Sniffing

Module 07

Sniffing a Network

A packet sniffer is a type of plug-and-play wiretap device attached to a computer that eavesdrops on network traffic. It monitors any bit of information entering or leaving a network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

"Sniffing" is the process of monitoring and capturing data packets passing through a given network using software or hardware devices. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Although passive sniffing was predominant in earlier days, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, it contains a few loopholes in switch-based network implementation that can open doors for an attacker to sniff network traffic.

Attackers hack the network using sniffers, where he/she mainly targets the protocols vulnerable to sniffing. Some of the protocols vulnerable to sniffing include HTTP, FTP, SMTP, POP, and so on. The sniffed traffic comprises FTP and Telnet passwords, chat sessions, email and web traffic, DNS traffic, and so on. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, it is essential to assess the security of the network's infrastructure, find the loopholes in it and patch them up to ensure a secure network environment. So, as an ethical hacker/penetration tester, your duties include:

- Implementing network auditing tools such as Wireshark, Cain & Abel, etc. in attempt to find loopholes in the network
- Using security tools such as PromqryUI to detect attacks on the network, and so on.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Objectives

The objective of this lab is to make students learn to sniff a network and analyze packets for any attacks on the network.

The primary objectives of this lab are to:

- Sniff the network
- Analyze incoming and outgoing packets
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

In this lab, you will need:

- A Web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 90 Minutes

Overview of Sniffing Network

Sniffing is performed to collect basic information from the target and its network. It helps to find vulnerabilities and select exploits for attack. It determines network, system, and organizational information.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing Passwords using **Wireshark**
- Analyzing a Network Using the **Capsa Network Analyzer**
- Sniffing the Network Using the **OmniPeek Network Analyzer**
- Spoofing MAC Address Using **SMAC**
- Performing Man-in-the-Middle Attack using **Cain & Abel**
- Detecting Systems running in **Promiscuous mode** in a Network using **PromqryUI**
- Detecting **ARP Poisoning** in a **Switch** Based Network
- Detecting ARP attacks with **XArp** tool
- Performing **DNS Poisoning** in a Switch Based Network

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer, which is used to capture network packets and display packet data in detail.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data traversing an HTTP channel is prone to MITM attacks, as it flows in plain-text format. Network administrators can use sniffers to troubleshoot network problems, examine security problems and debug protocol implementations. However, an attacker can use the tools such as Wireshark and sniffs the traffic flowing between the client and the server. This traffic obtained by the attacker might contain sensitive information such as login credentials, which can be used to perform malicious activities such as user-session impersonation.

As an ethical hacker, you need to perform network security assessments, and suggest proper troubleshooting techniques to mitigate attacks. This lab gives you hands-on experience of how to use Wireshark to sniff network traffic and capture it on a remote interface.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

The objective of this lab is to demonstrate sniffing to capture traffic from multiple interfaces and collect data from any network topology.

In this lab, you will learn how to:

- Capture Passwords of Local Interface and
- Capture traffic from Remote Interface

Lab Environment

In this lab, you will need:

- Wireshark, located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark**

- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as Host (Attacker) machine
- A virtual machine running Windows 8.1 (Victim machine)
- A Web browser with Internet connection
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.

Lab Duration

Time: 15 Minutes

Overview of Password Sniffing

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all of the network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

Lab Tasks

TASK 1

Install Wireshark

1. Before starting this lab, ensure that WinPcap is installed. Also, log into the virtual machine(s).
2. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark** and double-click **Wireshark-win64-1.10.5.exe**.
3. If **Open File - Security Warning** pop-up appears, click **Run**.

4. Follow the wizard-driven installation steps to install Wireshark.

FIGURE 1.1: Wireshark installation wizard

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

5. On completing the installation, launch **Wireshark** from the **Apps** screen.

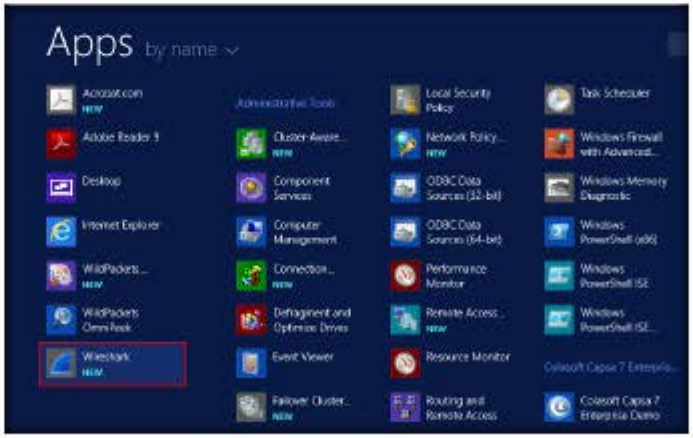


FIGURE 1.2: Windows Server 2012 - Apps screen

TASK 2

Configure Wireshark and Capture Traffic

6. The **Wireshark** main window appears, as shown in the screenshot:

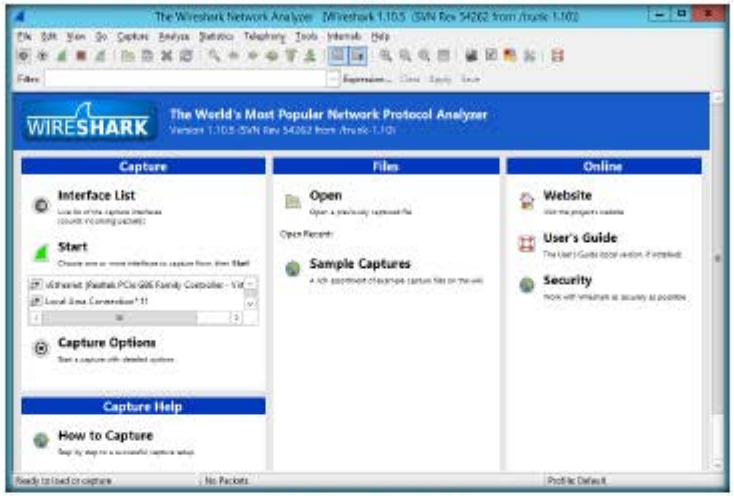


FIGURE 1.3: Wireshark Main Window

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well.

7. From the Wireshark menu bar, click **Capture → Interfaces (Ctrl+I)**.

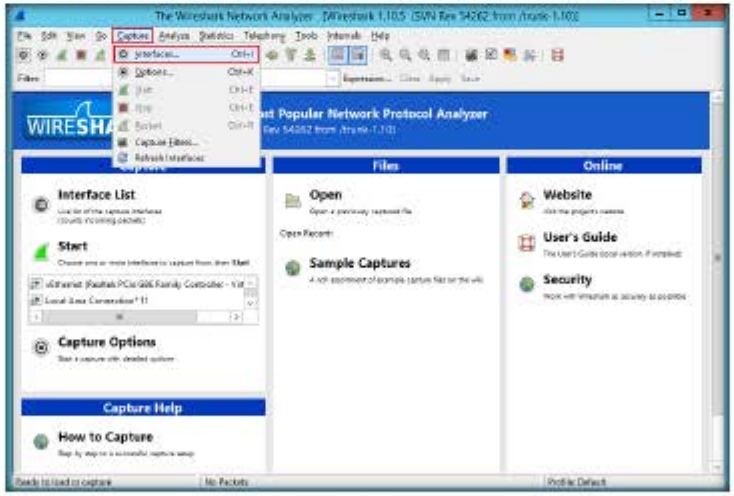


FIGURE 1.4: Wireshark Main Window with Interface Option

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

HaCkRhInO-TeaM ! Y0uR SeCuiTy iS N0t En0Ugh wE FrEE t0 FlY HaCkRhInO-TeaM !

8. The **Wireshark: Capture Interfaces** window appears, as shown in the screenshot:

A supported network card for capturing Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.

FIGURE 1.5: Wireshark Capture Interfaces Window

9. In the window, find and check the Ethernet Driver Interface connected to the system.
10. In the above screenshot, it is the **Ethernet**. The **interface** should show some packets passing through it, as it is connected to the network.

Note: This interface might vary in your lab environment.

11. Click **Start** to start capturing the traffic associated with the interface.

FIGURE 1.6: Wireshark Capture Interfaces Window – Starting Capture

12. Wireshark starts capturing the packets generated while any traffic is received or sent from your machine.

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs

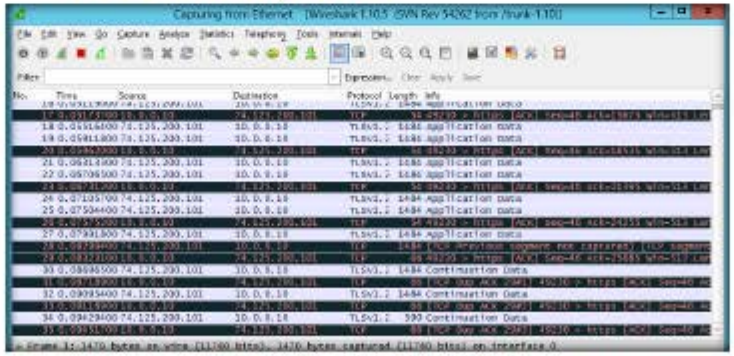


FIGURE 1.7: Wireshark Window with Packets Captured

13. Now, switch to the virtual machine (Windows 8.1), and log into your email account for which you would like to sniff the password.

TASK 3

Stop Live Capturing

14. **Stop the running live capture** by clicking  on the toolbar.

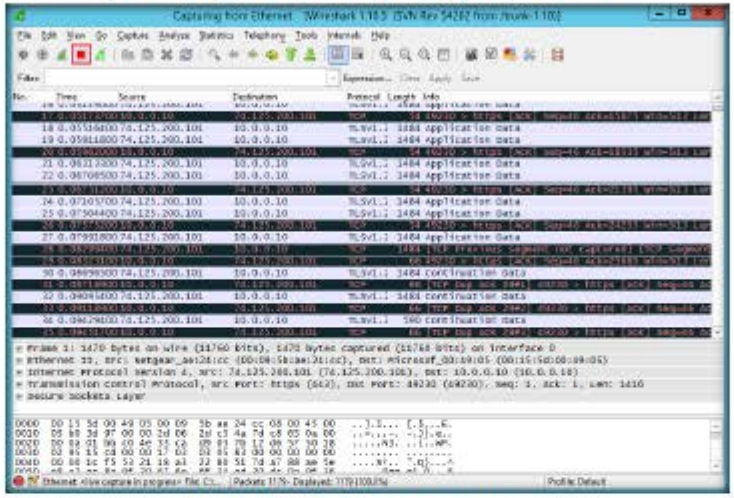


FIGURE 1.8: Wireshark Window - Stopping Live Capture

TASK 4

Save Captured Files

15. Click **File → Save As...** to save the captured packets.

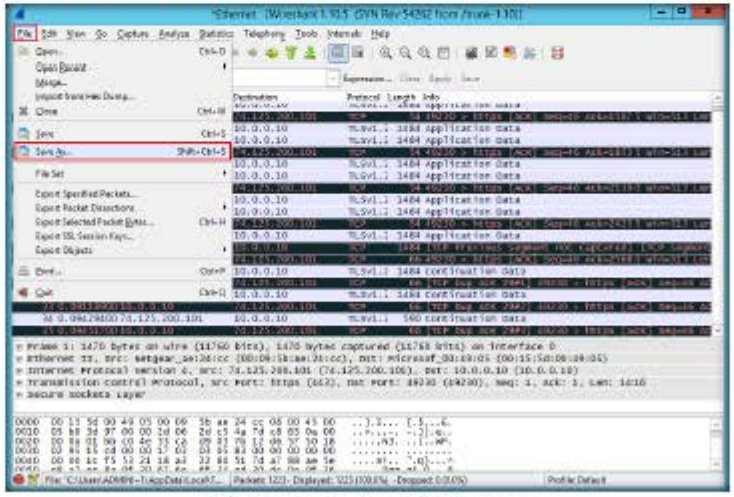


FIGURE 1.9: Wireshark - Saving the Captured Packets

16. Select a destination to save the file, specify a file name, and select a file format. Click **Save**. Here, **pcapng** format has been chosen.

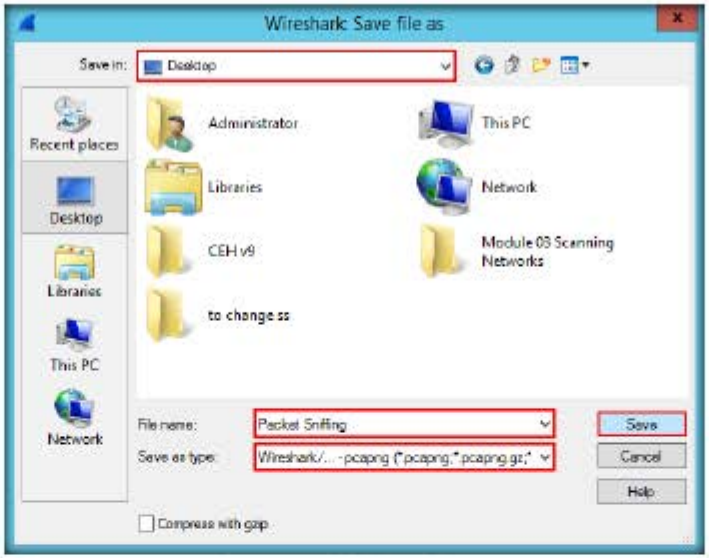


FIGURE 1.10 Wireshark Saving a packet capture

TASK 5

Look for passwords

17. Filter HTTP traffic by issuing **http** syntax in the Filter field, and click **Apply**.
18. Applying this syntax helps you narrow down the search for passwords.

Wireshark can save packets captured in a large number of formats of other capture programs.

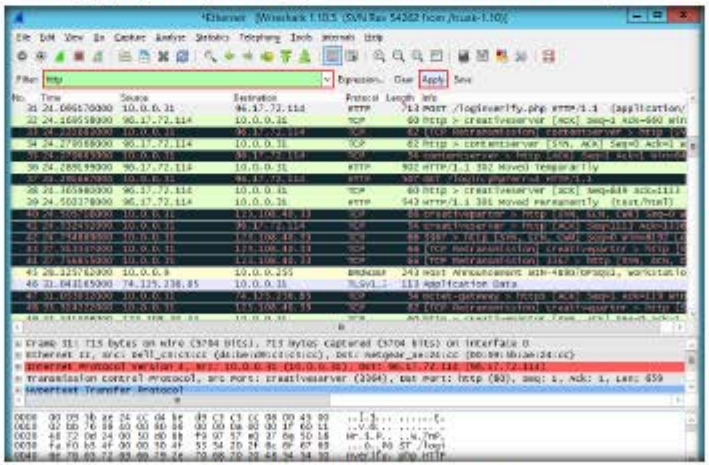


FIGURE 1.11: Wireshark - Filtering http traffic

19. Wireshark filters only http packets, as shown in the screenshot:

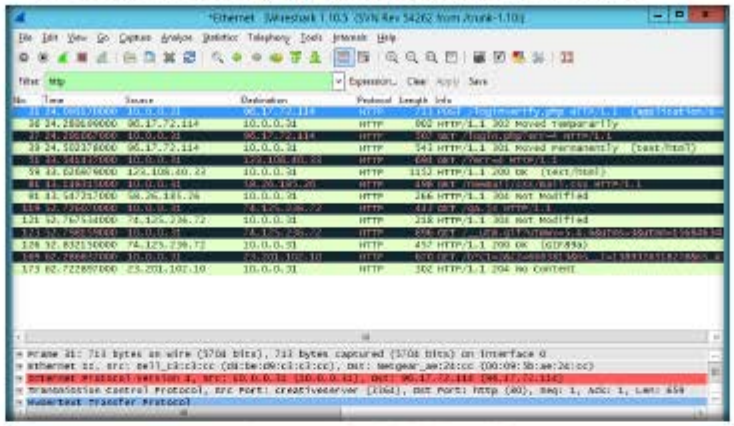


FIGURE 1.12: Wireshark - Filtering http traffic

20. Now, go to **Edit** and click **Find Packet...**

Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

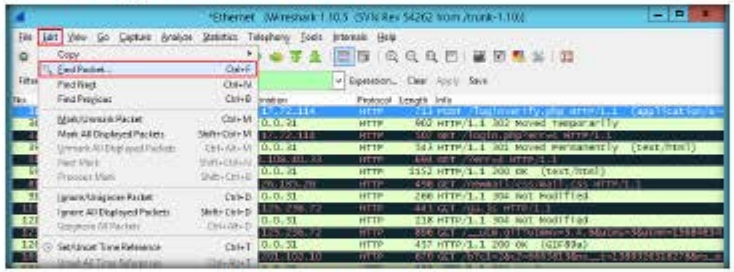


FIGURE 1.13: Wireshark - Finding Packet Option

21. The **Wireshark: Find Packet** window appears.

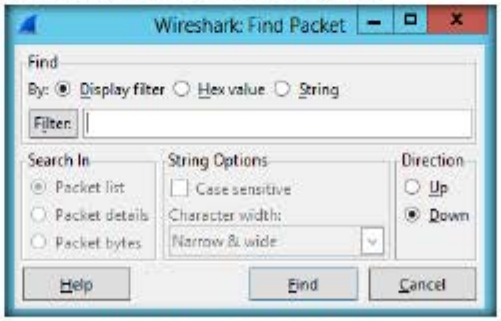


FIGURE 1.14: Wireshark - Find Packet Window

22. Under **Find**, select **String**, type **pwd** in the **Filter** field, select **Packet details**, and select **Narrow (UTF-8 / ASCII)** from the **Character width** drop-down list.
23. Select **Down**, and click **Find**.

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

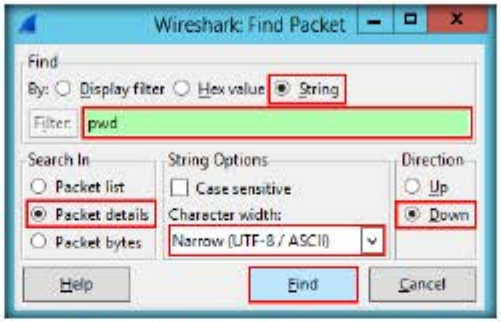


FIGURE 1.15: Wireshark - Selecting Options in Find Packet Window

24. Wireshark will now display the sniffed password from the captured packets.

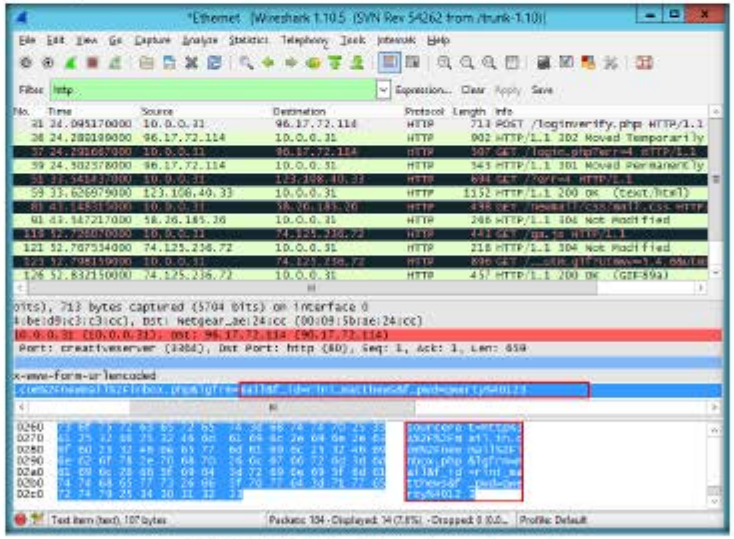


FIGURE 1.16: Wireshark - displaying the captured password

25. **Close** the window.

TASK 6

Capture remote network traffic using Wireshark

26. Before beginning this task, log onto the **Windows 8.1** virtual machine (assume this is the target machine) and sign into the **Jason** user account.

Note: Ensure that the **Jason** account has admin privileges.

FIGURE 1.17: Login to Jason account

27. Use L0phtCrack Password auditor to sniff the user credentials of the target machine. Here, you are the attacker.

28. Switch to the host machine (**Windows Server 2012**), and navigate to **Desktop**. Hover over the lower left of the screen, right-click **Windows,** and click **Search**.

FIGURE 1.18 Selecting Search option

29. Search for **Remote Desktop Connection** (in the **Search** box) and click **Remote Desktop Connection**.

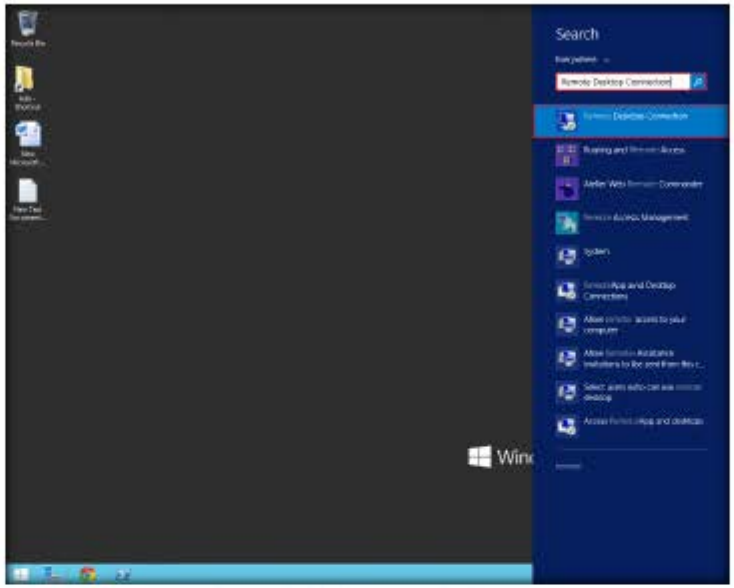


FIGURE 1.19: Searching for Remote Desktop Connection

30. The **Remote Desktop Connection** dialog box appears; click **Show Options**.

FIGURE 1.20: Remote Desktop Connection dialog box

31. The dialog box expands. Fill in the **Computer** and **User name** fields with the target machine's IP address and username.
32. Click **Connect**.

Note: The IP address and username may differ depending on your lab environment.

Here for instance, the username and password are **Jason** and **qwerty**. This is one of the user accounts in the machine with admin privileges.

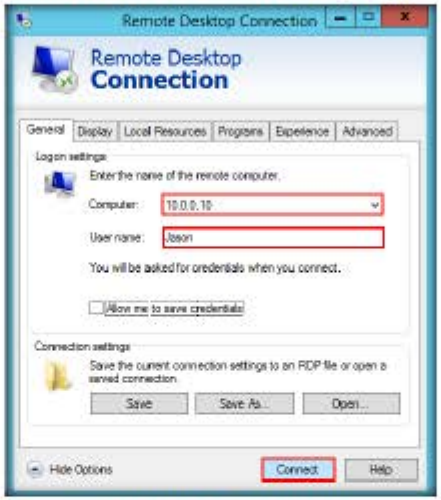


FIGURE 1.21: Connecting to remote desktop

33. The **Windows Security** pop-up appears. Enter the **password** (**qwerty**), and click **OK**.

FIGURE 1.22: Entering the credentials

34. The **Remote Desktop connection** pop-up appears; click **Yes**.

FIGURE 1.23: Establishing Remote Desktop Connection

35. Now the target computer is remotely logged into from the host machine, as shown in the screenshot:

FIGURE 1.24: Remote Desktop Connection successfully established

36. Install WinPcap in this machine.

Note: If the application is already installed, skip to **step 42**.

37. Double-click Network Drive (**Z:**). If **Windows Security** pop-up appears, enter the credentials of host machine and click **OK**.
38. Navigate to **Z:\CEHv9 Lab Prerequisites\Winpcap** and double-click **WinPcap_4_1_3.exe**.

Note: If a network drive is not mapped, enter **(IP address of the host machine)****CEH-Tools****CEHv9 Lab Prerequisites****Winpcap** and double-click **WinPcap_4_1_3.exe**.

39. If a User **Account Control** dialog-box appears, click **Yes**.
40. If **Windows Security** pop-up appears, enter the credentials of host machine and click **OK**.
41. The WinPcap Setup wizard appears; follow the wizard-driven installation steps to install WinPcap.

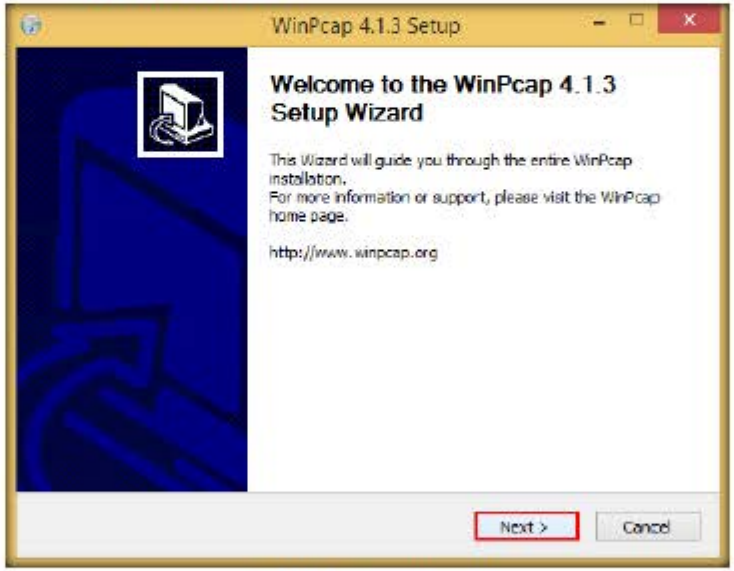


FIGURE 1.25: WinPcap installation wizard

42. Hover over the lower left of the screen; right-click **Windows**, and click **Control Panel**.

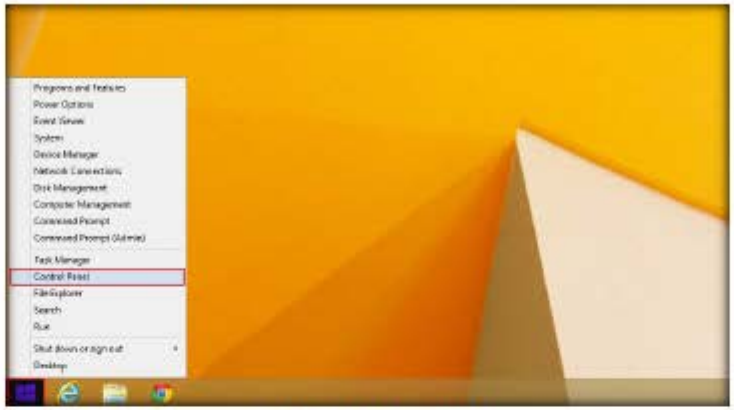


FIGURE 1.26: Selecting Control Panel

43. The **Control panel** window appears; select **Administrative Tools**.

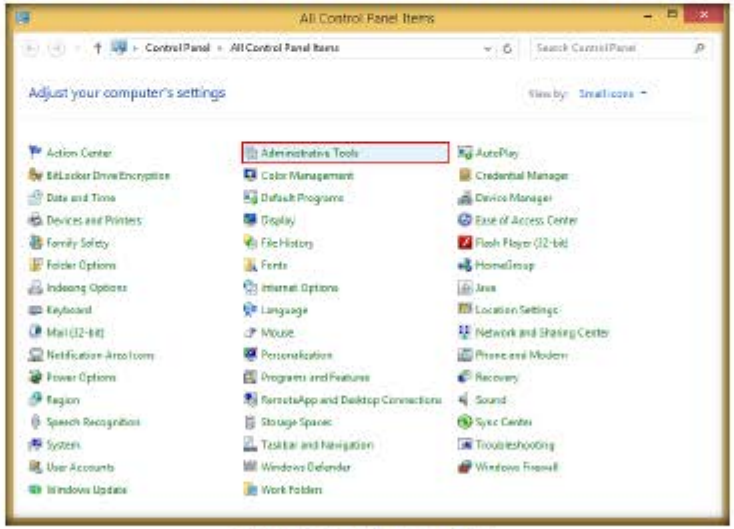


FIGURE 1.27: Selecting Administrative Tools

44. In the **Administrative Tools** control panel, double-click **Services**.

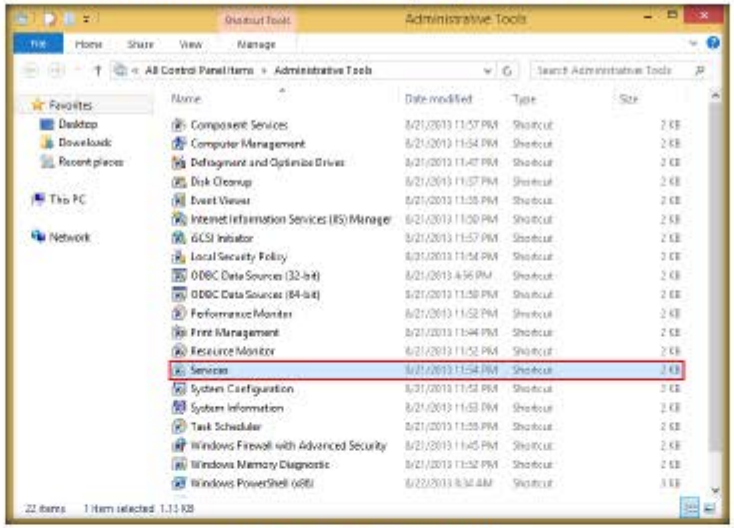


FIGURE 1.28: Launching Administrative Tools

45. In the **Services** control panel, choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service and click **Start**.

