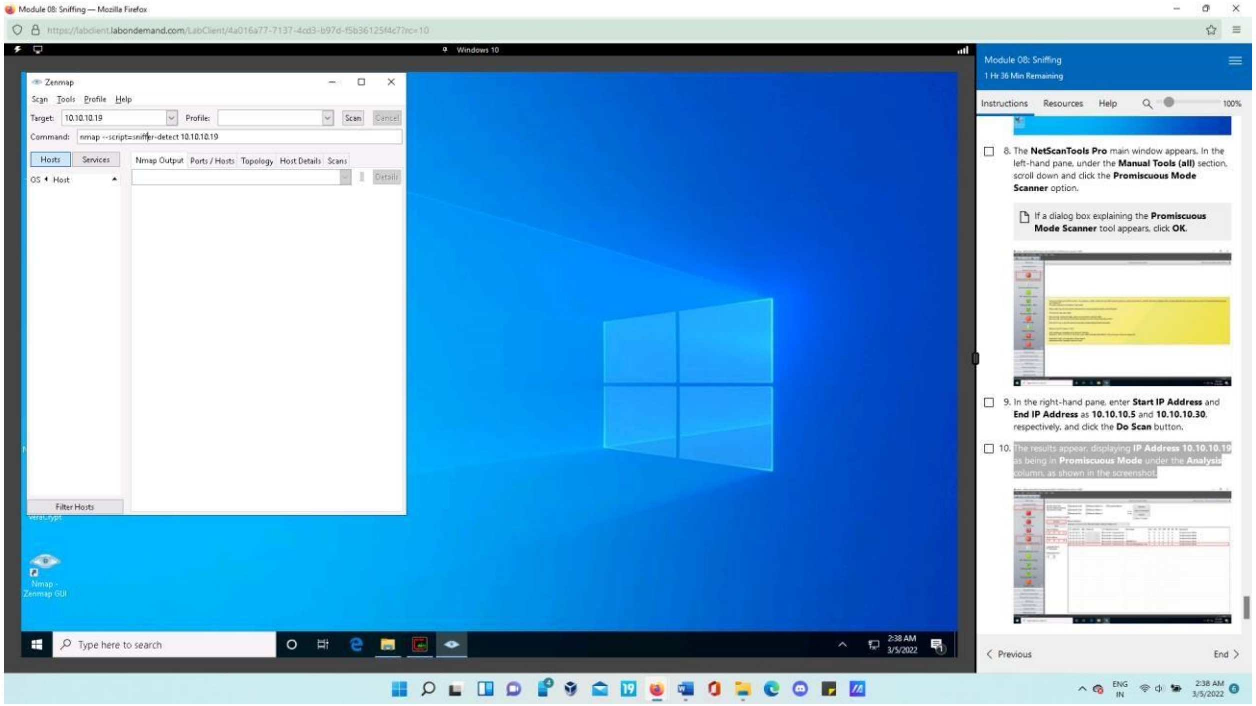
□ 1. Ensure that the ARP poisoning is still running from the previous task where we used the **Windows Server 2019** machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** machines.

□ 2. Click Windows 10 to switch to the **Windows 10** machine, double-click the **Nmap - Zenmap GUI** shortcut on **Desktop** to launch Nmap.

□ 3. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.10.19 [Windows Server 2019]**) and click Scan.

□ 4. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates

- Now execute the command nmap --script=sniffer-detect 10.10.10.19 and press scan