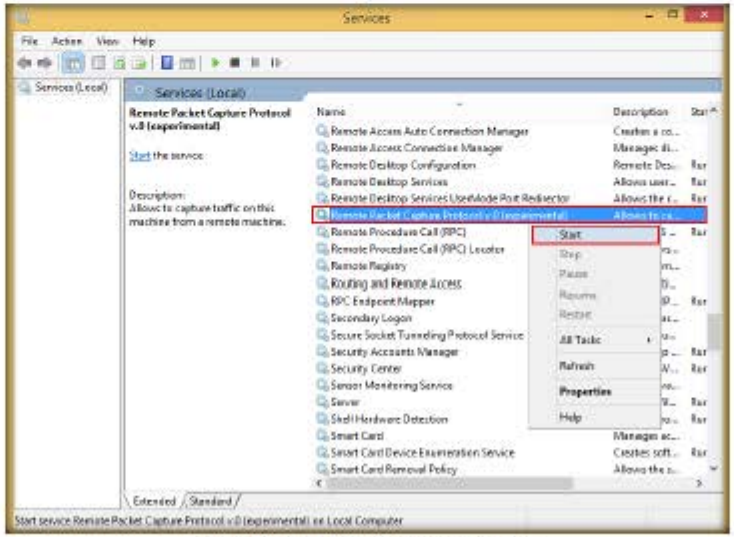


FIGURE 1.29: Starting Remote Packet Capture Protocol v.0

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

46. Close the Remote Desktop Connection.
47. Launch **Wireshark** application from the **Apps** screen of the Windows Server 2012 machine.
48. The **Wireshark** main window appears, as shown in the screenshot:

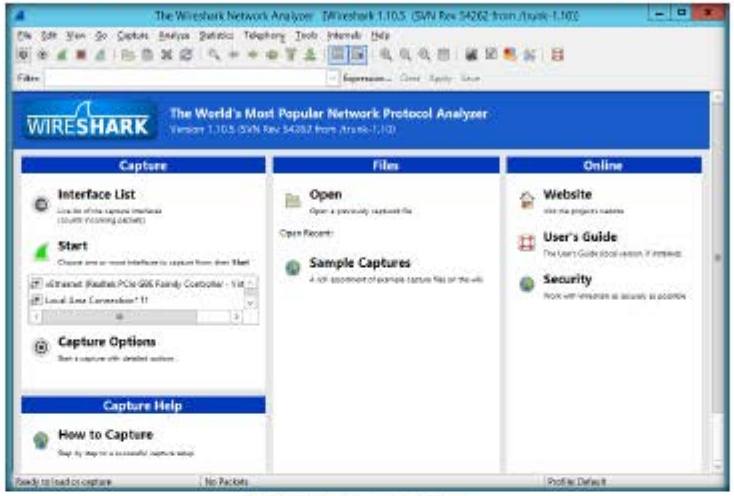


FIGURE 1.30: Wireshark Main Window

49. From the **Wireshark** menu bar, select **Capture → Options...**.

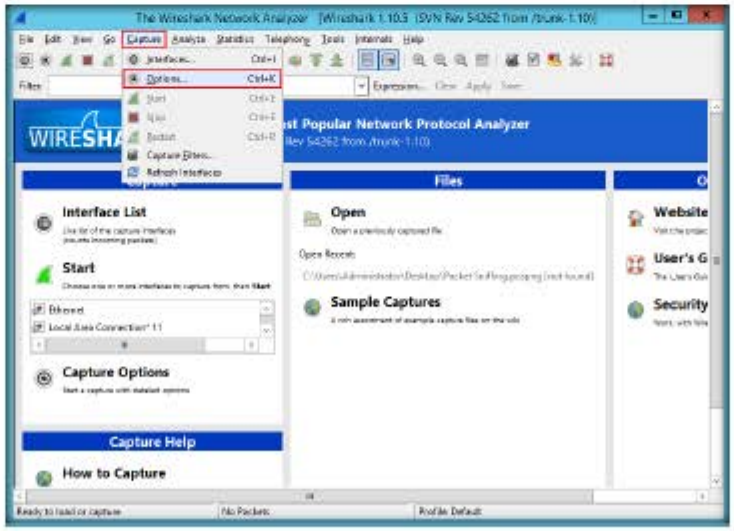


FIGURE 1.31: Selecting Options from Wireshark

50. The **Wireshark: Capture Options** window appears; click **Manage Interfaces**.

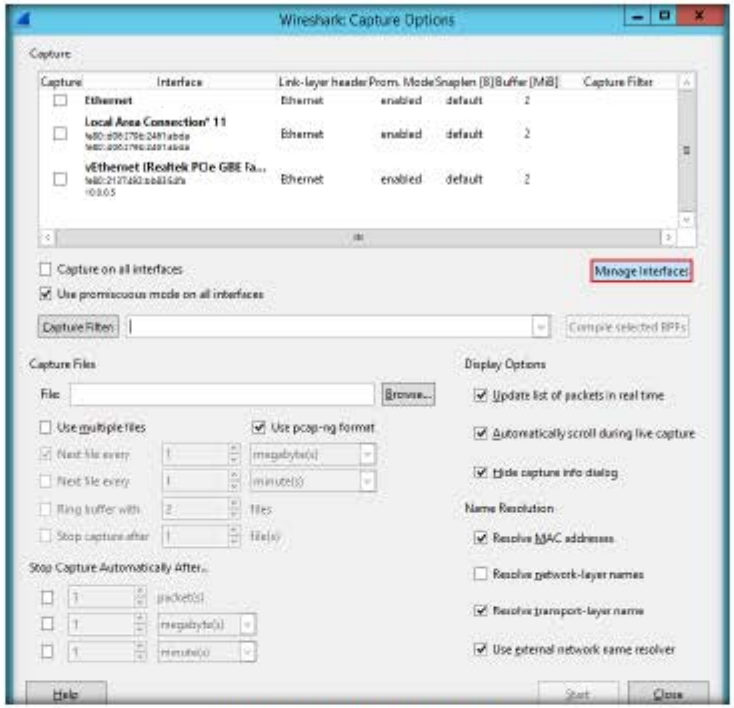


FIGURE 1.32: Selecting Options from Wireshark

51. The **Interface Management** window appears. Click the **Remote Interfaces** tab, and click **Add**.

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

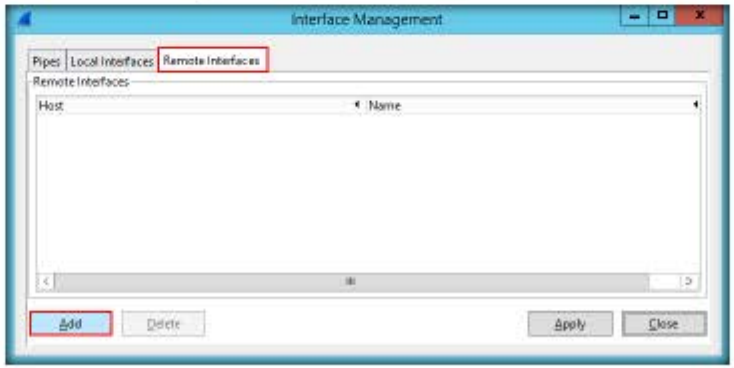


FIGURE 1.33: Interface Management window

52. The **Wireshark: Remote Interface** window appears.
53. In **Host** text field, enter the IP address of the target machine and in the **Port** text field, enter the port number **2002**.
54. Under **Authentication**, select **Password authentication,** and enter the target machine's user credentials.
55. Click **OK**.

Note: The IP address and user credentials may differ in your lab environment.

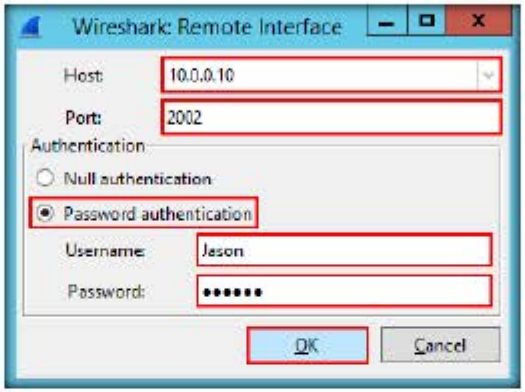


FIGURE 1.34 Wireshark: Remote Interface window

56. A new remote interface is added on the **Remote Interface** tab.
57. Select the host, click **Apply,** and click **Close**.

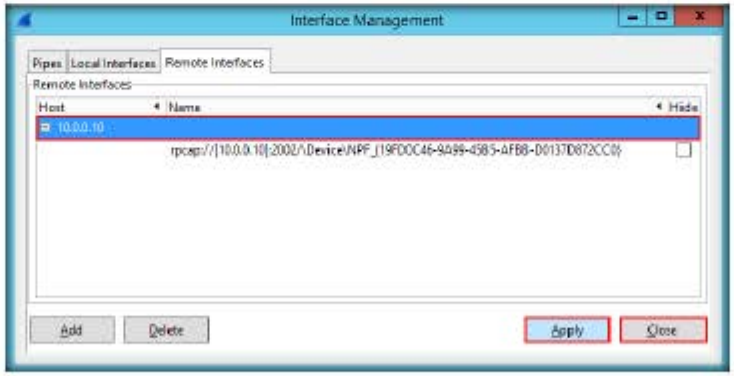


FIGURE 1.35: Applying the newly added interface

58. The newly added remote interface appears in the **Wireshark: Capture Options** window.
59. Check the interface under which IP address of the target machine is displayed, uncheck the other interfaces, and click **Start**.

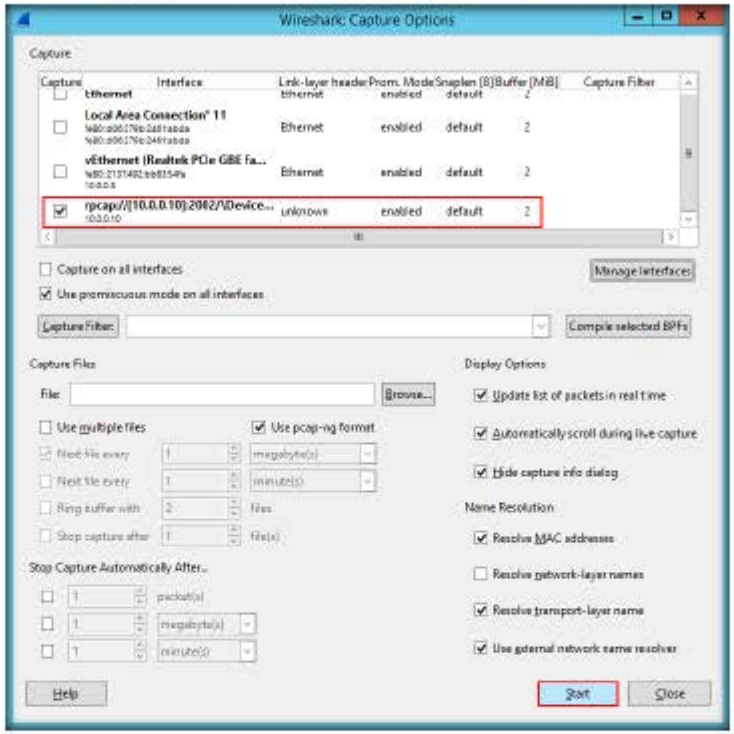


FIGURE L36: Wireshark: Capture Options window

60. Sign into the user account **Jason** in **Windows 8.1** virtual machine. Here, you are signing in as a victim.

Note: The Remote Desktop connection gets disconnected as soon as you sign into the virtual machine.

61. Browse the Internet from the target machine.

FIGURE 1.37: Browsing internet on Windows 8.1

62. Wireshark starts capturing as soon as the user (here, you) begins to browse the Internet, as shown in the screenshot:

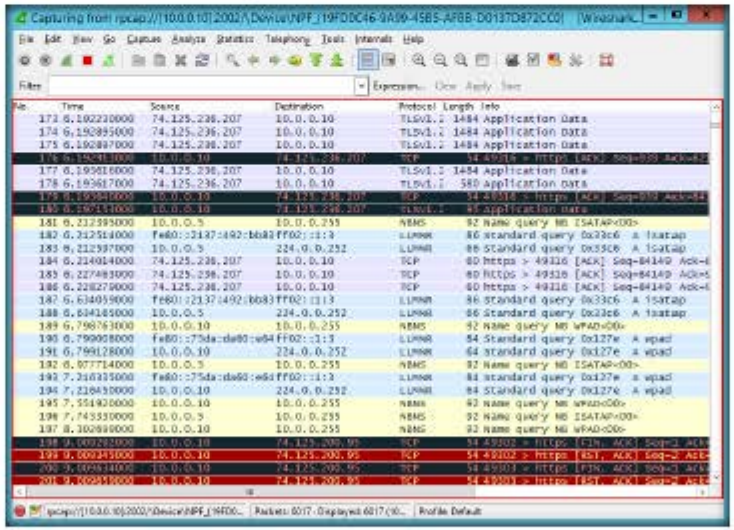


FIGURE 1.38: Wireshark Window with Packets Captured

63. Stop the running live capture after a while by clicking the stop button in the menu bar.

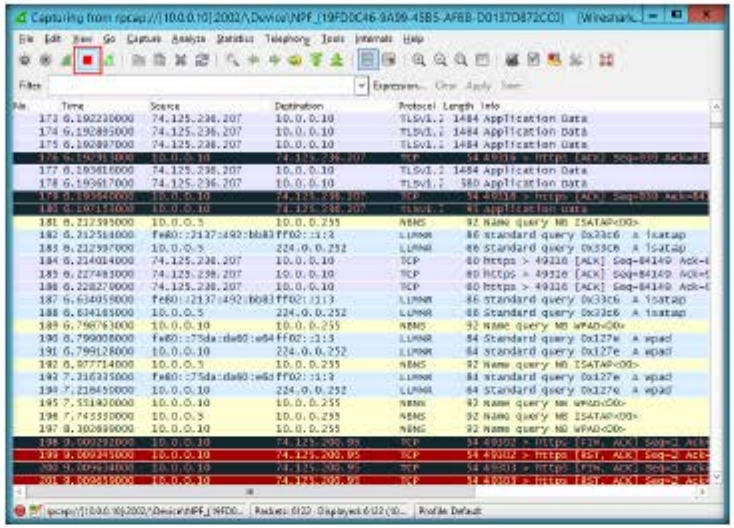


FIGURE 1.39: Stopping the running live capture

64. In this way, you can capture traffic on a remote interface using Wireshark.
65. In real time, when attackers gain the credentials of a victim machine, they attempt to capture its remote interface and monitor the traffic its user browses, to reveal confidential user information.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and "exposure" through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Analyzing a Network Using Capsa Network Analyzer

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information. Network administrators can use Capsa's comprehensive high-level window view for monitoring entire network, quick insight to network administrators or network engineers that allows rapidly pinpointing and resolving application problems.

Lab Objectives

The objective of this lab is to obtain information regarding the target organization that includes, but is not limited to:

- Network traffic analysis, communication monitoring
- Network communication monitoring
- Network problem diagnosis
- Network security analysis
- Network performance detecting
- Network protocol analysis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

ColasoftCapsa Network Analyzer runs on Server 2003 /Server 2008/7 with 64-bit Edition.

Lab Environment

To complete this lab, you will need:

- ColasoftCapsa Network Analyzer located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Capsa Network Analyzer**
- You can also download the latest version of ColasoftCapsa Network Analyzer from the link http://www.colasoft.com
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Administrative privileges to run tools
- A web browser with an Internet connection

Note: This lab requires active internet connection for license-key registration

Lab Duration

Time: 5 Minutes

Overview of Sniffing

Sniffing is performed to collect basic information of the target and its network. It helps to find vulnerabilities and select exploits for attack. It determines network information, system information, password information, and organizational information.

Sniffing can be Active or Passive.

Lab Tasks

TASK 1

Install Capsa Network Analyzer

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Capsa Network Analyzer** and double-click **capsa_ent_demo_7.7.2.4050.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard-driven installation steps to install Capsa Network Analyzer.

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

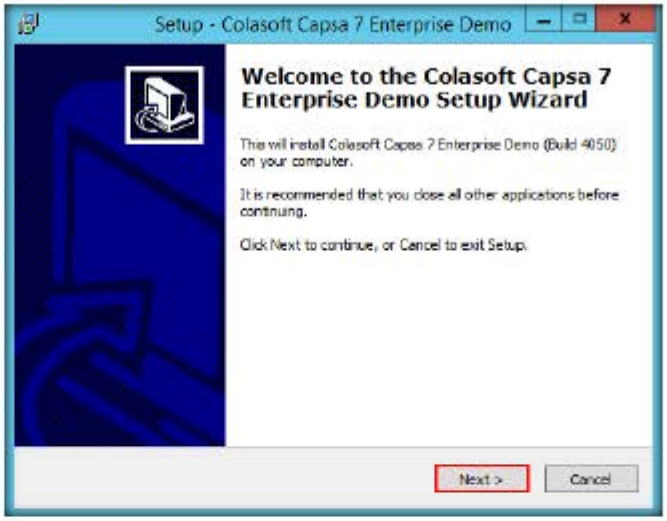


FIGURE 2.1: Colasoft Capsa installation wizard

Note: If a **Windows Security** dialog-box opens during installation, click **Install**.

4. On completing the installation, launch **Colasoft Capsa 7 Enterprise Demo** from the **Apps** screen.

FIGURE 2.2: Launching the application from Apps screen

5. The **Colasoft Capsa 7 Enterprise Demo** dialog-box appears; click **OK**.

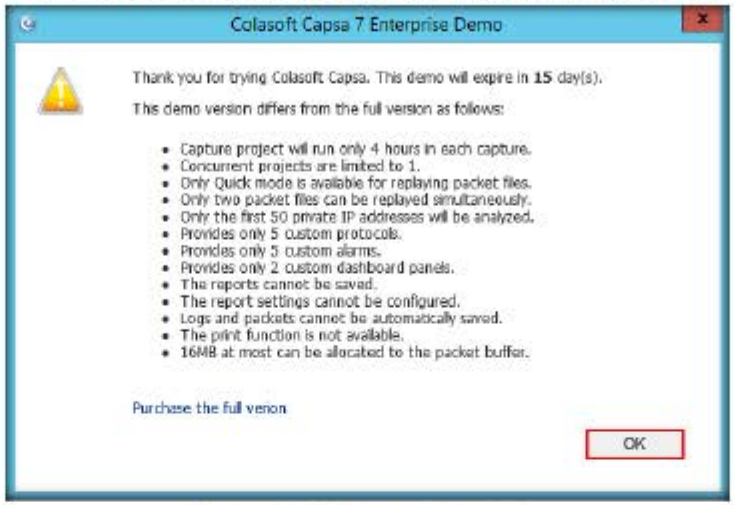


FIGURE 2.3: Colasoft Capsa 7 Enterprise Demo dialog-box

6. The **Colasoft Capsa 7 Enterprise Demo** main window appears, as shown in the following screenshot:

As a network analyzer, Capsa make it easy to monitor and analyze network traffic with its intuitive and information-rich tab views.

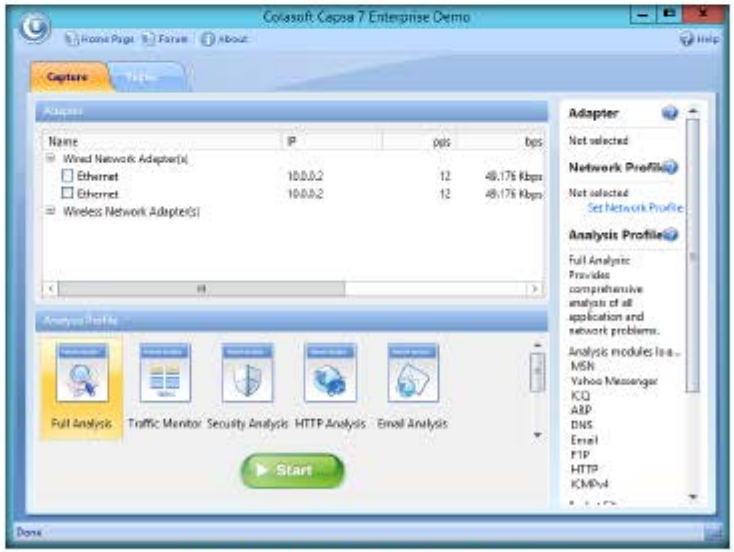


FIGURE 2.4: Colasoft Capsa Network Analyzer main window

TASK 2

Begin Packet Analysis

7. In the **Capture** tab, check **Ethernet** adapter and click **Start** to create a New Project.

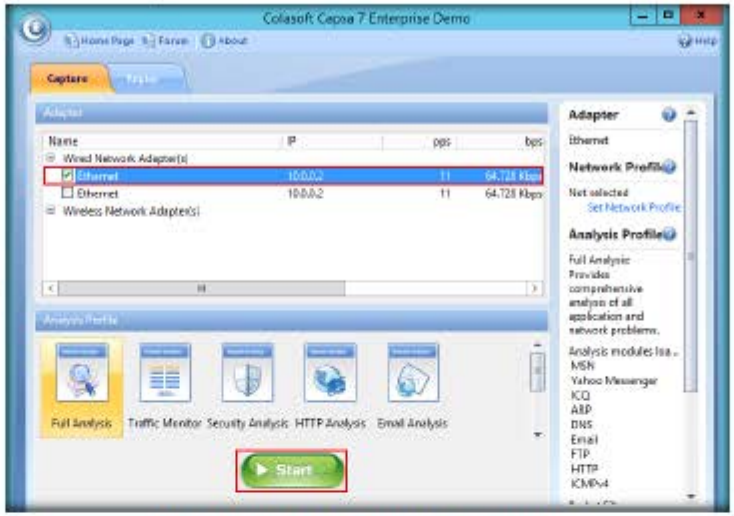


FIGURE 2.5: Colasoft Capsa Network Analyzer creating a New Project

The network utilization rate is the ratio of current network traffic to the maximum traffic that a port can handle. It indicates the bandwidth use in the network.

Note: 10.0.0.2 is the IP address of the host machine, which may differ in your lab environment.

TASK 3

Analyze the Dashboard Information

8. The **Dashboard** provides graphs and charts of the statistics.

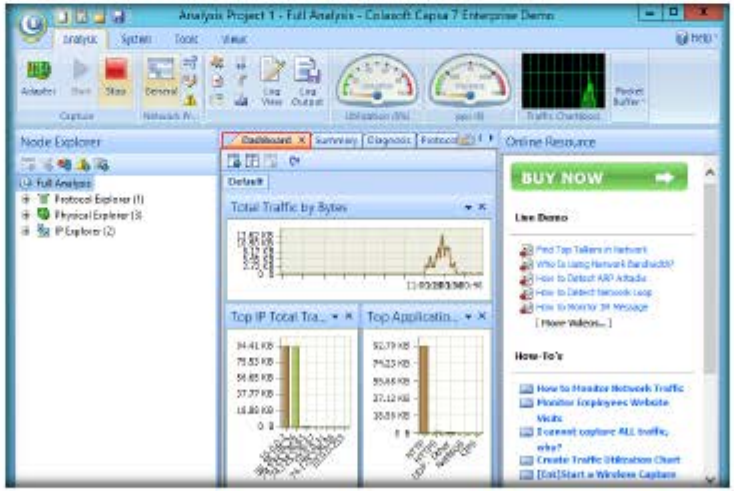


FIGURE 2.6: Colasoft Capsa Network Analyzer Dashboard

TASK 4

Examine the Summary Information

9. The **Summary** tab provides full general analysis and statistical information of the selected node in the Node Explorer window.

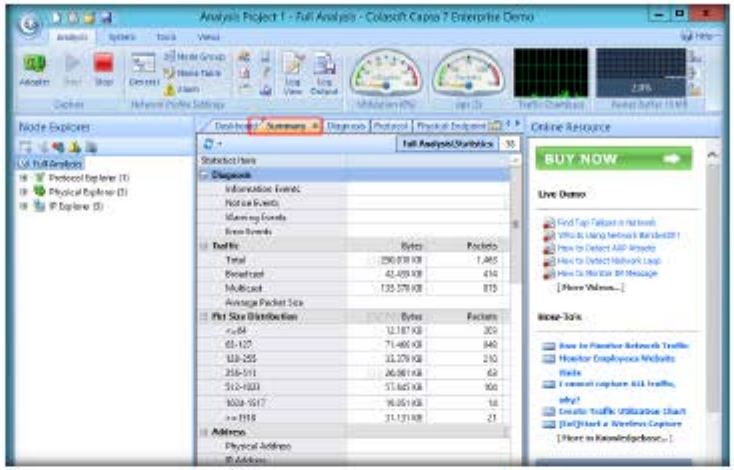


FIGURE 2.7: Colasoft Capsa Network Analyzer Summary

A high network utilization rate indicates the network is busy, whereas a low utilization rate indicates the network is idle.

TASK 5

Analyze the Diagnosis Information

10. The **Diagnosis** tab provides the real-time diagnosis events of global network by groups of protocol layers or security levels. With this tab you can view the performance of the protocols.
11. To view the TCP slow response, click **TCP Slow Response** in the **Transport Layer,** which in turn will highlight the slowest response in **Diagnosis Events**.

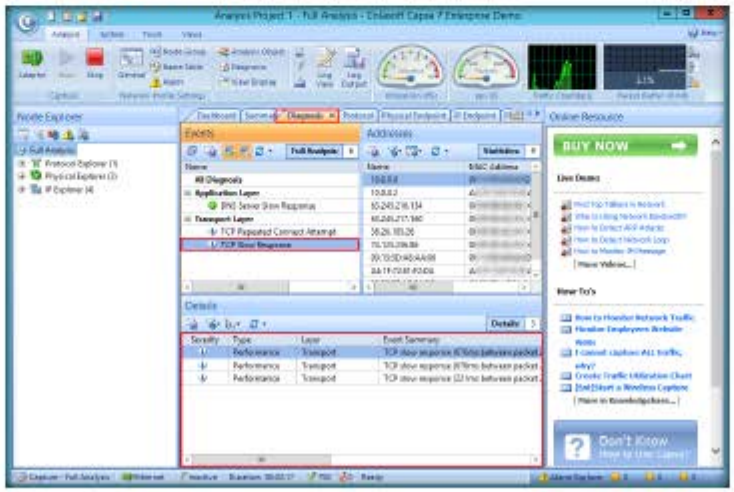


FIGURE 2.8: Colasoft Capsa Network Analyzer Diagnosis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

12. Double-click the highlighted **Diagnosis Event** to view its detailed information.

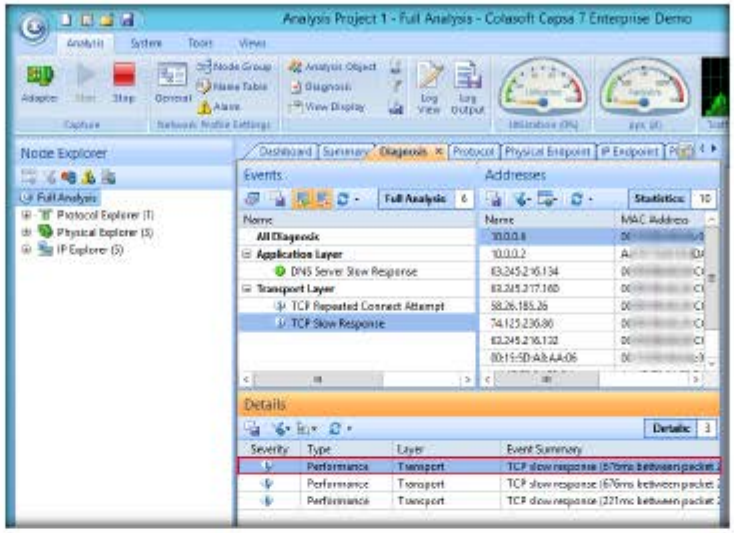


FIGURE 2.9: Analyzing Diagnosis Event

13. The **TCP Slow ACK - Data Stream of Diagnostic Information** window displays Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information related to the event.

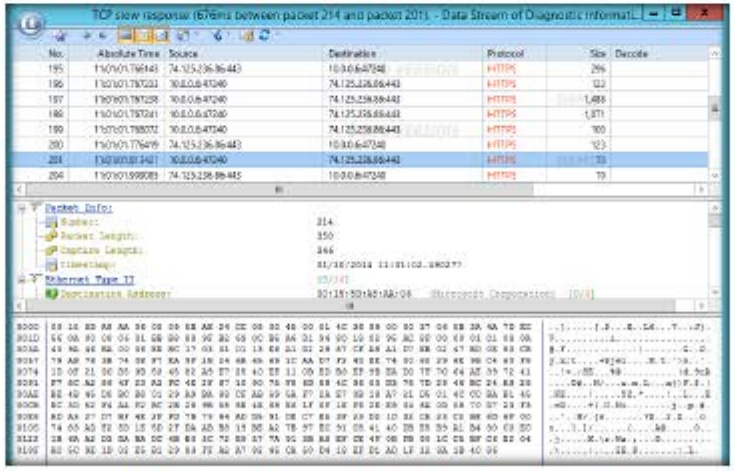


FIGURE 2.10: TCP Slow ACK - Data Stream of Diagnostic Information window

14. Close the **TCP Slow ACK - Data Stream of Diagnostic Information** window after analyzing the results.

TASK 6

Examine the Protocol Information

15. The **Protocol** tab lists statistics of all protocols used in network the transactions hierarchically. **Physical Endpoints** and **IP Endpoints** for the selected ports are displayed as well.

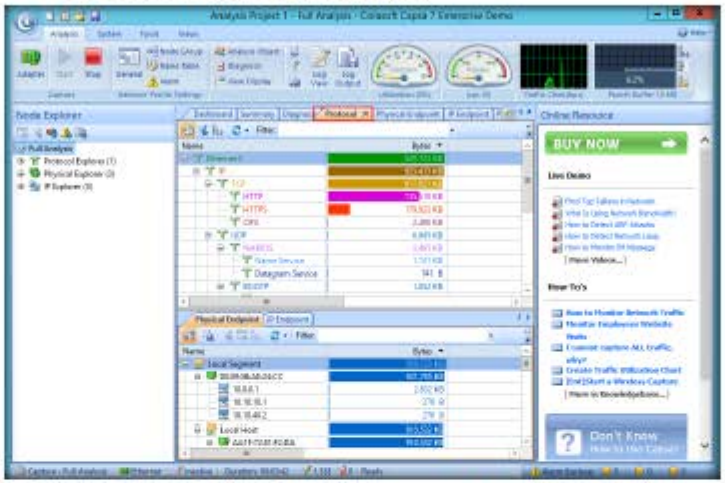


FIGURE 2.11: Colasoft Capsa Network Analyzer Protocol analysis

TASK 7

Examine the Physical Endpoint Information

16. The **Physical Endpoint** tab lists statistics of all MAC addresses that communicate in the network hierarchically.

FIGURE 2.12: Colasoft Capsa Network Analyzer Physical Endpoint analysis

TASK 8

Analyze the IP Endpoint Information

17. The **IP Endpoint** tab displays statistics of all IP addresses communicating in the Network.
18. On the **IP Endpoint** tab, you can easily find the nodes with the highest **traffic volumes**, and check if there is a **multicast storm** or **broadcast storm** in your network.

As a delicate work, network analysis always requires us to view the original packets and analyze them. However, not all the network failures can be found in a very short period. Sometimes network analysis requires a long period of monitoring and must be based on the baseline of the normal network.

FIGURE 2.13: Colasoft Capsa Network Analyzer IP Endpoint view

TASK 9

Examine the Physical Conversations

19. The **Physical Conversation** tab presents the conversations between two MAC addresses.

TTL tells the router whether the packet should be dropped if it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet is dropped. As TTL value is deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of the routers which the packet passed through before it was dropped.

FIGURE 2.14: Colasoft Capsa Network Analyzer Physical Conversations

TASK 10

Examine the IP Conversations

20. The **IP Conversation** tab presents IP conversations between pairs of nodes.
21. The lower pane of the IP Conversation section offers **UDP** and **TCP** conversation, which you can drill down to analyze.

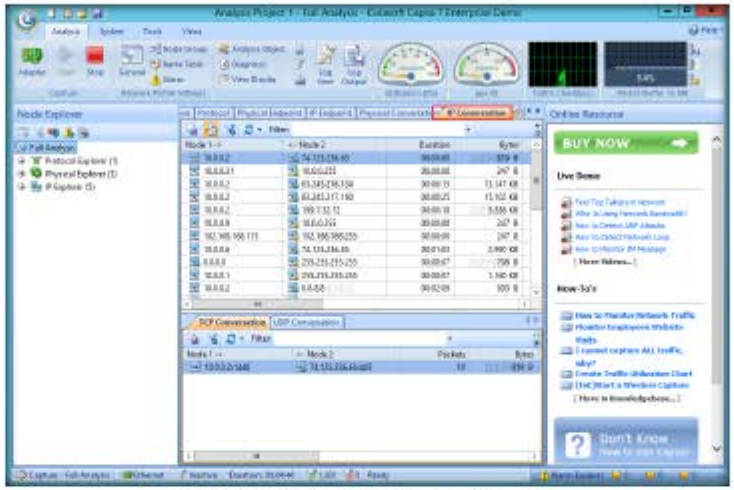


FIGURE 2.15: Colasoft Capsa Network Analyzer IP Conversations

22. Double-click a conversation in the **IP Conversation** list to view the full analysis of packets between two IPs. Here, we are checking the conversation between **10.0.0.9** and **10.0.0.255**.

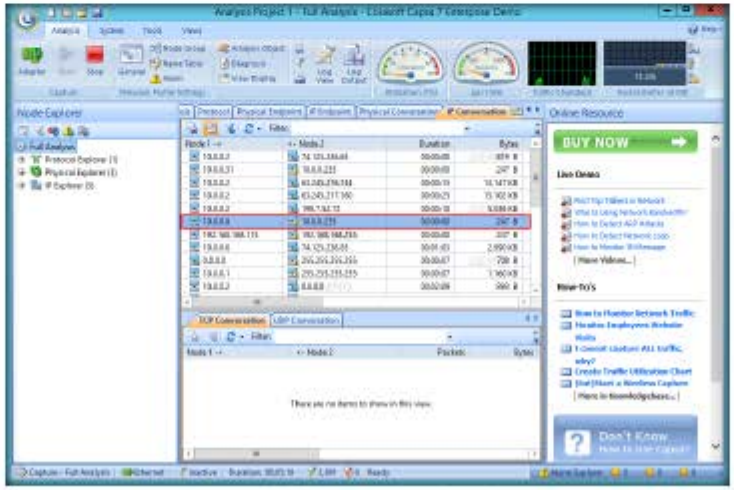
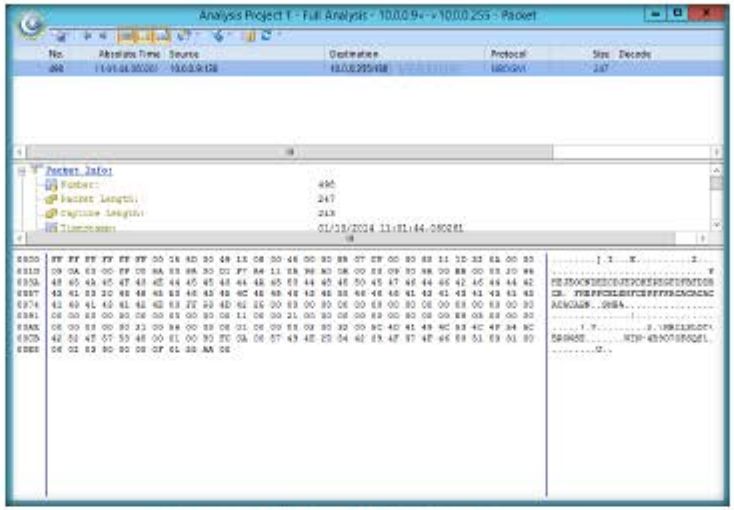


FIGURE 2.16: Colasoft Capsa Network Analyzer IP Conversations

23. A window displays full packet analysis between **10.0.0.9** and **10.0.0.255**.



A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on. While attempting to remain undetected, the backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

FIGURE 2.17: Full Packet Analysis of Nodes in IP Conversations

TASK 11

Examine the TCP Conversations

24. The **TCP Conversation** tab dynamically presents the real-time status of TCP conversations between pairs of nodes.
25. Double-click a node to display the full analysis of packets.

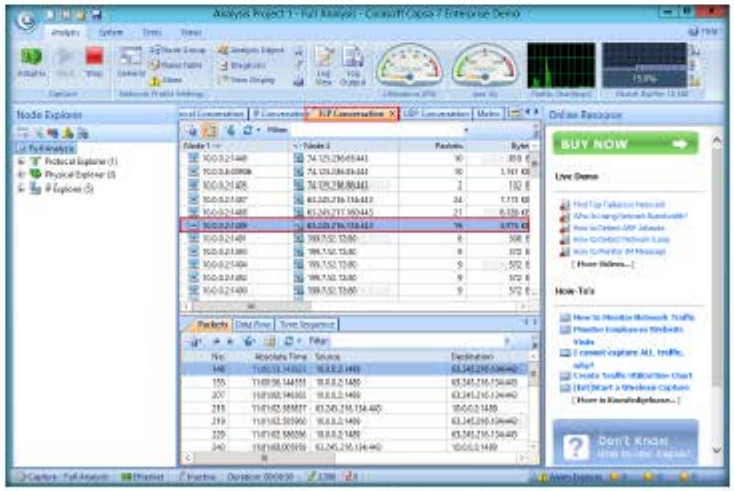


FIGURE 2.18: Colasoft Capsa Network Analyzer TCP Conversations

TASK 12

Examine the Transaction List

26. **Transaction List** displays the TCP transactions between the selected pair of nodes.

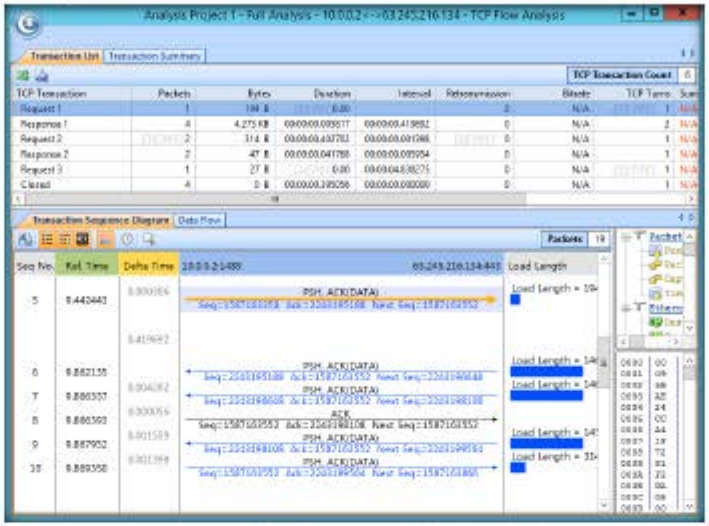


FIGURE 2.19: Colasoft Capsa Network Analyzer Transaction List

TASK 13

Analyze the Transaction Summary

27. The **Transaction Summary** tab displays the summary of the transactions.

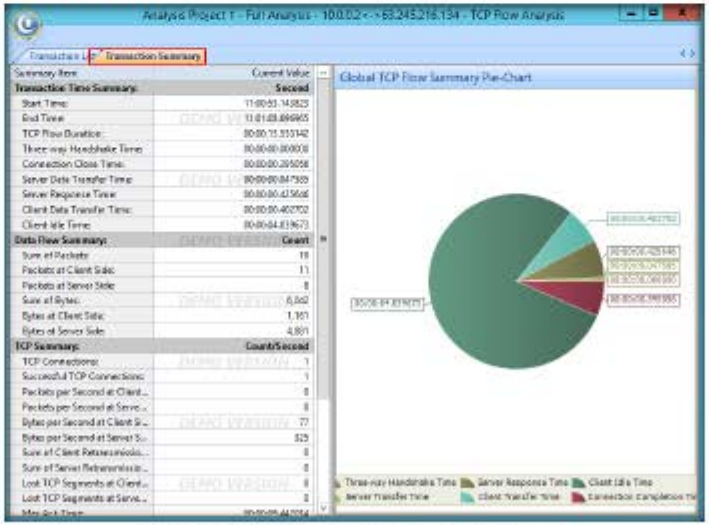


FIGURE 2.20: Colasoft Capsa Network Analyzer Transaction Summary

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 14

Examine the UDP Conversation

28. The **UDP Conversation** tab dynamically presents the real-time status of UDP conversations between two nodes.
29. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to **analyze the conversations**.

FIGURE 2.21: Colasoft Capsa Network Analyzer UDP Conversations

In networking, an email worm is a computer worm that can copy itself to the shared folder in a system and keeps sending infected emails to stochastic email addresses. In this way, it spreads fast via SMTP mail servers.

TASK 15

Examine the Matrix View

30. In the **Matrix** tab, you can view the nodes communicating in the network by graphically connecting them with lines.
31. The weight of each line indicates the volume of traffic between **nodes** arranged in an extensive **ellipse**.
32. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the **Node Explorer** window.

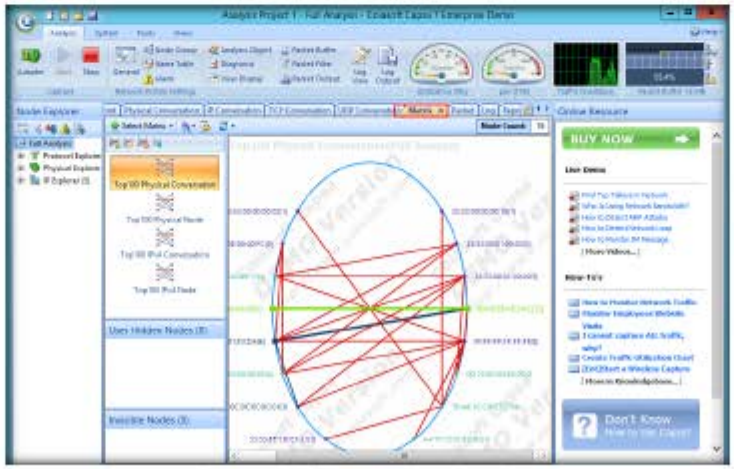


FIGURE 2.22: Colasoft Capsa Network Analyzer Matrix view

Once we encounter the network malfunction or attack, the most important thing we should pay attention to is the current total network traffic, sent/received traffic, network connection, etc., to get a clear direction to find the problem. All of these statistics are included in the endpoint tabs in ColasoftCapsa.

TASK 16

Analyze the Packet Details

33. The **Packet** tab provides original information for any packet. Double-click a packet to view its full analysis information of packet decode.

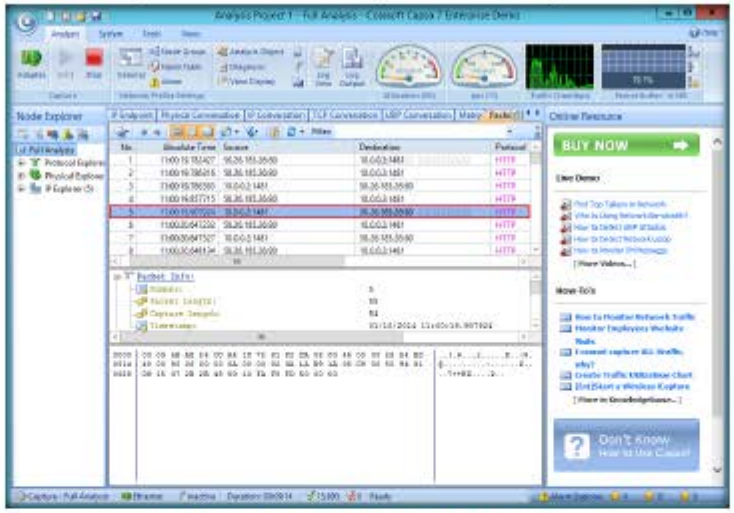


FIGURE 2.23: Colasoft Capsa Network Analyzer Packet information

Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.

34. The packet decode consists of two major views: **Hex View** and **Decode View**.

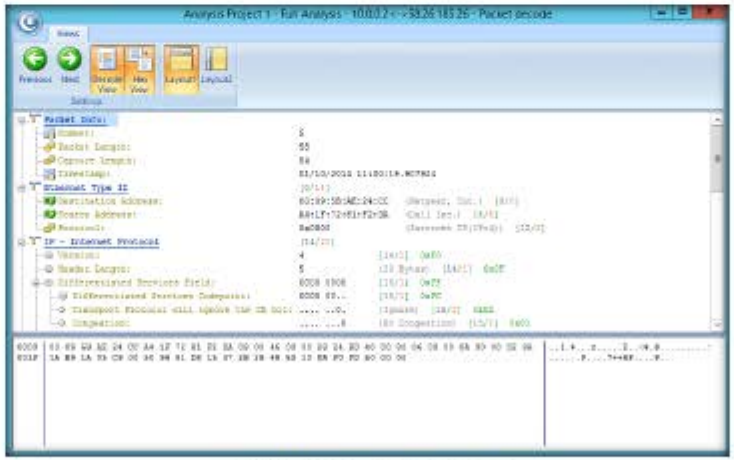


FIGURE 2.24: Full Analysis of Packet Decode

Protocol decoding is the basic functionality as well. There is a Packet tab, which collect all captured packets or traffic. Select a packet and we can see its hex digits as well as the meaning of each field. The figure below shows the structure of an ARP packet. This makes it easy to understand how the packet is encapsulated according to its protocol rule.

TASK 17

Analyze all the Logs

35. The **Log** tab provides a **Global Log**, **DNS Log**, **Email Log**, **FTP Log**, **HTTP Log**, **ICQ Log**, **MSN Log**, and **Yahoo Log.**
36. So, you can view the logs of **TCP conversations**, **Web access**, **DNS transactions**, **Email communications**, and others.

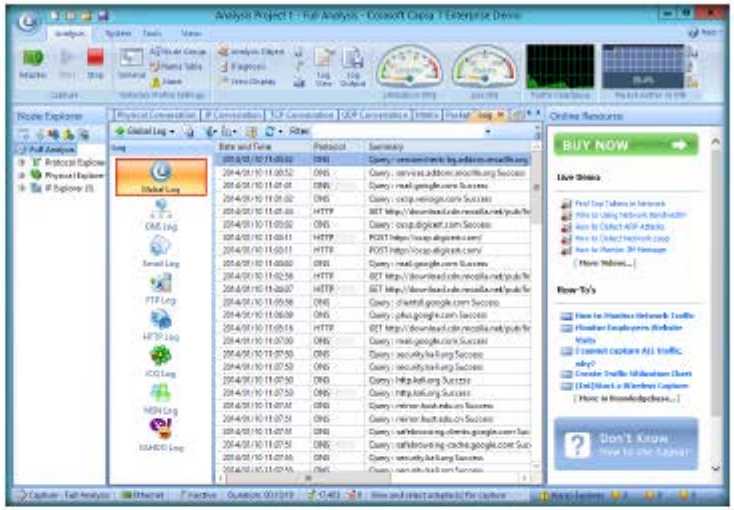


FIGURE 2.25: Colasoft Capsa Network Analyzer Global Log view

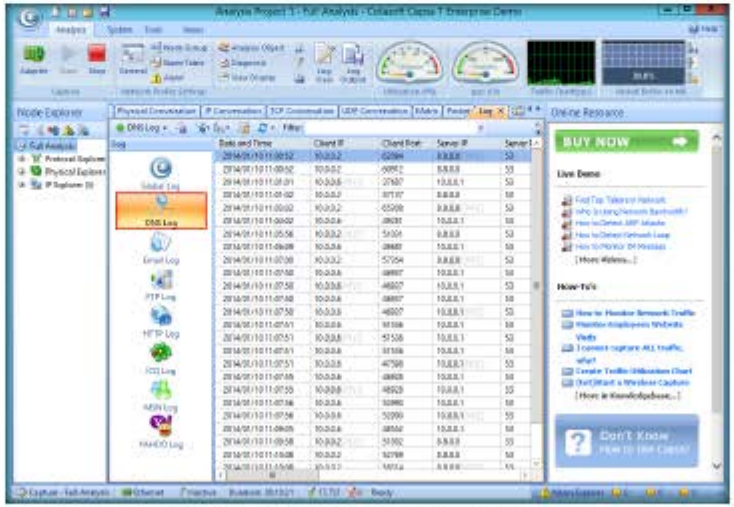


FIGURE 2.26: Colasoft Capsa Network Analyzer DNS Log view

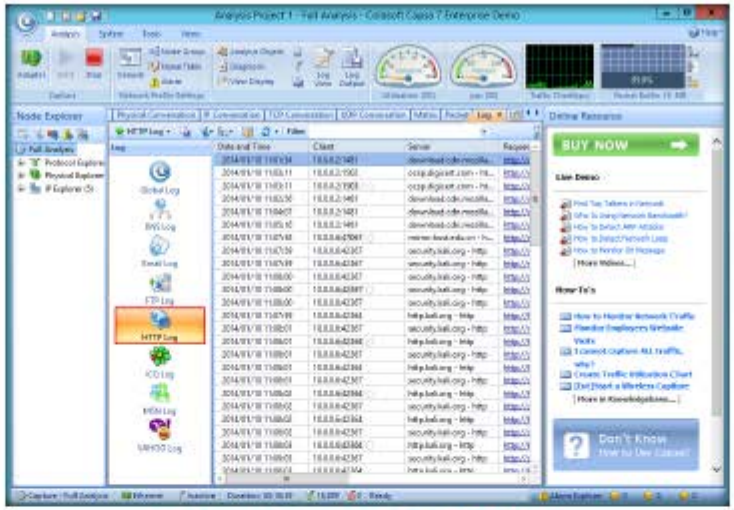


FIGURE 2.27: Colasoft Capsa Network Analyzer HTTP Log view

37. If you have MSN or Yahoo messenger running on your system, you can view the MSN and Yahoo logs.

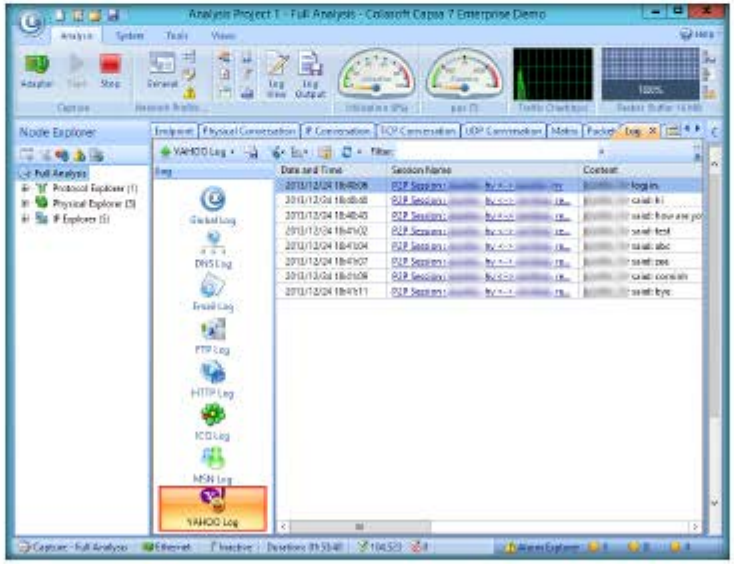


FIGURE 2.28: Colasoft Capsa Network Analyzer MSN Log view

TASK 18

Examine the Report

38. The **Report** tab provides **28** statistics reports from the global network to a specific network node.
39. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.

Almost all Trojans and worms need an access to the network, because they have to return data to the hacker. Only the useful data are sent for the Trojan to accomplish its mission. So it is a good solution to start from the aspect of traffic analysis and protocol analysis technology.

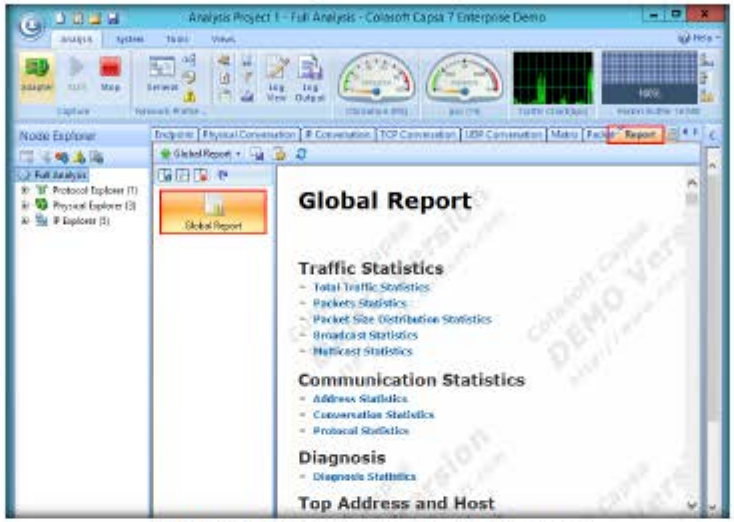


FIGURE 2.29: Colasoft Capsa Network Analyzer Full Analysis's Report

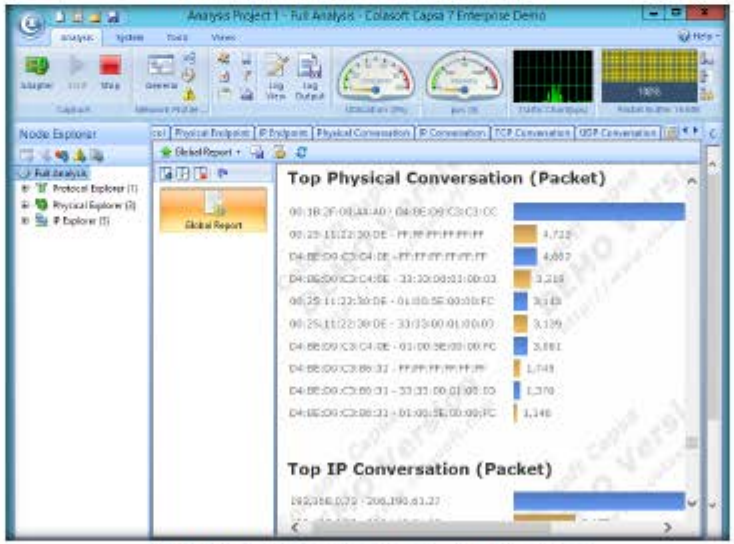


FIGURE 2.30: Colasoft Capsa Network Analyzer Full Analysis's Report

40. Click **Stop** after completing your task.

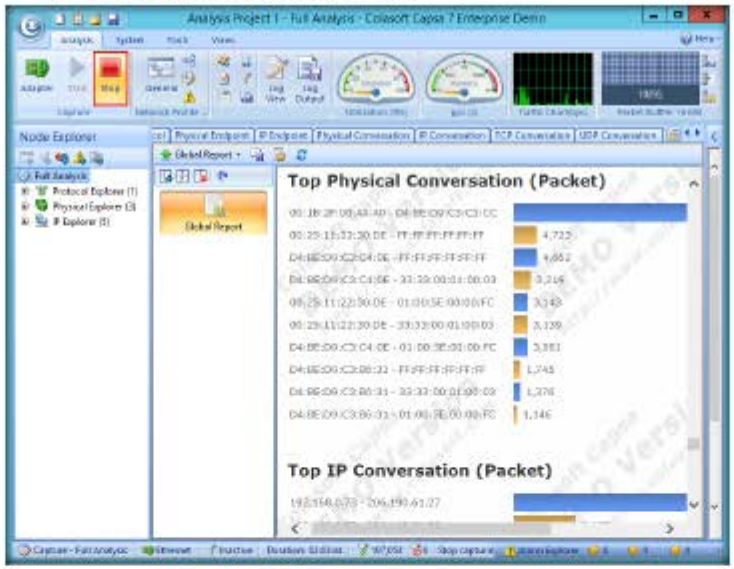


FIGURE 2.31: Colasoft Capsa Network Analyzer Stopping process

41. In real time, an attacker may perform this analysis in an attempt to obtain sensitive information, as well as to find any network loopholes.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

From the previous scenario, now you are aware of the importance of network sniffing. As an expert Ethical Hacker and Penetration Tester, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

In this lab, you will need:

- A web browser with internet access
- A business Email ID to download the tool
- A computer running Windows Server 2012 as host machine
- Windows 8.1 running on virtual machine as target machine
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of OmniPeek Network Analyzer

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, including

Ethernet, Gigabit, 10 Gigabit, VoIP, and Video to remote offices, and 802.11 a/b/g/n.

Lab Tasks

TASK 1

Download and Install OmniPeek Network Analyzer

1. Launch a web browser, type http://www.wildpackets.com/product_trials in the address box, and press **Enter**.
2. OmniPeek products window appears; click the **download button** for **OmniPeek Professional.**

FIGURE 3.1: OmniPeek products window

3. Fill in the details in all the required fields, type the captcha in the field provided, and click **Start Your Trial**.

Note: You need to specify a non-personal business email ID.

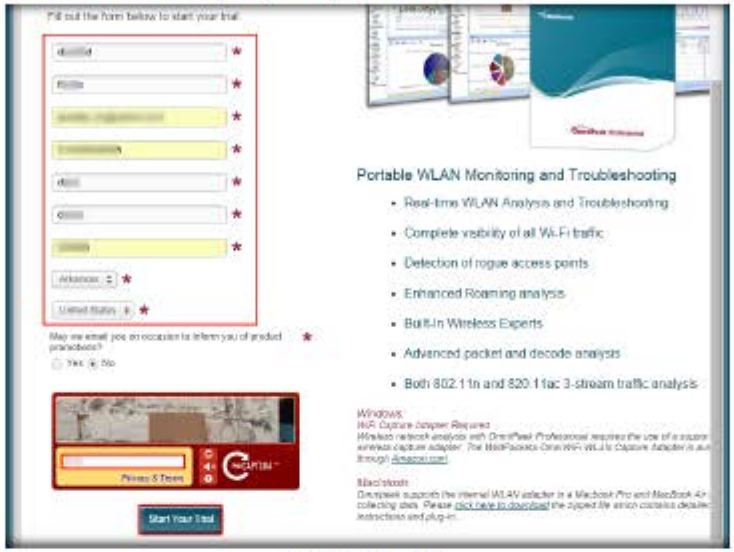


FIGURE 3.2: Filling the details

4. Now, log into the account related to the email ID specified in the registration page, and copy the download link.

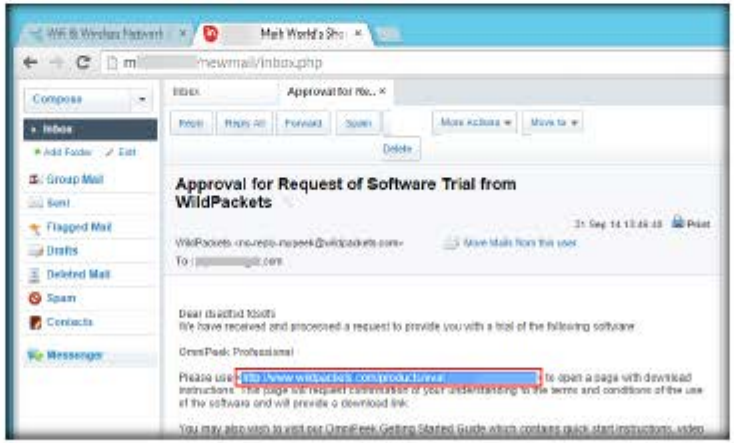


FIGURE 3.3: Email account containing the download link

5. Open a new tab, paste the download link that you copied in the previous step, and press **Enter**.
6. A webpage appears, displaying the terms and conditions. Scroll down and click **I accept**.

FIGURE 3.4: Accepting the License Agreement information

7. The OmniPeek download page appears, containing the Serial number and download link. Copy the serial number, and click **Download the Trial**.

FIGURE 3.5: Downloading Omnipeek

8. On completion of download, navigate to the downloaded tool, and double-click it.
9. If the **Open File - Security Warning** pop-up appears, click **Run**.
10. The **OmniPeek Install Wizard** appears; click **Next**.

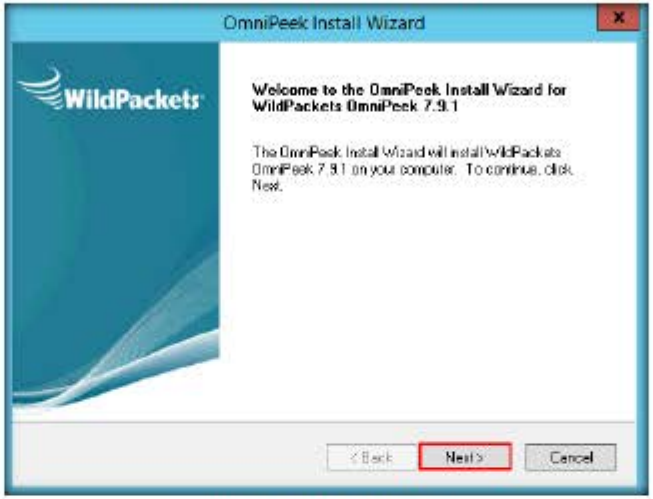


FIGURE 3.6: OmniPeek Installation Wizard

11. The **Product Activation** step appears; select **Automatic: via a secure Internet connection,** and click **Next**.

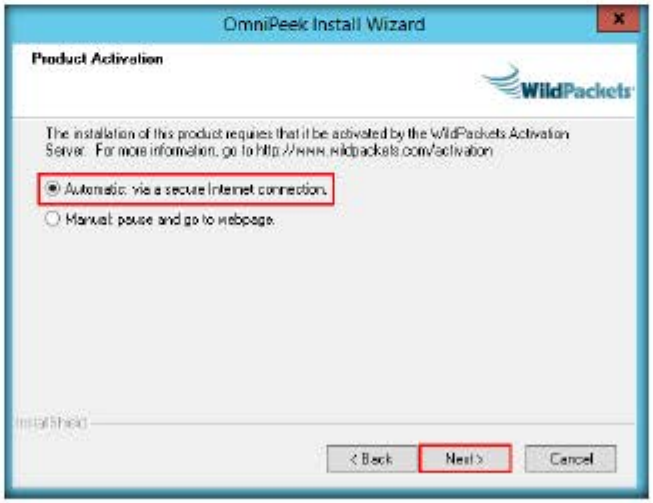


FIGURE 3.7: OmniPeek Product Activation section

12. The **Customer Information** step appears; type a **User name**, **Company name,** and enter the **Serial Number** you noted in **step 7**.
13. Click **Next**.

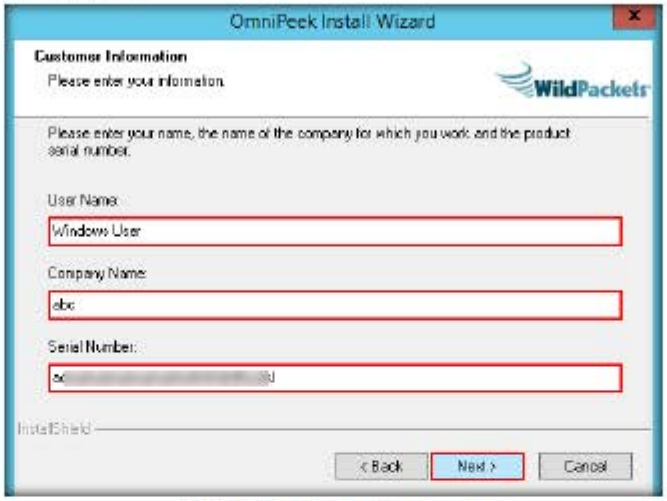


FIGURE 3.8: OmniPeek Customer Information section

Note: Specify the serial key that you obtained during registration.

14. The **Automatic Activation** section appears; enter your email ID and click **Next**.

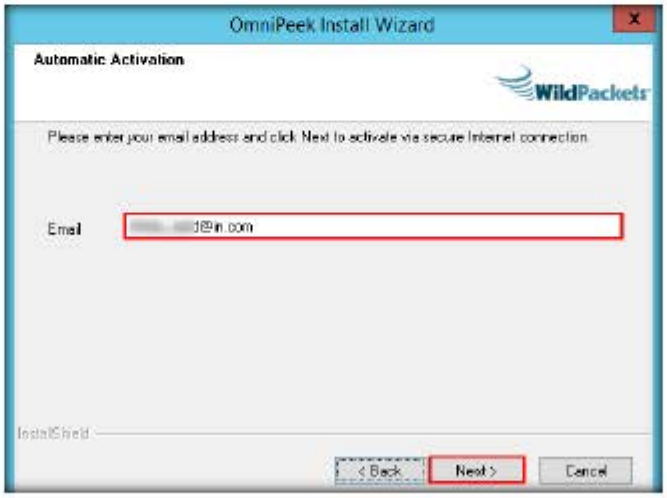


FIGURE 3.9: OmniPeek Automatic Activation section

15. The **System Information** section appears; check **Share my System Information,** and click **Next**.

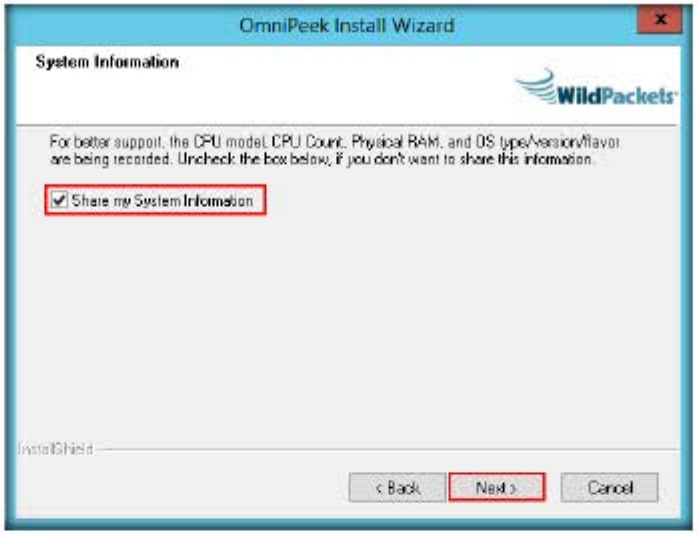


FIGURE 3.10: OmniPeek System Information section

16. The **License Agreement** step appears; accept the terms of license agreement, and click **Next**.

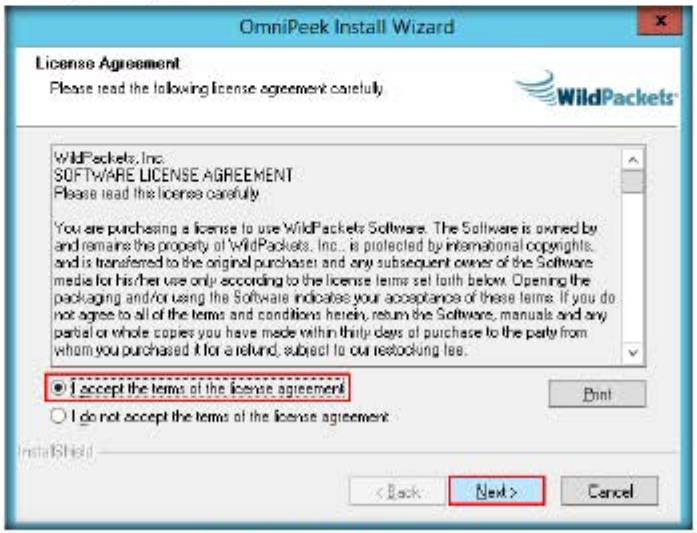


FIGURE 3.11: OmniPeek License Agreement section

17. The **Installation Notes** step appears; click **Next**.

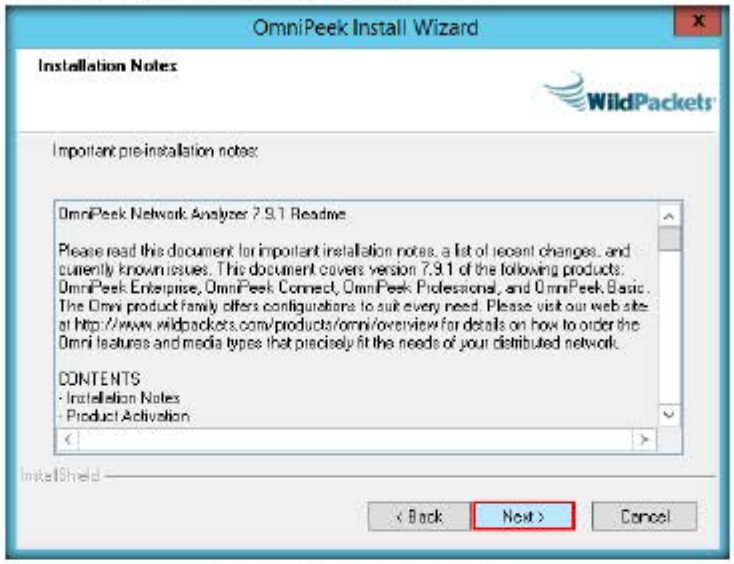


FIGURE 3.12: OmniPeek Installation Notes section

18. The **Setup Type** section appears; select **Complete,** and click **Next**.

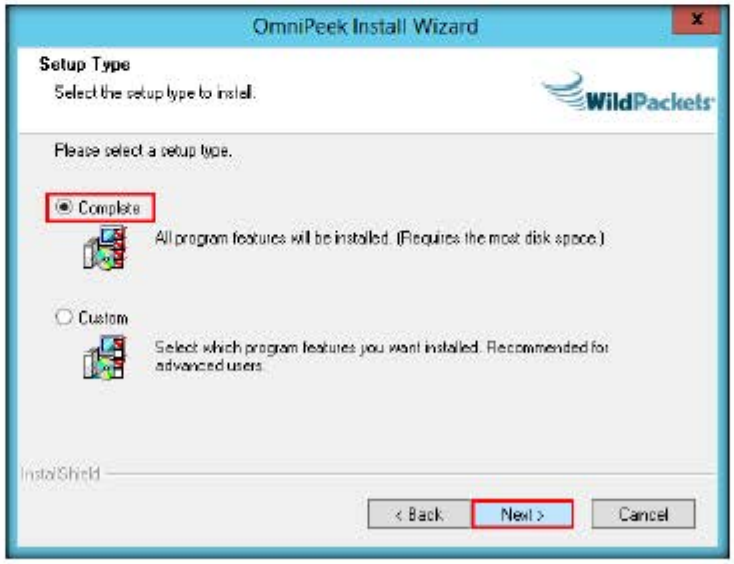


FIGURE 3.13: OmniPeek Setup Type section

19. The **Select Language Support** step appears; select a language, and click **Next**.

OmniPeek Enterprise provides users with the visibility and analysis they need to keep Voice and Video applications and non-media applications running optimally on the network

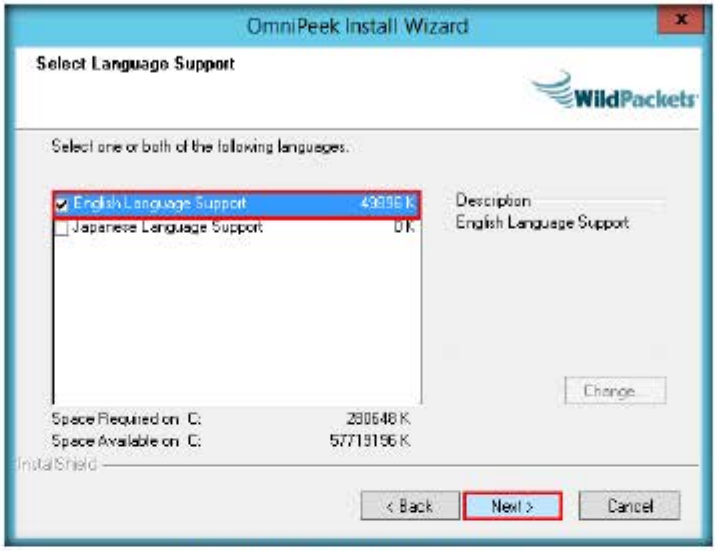


FIGURE 3.14: OmniPeek Select Language Support section

20. The **Start Copying Files** step appears; click **Next**.

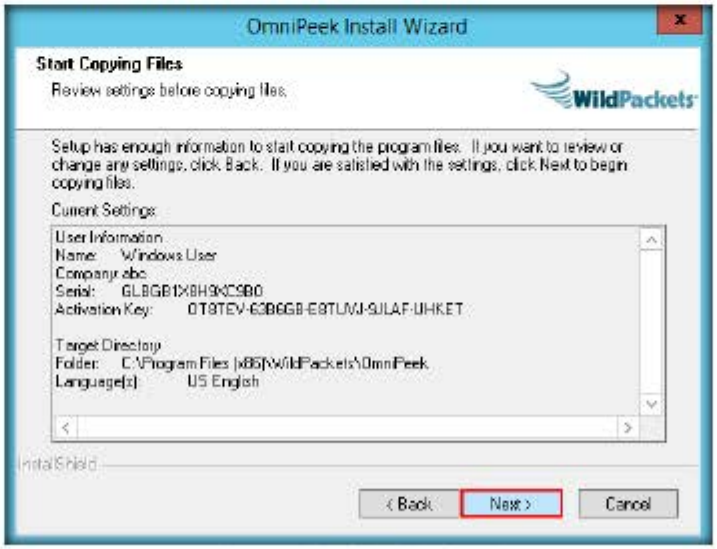


FIGURE 3.15: OmniPeek Start Copying Files section

21. On the completion of installation, the **OmniPeek Install Wizard Complete** step appears; uncheck **Yes, I would like to view the Readme,** and click **Finish**.