Module 08: Sniffing — Mozilla Firefox

Zenmap

Target: 10.10.10.19

Command: nmap --script=sniffer-detect 10.10.10.19

Module 08: Sniffing
1 Hr 36 Min Remaining

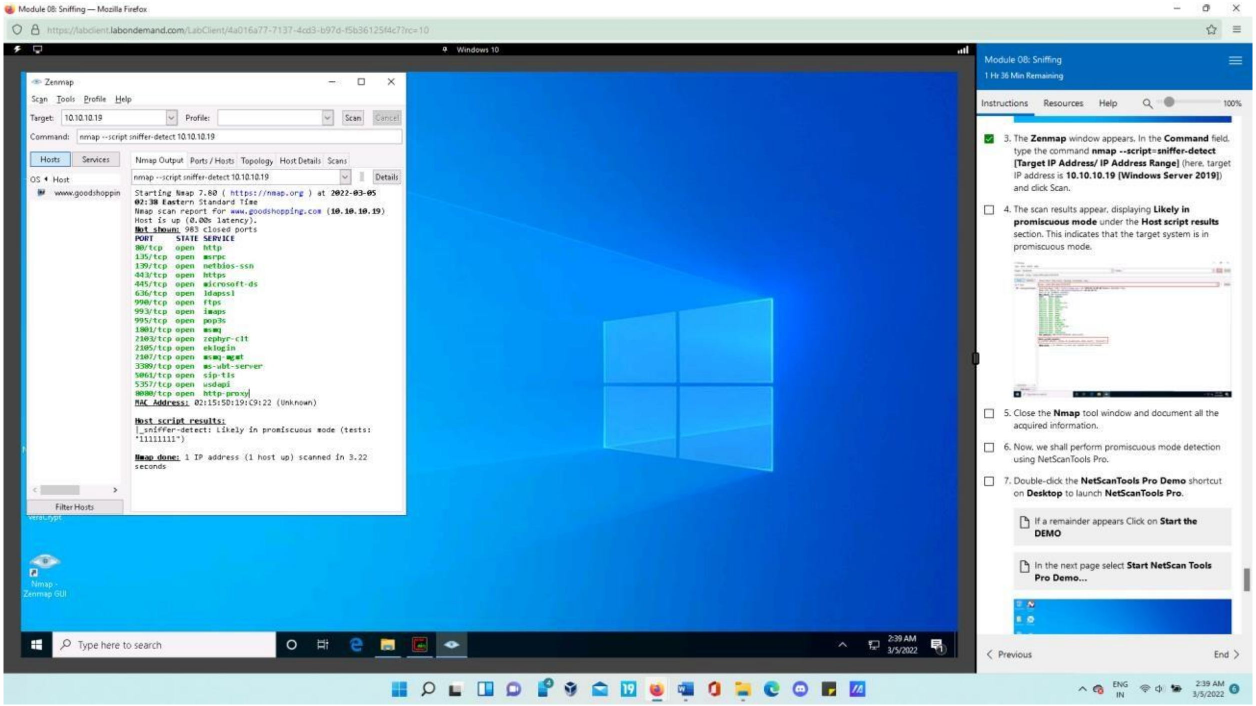
□ 8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

□ 9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.

□ 10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

Under the Host script results section, the scan results displayed, with Likely in promiscuous mode. The target system is in promiscuous mode, as shown by this. Close the Nmap tool window.



Module 08: Sniffing — Mozilla Firefox

Zenmap

Target: 10.10.10.19

Command: nmap --script sniffer-detect 10.10.10.19

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-05
02:38 Eastern Standard Time
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
636/tcp   open  ldapssl
990/tcp   open  ftps
993/tcp   open  imaps
995/tcp   open  pop3s
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5061/tcp  open  sip-tls
5357/tcp  open  wsdapi
8080/tcp  open  http-proxy
MAC Address: 02:15:5D:19:C9:22 (Unknown)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests:
"11111111")