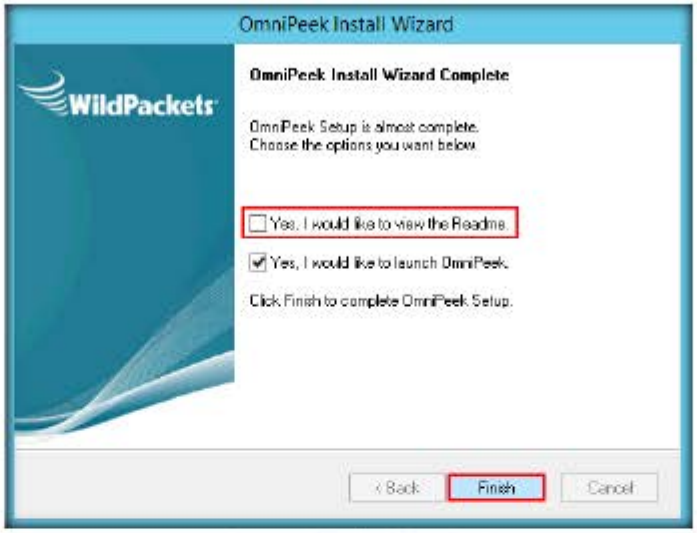


FIGURE 3.16: OmniPeek installation completed

To deploy and maintain Voice and Video over IP successfully, you need to be able to analyze and troubleshoot media traffic simultaneously with the network the media traffic is running on.

22. If the **OmniPeek** evaluation dialog box appears, click **OK**.
23. The main window of **WildPackets OmniPeek Demo** opens, as shown in the screenshot.

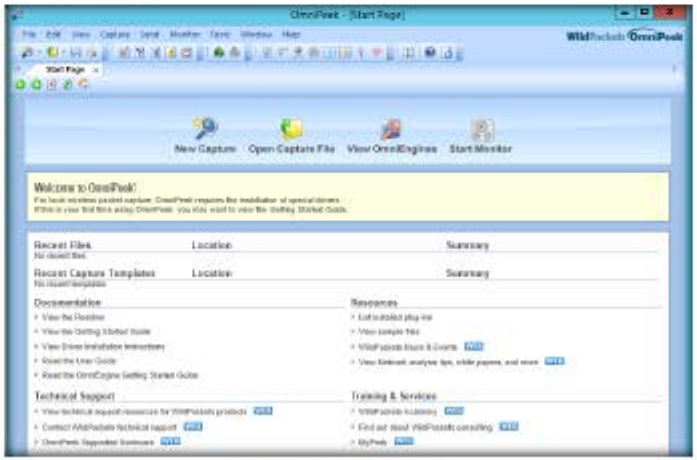


FIGURE 3.17: OmniPeek main window

TASK 2

Start a New Capture

24. Now, launch the **Windows 8.1** virtual machine.
25. Switch back to **Windows Server 2012,** and create an OmniPeek capture window, as follows:
    a. Click **New Capture,** on the main screen of OmniPeek.

OmniPeek Network Analyzer offers real-time high-level view of the entire network, expert analysis, and drill-down to packets, during capture.

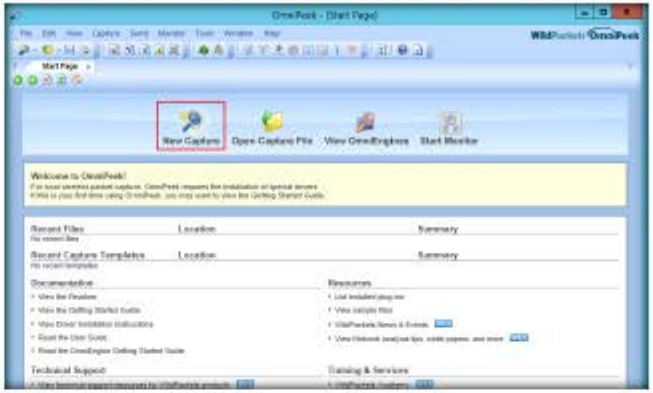


FIGURE 3.18: Starting a new capture

    b. View the **General** options in the **Capture Options** window.
    c. Leave the default general settings.

Network Coverage: With the Ethernet, Gigabit, 10G, and wireless capabilities, you can now effectively monitor and troubleshoot services running on your entire network. Using the same solution for troubleshooting wired and wireless networks reduces the total cost of ownership and illuminates network problems that would otherwise be difficult to detect.

FIGURE 3.19: OmniPeek capture options - General

d. Click **Adapter,** and select the adapter of the **host machine**, here **Ethernet 8**, and click **OK**.

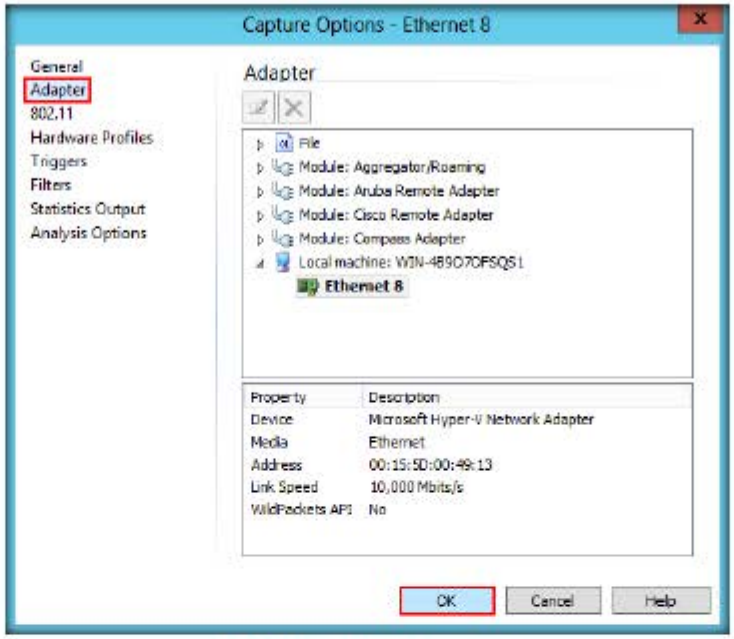
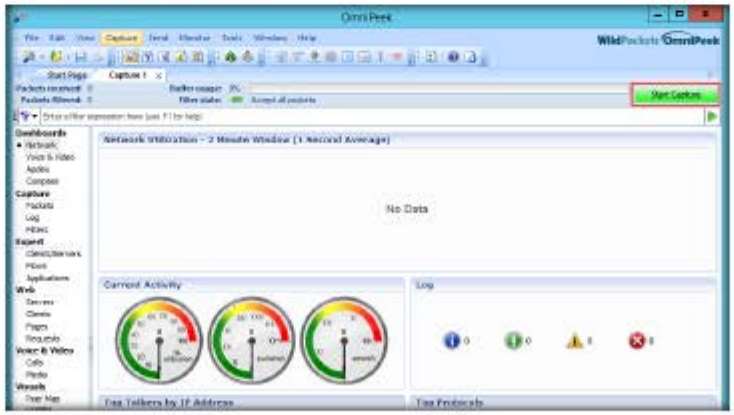


FIGURE 3.20: OmniPeek capture options - Adapter

26. Now, click **Start Capture** to begin capturing packets. The **Start Capture** tab changes to **Stop Capture,** and traffic statistics begin to populate the **Network Dashboard**.



Dashboards display important data that every network engineer needs to know regarding the network without spending lots of time analyzing the captured data.

FIGURE 3.21: Starting packet capture

FIGURE 3.22: Start Capture tab changes to Stop Capture

27. Switch to the **Windows 8.1** machine, browse the Internet, and then switch back to the host machine (**Windows Server 2012**).

TASK 3

Analyze the Capture Results

28. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

OmniPeek Professional expands the capabilities of OmniPeek Basic, extending its reach to all small businesses and corporate workgroups, regardless of the size of the network or the number of employees. OmniPeek Professional provides support for multiple network interfaces while still supporting up to 2 Omni Engines acting as both a full-featured network analyzer and console for remote network analysis.

FIGURE 3.23: OmniPeek statistical analysis of the data

29. To view the captured packets, select **Packets** (under **Capture**), in the left pane.

The OmniPeek Peer Map shows all communicating nodes within your network and is drawn as a vertically-oriented ellipse, able to grow to the size necessary. It is easy to read the maps, the thicker the line between nodes, the greater the traffic, the bigger the dot, the more traffic through that node. The number of nodes displayed can also be limited to the busiest and/or active nodes, or to any OmniPeek filters that may be in use.

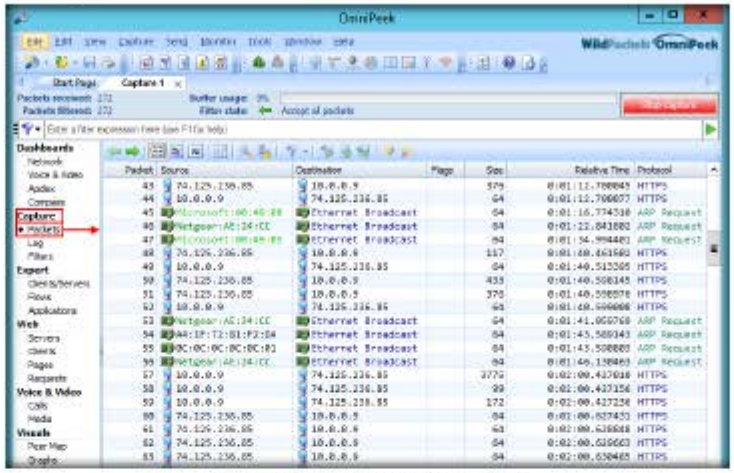


FIGURE 3.24: OmniPeek displaying Packets captured

30. Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard.**

31. You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

On-the-Fly Filters: You shouldn't have to stop your analysis to change what you're looking at. OmniPeek enables you to create filters and apply them immediately. The WildPackets "select related" feature selects the packets relevant to a particular node, protocol, conversation, or expert diagnosis, with a simple right click of the mouse.

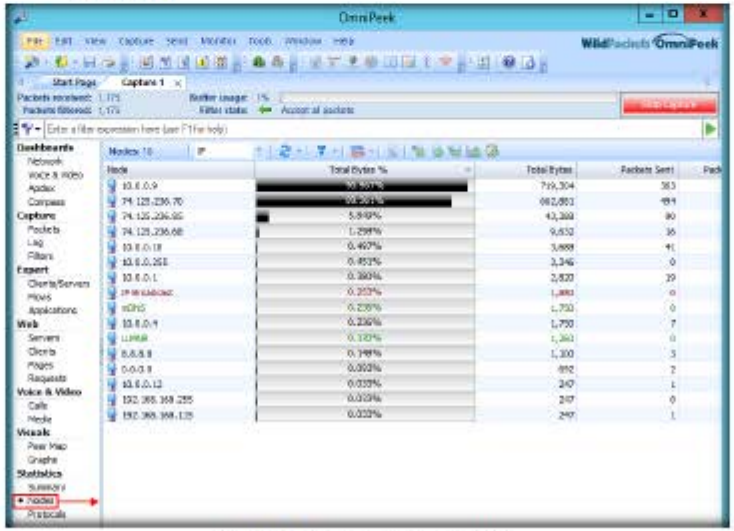


FIGURE 3.25: OmniPeek statistical reports of Nodes

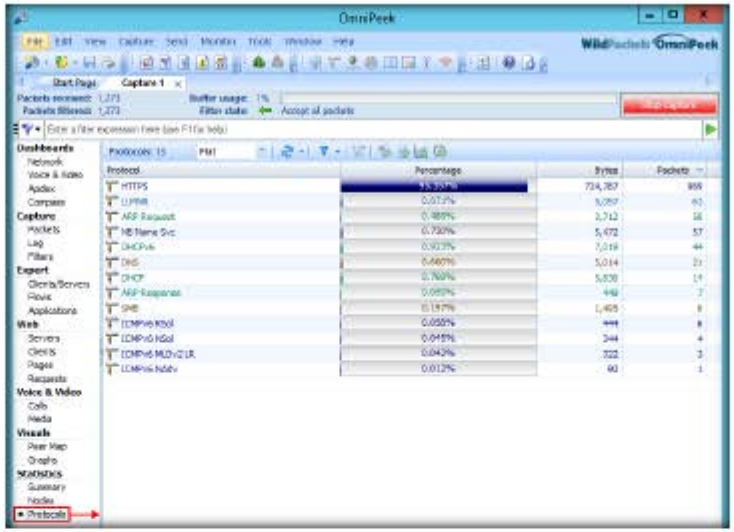
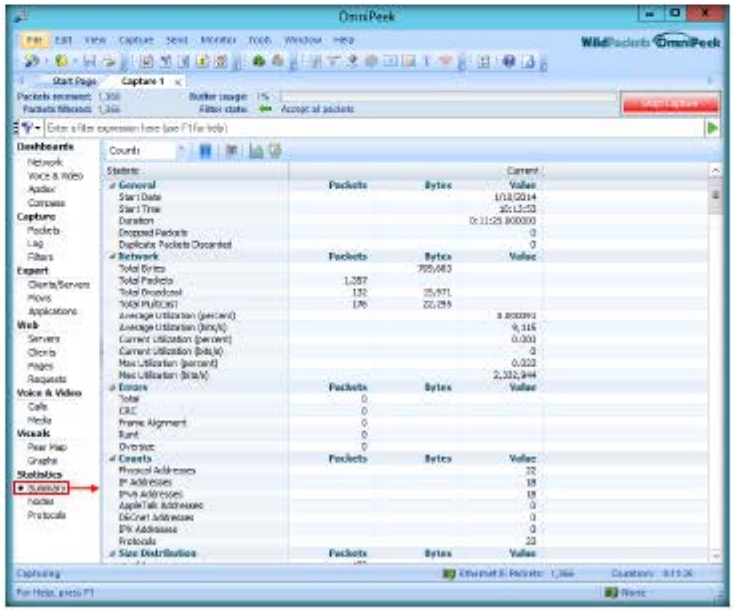


FIGURE 3.26: OmniPeek statistical reports of Protocols

32. You can view a complete **Summary** of your network from the **Statistics** section of the **Dashboard**.



Alarms and Notifications: Using its advanced alarms and notifications, OmniPeek uncovers hard-to-diagnose network problems and notifies the occurrence of issues immediately. OmniPeek alarms query a specified monitor statistics function once per second, testing for user-specified problem and resolution conditions.

FIGURE 3.27: OmniPeek Summary details

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 4

Save the Capture Results

33. To save the result, go to **File → Save Report**

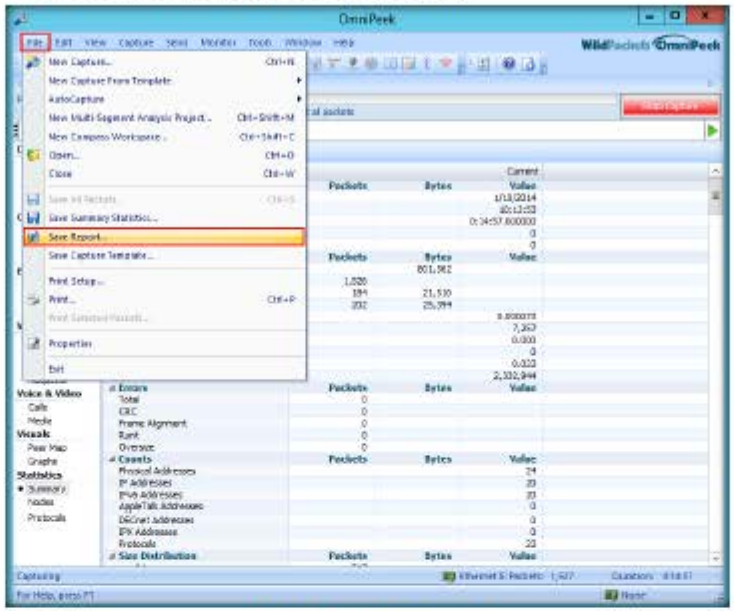


FIGURE 3.28: OmniPeek saving the results

Using OmniPeek's local capture capabilities, centralized console distributes OmniEngine intelligent software probes, Omnepliance®, TimeLine™ network recorders, and Expert Analysis.

34. Choose the format of the **Report type** and the destination **Report folder** from the **Save Report** window, and click **Save**.

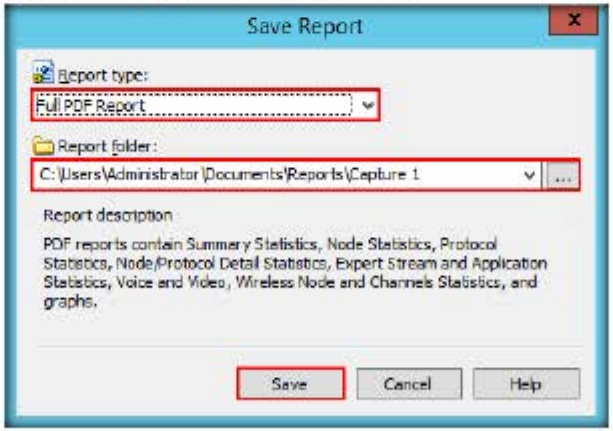


FIGURE 3.29: OmniPeek Selecting the Report format

Engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

35. The saved report can be viewed as in the screenshot below:

Compass Interactive Dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the Compass dashboard, multiple files can be aggregated and analyzed simultaneously.

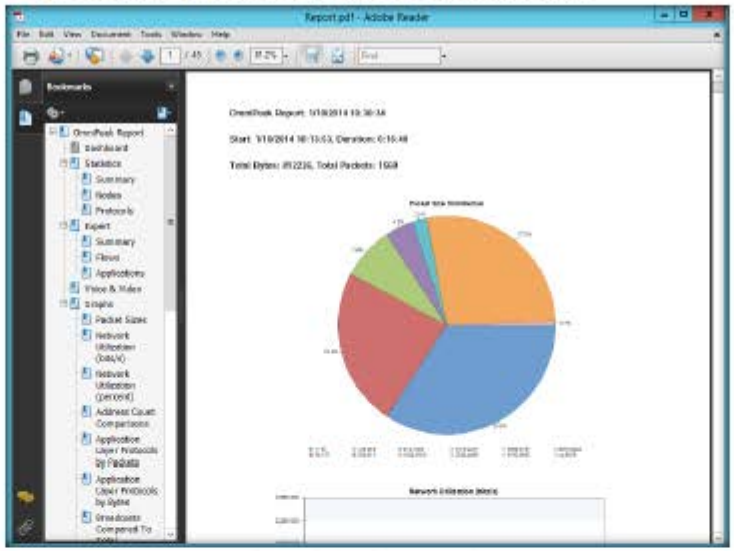


FIGURE 3.30: OmniPeek Report in PDF format

36. Scroll down the pdf to view the complete report.

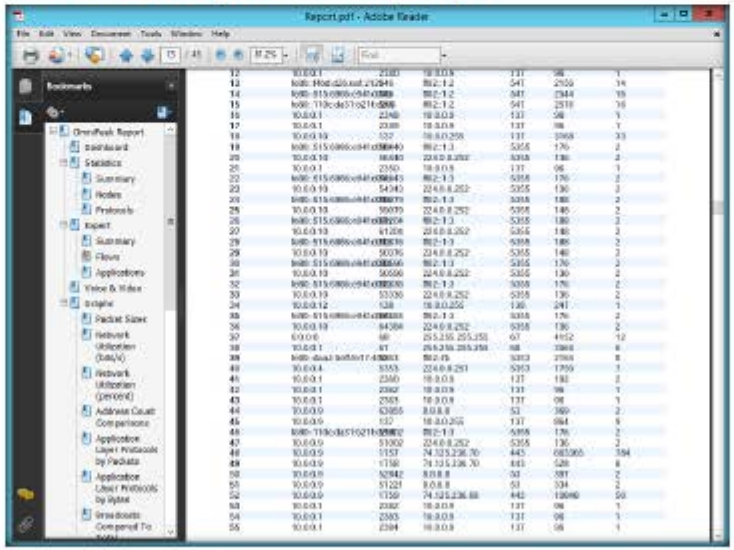


FIGURE 3.31: OmniPeek Report in PDF format

37. In real time, an attacker may perform this analysis in an attempt to obtain sensitive information, as well as find any network loopholes.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 4

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool for MAC address changer (spoofer). The tool can activate a new MAC address right after changing it automatically.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

MAC duplicating or spoofing attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker can receive all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user. If an administrator does not have the working packet-sniffing skills, it is hard to defend intrusions. So, as an Expert Ethical Hacker and Penetration Tester, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. In this lab, you will learn how to spoof a MAC address to remain unknown to an attacker.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

In this lab, you will learn how to spoof a MAC address.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

In the lab, you will need:

- SMAC located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of SMAC from the link **http://www.klcconsulting.net/smac/default.htm#smac27**
- If you decide to download the latest version, then screenshots shown in the lab might differ

- A computer running Windows Server 2012 as Host and Windows Server 2008 as Victim Machine
- Administrative privileges to run tools
- A Web browser with Internet access

Lab Duration

Time: 5 Minutes

Overview of SMAC

SMAC is a powerful yet easy-to-use and intuitive Windows MAC address modifying utility (MAC address spoofing) which allows users to change MAC addresses for almost any Network Interface Cards (NICs) on the Windows 2003systems, regardless of whether the manufacturers allow this option.

Spoofing MAC protects personal and individual privacy. Many organizations track wired or wireless network users via their MAC Addresses. In addition, there are more and more Wi-Fi wireless connections and wireless network use MAC Addresses to communicate these days. Thus, wireless network security and privacy has to do with MAC addresses.

Spoofing is carried out to perform security Vulnerability Testing, penetration testing on MAC address-based authentication and authorization systems (i.e., wireless access points).

Disclaimer: Authorization to perform these tests must be obtained from the system's owner(s).

Lab Tasks

TASK 1

Install SMAC

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\MAC Spoofing Tools\SMAC**, and double-click **smac20_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the wizard-driven installation steps to install SMAC.

SMAC works on the Network Interface Card (NIC), which is on the Microsoft hardware compatibility list (HCL).

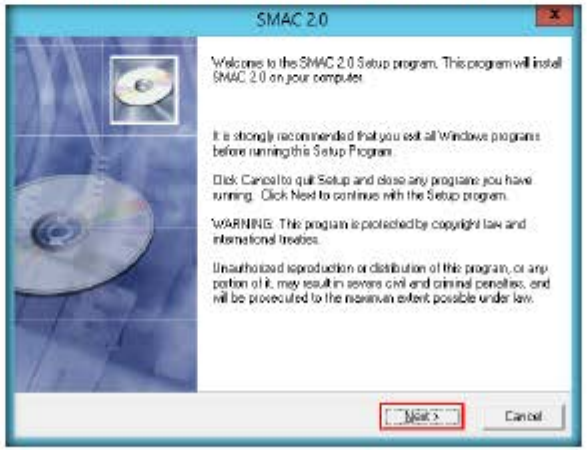


FIGURE 4.1: SMAC installation wizard

4. On completing the installation, launch **SMAC** from the **Apps** screen.

FIGURE 4.2 Launching SMAC from Windows Server 2012 - Apps screen

When you start SMAC program, you must start it as the administrator. You could do this by right click on the SMAC program icon and click on "Run as Administrator if not logged in as an administrator.

TASK 2

Configure SMAC

5. The SMAC main screen appears, along with the **License Agreement**. Click **I Accept** to continue.

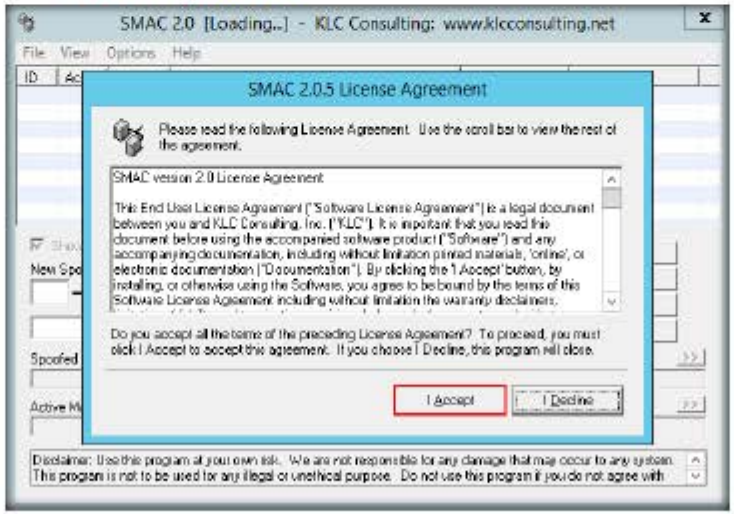


FIGURE 4.3: License Agreement window

6. The **Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.

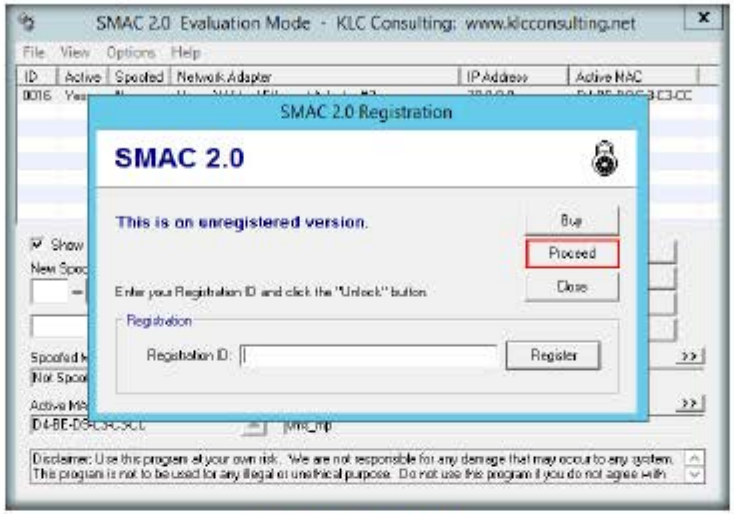


FIGURE 4.4: Registration window

7. The SMAC main window appears. Choose the network adapter of the machine whose MAC Address is to be spoofed.

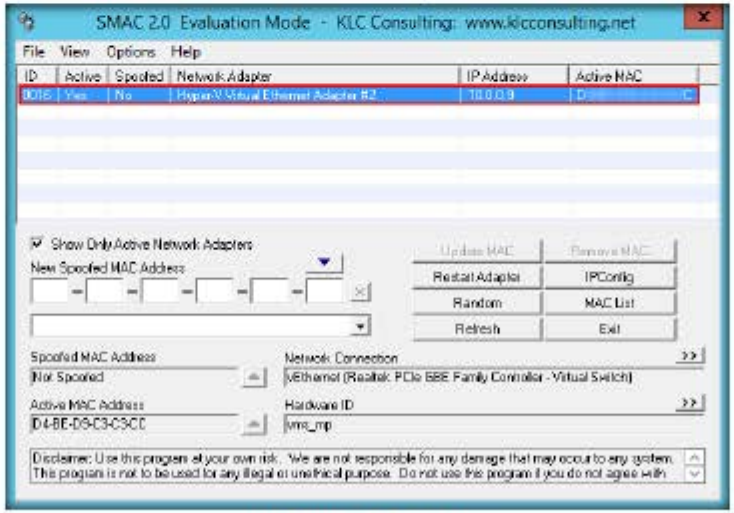


FIGURE 4.5: SMAC main window

8. To generate a random MAC address, click **Random**.

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network.

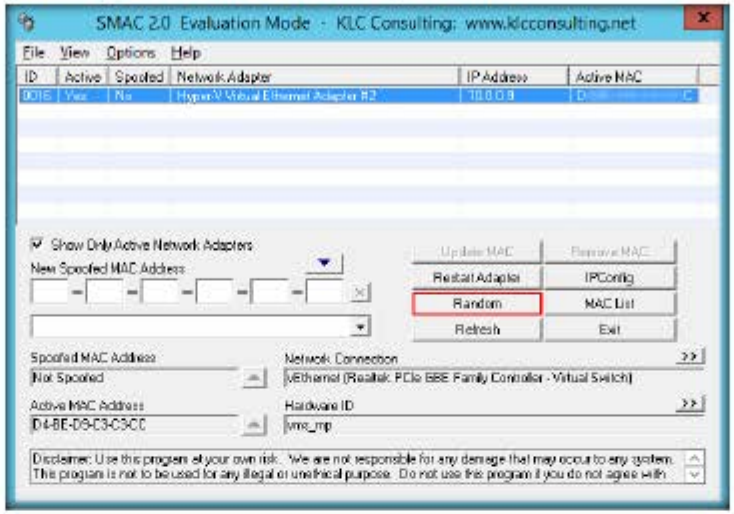


FIGURE 4.6: SMAC Random button to generate MAC addresses

9. Clicking **Random** inputs a new randomly **Spoofed MAC Address**.

SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS), test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and so on.

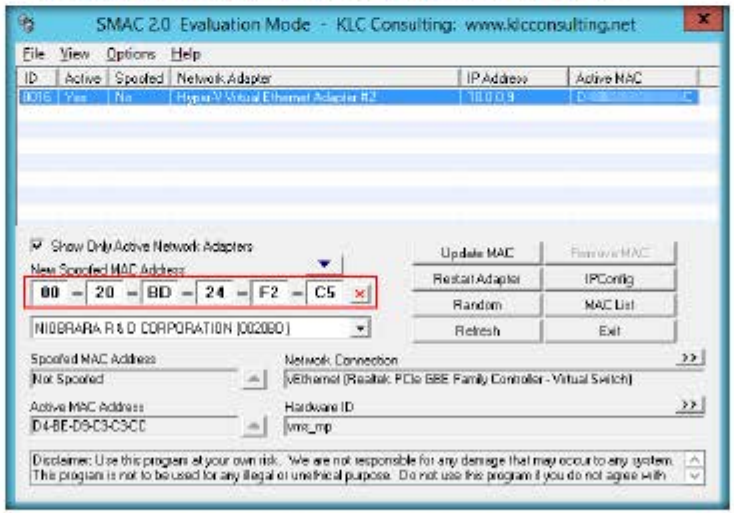


FIGURE 4.7: SMAC selecting a new spoofed MAC address

10. The Network Connection or Adapter displays its respective name.

11. Click the forward arrow button on **Network Connection** to display the **Network Adapter**.

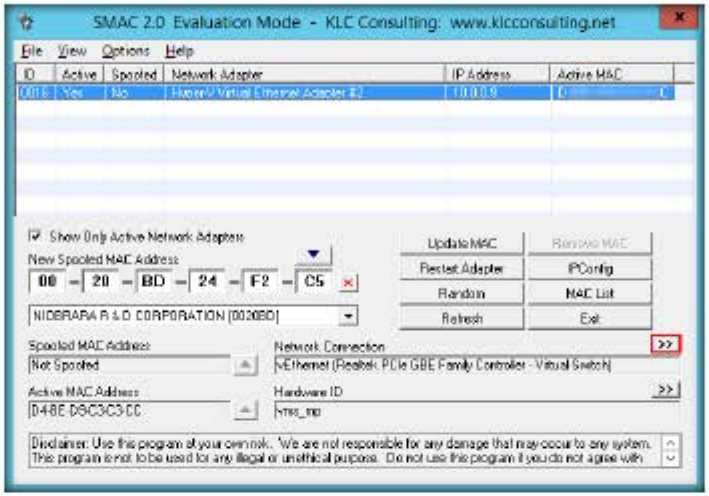


FIGURE 4.8: SMAC Network Connection information

12. Clicking the backward arrow button on **Network Adapter** will again display the **Network Connection**. These buttons allow to toggle between the Network Connection and Network Adapter.

SMAC does not change the hardware burned-in MAC addresses. SMAC changes the software-based MAC addresses, and the new MAC addresses you change are sustained from reboots.

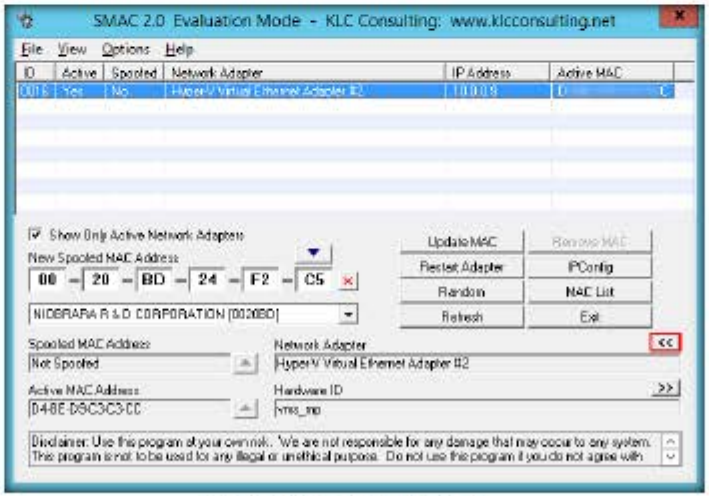


FIGURE 4.9: SMAC Network Adapter information

13. Similarly, the Hardware ID and Configuration ID display their respective information.
14. Click the forward arrow button on **Hardware ID** to display **Configuration ID** information.

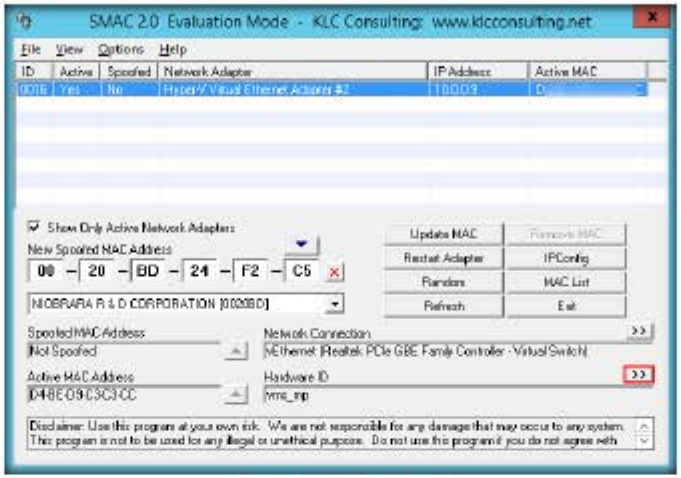


FIGURE 4.10: SMAC Hardware ID display

15. Clicking the backward arrow button on **Configuration ID** will again display **Hardware ID information**. These buttons toggle between Hardware ID and Configuration ID.

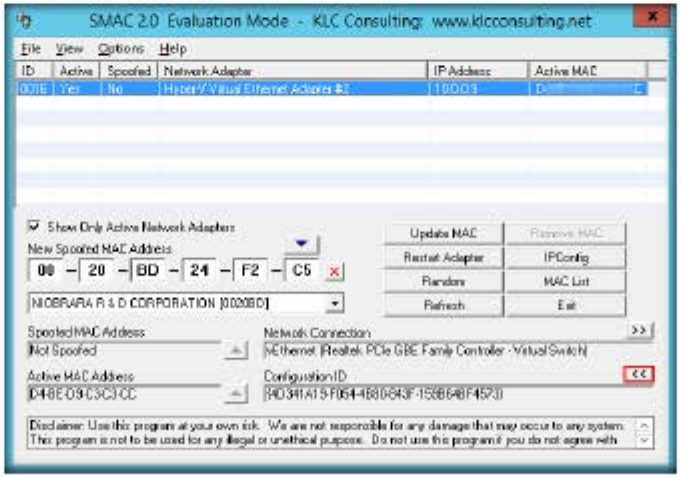


FIGURE 4.11: SMAC Configuration ID display

TASK 3

View IPConfig Information

16. To bring up the **ipconfig** information, click **IPConfig**.

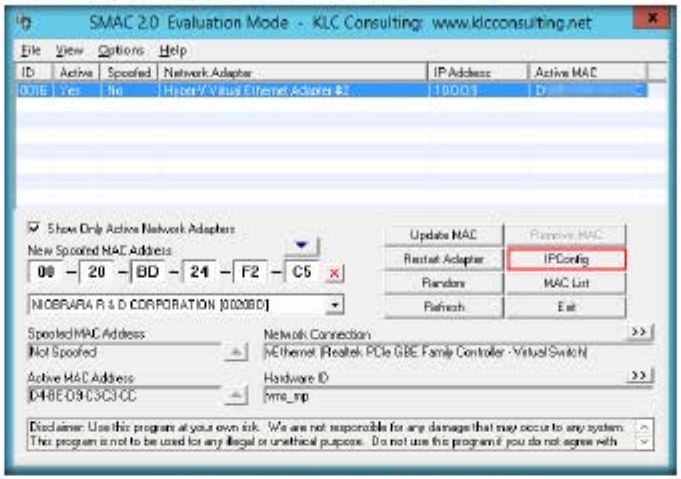


FIGURE 4.12: SMAC to view the information of IPConfig

17. The **IPConfig** window pops up, displaying the IP configuration details of the selected Network Adapter.
18. Click **Close** after analyzing the information.

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

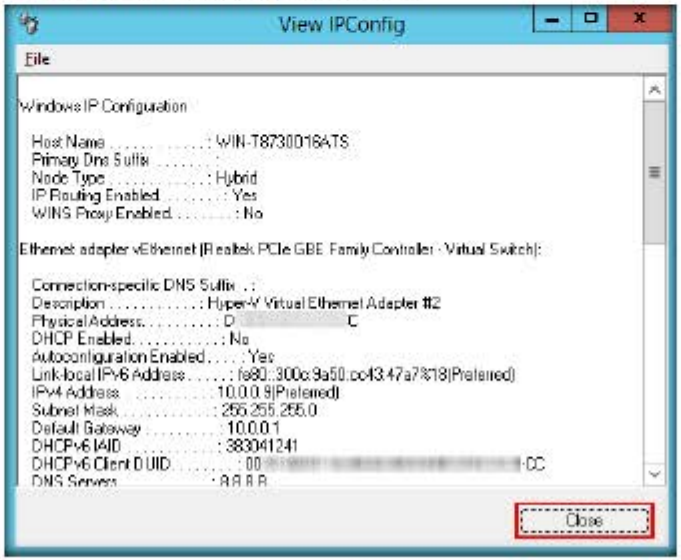


FIGURE 4.13: SMAC IPConfig information

TASK 4

Perform MAC Address Spoofing

19. You can also import the MAC address list into SMAC by clicking **MAC List**.

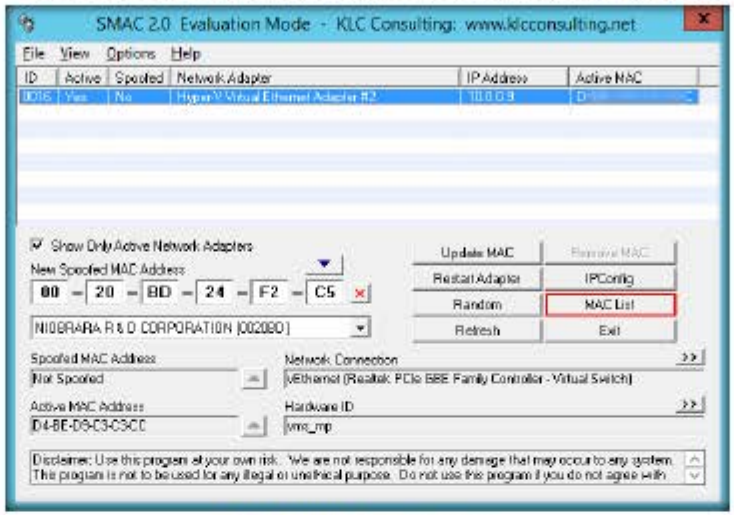


FIGURE 4.14: SMAC listing MAC addresses

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

20. If there is no address in the MAC address field, click **Load List** to select a MAC address list file you have created.

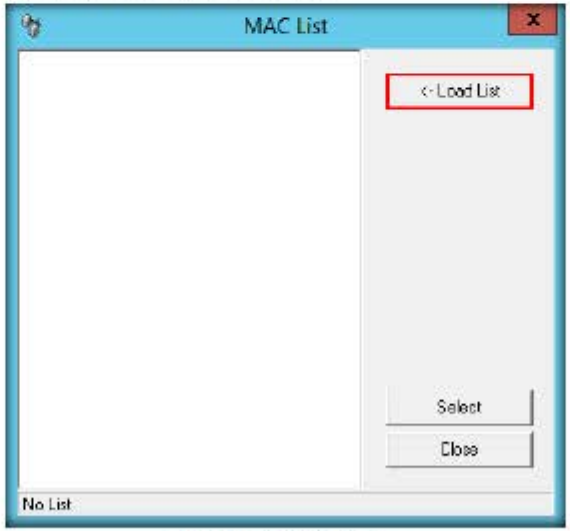


FIGURE 4.15 SMAC MAC List window

When changing MAC address, you MUST assign MAC addresses according to IANA Number Assignments database. For example, "00-00-00-00-00-00" is not a valid MAC address, therefore, even though you can update this address, it may be rejected by the NIC device driver because it is not valid, and TRUE MAC address will be used instead. Otherwise, "00-00-00-00-00-00" may be accepted by the NIC device driver, however, the device will not function.

21. Select **Sample_MAC_Address_List.txt** file from the **Load MAC List** window, and click **Open**.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSPs), Certified Information System Auditors (CISAs), Microsoft Certified Systems Engineers (MCSEs), and professional software engineers.

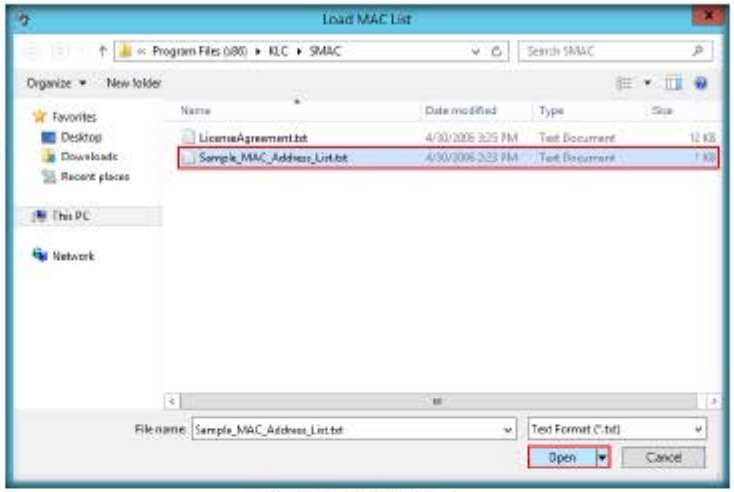


FIGURE 4.16: SMAC MAC List window

SMAC displays the following information about a Network Interface Card (NIC).

- Device ID
- Active Status
- NIC Description
- Spoofed status
- IP Address
- Active MAC address
- Spoofed MAC Address
- NIC Hardware ID
- NIC Configuration ID

22. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address,** and click **Select** to copy the MAC Address to the "**New Spoofed MAC Address**" in the main SMAC screen.

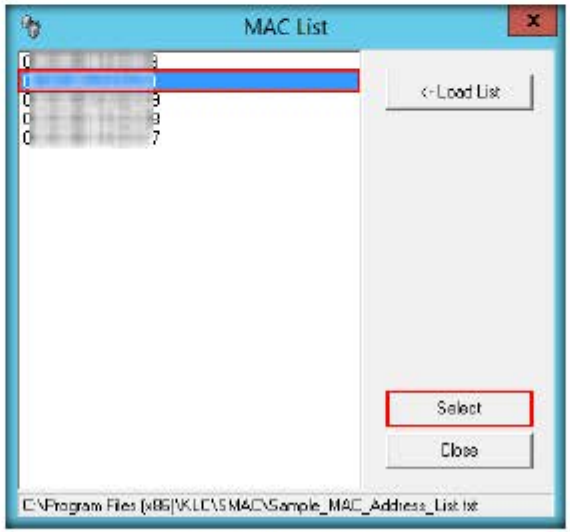


FIGURE 4.17: SMAC MAC List window

23. Click **Update MAC** to update the MAC address information of the machine.

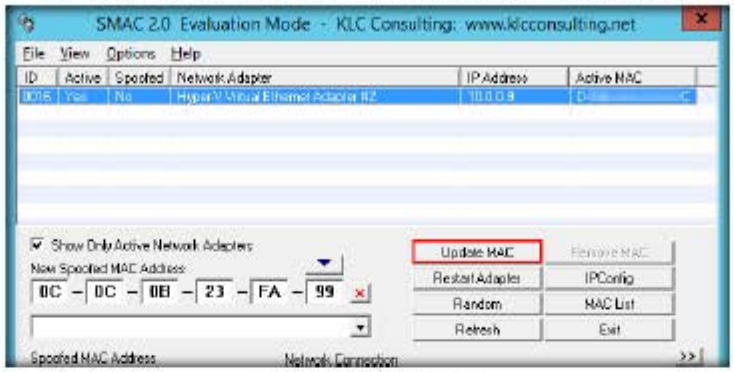


FIGURE 4.18: Updating MAC address

24. **SMAC 2.0** dialog-box appears, click **Yes**. It will cause a temporary disconnection in your Network Adapter.

Note: This dialog box appears only for the evaluation or trial version.

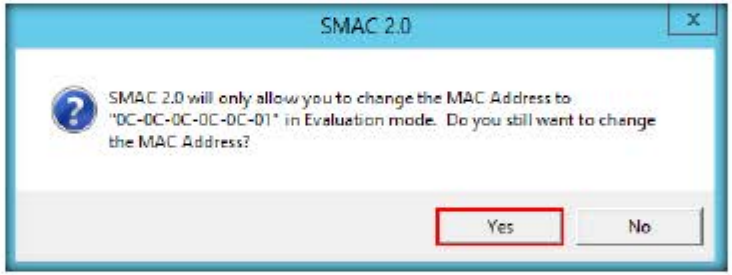


FIGURE 4.19: SMAC 2.0 dialog box

25. After successfully spoofing the MAC address, a **SMAC 2.0** pop-up appears, stating that the Adapter has been restarted; click **OK** to close the pop-up.

FIGURE 4.20: SMAC 2.0 dialog box

26. Once the adapter is restarted, the MAC address is assigned to your machine. By spoofing it, an attacker can simulate attacks such as ARP poisoning and MAC flooding, without revealing the actual MAC address of the attacker's machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Performing Man-in-the-Middle Attack using Cain & Abel

Cain &Abel is a password recovery tool that allows recovery of passwords by sniffing the network, and cracking encrypted passwords.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You learned in the previous lab how to obtains username and passwords using Wireshark. By merely capturing enough packets, attackers can extract the username and password if victims authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can simply log into the victim's email account or use that password to login to their PayPal and drain the victim's bank account. They can even change the password for the email. Attackers can use Wireshark to decrypt the frames with the victim's password they already have.

As a preventive measure, an organization's Administrator should advise employees not to provide sensitive information in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. As an expert Ethical Hacker and Penetration Tester you must have sound knowledge of sniffing, network protocols and their topology , TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanism, and encryption techniques.

Another method through which you can gain username and password is by using Cain & Abel to perform man-in-the-middle (MITM) attacks.

Lab Objectives

The objective of this lab to accomplish the following information regarding the target organization that includes, but is not limited to:

- Sniff network traffic and perform ARP Poisoning
- Launch Man-in-the-Middle attack
- Sniff network for password

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Environment

To carry-out the lab, you need:

- Cain and Abel, located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**
- You can also download the latest version of Cain & Abel from http://www.oxid.it.
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as Host machine
- Windows 8.1 running on virtual machine as Attacker machine
- Windows 2008 Server running on virtual machine as Victim machine
- A Web browser with Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of a Man-in-the-Middle Attack

You can download Cain & Abel from http://www.oxid.it.

An MITM is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

MITM attacks come in many variations and can be carried out on a switched LAN.

Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel** and double-click **ca_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard-driven installation steps to install Cain & Abel.

FIGURE 5.1: Cain & Abel installation

4. The **WinPcap Installation** pop-up appears; click **Don't install,** as you have already installed it during the lab setup.

Man in the Middle attacks has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.

FIGURE 5.2: WinPcap Installation pop-up

5. Launch the **Windows Server 2008** and **Windows 8.1** virtual machines.

6. Switch back to the host machine, and launch **Cain & Abel** from the **Apps** screen.

FIGURE 5.3: Launching Cain & Abel from Apps screen

7. The main Window of Cain & Abel appears, as shown in the screenshot:

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

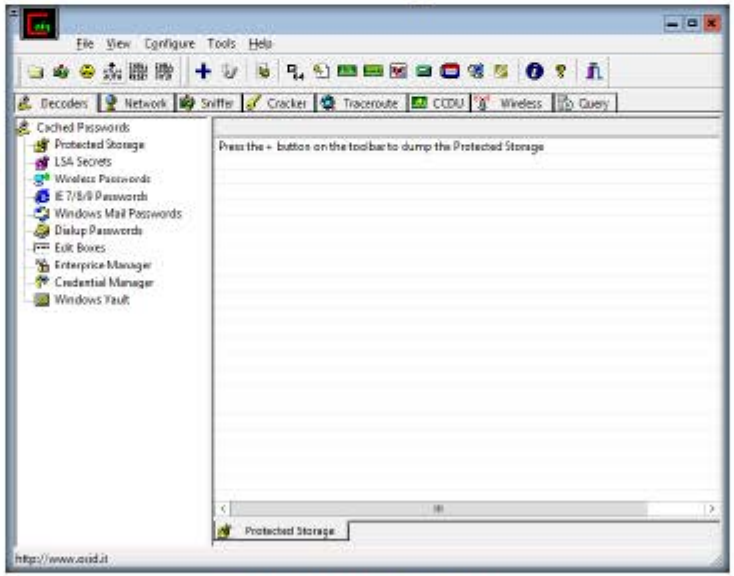


FIGURE 5.4: Cain & Abel Main Window

8. To configure **Ethernet card**, click **Configure** from menu bar.

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved to a text file. APR-HTTPS can intercept and forge digital certificates on the fly but because trusted authority does not sign these certificates a warning message will be displayed to the end user.

FIGURE 5.5: Cain & Abel Configuration Option

9. The **Configuration Dialog** window appears.

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

10. The window consists of several tabs. Click the **Sniffer** tab to select sniffing adapter.
11. Select the **Adapter** associated with the IP address of the machine, and click **Apply** and **OK**.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.

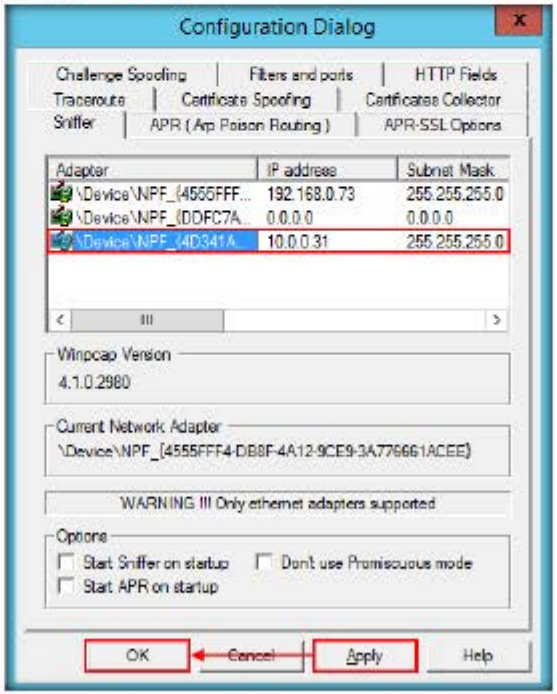


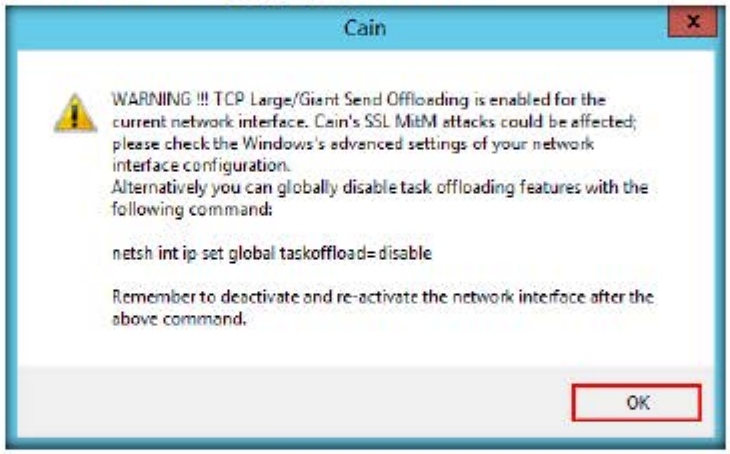
FIGURE 5.6: Cain & Abel Configuration Dialog Window

12. Click **Start/Stop Sniffer** on the toolbar to begin sniffing.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).

FIGURE 5.7: Starting a sniffer

Note: If the **Cain** Warning pop-up opens, click **OK**.



Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data.

FIGURE 5.8: Cain Warning pop-up

13. Now click the **Sniffer** tab.

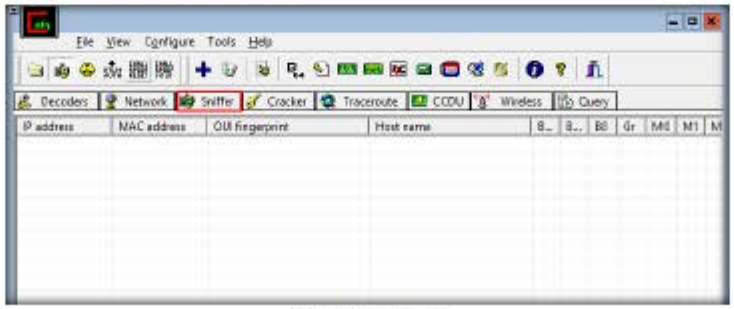


FIGURE 5.9: Sniffer tab

14. Click the plus (+) icon, or right click in the window, and select **Scan MAC Addresses** to scan the network for hosts.
15. The **MAC Address Scanner** window appears. Check **All hosts in my subnet** and **All Tests**, then click **OK.**

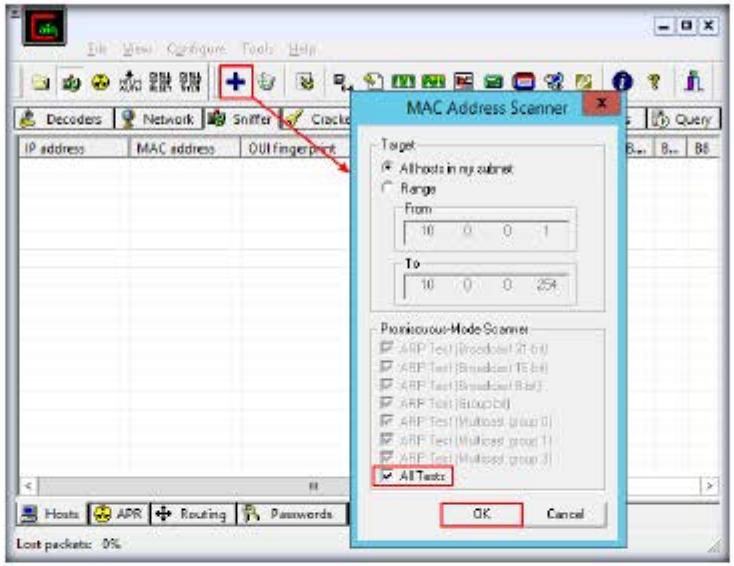


FIGURE 5.10: Cain & Abel - MAC Address Scanner Window

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

16. Cain & Abel starts **scanning** for MAC addresses and **lists** all those found.
17. After scanning is **completed**, a list of detected **MAC addresses** are displayed as shown in the screenshots:

Speeding up packet capture speed by wireless packet injection.

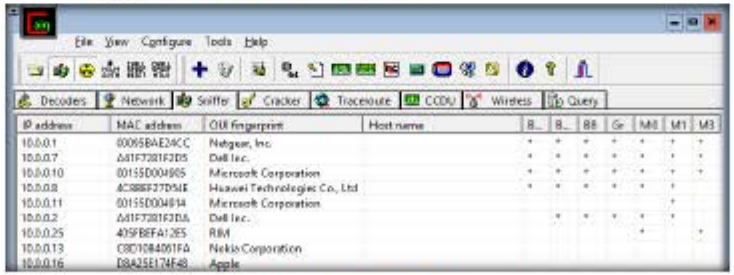


FIGURE 5.11: Cain & Abel - MAC Address Scanned

18. Click the **APR** tab at the lower end of the window.

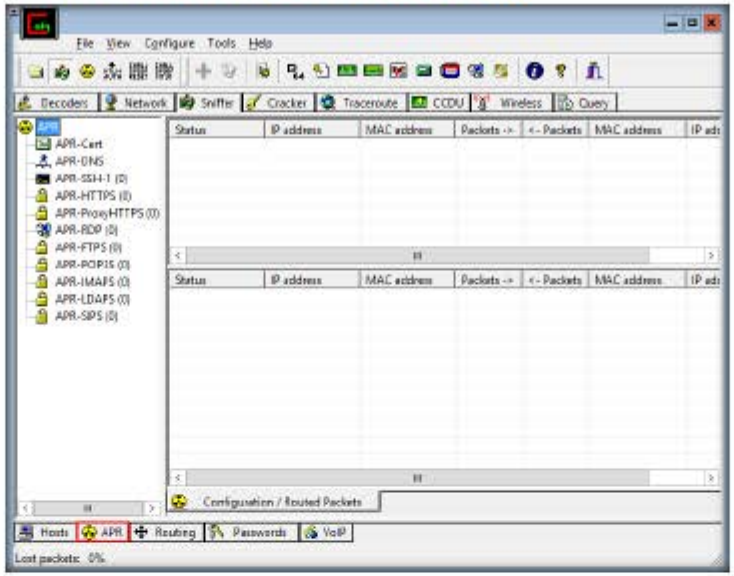


FIGURE 5.12: Cain & Abel ARP Tab

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all packets of an entire direction so it cannot grab authentications that use a challenge-response mechanism.

Note that Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

19. Click anywhere on the top most section in the right pane to activate the **+** icon.

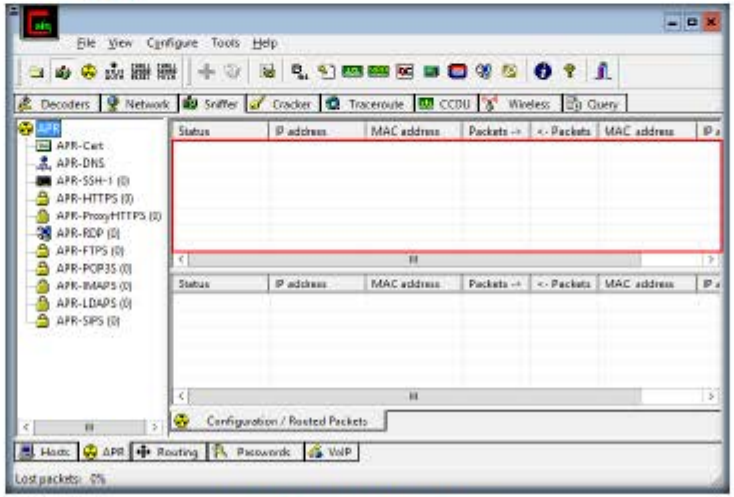


FIGURE 5.13: Cain & Abel Sniffer Section

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.

20. Click the Plus (+) icon; the **New ARP Poison Routing** window opens, from which we can add IPs to listen to traffic.

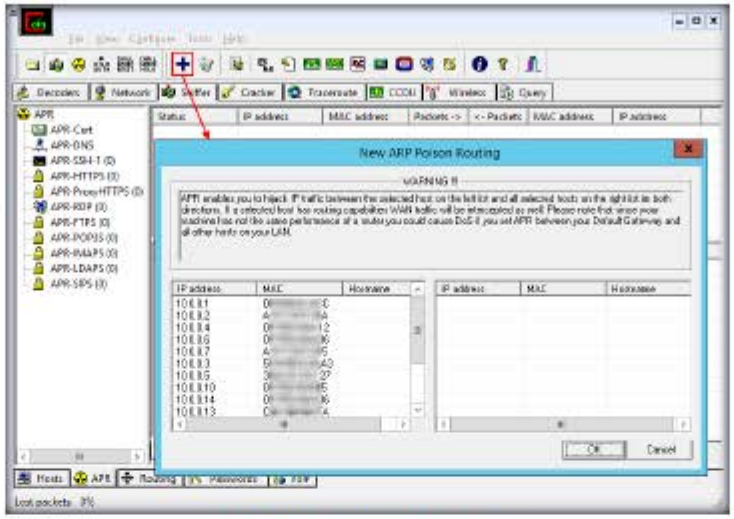


FIGURE 5.14: New ARP Poison Routing window

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primarily use is to securely store private keys that have been issued to a user.

21. To monitor the traffic between two computers, select **10.0.0.10 (Windows 8.1)** and **10.0.0.11 (Windows Server 2008)**. Click **OK**

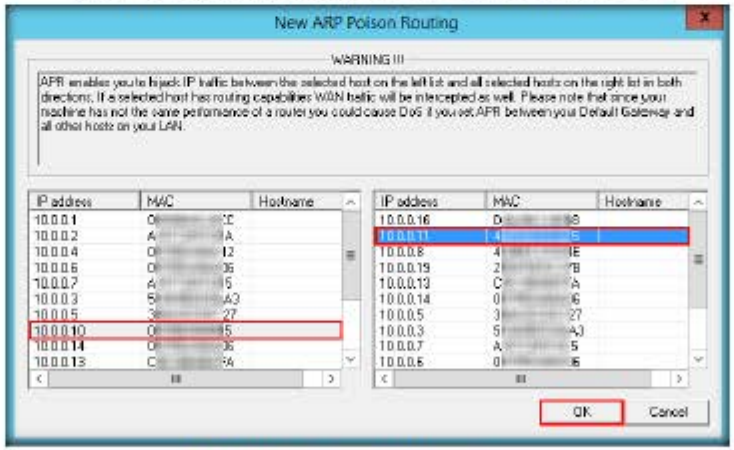


FIGURE 5.15: Monitoring the traffic between two computers

All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

22. Select the added IP address in the **Configuration/Routed** packets, and click **Start/Stop APR**.

Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

Note: If the **Couldn't bind HTTPS acceptor socket** pop-up appears, click **OK**.