Nmap done: 1 IP address (1 host up) scanned in 3.22
seconds
```

Module 08: Sniffing
1 Hr 36 Min Remaining

☑ 3. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.10.19 [Windows Server 2019]**) and click Scan.

□ 4. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.

□ 5. Close the **Nmap** tool window and document all the acquired information.

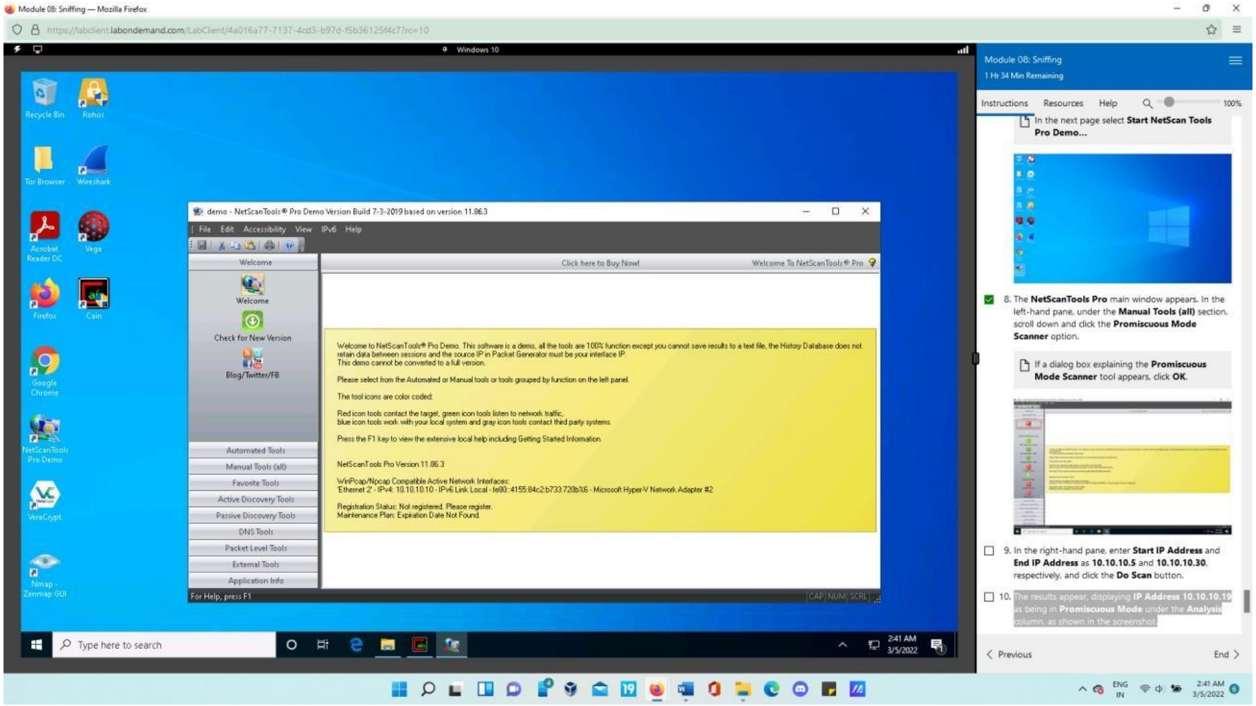
□ 6. Now, we shall perform promiscuous mode detection using NetScanTools Pro.

□ 7. Double-click the **NetScanTools Pro Demo** shortcut on **Desktop** to launch **NetScanTools Pro**.

If a remainder appears Click on **Start the DEMO**

In the next page select **Start NetScan Tools Pro Demo...**

- Now, Launch **NetScanTools Pro** from Desktop.



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 11.86.3

WinPcap/Npcap Compatible Active Network Interfaces:
'Ethernet 2' - IPv4: 10.10.10.10 - IPv6 Link Local - fe80::4155:84c2:b733:720b%6 - Microsoft Hyper-V Network Adapter #2

Registration Status: Not registered. Please register.