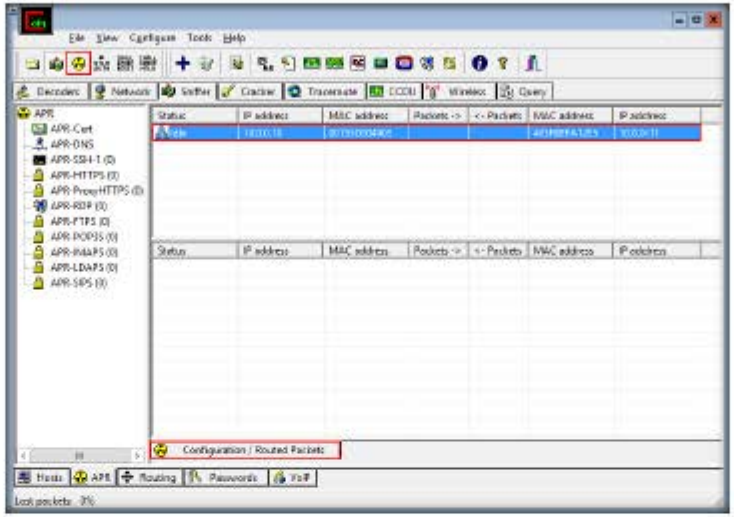


FIGURE 5.16: Cain & Abel ARP Poisoning

23. Now, launch command prompt in Windows Server 2008, and type **ftp 10.0.0.10** (IP address of Windows 8.1) and press **Enter**.

24. When prompted for a username, type "**Martin**" and press **Enter;** for a password, type "**apple**" and press **Enter**.

There is also another set used for credentials that should persist on the local machine only and cannot be used in roaming profiles, this is called "Local Credential Set" and it refers to the file \Documents and Settings\%Username%\Local Settings\Application Data\Microsoft\Credentials\%UserSID%\Credentials

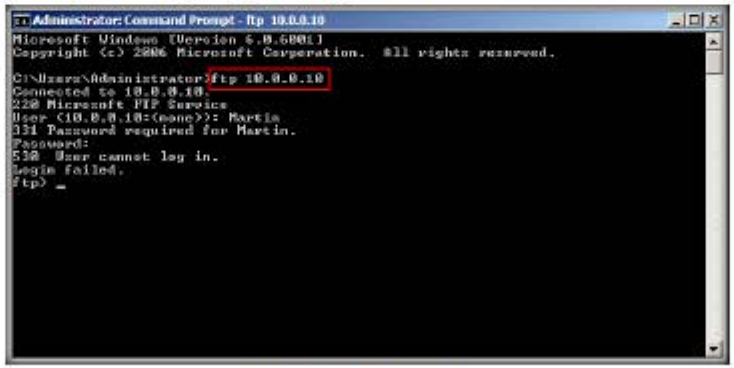


FIGURE 5.17: Start ftp://10.0.0.10

Note: Irrespective of a successful login (or even of login failure), Cain & Abel captures the password entered during login.

25. On the host machine, observe the tool listing some packet exchange.

Credentials are stored in the registry under the key HKEY_CURRENT_USER \Software\Microsoft\Protected Storage System Provider\.

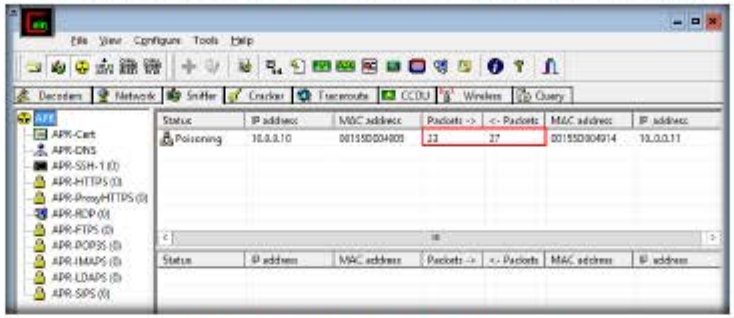


FIGURE 5.18: Sniffer window with more packets exchanged

26. Click the **Passwords** tab, as shown in the screenshot, to view the sniffed password for **ftp 10.0.0.10**.

This set of credentials is stored in the file \Documents and Settings\%Username%\Application Data\Microsoft\Credentials \%UserSID%\Credentials.

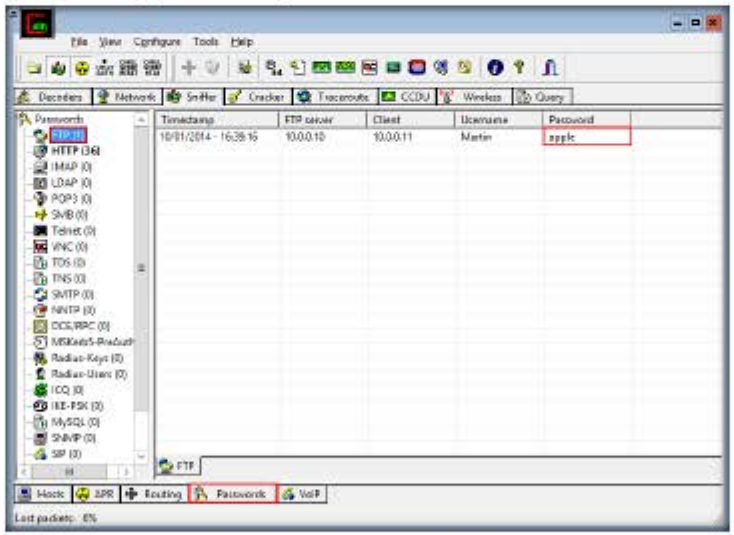


FIGURE 5.19: Passwords displayed in plain text

27. This way, an attacker can obtain passwords in clear text if the channel through which information is passing doesn't provide encryption.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and "exposure" through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 6

Detecting Systems running in Promiscuous mode in a Network using PromqryUI

PromqryUI is a tool with a Windows GUI that can be used to detect network interfaces running in promiscuous mode.

Lab Scenario

ICON KEY
- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

In an ARP storm attack, an attacker collects the IP and MAC addresses of network machines to use in later attacks. The attackers send ARP packets to a network; if an ARP packet with forged gateway MAC address is pushed to the LAN, all communications within the LAN may fail. This attack uses all resources of both victim and non-victim computers.

As a network administrator, you must always diagnose network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific protocol analyzer technique, you should be able to identify the cause of any broadcast storm and a method for resolving it. Identify susceptible points in the network and protect them before attackers discover and exploit its vulnerabilities, especially in ARP-enabled LAN systems known for their security loopholes and thereby allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all packets that pass over a network. As an Expert Ethical Hacker and Penetration Tester, you must be aware of tools for detecting network interfaces running in promiscuous mode that might be network sniffers. In this lab, you will learn to use PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab is:

- To detect promiscuous systems in a network

Lab Environment

To complete this lab, you will need:

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv9 Module 07 Sniffing**

- PromqryUI is located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI**
- You can also download the latest version of PromqryUI from http://www.microsoft.com/en-us/download/details.aspx?id=16883
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 (host machine)
- A computer running Windows Server 2008 on a virtual machine
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern Windows system has network interfaces running in promiscuous mode. If so, this could indicate the presence of a network sniffer in the system.

PromqryUI cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

Lab Tasks

TASK 1

Extract PromqryUI

1. Log onto the **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI** and double-click **promqryui.exe**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.

4. Click **Yes** in the **PromqryUI License Agreement** window.

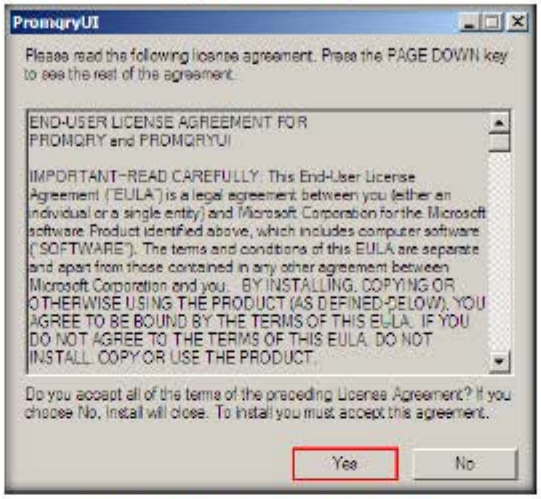


FIGURE 6.1: PromqryUI - License Agreement dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

5. The **WinZip Self-Extractor** dialog box appears. Browse to a desired location (default is **c:\promqryui**) to save the unzipped folder, and click **Unzip**.

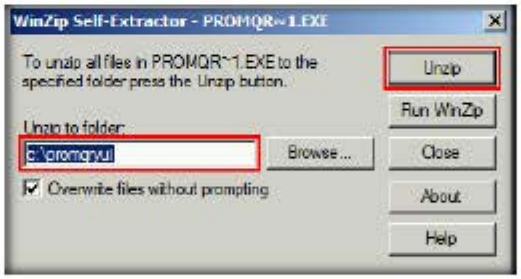


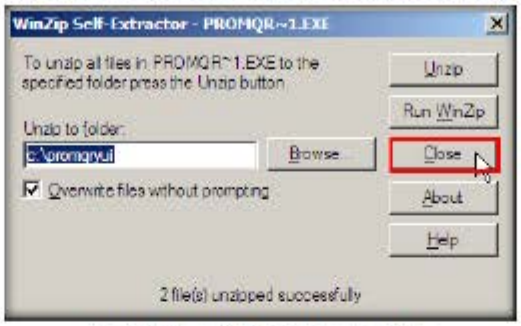
FIGURE 6.2: PromqryUI - WinZip Self-Extractor dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

6. The **WinZip Self-Extractor** pop-up appears; click **OK** to close it.

FIGURE 6.3: WinZip Self-Extractor dialog box

7. Now, click **Close** to close the **WinZip Self-Extractor** dialog box.



Unzip to folder allows you to browse and select a destination of your choice to save the setup file.

FIGURE 6.4: PromqryUI - WinZip Self-Extractor dialog box

8. Now, install **.NET Framework 1.1** by double-clicking **dotnetfx.exe,** located at **Z:\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI**.

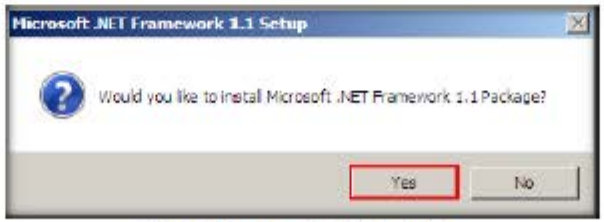
TASK 2

Install .NET Framework 1.1

9. Click **Run**.

FIGURE 6.5: Open File - Security Warning dialog box

10. Click **Yes** to initiate the .NET Framework installation.



The .NET Framework version 1.1 redistributable package that includes everything you need to run applications developed using the .NET Framework.

FIGURE 6.6: .NET Framework - Installation dialog box

11. While attempting to install .NET Framework 1.1, a **Program Compatibility Assistant** dialog box appears. Click **Run Program**.

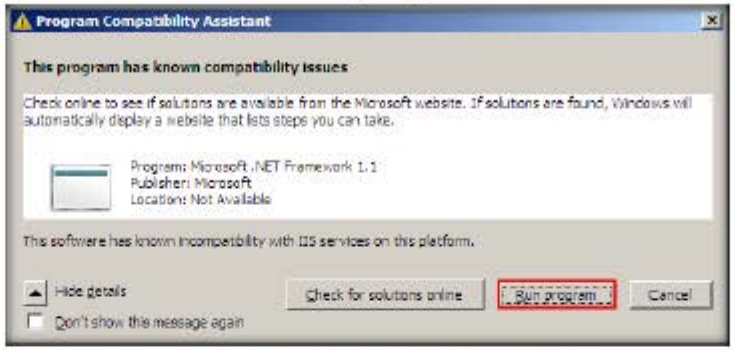


FIGURE 6.7: .NET Framework - Program Compatibility Assistant dialog box

12. The **License Agreement** dialog box is displayed; select **I agree,** and click **Install**. Follow the wizard-driven installation steps to install **.NET Framework 1.1**.

FIGURE 6.8: .NET Framework - License Agreement dialog box

13. Once installation is complete, the **Microsoft .NET Framework 1.1 Setup** dialog box appears; click **OK**.

FIGURE 6.9: .NET Framework – Installation complete message box

TASK 3

Install PromqryUI

14. Navigate to **C:\promqryui**, double-click **pqsetup.msi,** and follow the wizard-driven installation steps to install PromqryUI.

FIGURE 6.10: Promqryui installation wizard

15. Once installation is complete, go to **Start → All Programs,** and click **Promqry** to launch it.

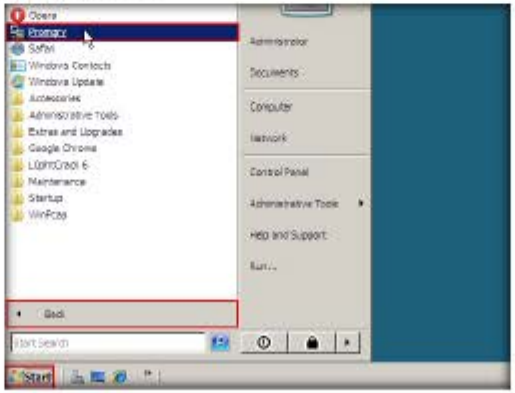


FIGURE 6.11: Windows 2008 Server - Start menu

Promiscuous mode can be used in a malicious way to sniff on a network. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this by using carefully designed firewall settings.

16. The main window of Promqry appears. Click **Add**.

With the PromqryUI tool, you can add either a single system or multiple systems to query.

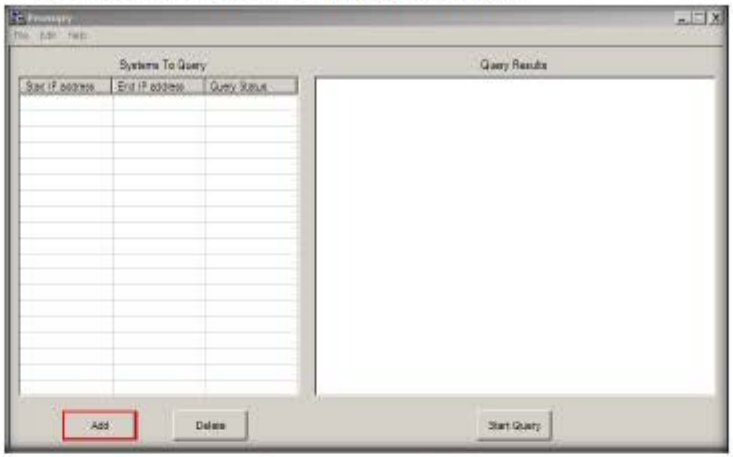


FIGURE 6.12: PromqryUI - Main window

17. The **Select Addition Type** dialog box appears; click **Add Single System**.

FIGURE 6.13: PromqryUI - Adding system

18. The **Add System to Query** dialog box appears; type the IP Address of the system you want to check in the **IP Address** field, and click **Save**.

For systems that you need to query, a range of IP addresses can be provided. Also, you can just carry a query for a local system.

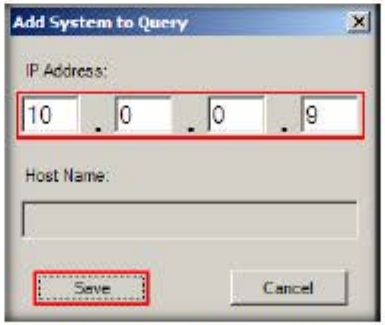


FIGURE 6.14: PromqryUI - Add System to Query

Note: 10.0.0.9 is the IP address of the host machine (i.e., **Windows Server 2012**), which might differ in your lab environment.

19. Check the added IP Address in **Systems To Query** section, and click **Start Query**.

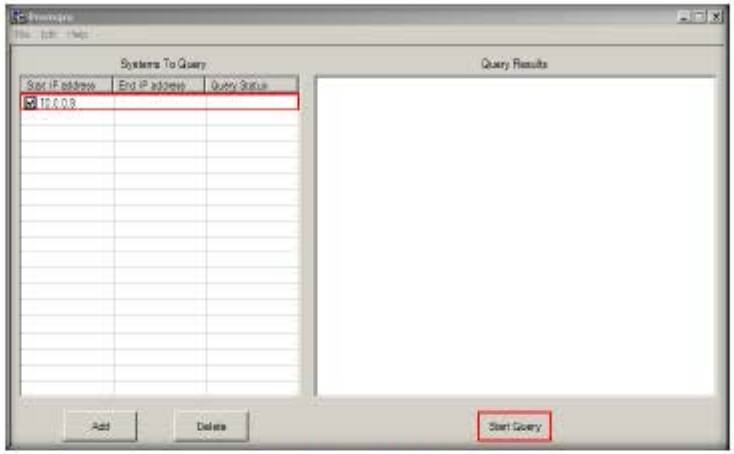


FIGURE 6.15: PromqryUI – Querying system

20. The results will be displayed in **Query Results**. Scroll down to analyze the complete results.

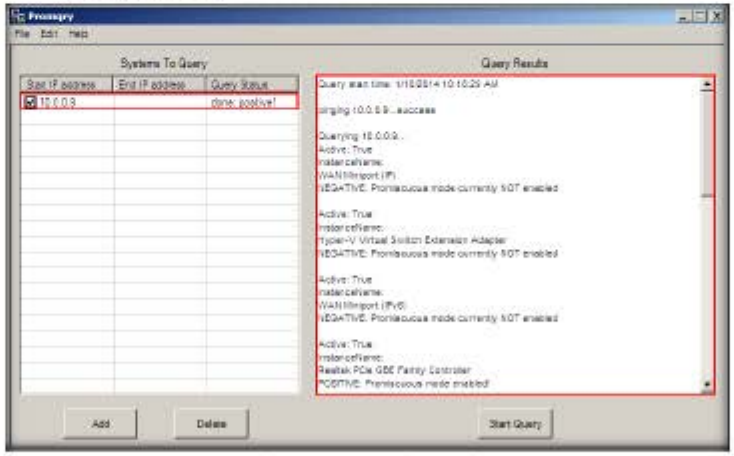


FIGURE 6.16: PromqryUI - Query Results

Query results will let you know if the system is promiscuous mode or not and provides other information like Computer name, Domain, Computer Model, Manufacturer, Owner, and so on.

21. Scroll down the Query Results section to view the system summary.

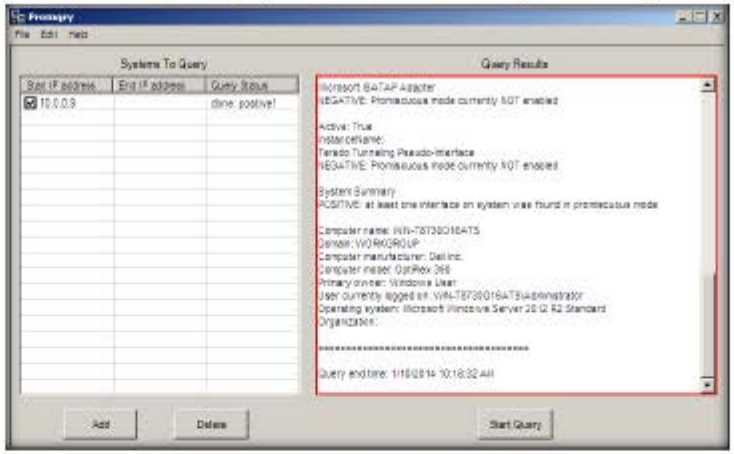


FIGURE 6.17: PromqryUI - Query Results

22. This way, you can search for all the machines running in promiscuous mode, and block them from interacting with your machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Detecting ARP Poisoning in a Switch-Based Network

ARP spoofing is a technique by which attackers send Address Resolution Protocol messages onto a local area network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

ARP cache poisoning is a method of attacking a LAN network by updating the target computer's ARP cache with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address (i.e., that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

You, as an ethical hacker and pen tester, must assess your organization or a target of evaluation for ARP poisoning vulnerabilities.

Lab Objectives

The objective of this lab is to help students understand how to:

- Perform ARP Poisoning on a switch based network
- Detect ARP Poisoning using Wireshark

Lab Environment

To perform this lab, you will need:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine
- Windows 8.1 running as a virtual machine

Lab Duration

Time: 15 Minutes

Overview of ARP Poisoning

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. Indeed, systems which haven't made an ARP request also accept the ARP reply coming from other devices.

Lab Tasks

Note: Launch the **Windows 8.1** and **Kali Linux** virtual machines before beginning this lab.

TASK 1

Install Cain & Abel

1. Switch to **Windows 8.1** machine, navigate to **Z:\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**, double-click **ca_setup.exe**, and follow the wizard-driven installation steps to install Cain & Abel.

Note:

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

If a **Window Security** dialog-box appears, asking you to enter network credentials, type the following credentials and click **OK**:

User name: Administrator

Password: qwerty@123

FIGURE 7.1: Installing Cain & Abel

2. During installation, the **WinPcap Installation** pop-up appears; click **Install.**

FIGURE 7.2: Installing WinPcap

3. Follow the wizard-driven installation steps to install WinPcap.

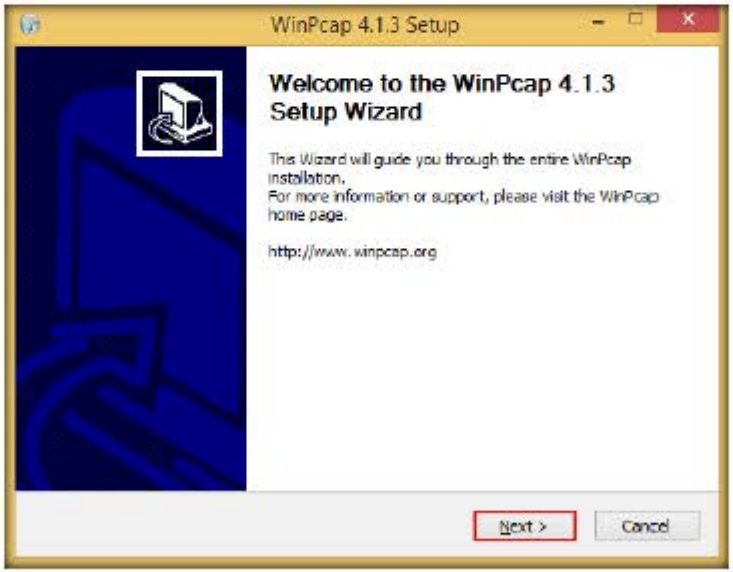


FIGURE 7.3: Installing WinPcap

TASK 2

Install Wireshark

4. Navigate to **Z:\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark**, double-click **Wireshark-win64-1.10.5.exe,** and follow the wizard-driven installation steps to install the application.

Note: If the **User Account Control** pop-up appears, click **Yes**.

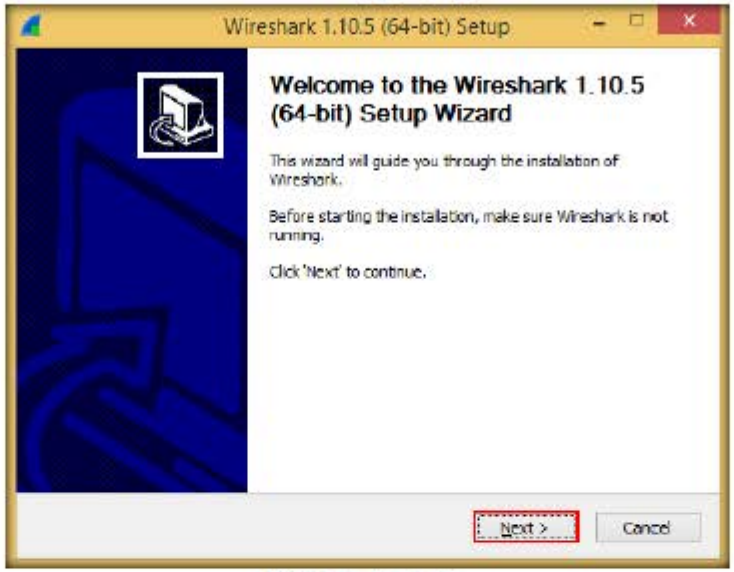


FIGURE 7.4: Installing Wireshark

TASK 3

Perform ARP Poisoning

5. Now, double-click **Cain** to launch it.

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

FIGURE 7.5: Launching Cain & Abel

6. The Cain window appears; click **Configure** in the menu bar.

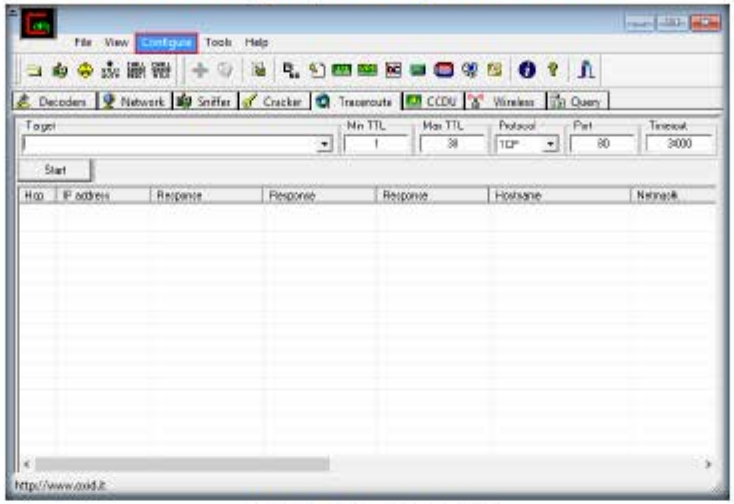


FIGURE 7.6: Configuring Cain & Abel

7. The **Configuration Dialog** window appears; click the **Sniffer** tab.
8. Select the adapter, and click **OK**.

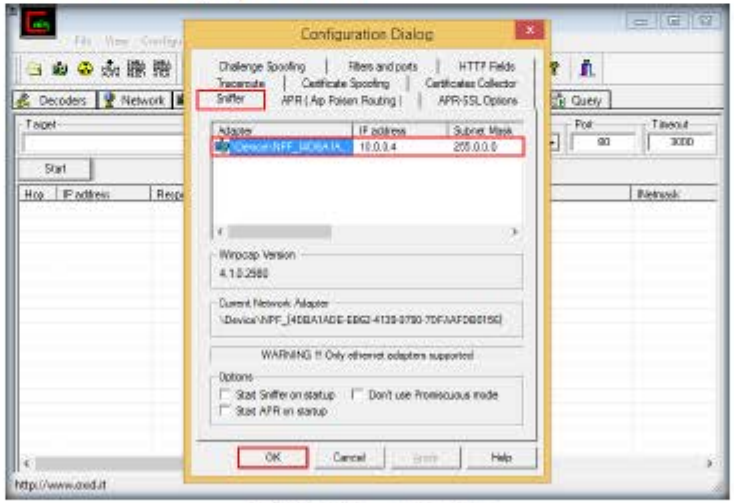


FIGURE 7.7: Configuring Cain & Abel

9. Now, click **Start/Stop Sniffer** in the toolbar.

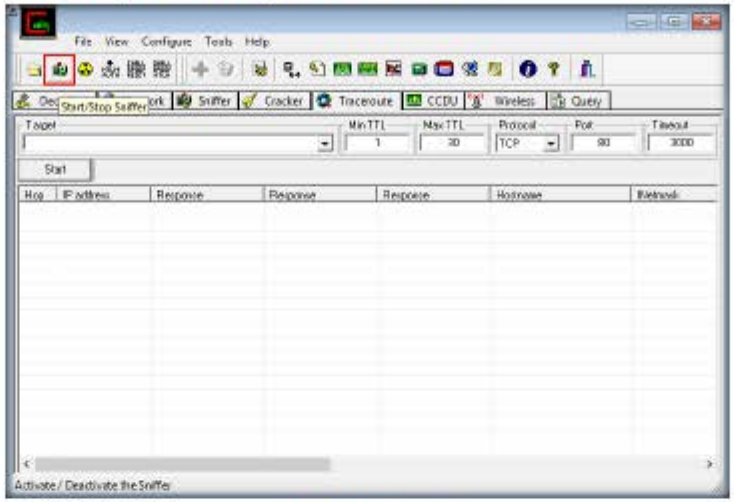


FIGURE 7.8: Starting Sniffer

10. If the **Cain** pop-up appears, click **OK**.

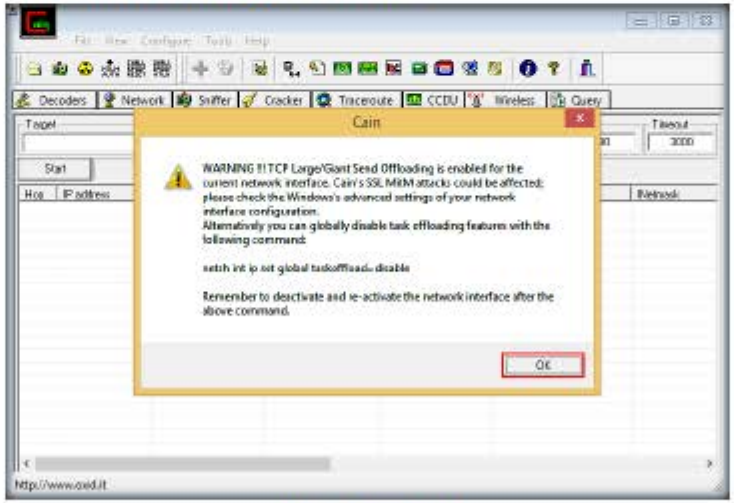


FIGURE 7.9: Cain Pop-Up

11. Click the **Sniffer** tab.

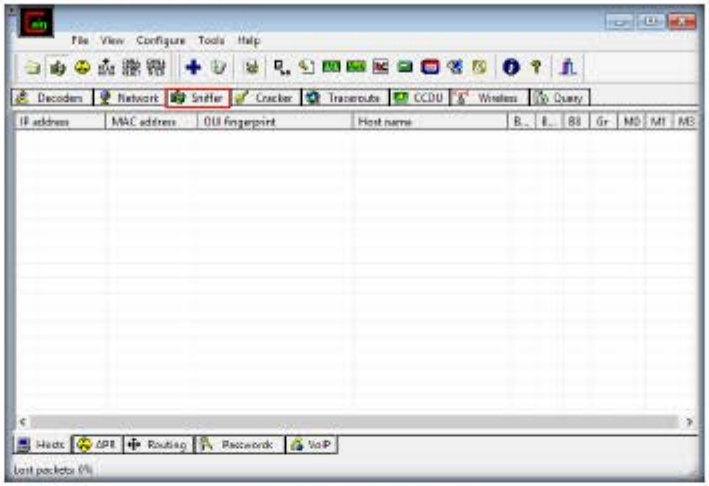


FIGURE 7.10: Clicking Sniffer Tab

12. Click **+** in the toolbar.
13. The **MAC Address Scanner** window appears; click **Range**.
14. Specify the IP address range you want to scan (here, **10.0.0.1-10.0.0.30**, which might differ in your lab environment).
15. Check **All Tests**, and click **OK**.

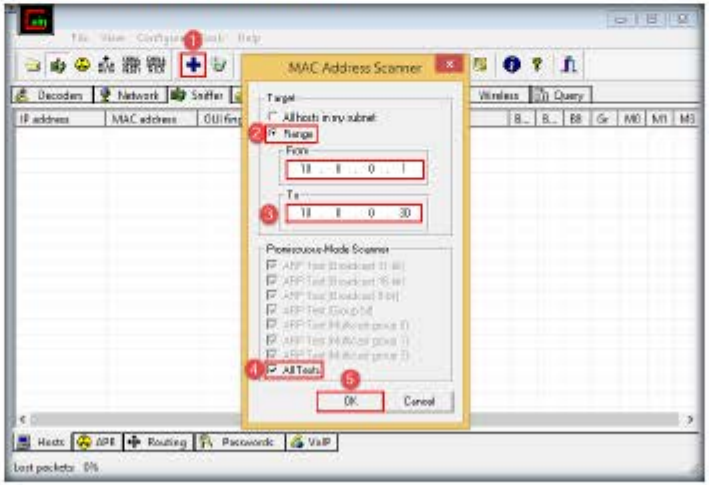


FIGURE 7.11: Scanning MAC Addresses

16. The application begins to perform ARP tests on the IP address range and displays it in the Sniffer window, as shown in the screenshot:

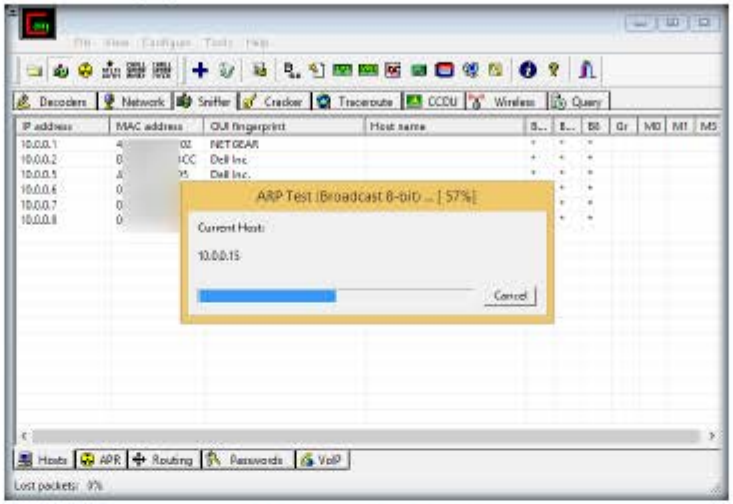


FIGURE 7.12: Scanning MAC Addresses

17. On completing the ARP tests, all the MAC and their associated IP addresses that responded to the ARP requests are displayed, as shown in the screenshot:

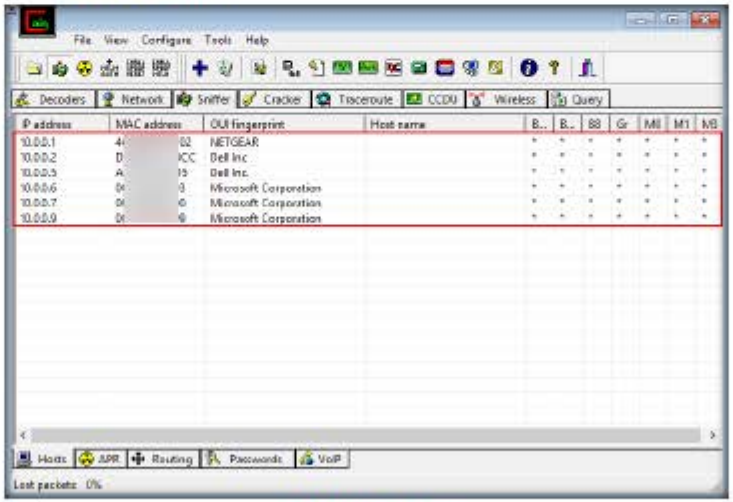


FIGURE 7.13: Sniffer Tab

18. Now, click the **APR** tab.
19. Click anywhere on the topmost section (in the right pane) to activate the **+** icon.
20. Once the **+** icon is activated, click it.

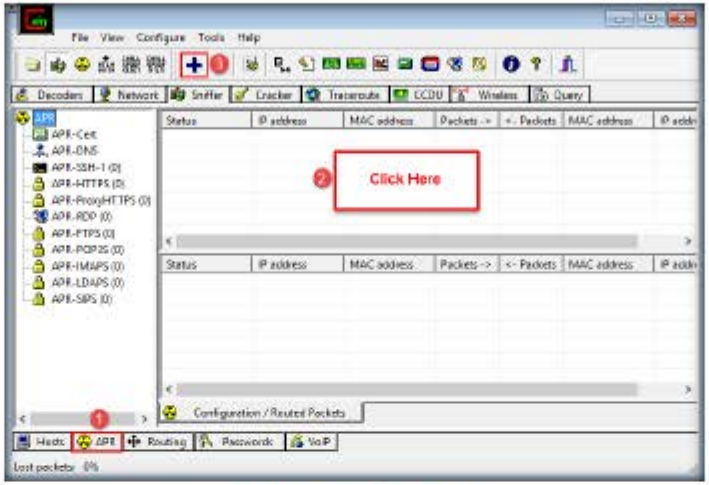


FIGURE 7.14: ARP Poison Routing

21. The **New ARP Poison Routing** window appears. Now, you need to select the machines between which you want to intercept traffic.
22. Select the first target (here, **10.0.0.2,** the **Windows Server 2012** machine) from the list of IP addresses displayed in the left pane.

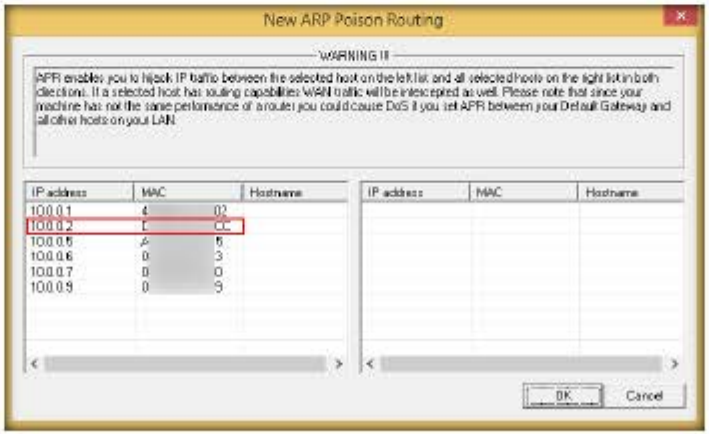


FIGURE 7.15: New ARP Poison Routing Window

23. Upon selecting the first target, a list of IP addresses excluding the first target appears in the right pane.
24. You need to select the second target IP address (here, **10.0.0.9,** the **Kali Linux** machine) from the right-pane. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

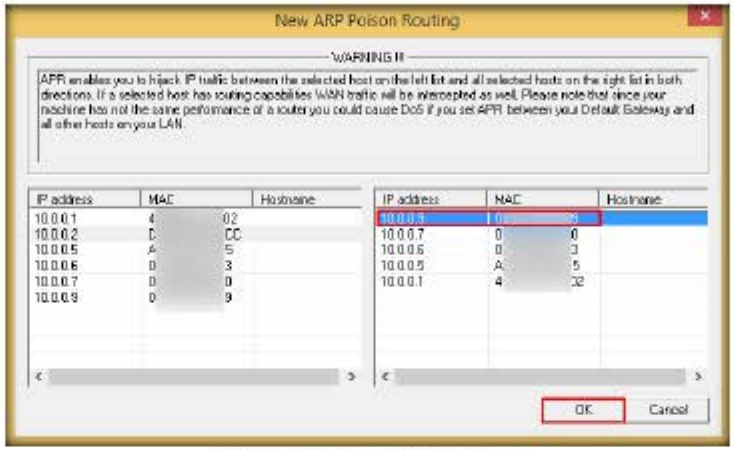


FIGURE 7.16: Performing ARP Poison Routing

25. Once complete, the selected targets appear in the top section.
26. Now, click the **Start/Stop APR** button to initiate the ARP Poison Routing attack.

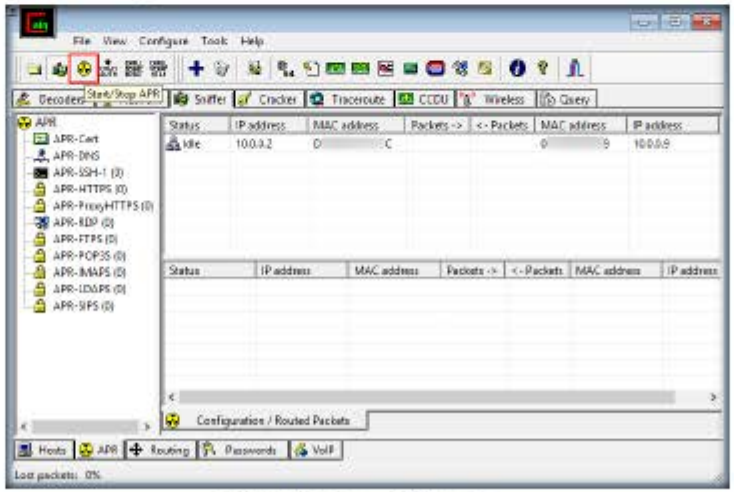


FIGURE 7.17: Performing ARP Poison Routing

27. The status of the attack changes to **Poisoning**, as shown in the screenshot:

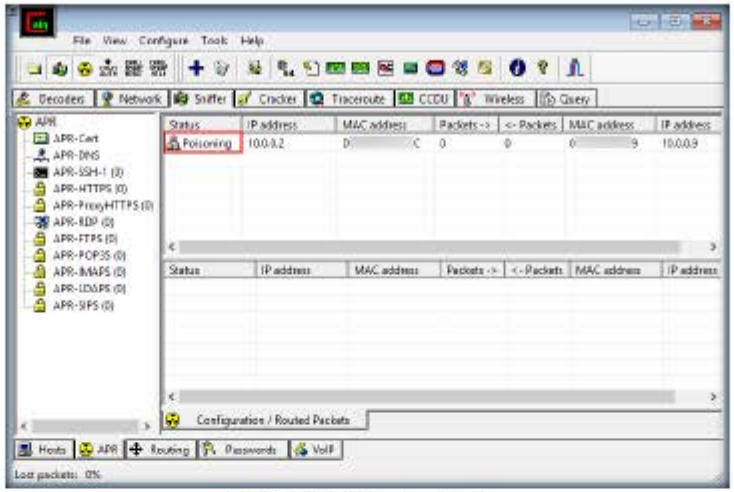


FIGURE 7.18: ARP Poison Routing Begun

28. Cain & Abel is intercepting the traffic traversing between these two machines.
29. To generate traffic between the machines, you need to ping one target machine using the other.

TASK 4

Ping Windows 8.1 Machine

30. Switch to Kali Linux, and launch a command-line terminal.

FIGURE 7.19: Command Line Terminal

31. Type **hping3 [IP address of Windows Server 2012] -c 100000** and press **Enter** to ping Windows Server 2012 with 100000 packets.

Note: In this lab, the IP address of Windows Server 2012 is 10.0.0.2, which might differ in your lab environment.

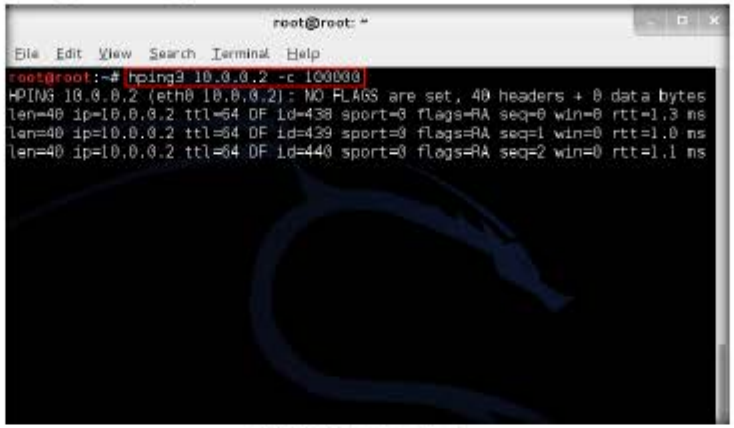


FIGURE 7.20: Performing Flooding

TASK 5

Detect ARP Poisoning/ IP Address Spoofing

32. Now, immediately switch to **Windows 8.1** machine, go to the **Apps** screen, and click **Wireshark** to launch it.

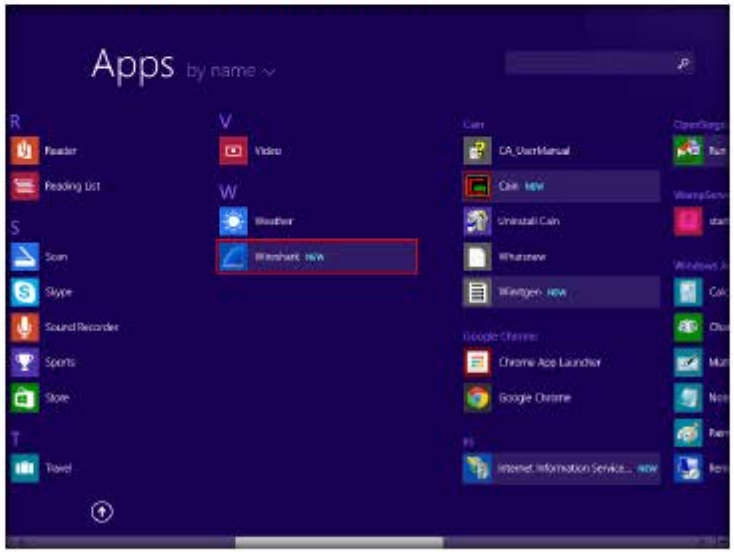


FIGURE 7.21: Launching Wireshark

33. The **Wireshark** main window appears; click **Edit** in the menu bar, and select **Preferences...**.

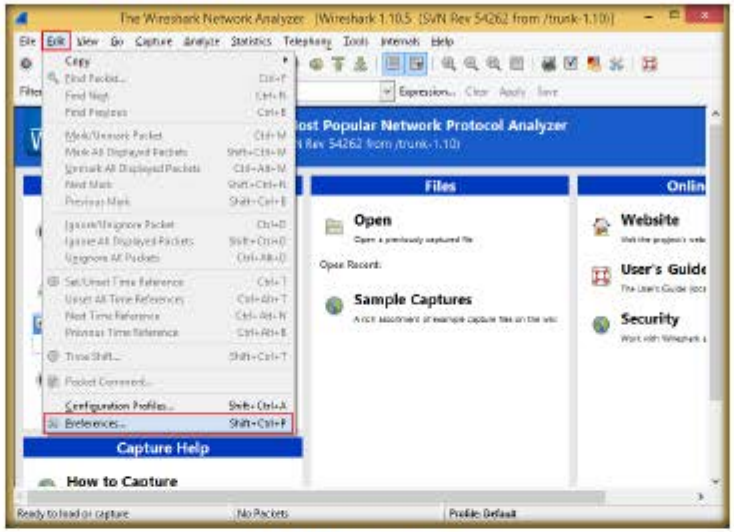


FIGURE 7.22: Launching Preferences

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

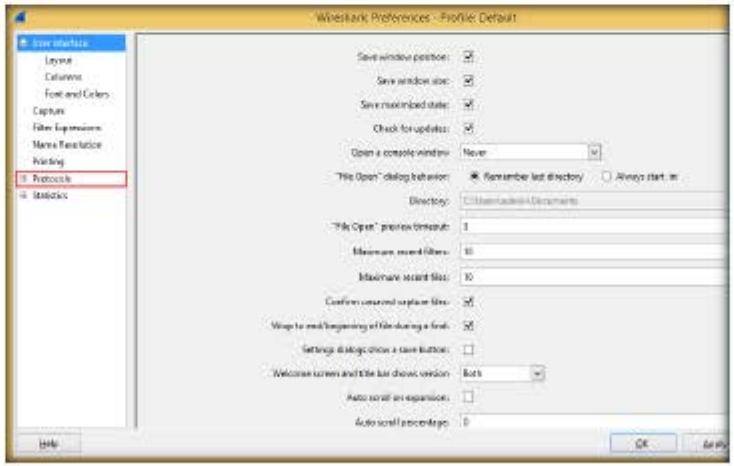


FIGURE 7.23: Viewing Protocols

35. Select the **ARP/RARP** node.
36. Ensure that **Detect ARP request storms** and **Detect duplicate IP address configuration** are checked.
37. Click **Apply**, and then click **OK**.

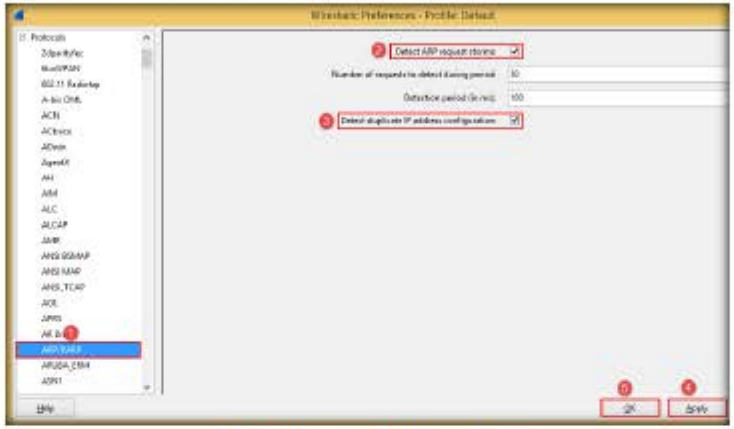


FIGURE 7.24: Configuring ARP Detection Settings

38. Now, select the interface associated with your network, then click **Start**.

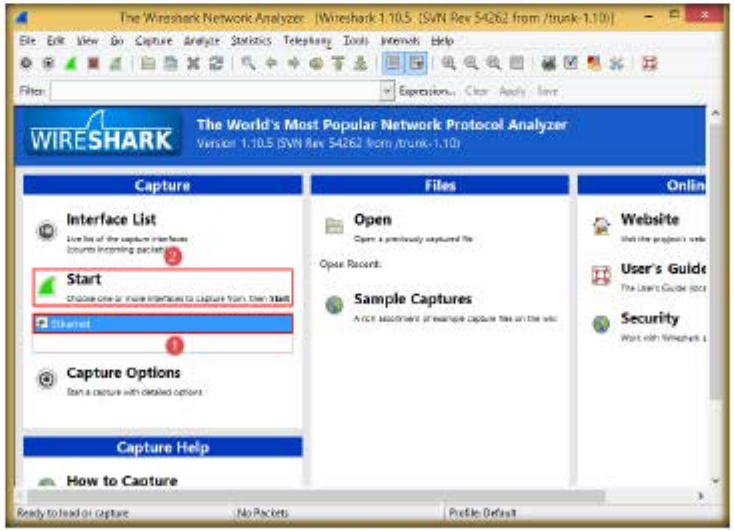


FIGURE 7.25: Starting Capture

39. Wireshark begins to capture traffic between the two machines.

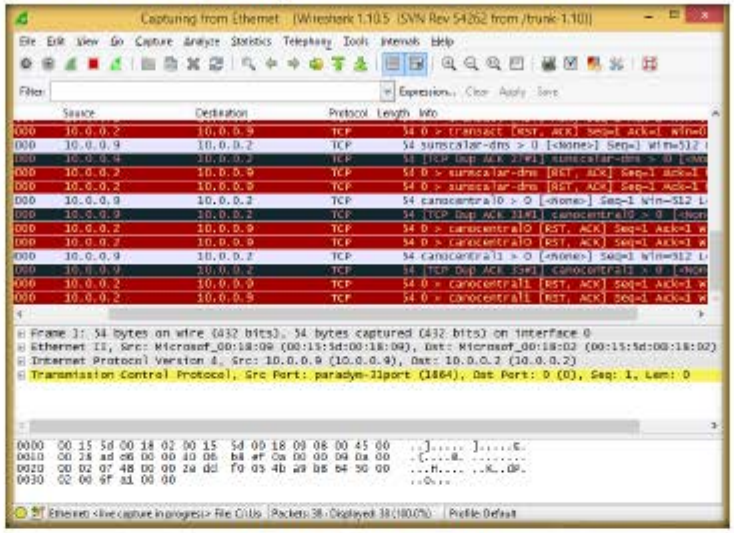


FIGURE 7.26: Wireshark Capturing Packets

40. Switch to Cain & Abel to observe the packets flowing between the two machines.

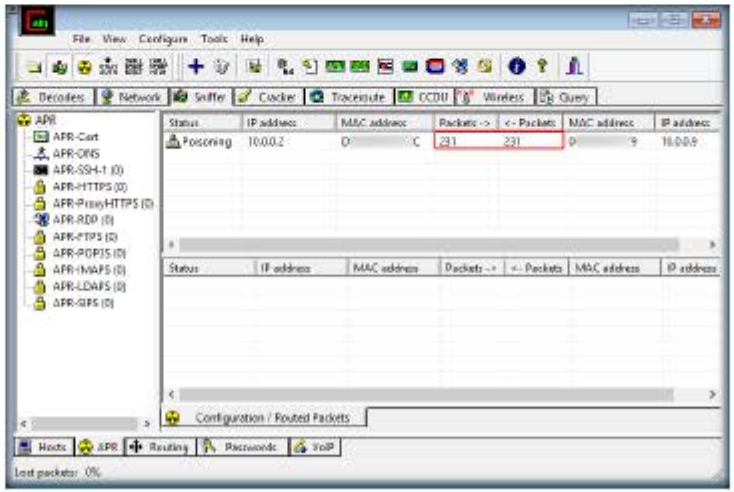


FIGURE 7.27: ARP Poisoning Detected

41. Now, switch to **Wireshark,** and click **Stop** to stop packet capture.

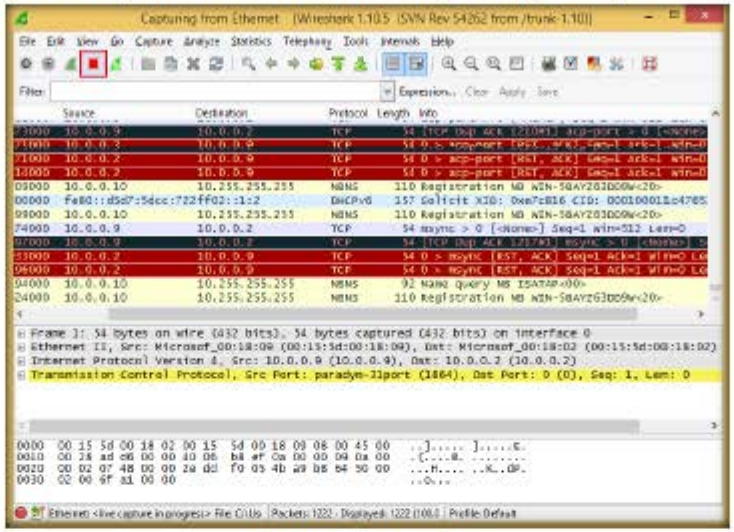


FIGURE 7.28: Stopping Packet Capture

42. Click **Analyze** in the menu bar, and select **Expert Info.**

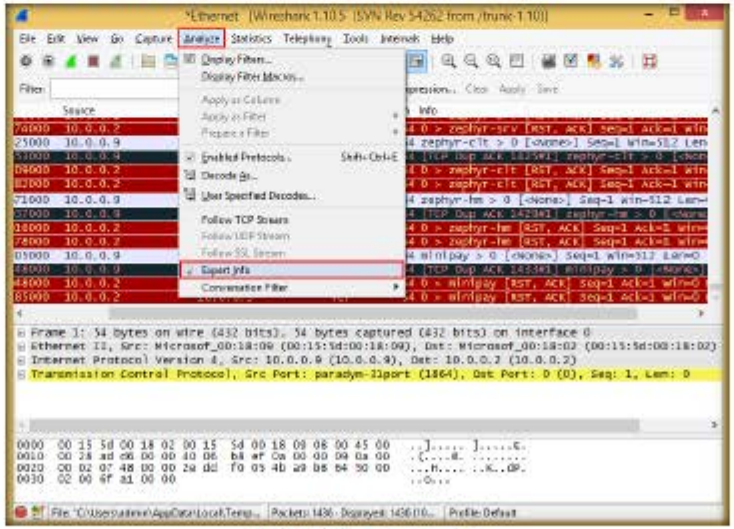


FIGURE 7.29: Analyzing Expert Info

43. The **Expert Infos** window appears; click the **Warnings** tab. Duplicate IP addresses have been configured, using ARP protocol, as shown in the screenshot:

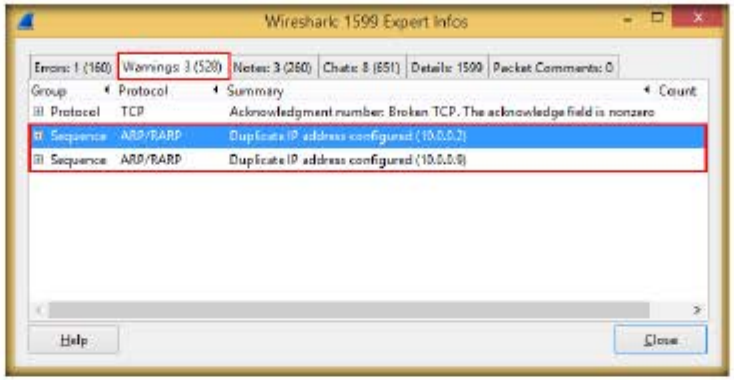


FIGURE 7.30: Viewing Warnings

44. Keep the **Expert Infos** window above the **Wireshark** window, so you can view the **packet** number and the **Packet details** section.
45. Expand a **Sequence** node, and select a packet (here, **108**).
46. On selecting the packet number, Wireshark highlights the packet, and its associated information is displayed under Packet Details.
47. Observe the warnings highlighted in yellow, as shown in the screenshot:

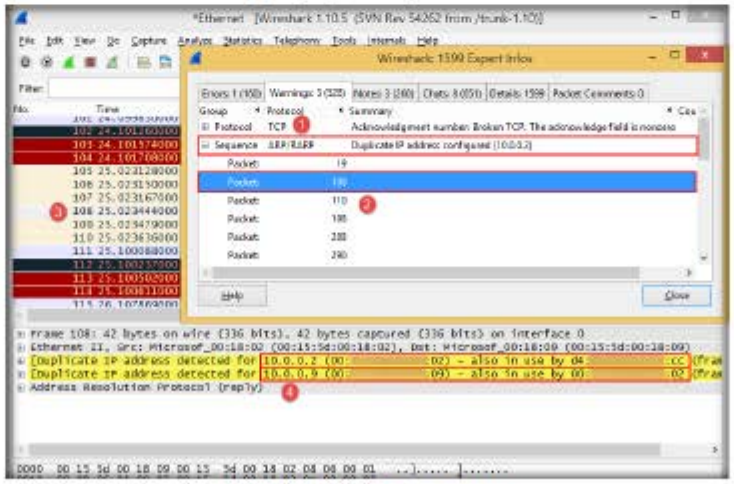


FIGURE 7.31: Duplicate IP Address Detected

48. The yellow warnings indicate that duplicate IP addresses have been detected at one MAC address.
49. One MAC address corresponds to the attacker machine (Windows 8.1) and the other to the target machine.
50. Thus, ARP spoofing has been successfully detected using Wireshark.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

Detecting ARP Attacks with XArp Tool

XArp is a security application that uses advanced techniques to detect ARP-based attacks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Scenario

ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use XArp tool, which has advanced techniques for preventing such attacks and protecting data.

Lab Objectives

The objective of this lab is:

- To detect ARP attacks

Lab Environment

To complete this lab, you will need:

- XArp is located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Spoofing Detection Tools\XArp**
- You can also download the latest version of XArp from http://www.chrismc.de/development/xarp/index.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of XArp

XArp helps users detect ARP attacks and keep their data private. Administrators can use XArp to monitor whole subnets for such attacks. Different security levels and fine-tuning possibilities allow typical and power users to use XArp to detect ARP attacks.

Lab Tasks

TASK 1

Launching the XArp tool

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Spoofing Detection Tools\XArp,** and double-click **xarp-2.2.2-win.exe**.
2. The **Open File - Security Warning** appears; click **Run**.
3. Follow the wizard-driven installation steps to install XArp.

FIGURE 8.1: XArp Installation Wizard

4. On completing the installation, launch XArp from the Apps screen.

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

FIGURE 8.2 Windows Server 2012 - Apps

5. The main window of XArp appears, displaying a list of IPs, MAC addresses, and other information for machines in the network.

A MAC address is a unique identifier for network nodes on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

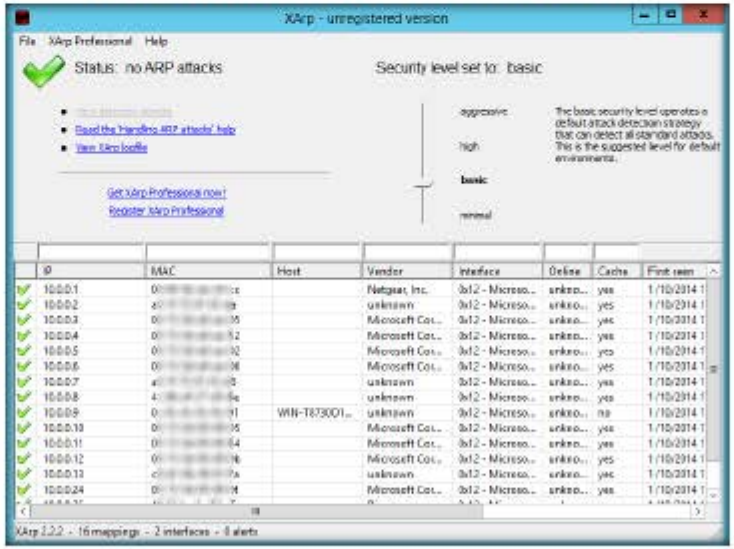


FIGURE 8.3: XArp status when security level set to high

6. On the host machine, XArp displays **no ARP attacks**.

Note: If you observe these results, log onto a virtual machine. You can run Cain & Abel to initiate ARP Poisoning of the host machine.

7. By default, the Security level is set to **basic**; set it to **aggressive**.

An attacker can alter the MAC address of the device that is used to connect the network to Internet and can disable access to the web and other external networks.

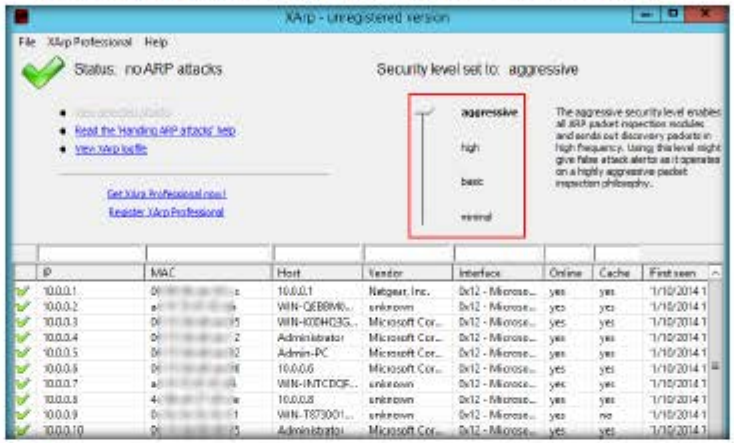


FIGURE 8.4: XArp status when security level set to aggressive

8. Log onto the Windows Server 2008 and Windows 8.1 virtual machines.
9. Perform ARP poisoning using Cain & Abel.

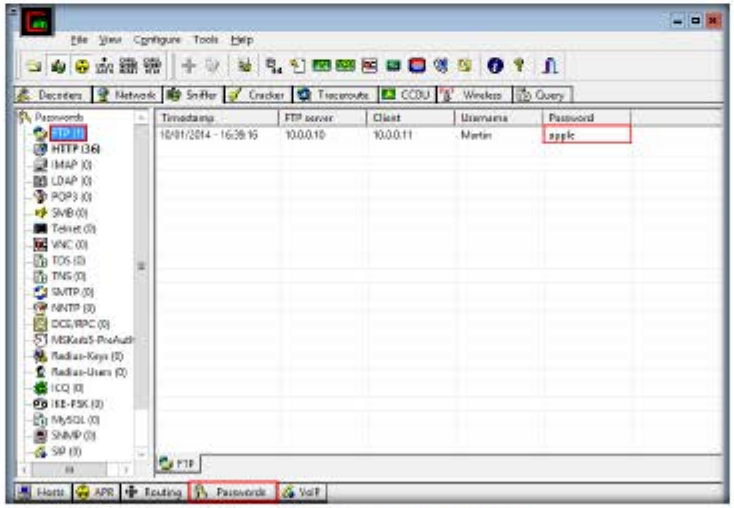


FIGURE 8.5: ARP poisoning using Cain & Abel

10. The XArp pop-up appears, displaying the Alerts.

XArp allows alert filtering for excluding specific hosts. Another feature includes settings for alerting intensity and how the alerts are presented. Also allows sending alerts through email and detailed alerting configuration.