Maintenance Plan: Expiration Date Not Found.

In the next page select **Start NetScan Tools Pro Demo...**

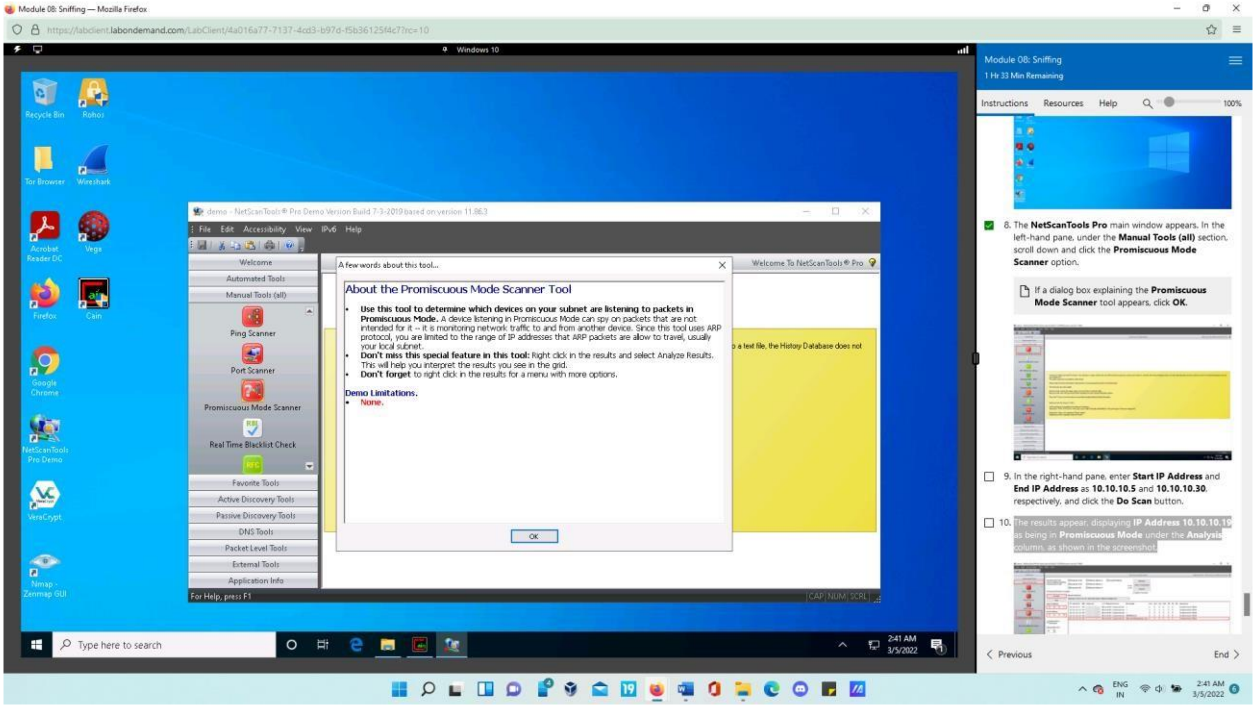
☑ 8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

☐ 9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.

☐ 10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

- Select Promiscuous mode scanner option from the left-pane under Manual tools section.



About the Promiscuous Mode Scanner Tool

- **Use this tool to determine which devices on your subnet are listening to packets in Promiscuous Mode.** A device listening in Promiscuous Mode can spy on packets that are not intended for it -- it is monitoring network traffic to and from another device. Since this tool uses ARP protocol, you are limited to the range of IP addresses that ARP packets are allow to travel, usually your local subnet.
- **Don't miss this special feature in this tool:** Right click in the results and select Analyze Results. This will help you interpret the results you see in the grid.
- **Don't forget** to right click in the results for a menu with more options.

Demo Limitations.

- None.

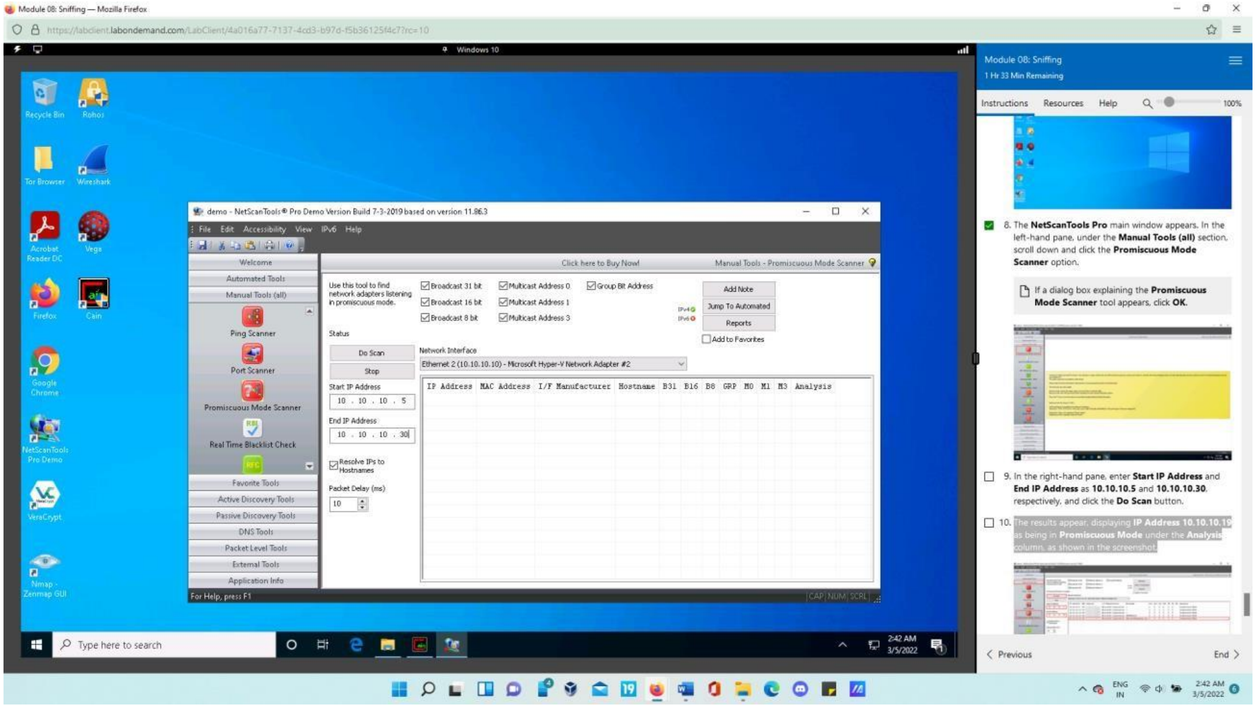
☑ 8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

☐ 9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.

☐ 10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

- Use 10.10.10.5 and 10.10.10.30 as start and end IP respectively in the right-pane and press Do scan button.



Module 08: Sniffing — Mozilla Firefox

https://labclient.labondemand.com/LabClient/4a016a77-7137-4cd3-b97d-f5b36125f4c7?rc=10

demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3

Use this tool to find network adapters listening in promiscuous mode.

☑ Broadcast 31 bit ☑ Multicast Address 0 ☑ Group Bit Address
☑ Broadcast 16 bit ☑ Multicast Address 1
☑ Broadcast 8 bit ☑ Multicast Address 3

Network Interface: Ethernet 2 (10.10.10.10) - Microsoft Hyper-V Network Adapter #2

Start IP Address: 10 . 10 . 10 . 5

End IP Address: 10 . 10 . 10 . 30

☑ Resolve IPs to Hostnames

Packet Delay (ms): 10

```
IP Address  MAC Address  I/F Manufacturer  Hostname  B31  B16  B8  GRP  M0  M1  M3  Analysis
```

Module 08: Sniffing

1 Hr 33 Min Remaining

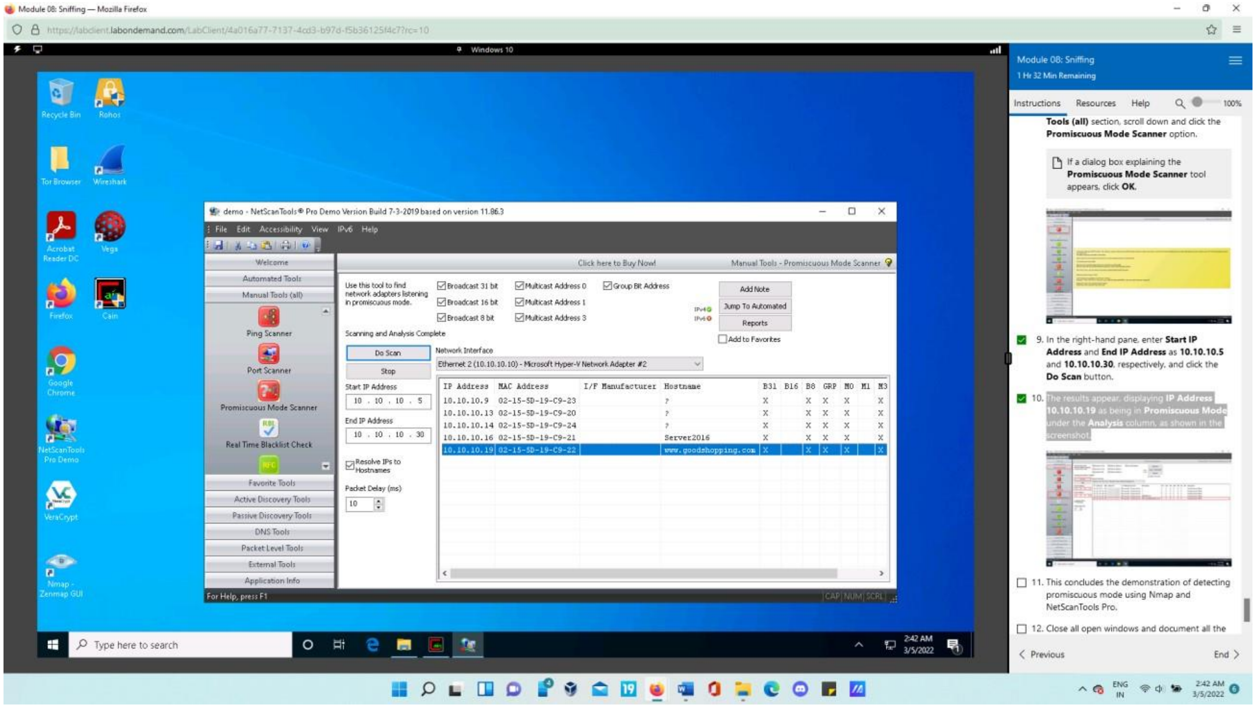
☑ 8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

☐ 9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.

☐ 10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

Under the Analysis column, IP Address 10.10.10.19 is displayed as being in Promiscuous Mode.



Module 08: Sniffing — Mozilla Firefox

demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3

Scanning and Analysis Complete

Network Interface: Ethernet 2 (10.10.10.10) - Microsoft Hyper-V Network Adapter #2

Start IP Address: 10 . 10 . 10 . 5

End IP Address: 10 . 10 . 10 . 30

☑ Resolve IPs to Hostnames

Packet Delay (ms): 10

```
IP Address   MAC Address        I/F Manufacturer  Hostname              B31  B16  B8  GRP  M0  M1  M3
10.10.10.9   02-15-5D-19-C9-23                    ?                     X         X   X    X       X
10.10.10.13  02-15-5D-19-C9-20                    ?                     X         X   X    X       X
10.10.10.14  02-15-5D-19-C9-24                    ?                     X         X   X    X       X
10.10.10.16  02-15-5D-19-C9-21                    Server2016            X         X   X    X       X
10.10.10.19  02-15-5D-19-C9-22                    www.goodshopping.com  X         X   X    X       X
```

Module 08: Sniffing

1 Hr 32 Min Remaining

Tools (all) section, scroll down and click the **Promiscuous Mode Scanner** option.

If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

☑ 9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.

☑ 10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

☐ 11. This concludes the demonstration of detecting promiscuous mode using Nmap and NetScanTools Pro.

☐ 12. Close all open windows and document all the