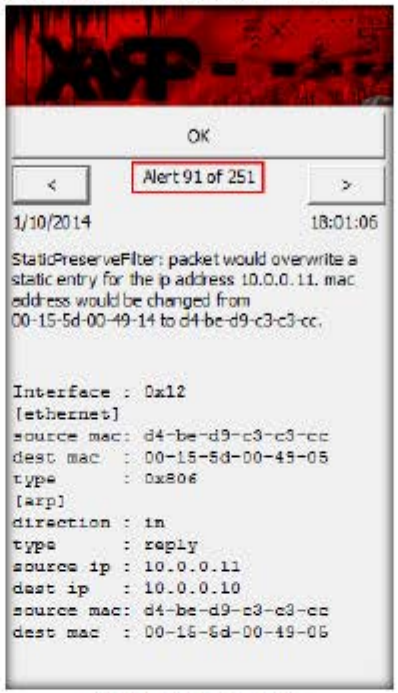


FIGURE 8.6: XArp displaying Alerts

11. The status changes to **ARP attacks detected**.

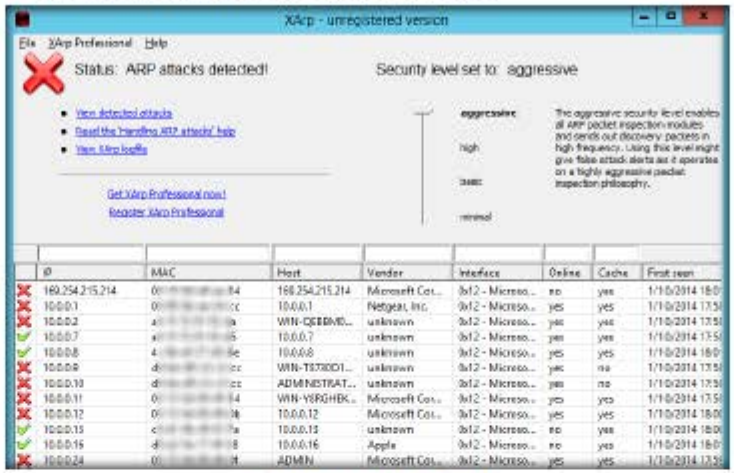


FIGURE 8.7: XArp - ARP attacks detected

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. This only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n*n) ARP caches that have to be configured. AntiARP also provides Windows-based spoofing prevention at the kernel level.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 9

Performing DNS Poisoning in a Switch Based Network

DNS spoofing (or DNS poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer)..

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Hackers employ the DNS Poisoning technique to corrupt the cache of a DNS which translates domain names into IP addresses. Hackers replace the original IP address with those of a server which they control. The ulterior motive of this hack is to redirect the traffic, intended for a particular site, to their servers in order to steal users' data.

On these servers, hackers create a clone website which resembles a bank or an e-commerce site. Users, who are unknowingly redirected to these servers, enter their banking or other financial instrument credentials on the cloned site thus giving it to the hackers.

Lab Objectives

The objective of this lab is to help students understand how to:

- Perform DNS Poisoning on a switch based network

Lab Environment

To perform the lab, you need:

- A computer running with Windows Server 2012 as the host machine
- Windows 8.1 running as a virtual machine

Lab Duration

Time: 10 Minutes

Overview of DNS Poisoning

DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.

Lab Tasks

TASK 1

Install Cain & Abel

1. Log in to Windows 8.1 and Windows Server 2008 virtual machines before starting this lab.
2. Switch to **Windows 8.1** machine, navigate to **Z:\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**, double-click **ca_setup.exe** and follow the wizard driven installation steps to install Cain & Abel.
3. If you have already installed the application, skip to **step no. 6**.

Note:

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

If a **Window Security** dialog box appears asking you to enter the network credentials, type in the following credentials and click **OK**:

User name: **Administrator**

Password: **qwerty@123**

FIGURE 9.1: Installing Cain & Abel

4. During installation, a **WinPcap Installation** pop-up appears, click **Install**

FIGURE 9.2: Installing WinPcap

5. Follow the wizard driven installation steps to install WinPcap

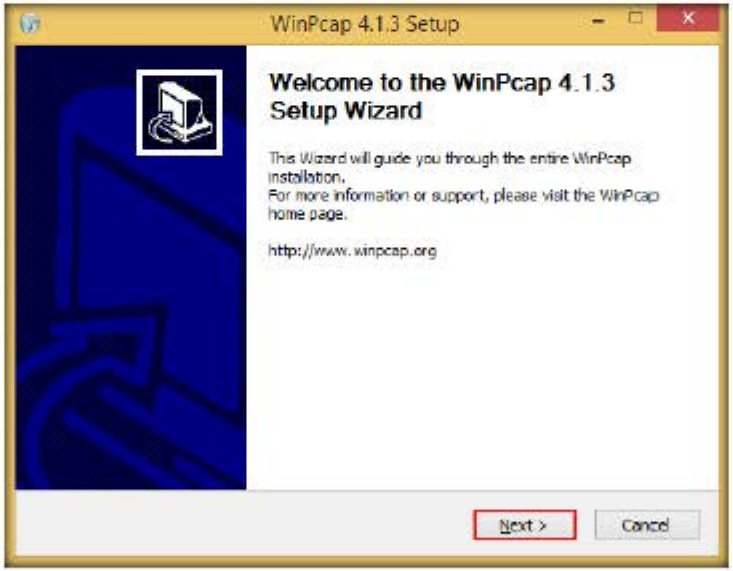


FIGURE 9.3: Installing WinPcap

TASK 2

Perform ARP Poisoning

6. Now, double-click **Cain** icon on **Desktop** in order to launch the application.

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

FIGURE 9.4: Launching Cain & Abel

7. Cain window appears; click **Configure** from the menu bar.

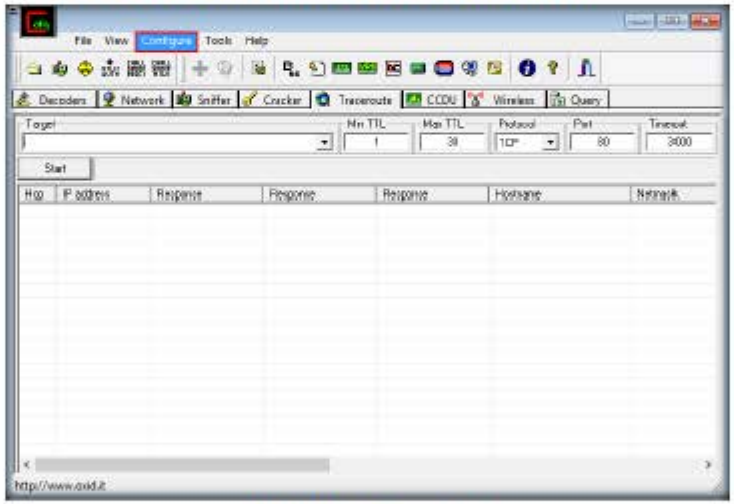


FIGURE 9.5: Configuring Cain & Abel

8. **Configuration Dialog** window appears, click **Sniffer** tab.
9. Select the adapter and click **OK**.

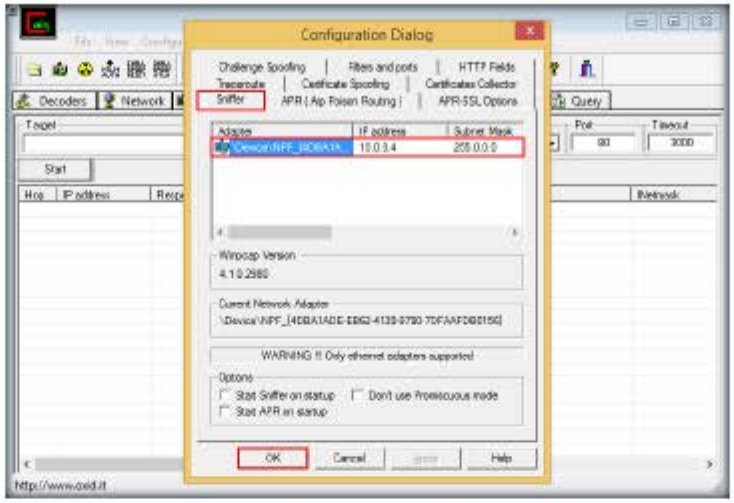


FIGURE 9.6: Configuring Cain & Abel

10. Now, click **Start/Stop Sniffer** icon on the toolbar.

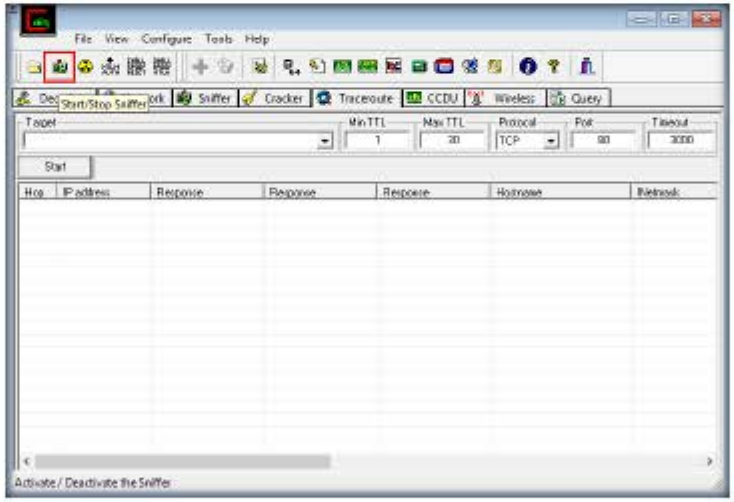


FIGURE 9.7: Starting Sniffer

11. If a **Cain** pop-up appears, click **OK** button.

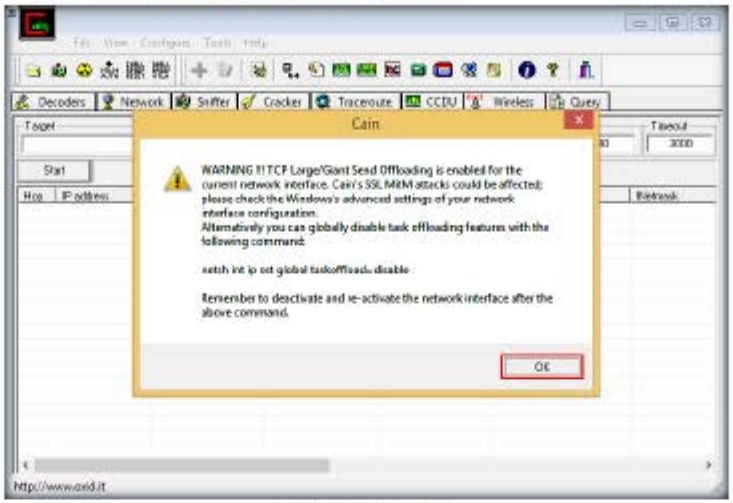


FIGURE 9.8: Cain Pop-Up

12. Click **Sniffer** tab.

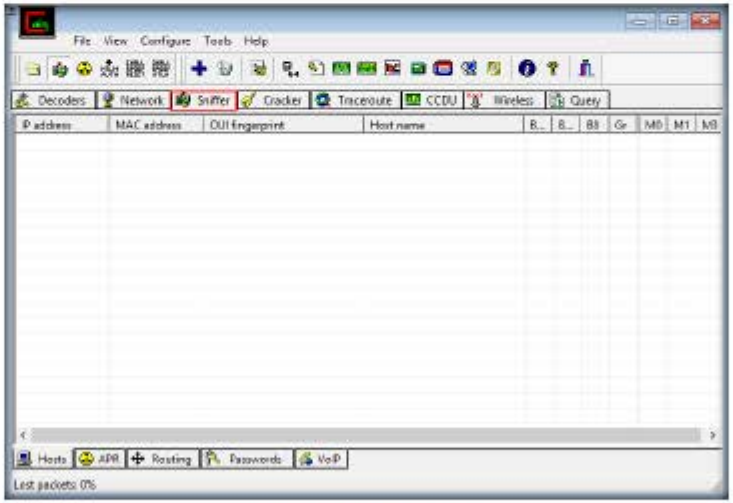


FIGURE 9.9: Clicking Sniffer Tab

13. Click **+** icon on the toolbar.
14. **MAC Address Scanner** window appears, click **Range** radio button.
15. Specify the IP address range on which you want to perform scan (here **10.0.0.1-10.0.0.30** is the IP address range used in this lab. This might vary in your lab environment).
16. Check **All Tests** option and then click **OK**.

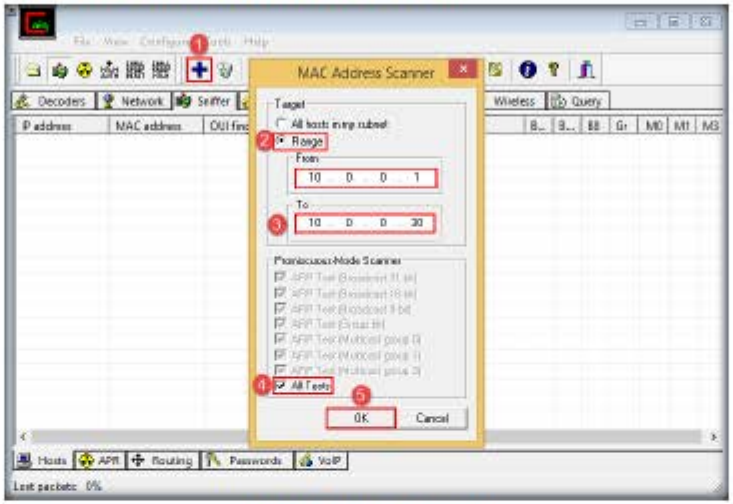


FIGURE 9.10: Scanning MAC Addresses

17. The application begins to perform ARP tests on the above mentioned IP address range and displays the detected address in the Sniffer window as shown in the following screenshot:

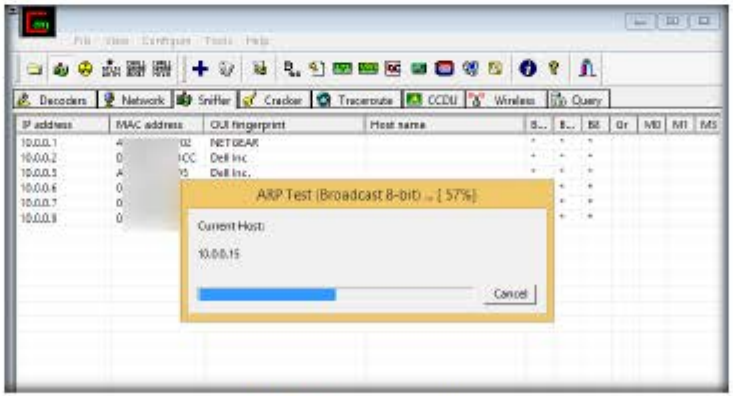


FIGURE 9.11: Scanning MAC Addresses

18. On completing the ARP tests, all the MAC and their associated IP addresses that responded to the ARP requests are displayed as shown in the following screenshot:

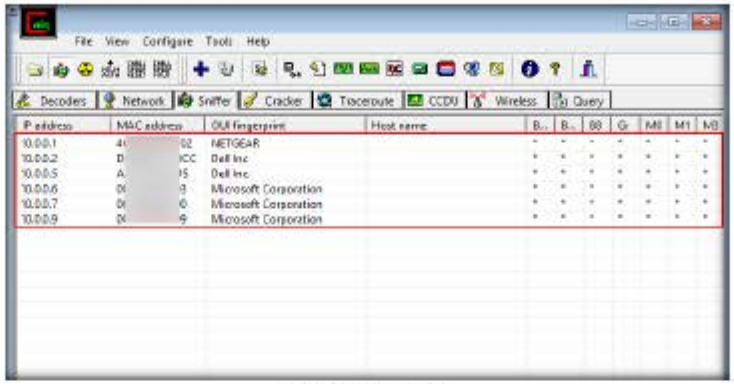


FIGURE 9.12: Sniffer Tab

19. Now, click **APR** tab at the lower section of the screen.
20. Click anywhere on the top most section in the right-hand pane under the Sniffer tab to activate the **+** icon
21. Once the **+** icon is activated, click it.

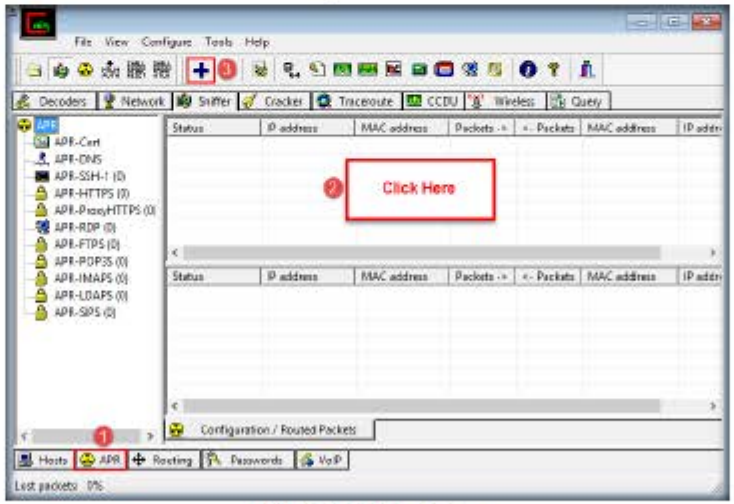


FIGURE 9.13: ARP Poison Routing

22. **New ARP Poison Routing** window appears. Now, you need to select the machines whose data exchange you want to intercept.

23. Select the first target (here **10.0.0.4** which refers to **Windows Server 2008** machine) from the list of IP addresses displayed in the left-hand pane.

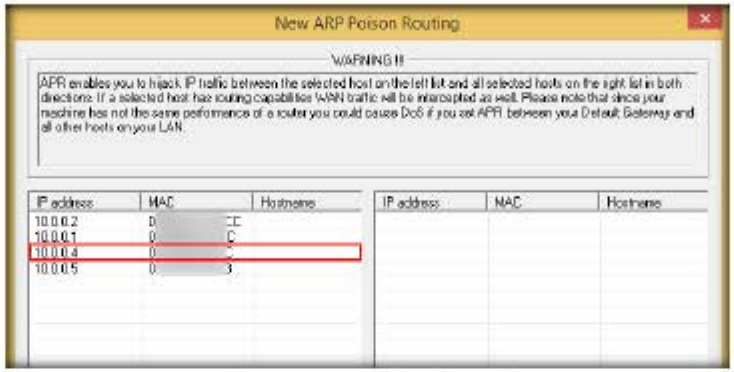


FIGURE 9.14: New ARP Poison Routing Window

Note: The IP Address of **Windows Server 2008** virtual machine might vary in your lab environment.

24. Upon selecting the first target, a list of IP addresses excluding the first target, appears in the right-hand pane.
25. You need to select the second target IP address (here **10.0.0.1** which refers to the **router**) from the right-hand pane. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.
26. Click **OK**.

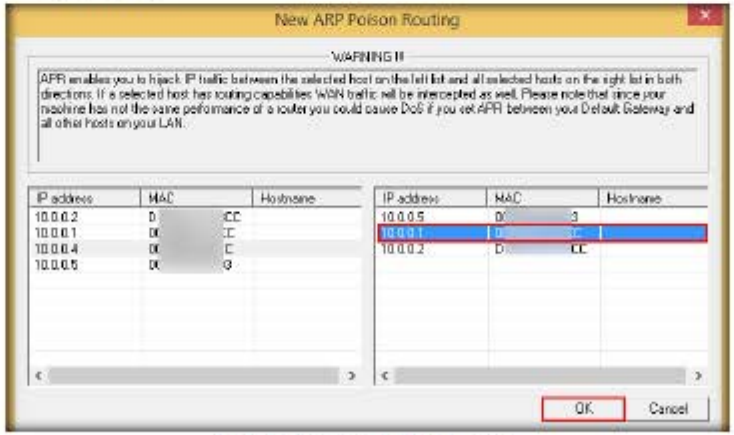


FIGURE 9.15: Performing ARP Poison Routing

27. Now all the requests sent from the **Windows Server 2008** machine pass through the router.
28. At this point, the selected targets appear in the top section under Sniffer tab.

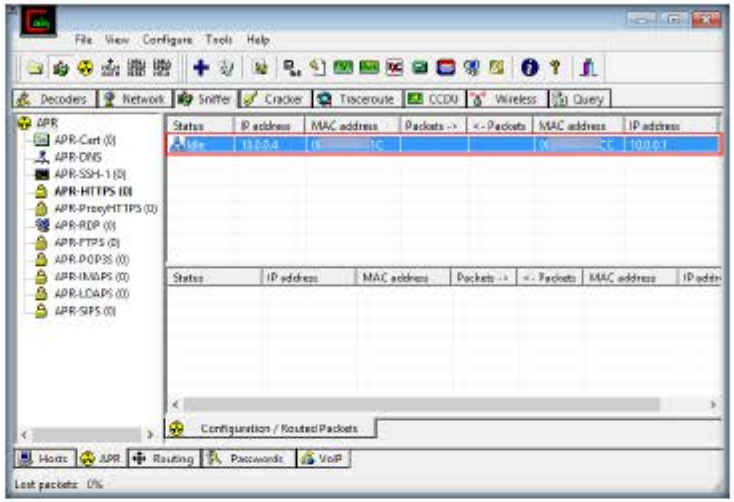


FIGURE 9.16: Performing ARP Poison Routing

29. In the same way, follow the steps **19-26** to perform ARP poison routing between **Kali Linux** virtual and the router.

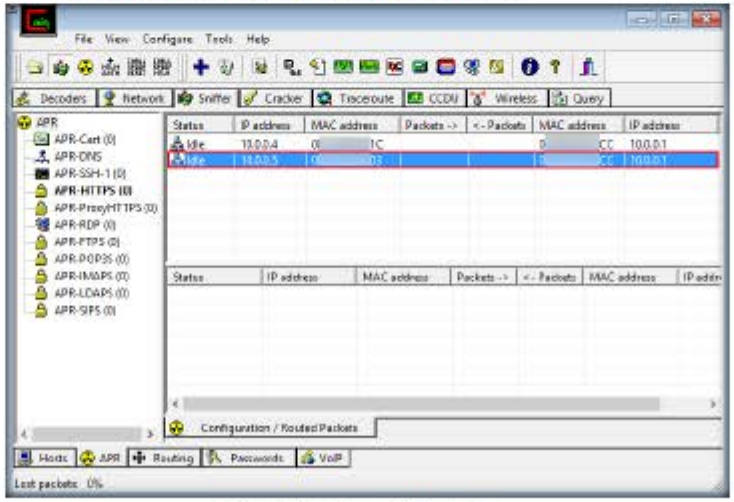


FIGURE 9.17: Performing ARP Poison Routing

TASK 3

Perform DNS Poisoning

30. In this lab, we are going to perform DNS poisoning on both **Windows Server 2008** and **Kali Linux** virtual machines.
31. Click **APR-DNS** from the left-hand pane. When the APR-DNS section appears, right-click anywhere inside the section. A context menu appears; select **Add to list** option.

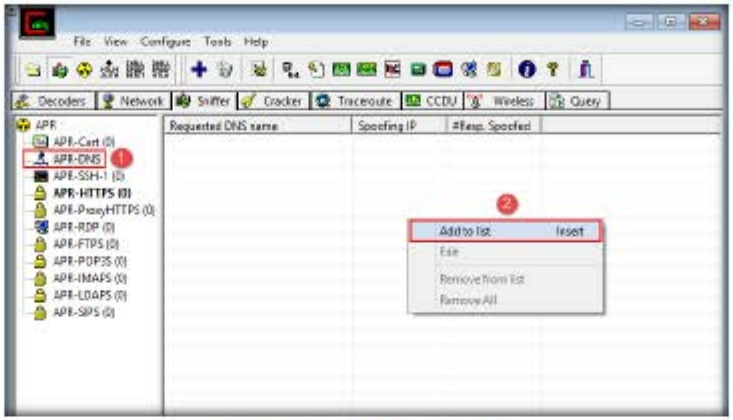


FIGURE 9.18: Configuring DNS Poison Routing

32. **DNS Spoofer for APR** dialog box appears, enter the target domain name (here **www.certifiedhacker.com**) in **DNS Name Required** field and click the **Resolve** button.

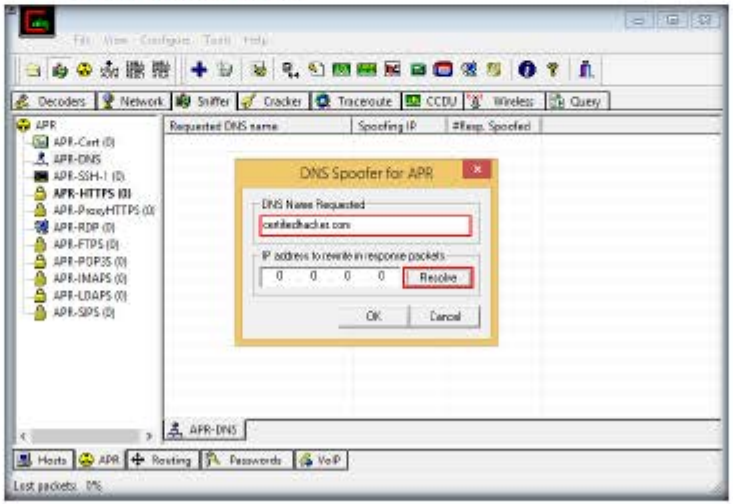


FIGURE 9.19: Configuring DNS Poison Routing

33. **Hostname to Resolve** dialog box appears, enter a domain name (here **www.google.com**) and click **OK**.

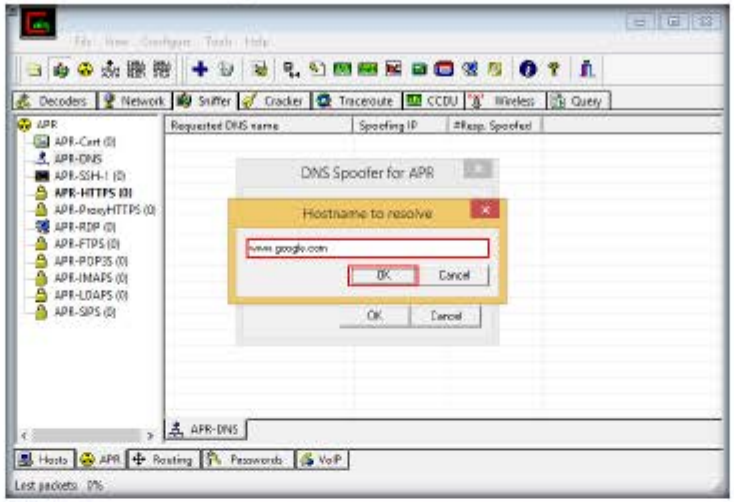


FIGURE 9.20: Configuring DNS Poison Routing

34. The application automatically translates the domain name to its corresponding IP Address.

35. Click **OK**.

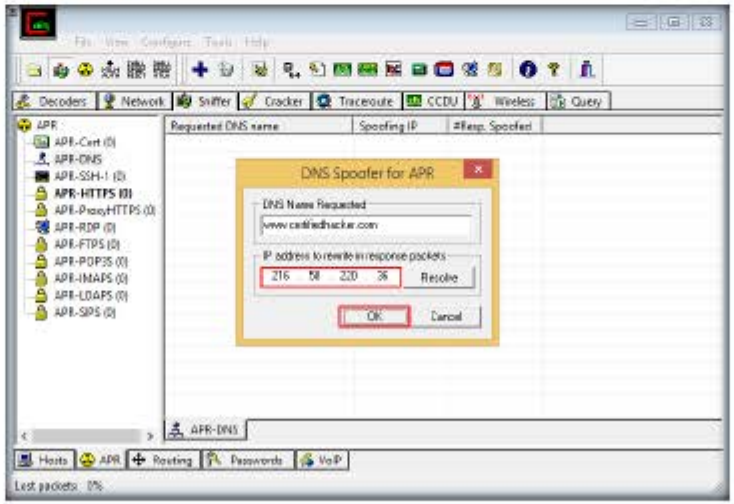


FIGURE 9.21: Configuring DNS Poison Routing

36. By doing so, whenever a user victim attempts to browse www.certifiedhacker.com website, he/she will be redirected to www.google.com, resulting in DNS spoofing/poisoning.
37. The Requested DNS appears in the APR-DNS section.

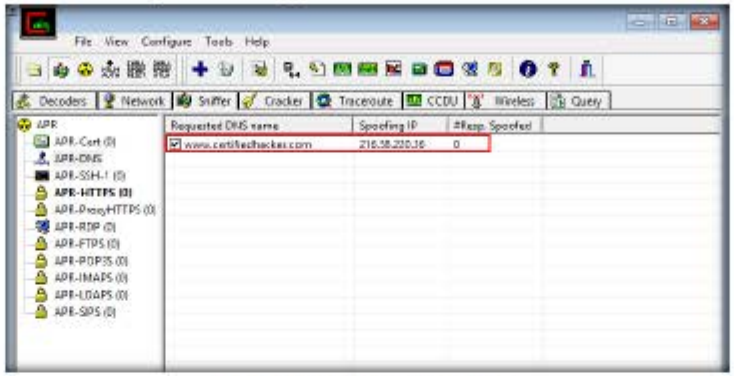


FIGURE 9.22: DNS Poison Routing Configured

38. Now you are all set to perform DNS poisoning on the victim machines Windows Server 2008 and Kali Linux.
39. Click **APR** in the left-hand pane. The ARP Poison routing section appears, click Start/Stop APR button on the toolbar to begin DNS poisoning along with ARP poisoning.

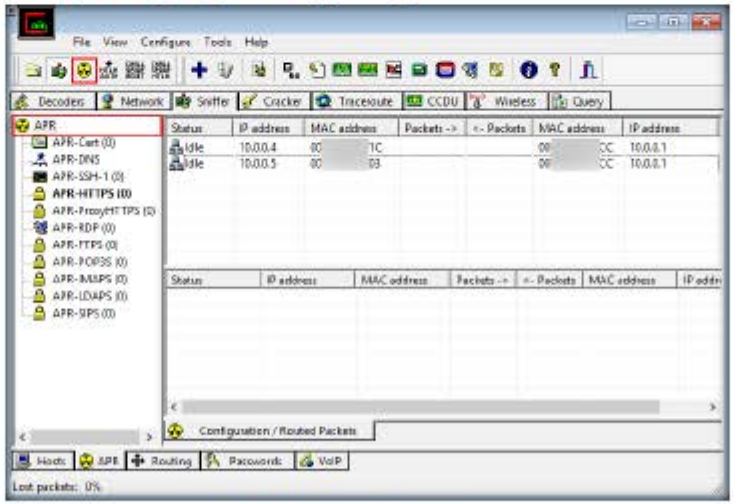


FIGURE 9.23: Initiating ARP Poison Routing

40. Now switch to **Windows Server 2008** virtual machine, launch Mozilla firefox web browser, type the URL **www.certifiedhacker.com** in the address bar and press **Enter**.

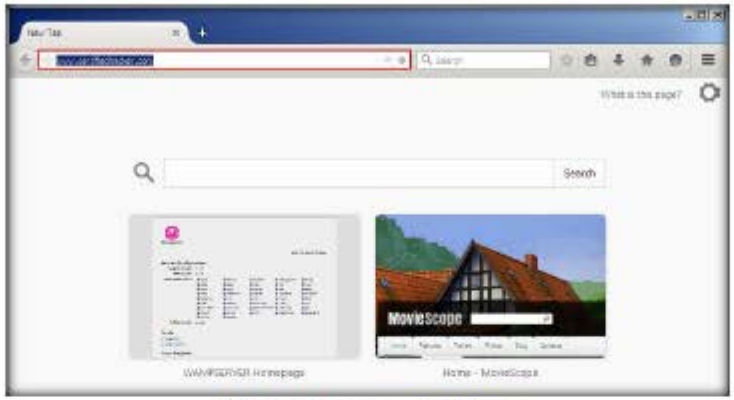


FIGURE 9.24: Browsing www.certifiedhacker.com

41. You will be redirected to **google** webpage instead of **certifiedhacker** homepage, confirming that DNS poisoning was successful.

Note: If a webpage appears stating that the connection is not trusted, click **I Understand the Risks**. Scroll down the webpage and click **Add Exception...** button. **Add Security Exception** window appears, click **Confirm Security Exception** button.

FIGURE 9.25: DNS Poisoning Performed

42. In the same way, you may attempt to browse **www.certifiedhacker.com** on **Kali Linux** machine.
43. You will be redirected www.google.com as shown in the following screenshot:

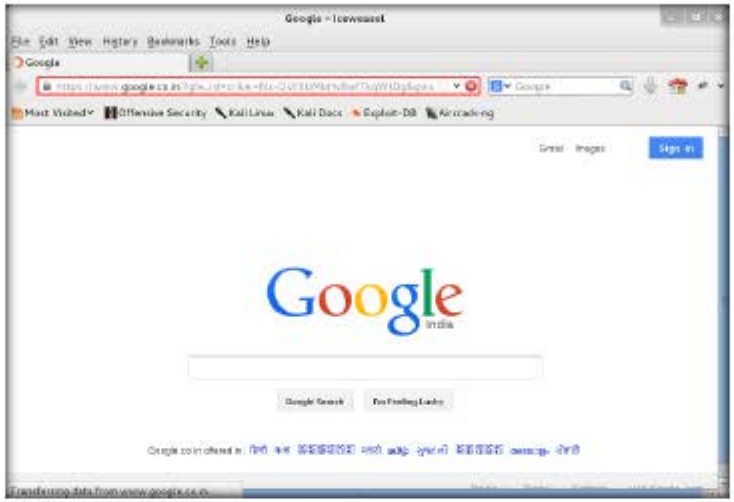


FIGURE 9.26: DNS Poisoning Performed

44. Thus, you have successfully performed DNS poison routing on the victim machines.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs