

Sniffers

Module 08

Sniffing a Network

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Sniffing is a technique used to **intercept data** in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to **steal data**, such as sensitive information, email text, etc.

Network sniffing involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A **packet sniffer** is also referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same.

Similarly, sniffing tools can be used by attackers in **promiscuous** mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the **user name** and **password** information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for a network administrator to be familiar with **network traffic analyzers** and he or she should be able to **maintain** and **monitor** a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, **ARP poisoning**, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Lab Objectives

The objective of this lab is to familiarize students with how 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

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

- Secure the network from attacks

Lab Environment

In this lab, you need:

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

Lab Duration

Time: 80 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 information, system information, 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 perhaps a nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing the network using the **Colasoft Packet Builder**
- Sniffing the network using the **OmniPeek Network Analyzer**
- Spoofing MAC address using **SMAC**
- Sniffing the network using the **WinArpAttacker** tool
- Analyzing the network using the **Colasoft Network Analyzer**
- Sniffing passwords using **Wireshark**
- Performing man-in-the-middle attack using **Cain & Abel**
- Advanced ARP spoofing detection using **XArp**
- Detecting Systems running in promiscuous mode in a network using **PromqryUI**
- Sniffing a password from captured packets using **Sniff – O – Matic**

Lab Analysis

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

Module 08 – Sniffers

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



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

In this lab, you need:

 **Tools** demonstrated in this lab are available in **D:\CEH-Tools\CEHv8 Module 08 Sniffing**

- **OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link http://www.wildpackets.com/products/omnipeek_network_analyzer
- 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** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install **OmniPeek682demo.exe**
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of OmniPeekNetwork 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, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, video to remote offices, and 802.

Lab Tasks

TASK 1

Installing OmniPeek Network Analyzer

1. Install **OmniPeek Network Analyzer** on the host machine **Windows Server 2012**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

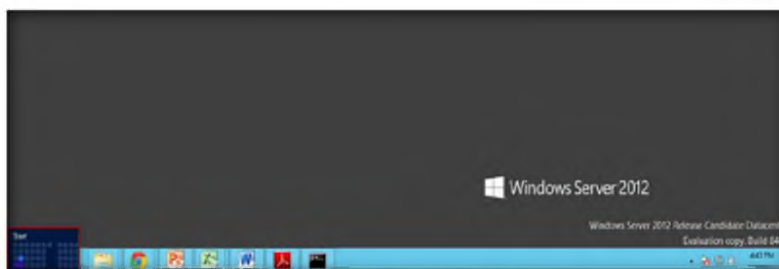


FIGURE 1.1: Windows Server 2012 – Desktop view

3. Click the **WildPackets OmniPeek Demo** app in the **Start** menu to launch the tool.

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

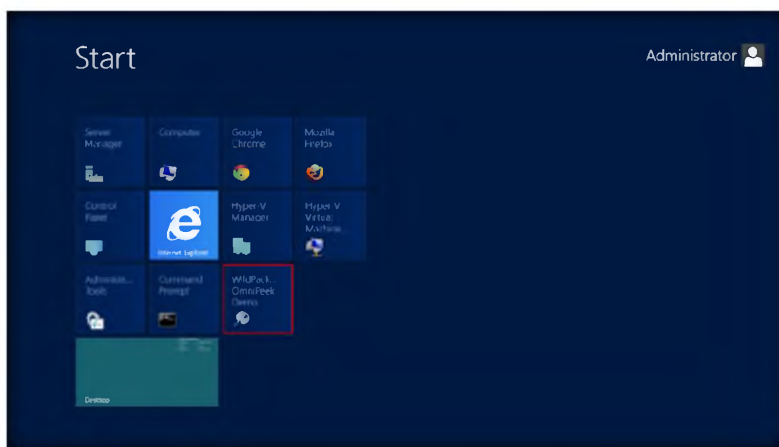


FIGURE 1.2: Windows Server 2012 – Start menu

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

4. The main window of **WildPackets OmniPeek Demo** appears, as shown in the following screenshot.

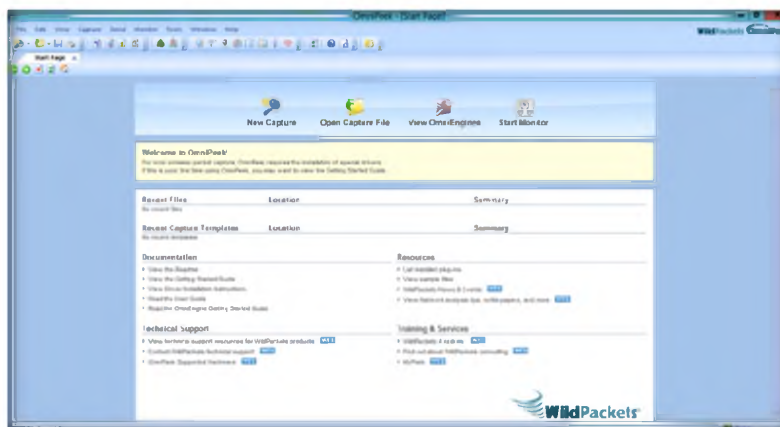


FIGURE 1.3: OmniPeek main screen

5. **Launch** Windows 8 Virtual Machine.
6. Now, in **Windows Server 2012** create an OmniPeek capture window as follows:
 - a. Click the **New Capture** icon on the main screen of OmniPeek.
 - b. View the **General** options in the **OmniPeek Capture Options** dialog box when it appears.
 - c. Leave the default general settings and click **OK**.

TASK 2

Starting New Capture

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

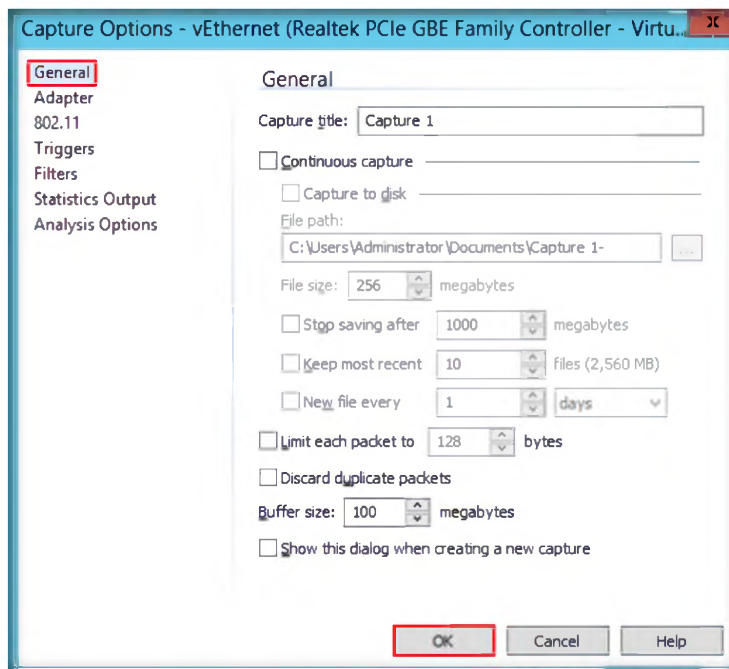


FIGURE 1.4: OmniPeek capture options - General

- d. Click **Adapter** and select **Ethernet** in the list for **Local machine**. Click **OK**.

 **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.

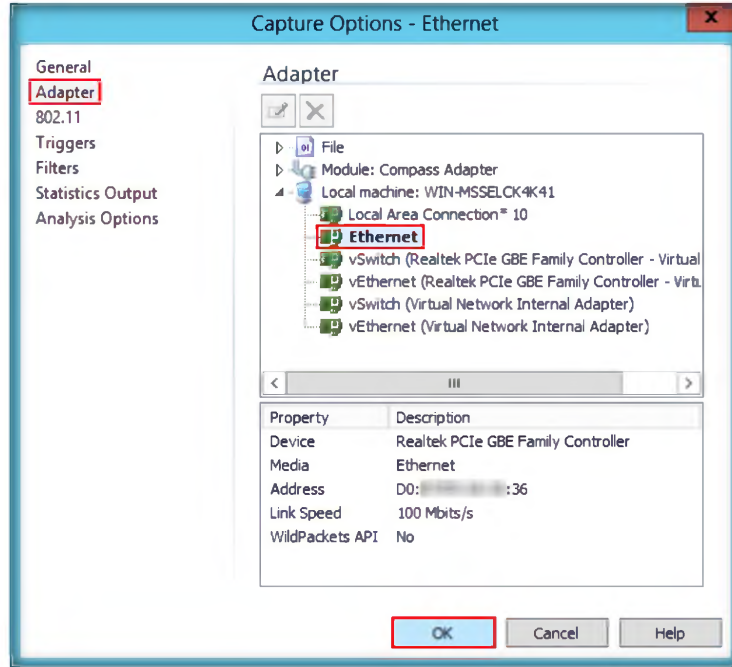


FIGURE 1.5: OmniPeek capture options - Adapter

7. 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** in the capture window of OmniPeek.

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

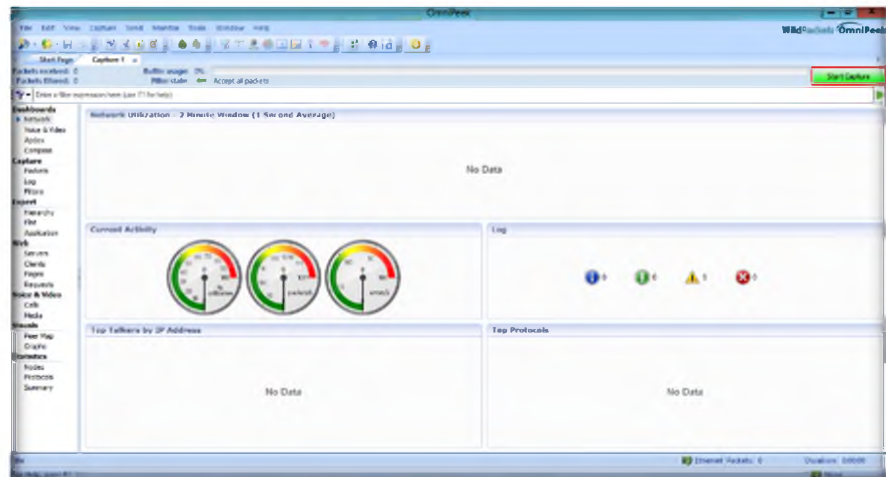


FIGURE 1.6: OmniPeek creating a capture window

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.

8. The captured statistical analysis of the data is displayed on the **Capture** tab of the navigation bar.

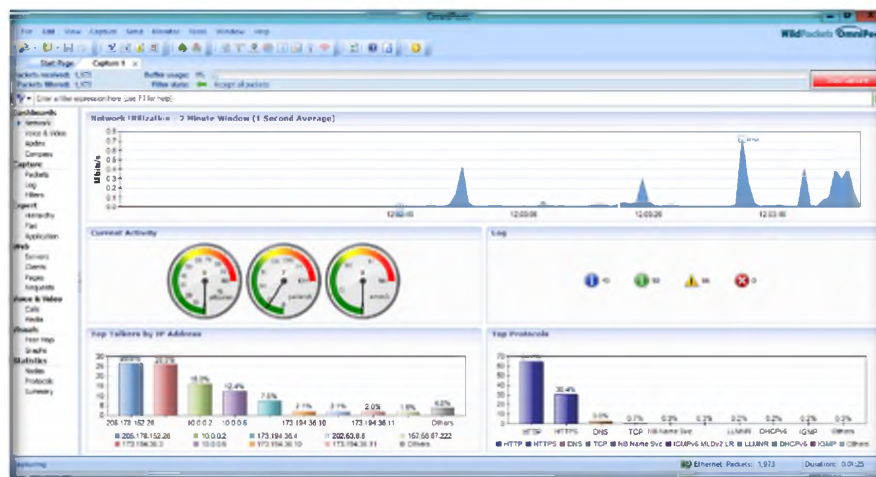


FIGURE 1.7: OmniPeek statistical analysis of the data

9. To view the captured packets, select **Packets** in a **Capture** section of the **Dashboard** in the left pane of the window.

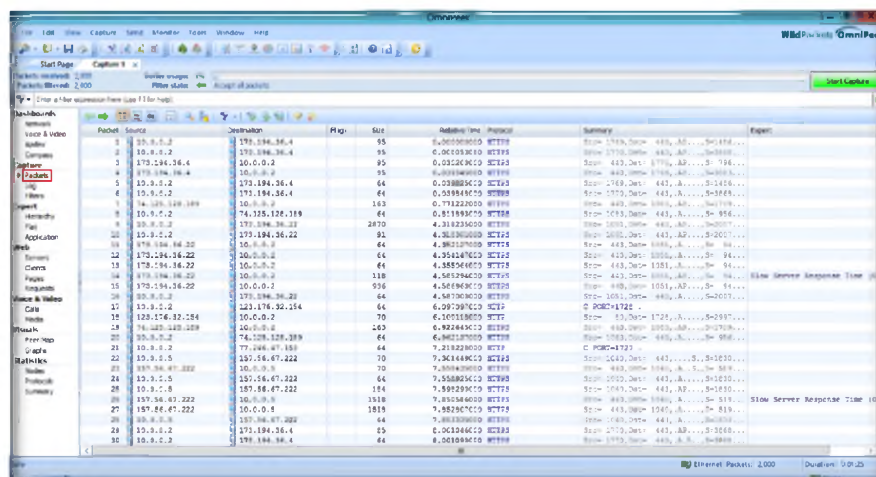


FIGURE 1.8: OmniPeek displaying Packets captured

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.

10. Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard**.
11. You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

Module 08 – Sniffers

 **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.

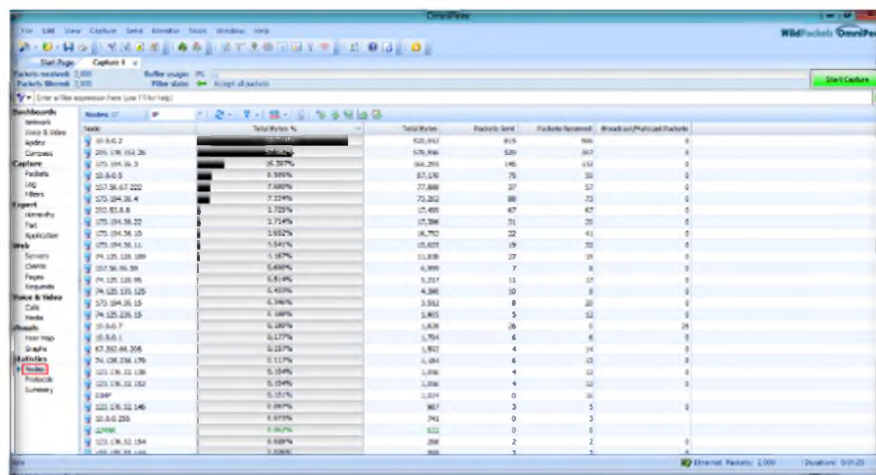


FIGURE 1.9: OmniPeek statistical reports of Nodes

12. 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.

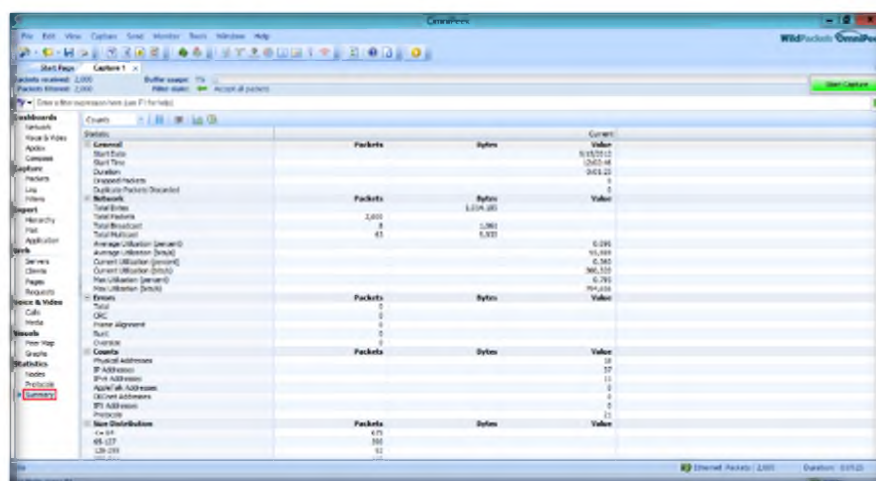


FIGURE 1.10: OmniPeek Summary details

13. To **save** the result, select **File→Save Report**.

Module 08 – Sniffers

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

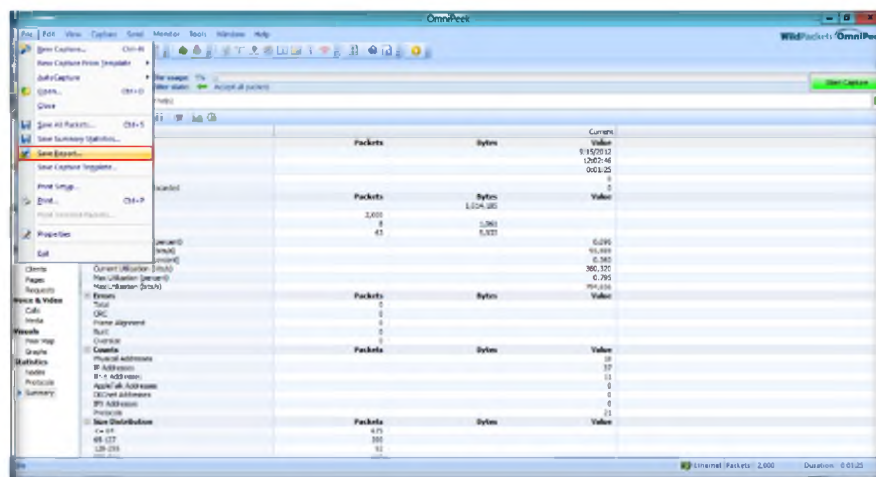


FIGURE 1.11: OmniPeek saving the results

14. Choose the format of the report type from the **Save Report** window and then click **Save**.

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

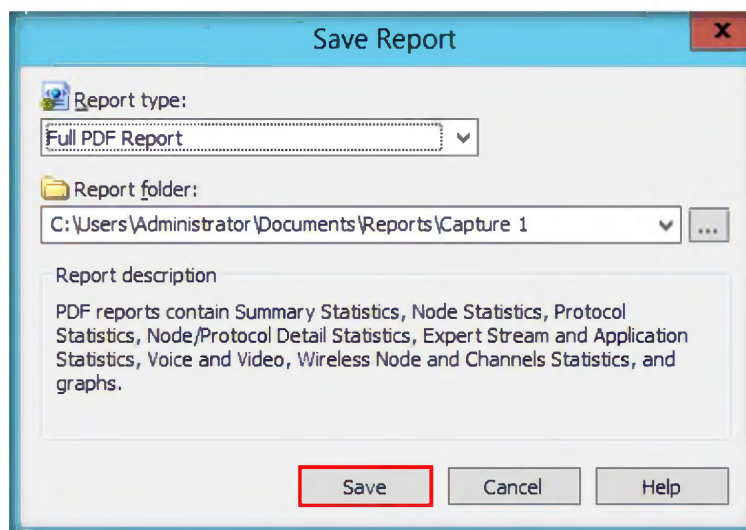


FIGURE 1.12: OmniPeek Selecting the Report format

FIGURE 1.12: OmniPeek Selecting the Report format

15. The report can be viewed as a PDF.

Module 08 – Sniffers

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.

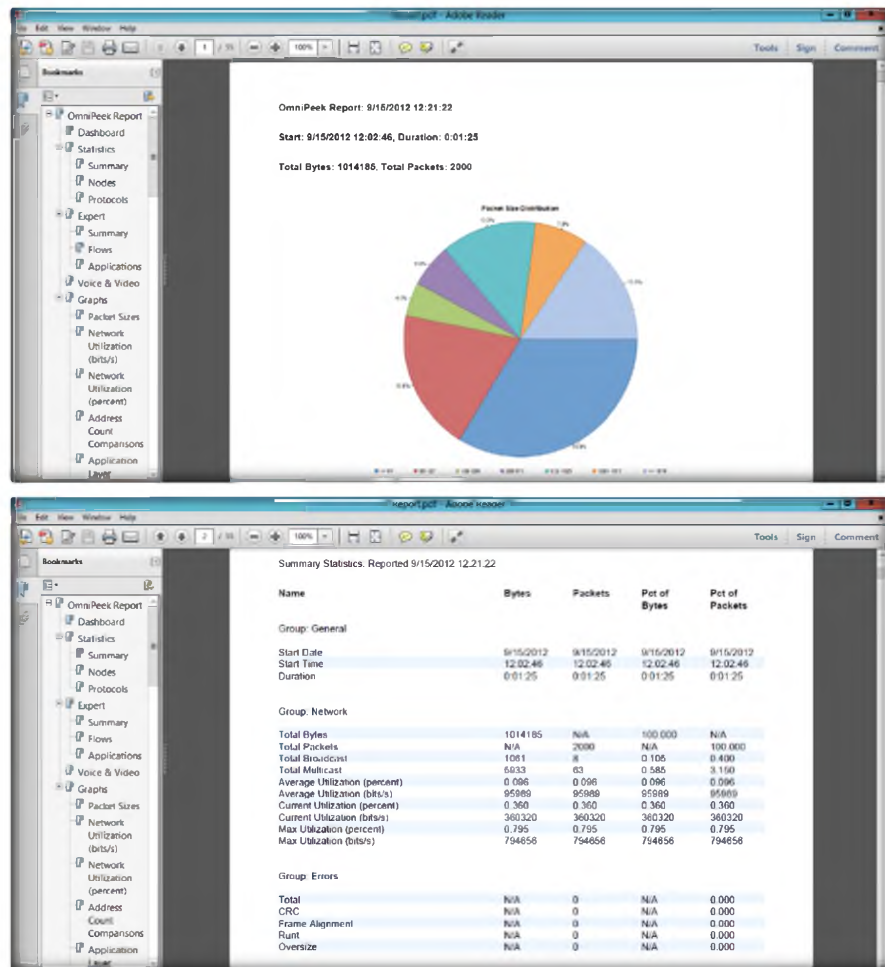


FIGURE 1.13: OmniPeek Report in PDF format

Lab Analysis

Analyze and document the results related to the lab exercise.

Module 08 – Sniffers

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	Network Information: ▪ Network Utilization ▪ Current Activity ▪ Log ▪ Top Talkers by IP Address ▪ Top Protocols
	Packets Information: ▪ Source ▪ Destination ▪ Size ▪ Protocol
	Nodes Statistics: ▪ Total Bytes for a Node ▪ Packets Sent ▪ Packets Received ▪ Broadcast/Multicast Packets
	Summary includes Information such as: ▪ General ▪ Network ▪ Errors ▪ Counts ▪ Size Distribution

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

Questions

1. Analyze what 802.11n adapters are supported in OmniPeek Network Analyzer.
2. Determine how you can use the OmniPeek Analyzer to assist with firewall rules.
3. Evaluate how you create a filter to span multiple ports.

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

Lab

2

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool that is a MAC address changer (spoofers). 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

In the previous lab you learned how to use OmniPeek Network Analyzer to capture network packets and analyze the packets to determine if any vulnerability is present in the network. If an attacker is able to capture the network packets using such tools, he or she can gain information such as packet source and destination, total packets sent and received, errors, etc., which will allow the attacker to analyze the captured packets and exploit all the computers in a network.

If an administrator does not have a certain level of working skills of a packet sniffer, it is really 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 examine 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\CEHv8
Module 08
Sniffing**

In the lab, you need:

- **SMAC** located at **D:\CEH-Tools\CEHv8 Module 08 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**
- Double-click **smac27beta_setup.exe** and follow the wizard-driven installation steps to install SMAC
- **Administrative** privileges to run tools
- A web browser with Internet access

Lab Duration

Time: 10 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 2003 systems, regardless of whether the manufacturers allow this option.

Spoofing a 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 available these days and wireless networks use MAC addresses to **communicate**. Wireless network security and privacy is all about 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

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

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

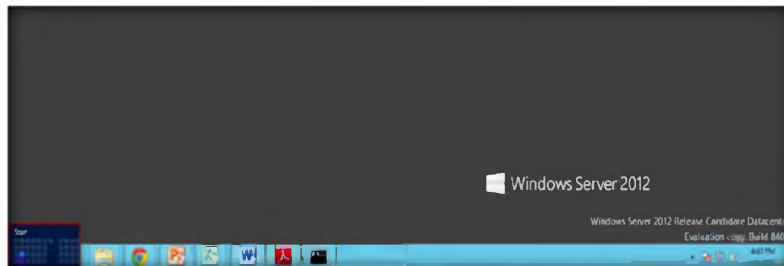


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **SMAC 2.7** app in the **Start** menu to launch the tool.

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."

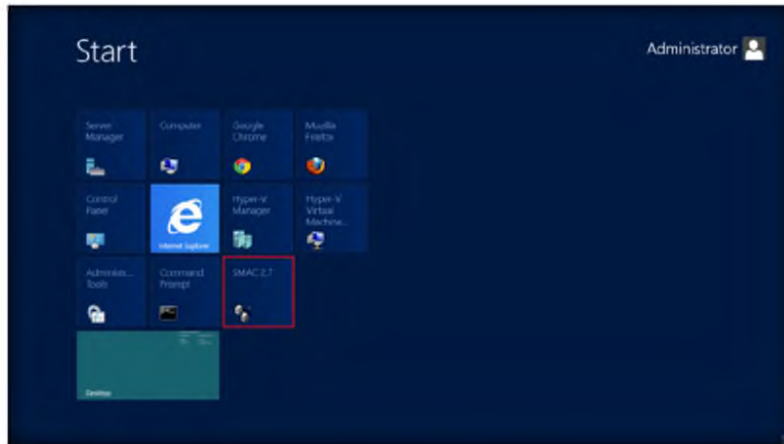


FIGURE 2.2: Windows Server 2012 – Start menu

TASK 1

Spooing MAC Address

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

3. The **SMAC** main screen appears. Choose a network adapter to spoof a MAC address.

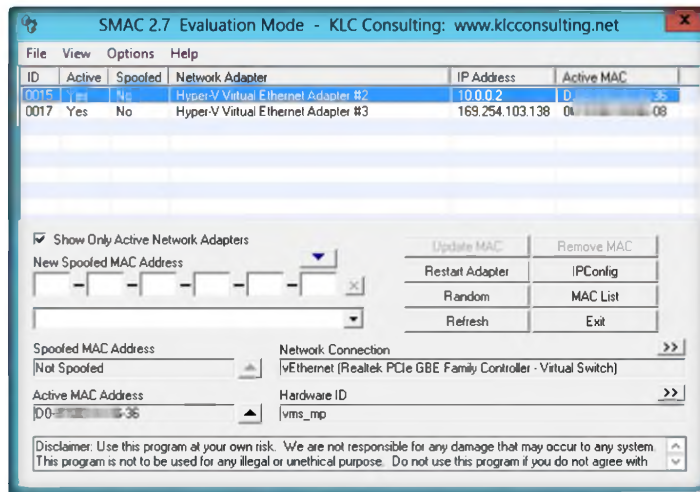


FIGURE 2.3: SMAC main screen

4. To generate a random MAC address, **Random**.

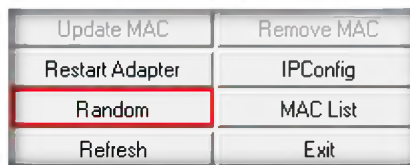


FIGURE 2.4: SMAC Random button to generate MAC addresses

5. Clicking the **Random** button also inputs the **New Spoofed MAC Address** to simply MAC address spoofing.

Module 08 – Sniffers

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 etc.

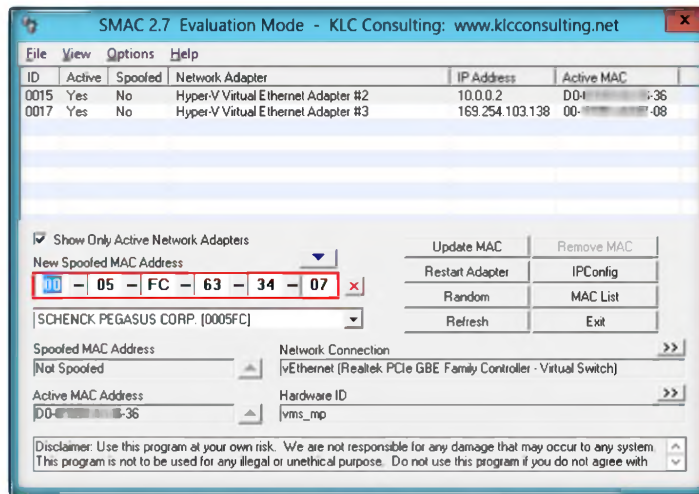


FIGURE 2.5: SMAC selecting a new spoofed MAC address

6. The Network Connection or Adapter display their respective names.
7. Click the forward arrow button in **Network Connection** to display the **Network Adapter** information.



FIGURE 2.6: SMAC Network Connection information

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



FIGURE 2.7: SMAC Network Adapter information

9. Similarly, the Hardware ID and Configuration ID display their respective names.
10. Click the forward arrow button in **Hardware ID** to display the **Configuration ID** information.



FIGURE 2.8: SMAC Hardware ID display

11. Clicking the backward arrow button in **Configuration ID** will again display the **Hardware ID** information. These buttons allow to toggle between the Hardware ID and Configuration ID information.

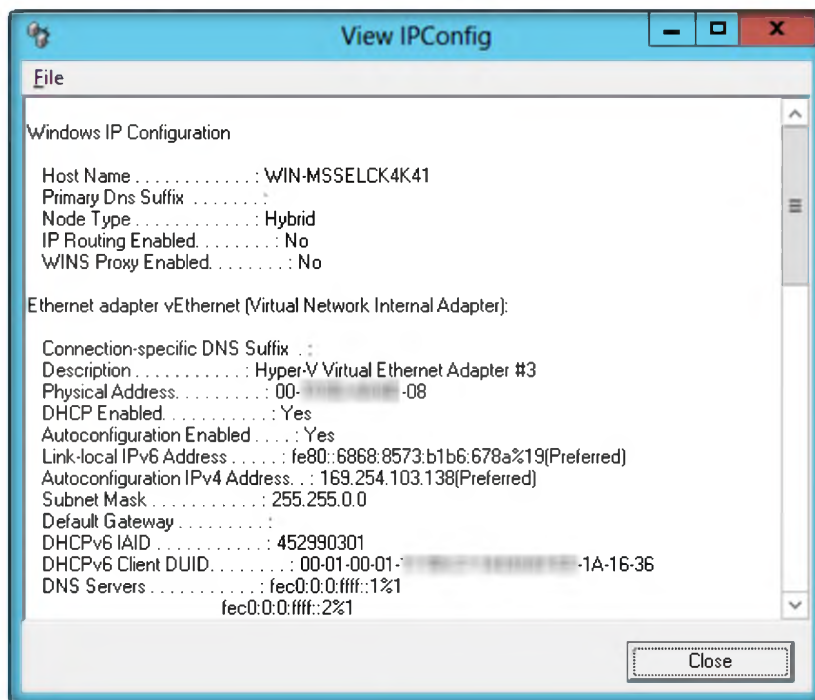


FIGURE 2.9: SMAC Configuration ID display

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.

- | | |
|-----------------|-----------------|
| Update MAC | Remove MAC |
| Restart Adapter | IPConfig |
| Random | MAC List |
| Refresh | Exit |

13. The **IPConfig** window pops up, and you can also save the information by clicking the **File** menu at the top of the window.



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

Update MAC	Remove MAC
Restart Adapter	IPConfig
Random	MAC List
Refresh	Exit

FIGURE 2.12: 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.

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

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

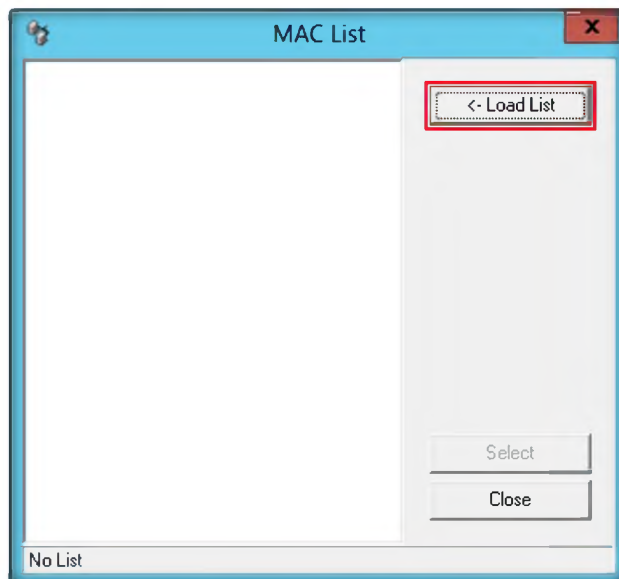


FIGURE 2.13 SMAC MAC List window

16. Select the **Sample_MAC_Address_List.txt** file from the **Load 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.

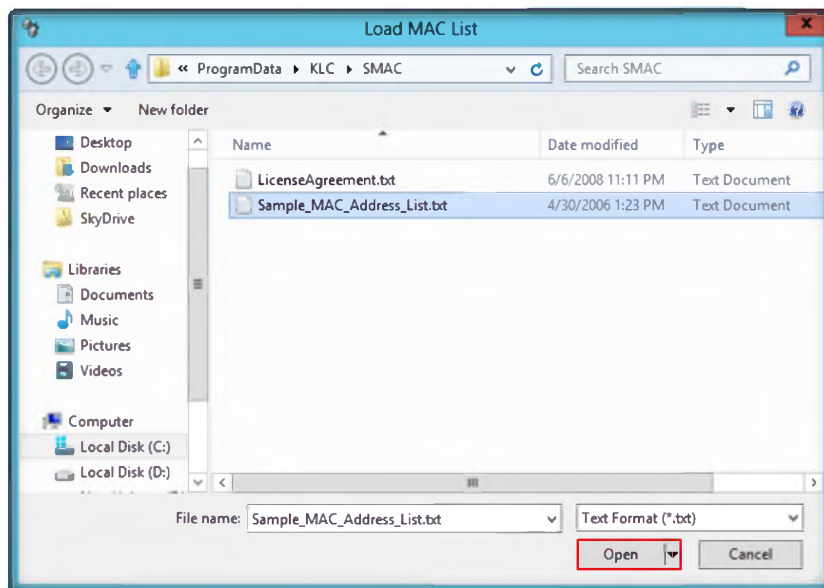


FIGURE 2.14: SMAC MAC List window

17. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address** and click **Select**. This MAC Address will be copied to **New Spoofed MAC Address** on the main SMAC screen.

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.

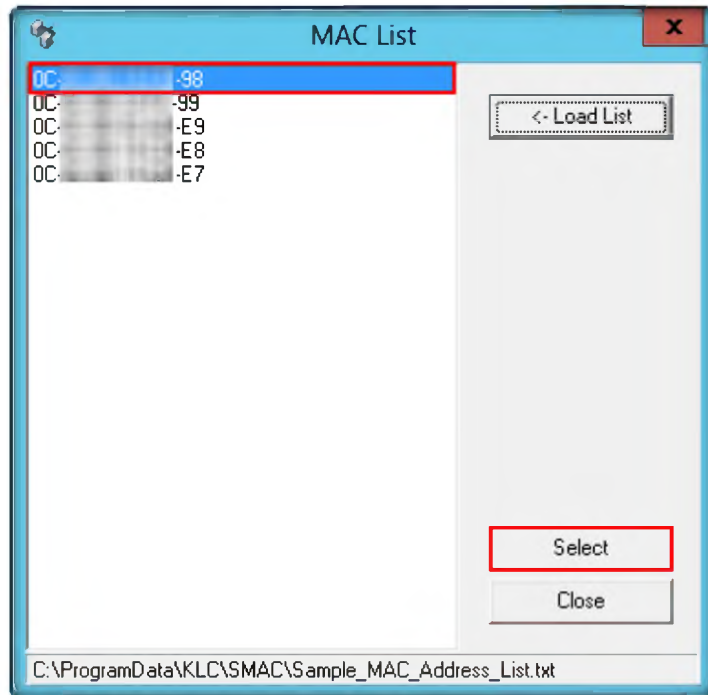


FIGURE 2.15: SMAC MAC List window

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

18. To restart Network Adapter, click **Restart Adapter**, which restarts the selected **Network Adapter**. Restarting the adapter causes a temporary disconnection problem for your Network Adapter.

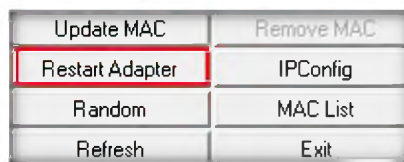


FIGURE 2.16 SMAC Restarting Network Adapter

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SMAC	▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

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

Questions

1. Evaluate and list the legitimate use of SMAC.
2. Determine whether SMAC changes hardware MAC addresses.
3. Analyze how you can remove the spoofed MAC address using the SMAC.

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



Sniffing a Network Using the WinArpAttacker Tool

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network (LAN).

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

You have already learned in the previous lab that you can conceal your identity by spoofing the MAC address. An attacker too can alter his or her MAC address and attempt to evade network intrusion detection systems, bypass access control lists, and impersonate as an authenticated user and can continue to communicate within the network when the authenticated user goes offline. Attackers can also push MAC flooding to compromise the security of network switches.

As an administrator, it is very important for you to detect odd MAC addresses on the network; you must have sound knowledge of footprinting, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. You can enable port security on the switch to specify one or more MAC addresses for each port. Another way to avoid attacker sniffing on your network is by using static ARP entries. In this lab, you will learn to run the tool WinArpAttacker to sniff a network and prevent it from attacks.

Lab Objectives

The objectives of this lab are to:

- **Scan, Detect, Protect,** and **Attack** computers on local area networks (LANs):
- Scan and show the active hosts on the **LAN** within a very short time period of 2-3 seconds
- **Save** and **load** computer list files, and save the LAN regularly for a new computer list
- Update the computer list in **passive mode** using sniffing technology

- Freely **provide information** regarding the type of operating systems they employ?
- Discover the kind of **firewall**, **wireless access point** and **remote access**
- Discover any published information on the topology of the **network**
- Discover if the site is seeking help for **IT positions** that could give information regarding the network services provided by the organization
- Identify actual users and discover if they give out too much personal information, which could be used for social engineering purposes

Lab Environment

To conduct the lab you need to have:

- **WinArpAttacker** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\WinArpAttacker**
- You can also download the latest version of **WinArpAttacker** from the link <http://www.xfocus.net>
- 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 2008** running on virtual machine as target machine
- A computer updated with network devices and drivers
- Installed version of **WinPcap** drivers
- Double-click **WinArpAttacker.exe** to launch WinArpAttacker
- **Administrative** privileges to run tools

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

Lab Duration

Time: 10 Minutes

 **WinArpAttacker**
works on computers
running Windows /2003.

Overview of Sniffing

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

Lab Tasks

TASK 1

**Scanning Hosts
on the LAN**

1. **Launch** Windows 8 Virtual Machine.
2. Launch **WinArpAttacker** in the host machine.

Module 08 – Sniffers

Caution: This program is dangerous, released just for research. Any possible loss caused by this program bears no relation to the author (unshadow), if you don't agree with this, you must delete it immediately.

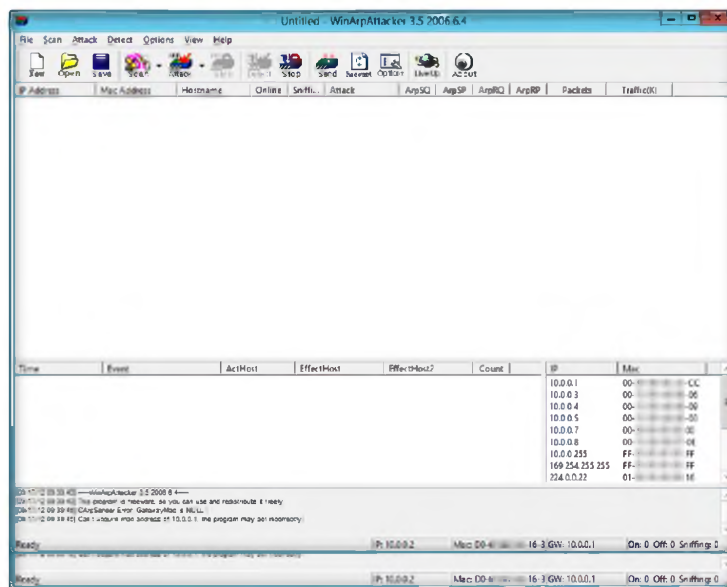


FIGURE 31: WinArpAttacker main window

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network.

- Click the **Scan** option from the toolbar menu and select **Scan LAN**.
- The scan shows the **active hosts** on the LAN in a very short period of time (2-3 seconds).
- The **Scan** option has two modes: **Normal scan** and **Antisniff scan**.

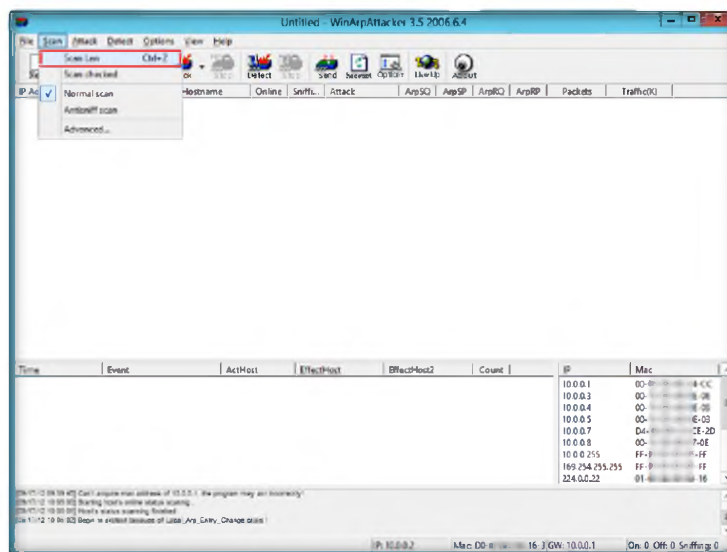


FIGURE 32: WinArpAttacker Scan options

The option scan can scan and show the active hosts on the LAN within a very short time. It has two scan modes, Normal and Antisniff. The second is to find who is sniffing on the LAN.

- Scanning saves and loads a computer list file and also scans the LAN regularly for new computer lists.

Module 08 – Sniffers

In this tool, attacks can pull and collect all the packets on the LAN.

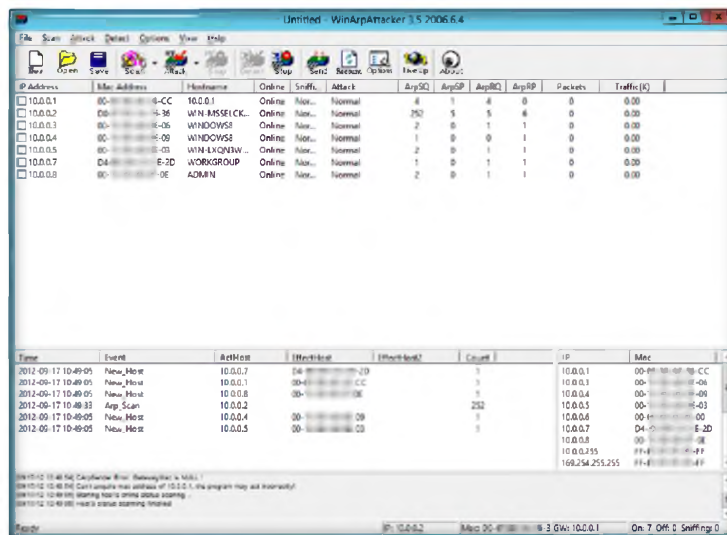


FIGURE 3.3: WinArpAttacker Loading a Computer List window

TASK 2

ARP Attack

- By performing the attack action, scanning can pull and collect all the packets on the LAN.
- Select a host (10.0.0.5 – Windows Server 2008) from the displayed list and select **Attack -> Flood**.

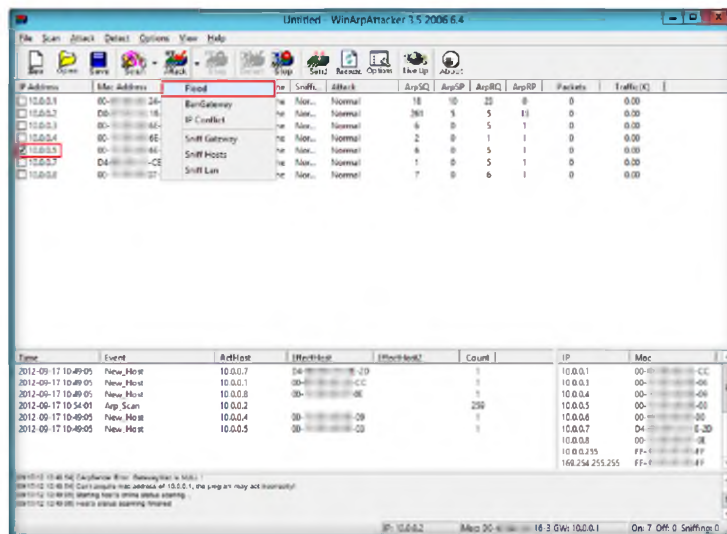


FIGURE 3.4: WinArpAttacker ARP Attack type

The Flood option sends IP conflict packets to target computers as fast as possible. If you send too many, the target computers go down.

- Scanning acts as another gateway or IP-forwarder without other user recognition on the LAN, while spoofing ARP tables.
- All the data sniffed by spoofing and forwarded by the WinArpAttackerIP-forward functions are counted, as shown in the main interface.

Module 08 – Sniffers



The BanGateway option tells the gateway wrong MAC addresses of target computers, so the targets can't receive packets from the Internet. This attack is to forbid the targets access the Internet.

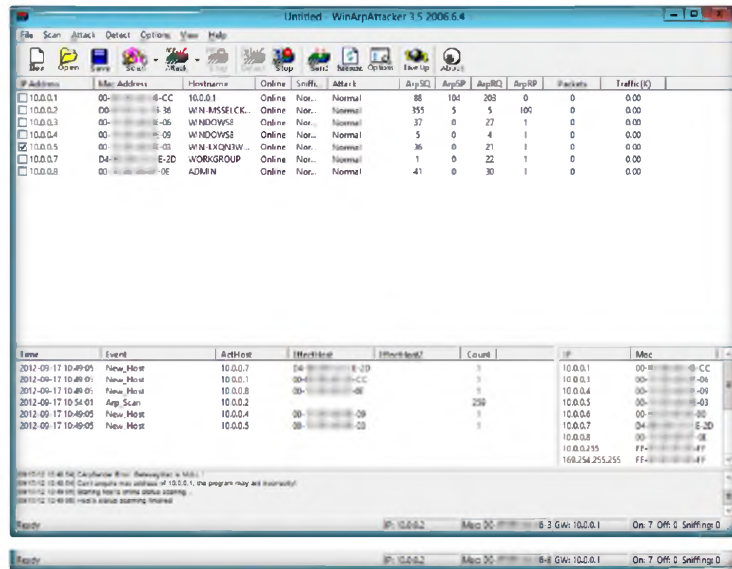


FIGURE 3.5: WinArpAttacker data sniffed by spoofing



The option, IPConflict, like ARP Flood, regularly sends IP conflict packets to target computers, so that users may not be able to work because of regular IP conflict messages. In addition, the targets can't access the LAN.

11. Click **Save** to save the report.

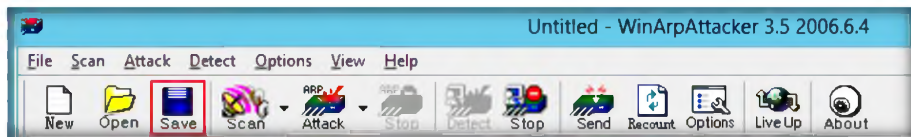


FIGURE 3.6: WinArpAttacker toolbar options

12. Select a desired location and click **Save** to save the report..

Lab Analysis

Analyze and document the scanned, attacked IP addresses discovered in the lab.

Tool/Utility	Information Collected/Objectives Achieved
WinArpAttacker	- Host Name - Node Type - MAC Address - IP Address - DHCP Enabled - Subnet Mask - DNS Servers

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

Questions

1. WinAtp

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

A gray square containing the word "Lab" in a small, black, sans-serif font at the top, and a large, white, stylized number "4" in the center.

Analyzing a Network Using the 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

Using WinArpAttacker you were able to sniff the network to find information like host name, MAC address, IP address, subnet mask, DNS server, etc. An attacker, too, can use this tool to gain all such information and can set up a rogue DHCP server serving clients with false details. A DNS attack can be performed using an extension to the DNS protocol.

To prevent this, network administrators must securely configure client systems and use antivirus protection so that the attacker is unable to recruit his or her botnet army. Securely configure name servers to reduce the attacker's ability to corrupt a zone file with the amplification record. As a 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), and authentication mechanisms. This lab will teach you about using other network analyzers such as Capsa Network Analyzer to capture and analyze network traffic.

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\CEHv8
Module 08
Sniffing**

Lab Environment

To carry out the lab, you need:

- **ColasoftCapsa Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 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
- Windows 8 running on virtual machine as target machine
- Double-click **capsa_free_7.4.1.2626.exe** and follow the wizard-driven installation steps to install Colasoft Capsa Free Network Analyzer
- **Administrative** privileges to run tools
- A web browser with an Internet connection

Note: This lab requires an active Internet connection for license key registration

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

Lab Duration

Time: 20 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

Analyze Network

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

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

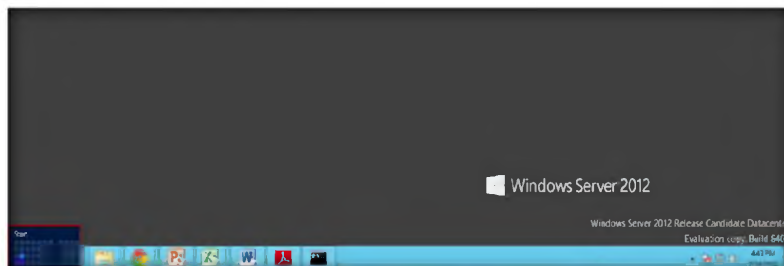


FIGURE 4.1: Windows Server 2012 – Desktop view

Module 08 – Sniffers

2. Click **Colasoft Capsa 7 Free Network Analyzer** to launch the Network Analyzer tool.

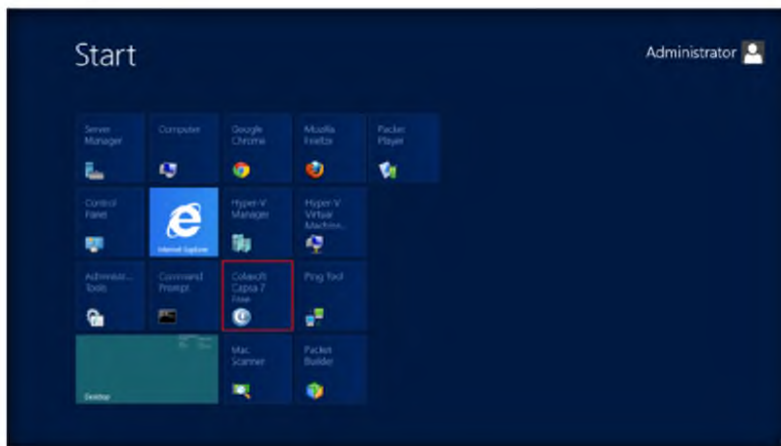


FIGURE 4.2: Windows Server 2012 – Start menu

3. The **Colasoft Capsa 7 Free - Activation Guide** window will appear. Type the activation key that you receive in your registered email and click **Next**.

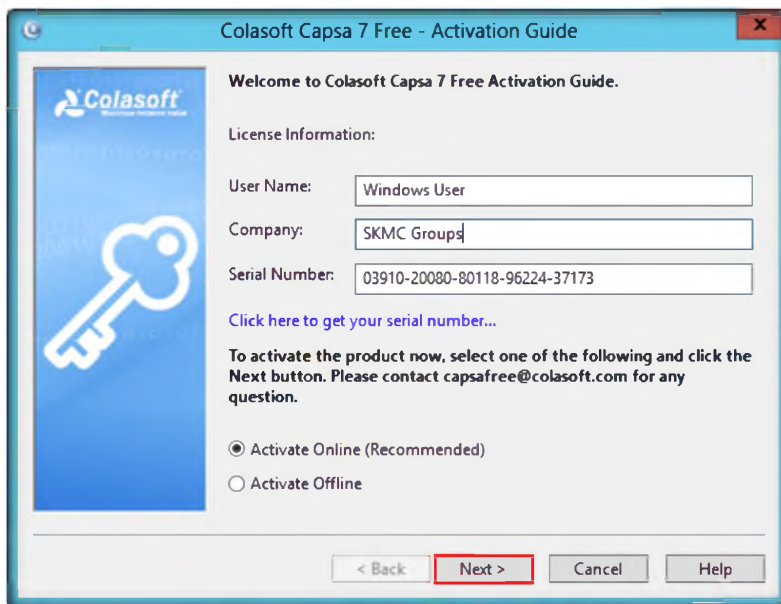


FIGURE 4.3: Colasoft Capsa 7 Free Network Analyzer – Activation Guide window

4. Continue to click **Next** on the Activation Guide and click **Finish**.

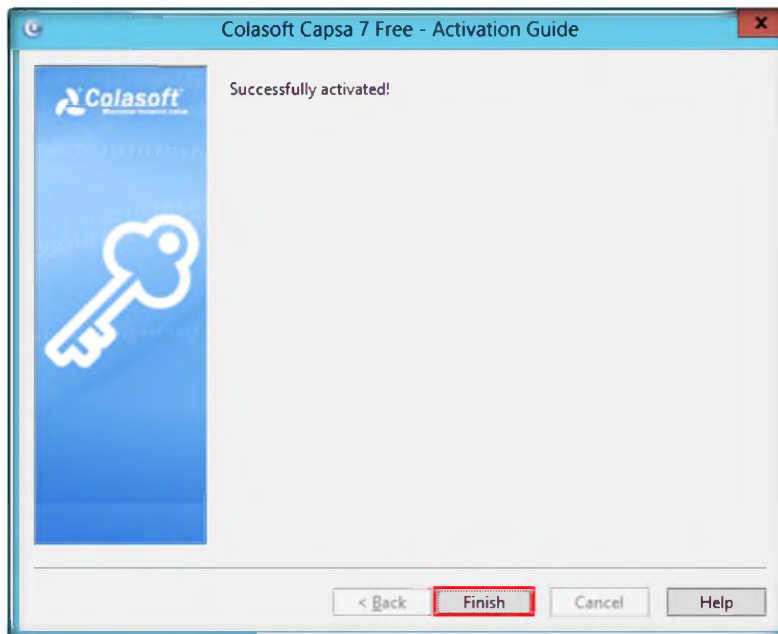


FIGURE 4.4: Colasoft Capsa 7 Free Network Analyzer – Activation successful

5. The **Colasoft Capsa 7 Free Network Analyzer** main window appears.

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

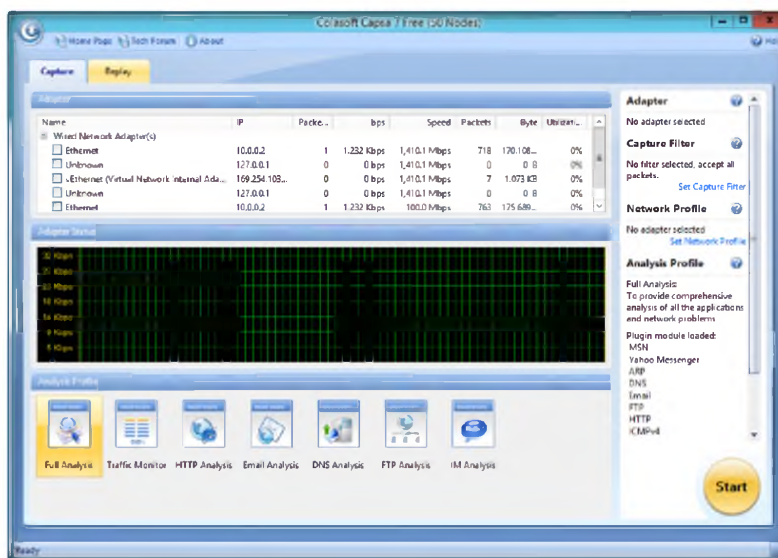


FIGURE 4.5: Colasoft Capsa Network Analyzer main screen

Module 08 – Sniffers

- In the **Capture** tab of the main window, select the **Ethernet** check box in **Adapter** and click **Start** to create a new project.

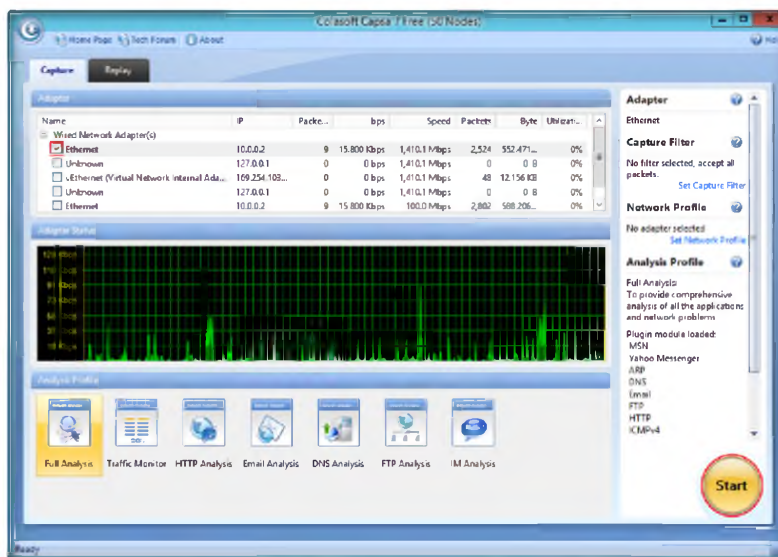


FIGURE 4.6: Colasoft Capsa Network Analyzer creating a New Project

- Dashboard** provides various graphs and charts of the statistics. You can view the analysis report in a graphical format in the **Dashboard** section of **Node Explorer**.

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.

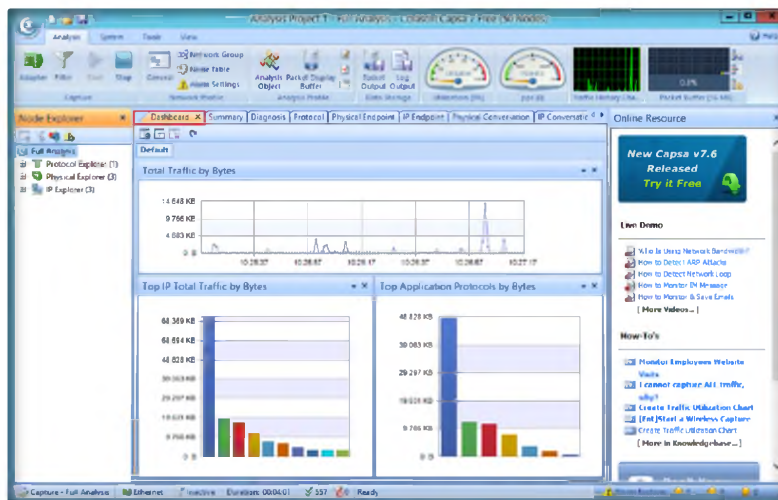


FIGURE 4.7: Colasoft Capsa Network Analyzer Dashboard

Module 08 – Sniffers

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

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

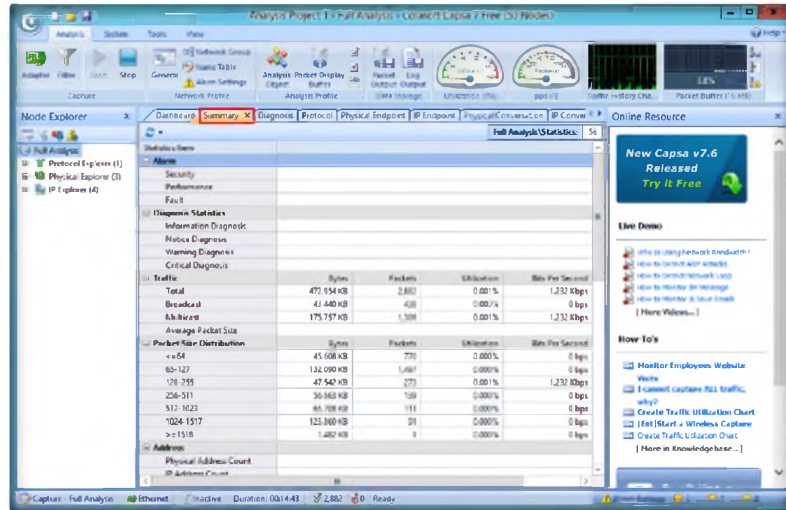


FIGURE 4.8: Colasoft Capsa Network Analyzer Summary

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

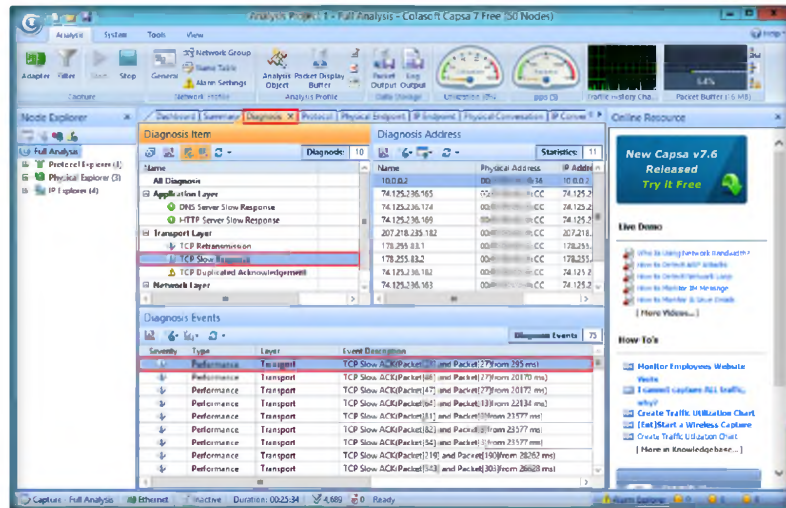


FIGURE 4.9: Colasoft Capsa Network Analyzer Diagnoses

Module 08 – Sniffers

- Double-click the highlighted **Diagnosis Event** to view the detailed information of this event.

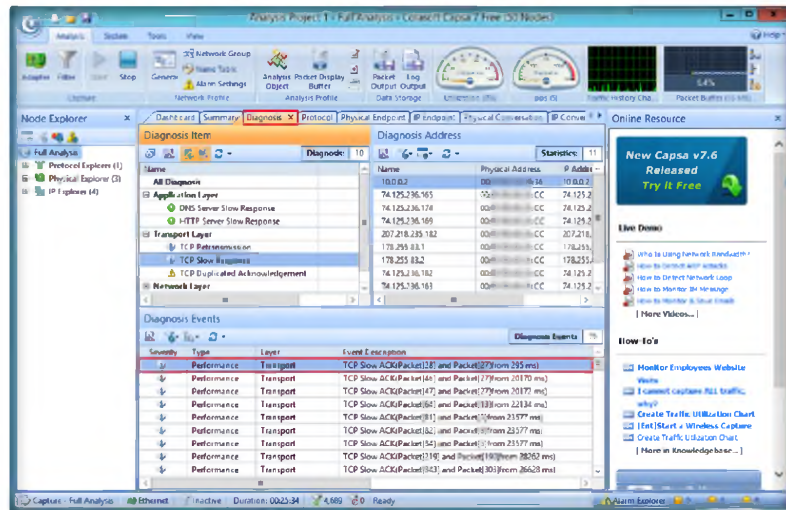


FIGURE 4.10: Analyzing Diagnosis Event

- The **TCP Slow ACK – Data Stream of Diagnostic Information** window appears, displaying Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information.

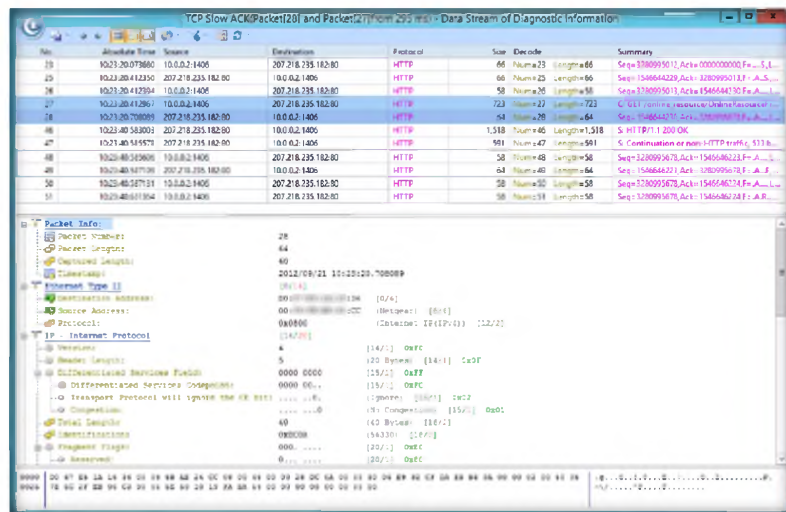


FIGURE 4.11: TCP Slow ACK – Data Stream of Diagnostic Information window

- The **Protocol** tab lists statistics of all protocols used in network transactions hierarchically, allowing you to view and analyze the protocols.

Module 08 – Sniffers

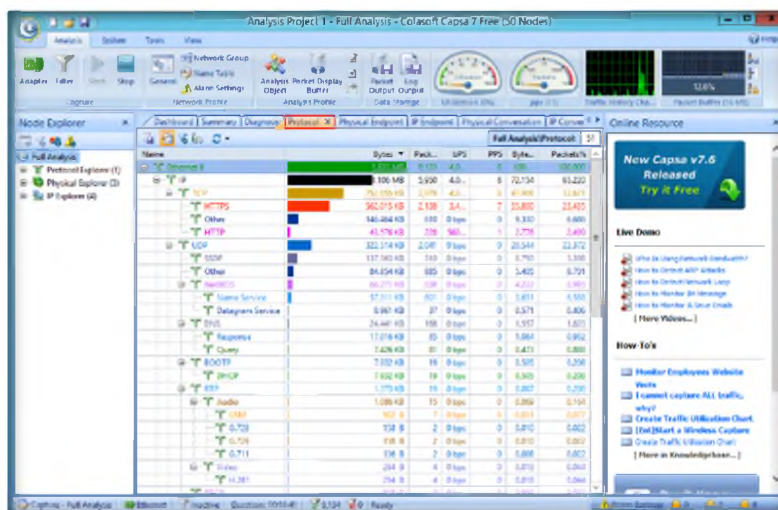


FIGURE 4.12: Colasoft Capsa Network Analyzer Protocol analysis

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

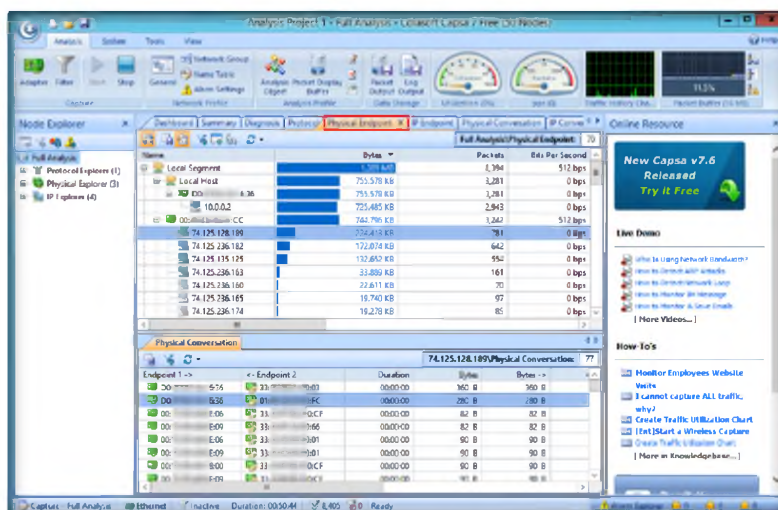


FIGURE 4.13: Colasoft Capsa Network Analyzer Physical Endpoint analysis

- The **IP Endpoint** tab displays statistics of all IP addresses communicating within the network.
- 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.

Module 08 – Sniffers

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.

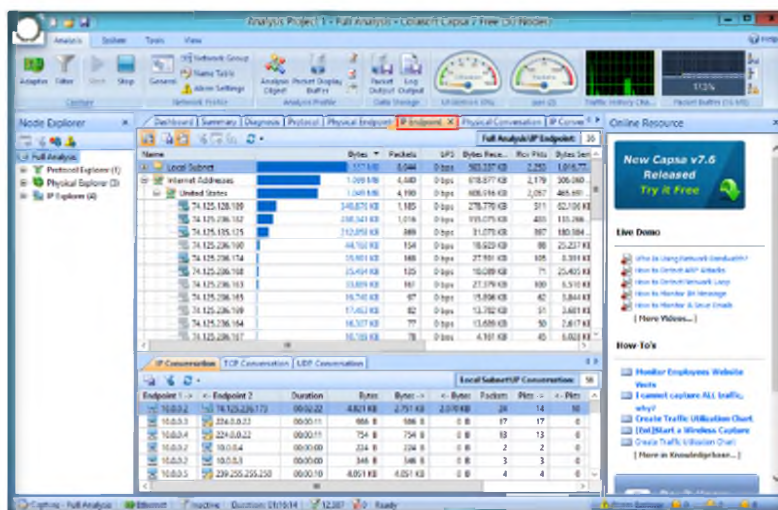


FIGURE 4.14: Colasoft Capsa Network Analyzer IP Endpoint view

17. 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.

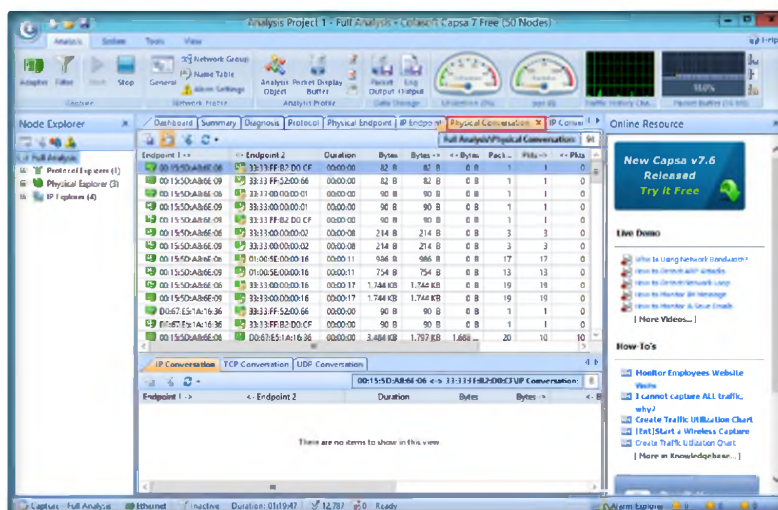


FIGURE 4.15: Colasoft Capsa Network Analyzer Physical Conversations

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

Module 08 – Sniffers

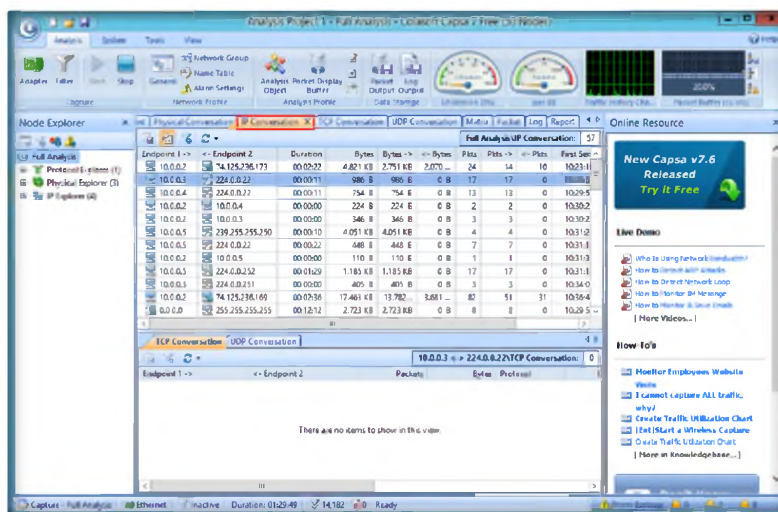


FIGURE 4.16: Colasoft Capsa Network Analyzer IP Conversations

20. 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 10.0.0.5 and 239.255.255.250.

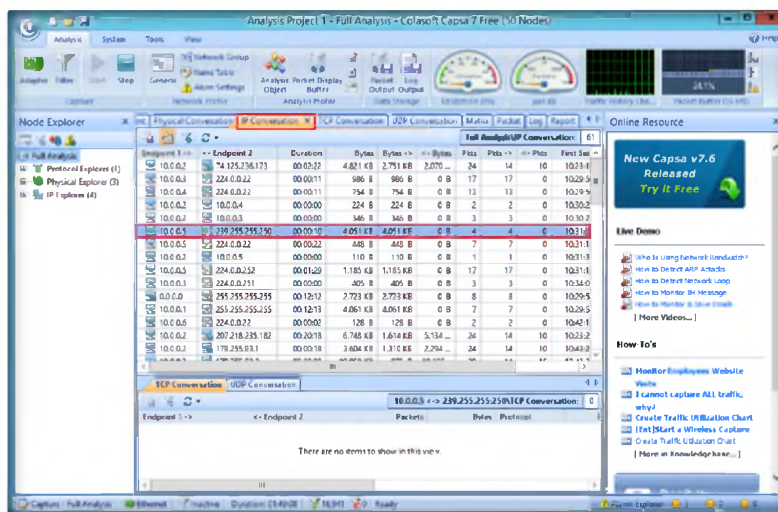


FIGURE 4.17: Colasoft Capsa Network Analyzer IP Conversations

21. A window opens displaying full packet analysis between 10.0.0.5 and 239.255.255.250.

Module 08 – Sniffers

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.

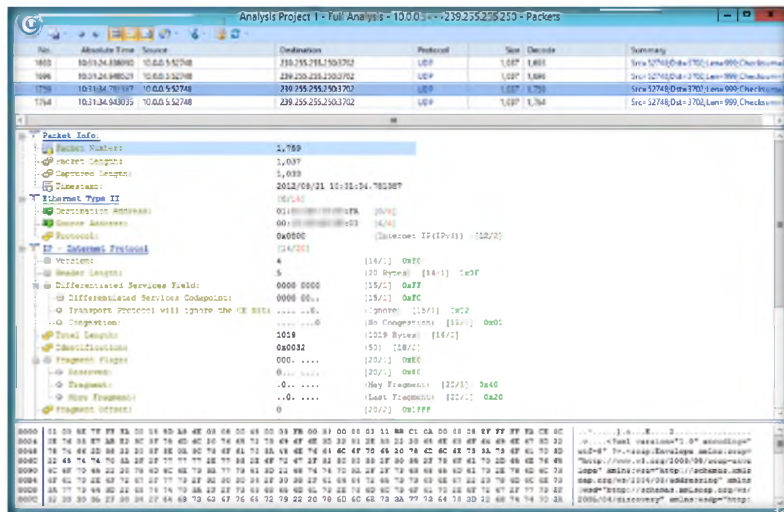


FIGURE 4.18: Full Packet Analysis of Nodes in IP Conversations

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

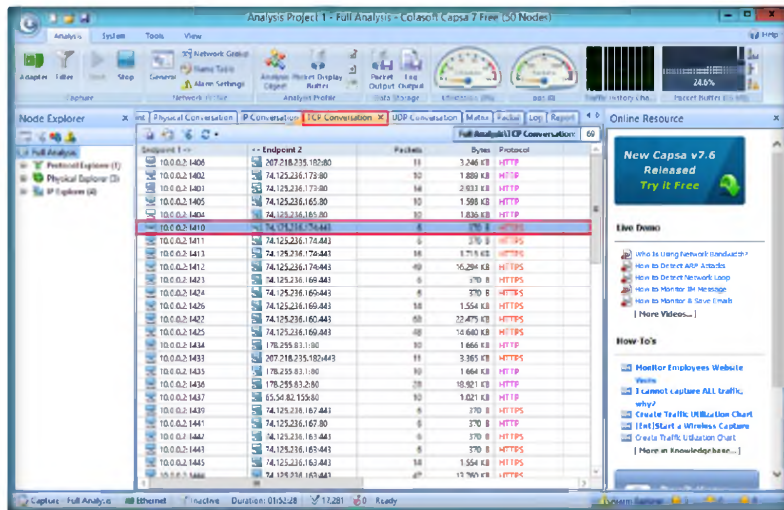


FIGURE 4.19: Colasoft Capsa Network Analyzer TCP Conversations

24. A **Full Analysis** window is opened displaying detailed information of conversation between two nodes.

Module 08 – Sniffers

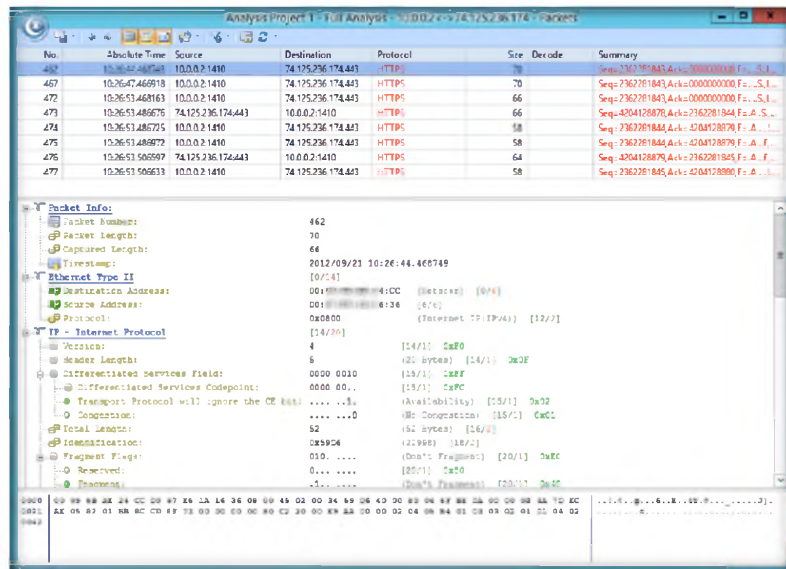


FIGURE 4.20: Full Packet Analysis of Nodes in TCP Conversations

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

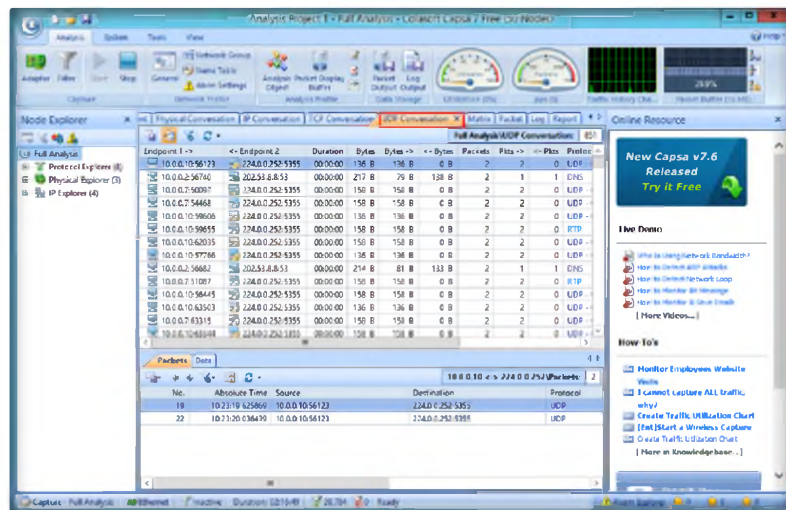


FIGURE 4.21: Colasoft Capsa Network Analyzer UDP Conversations

27. On the **Matrix** tab, you can view the nodes communicating in the network by connecting them in lines graphically.
28. The weight of the line indicates the volume of traffic between nodes arranged in an extensive ellipse.

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.

29. 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.

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 Colasoftware Capsa.

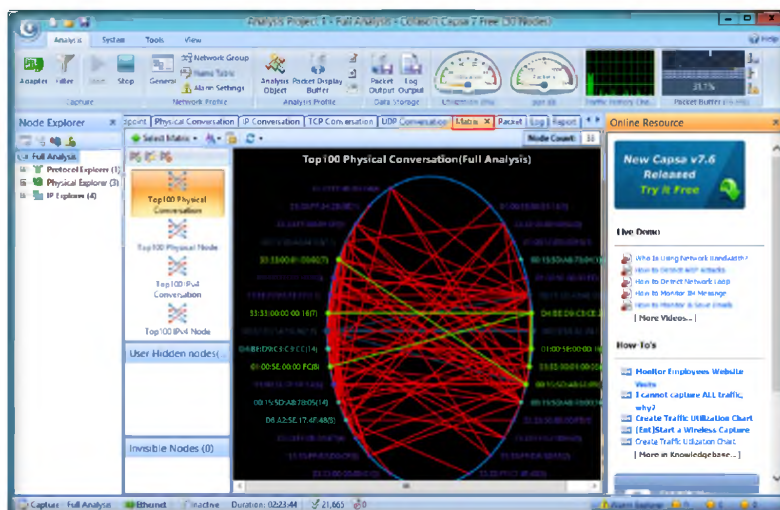


FIGURE 4.22: Colasoftware Capsa Network Analyzer Matrix view

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

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.

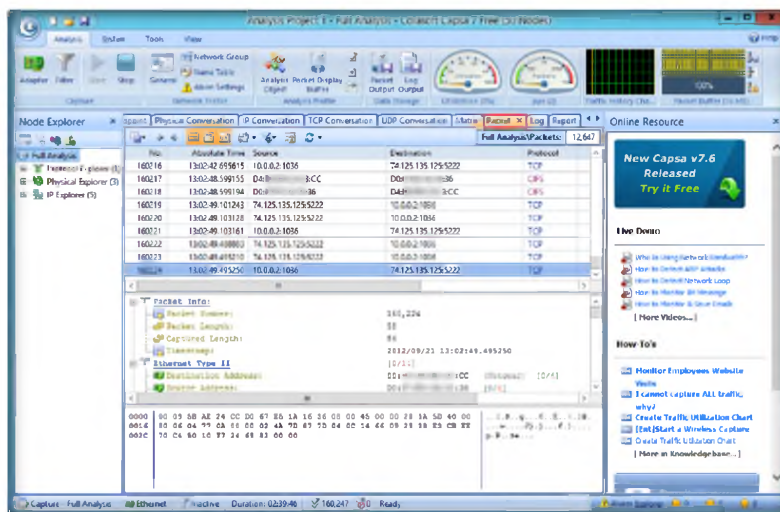


FIGURE 4.23: Colasoftware Capsa Network Analyzer Packet information

31. The Packet decode consists of two major parts: **Hex View** and **Decode View**.

Module 08 – Sniffers

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.

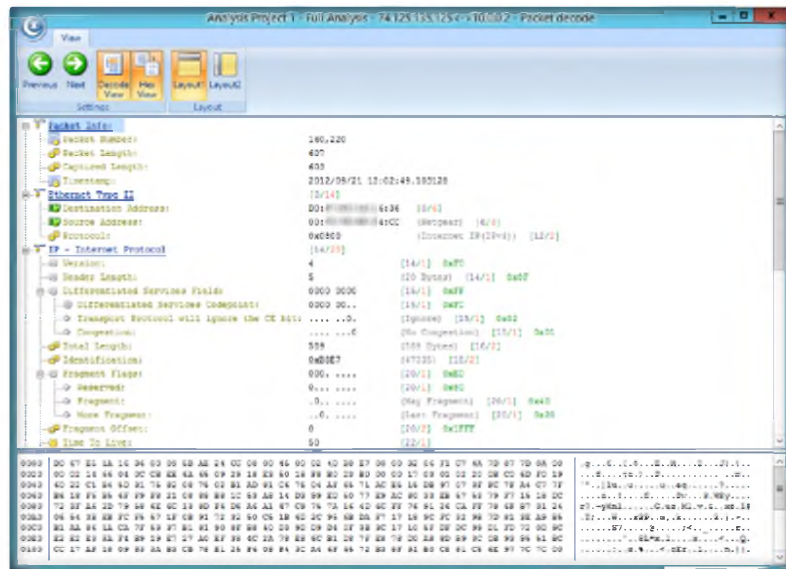


FIGURE 4.24: Full Analysis of Packet Decode

32. The **Log** tab provides a **Global Log, DNS Log, Email Log, FTP Log, HTTP Log, MSN Log** and **Yahoo Log**.
33. You can view the logs of **TCP conversations, Web access, DNS transactions, Email communications**, etc.

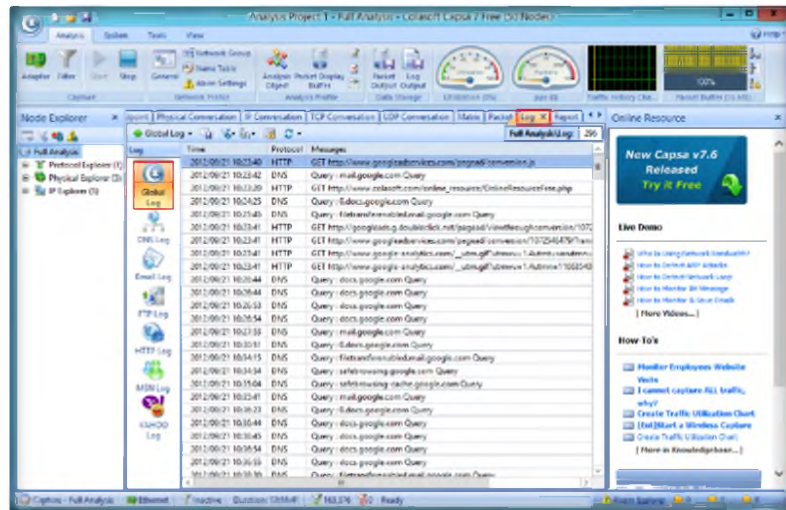


FIGURE 4.25: Colasoft Capsa Network Analyzer Global Log view

Module 08 – Sniffers

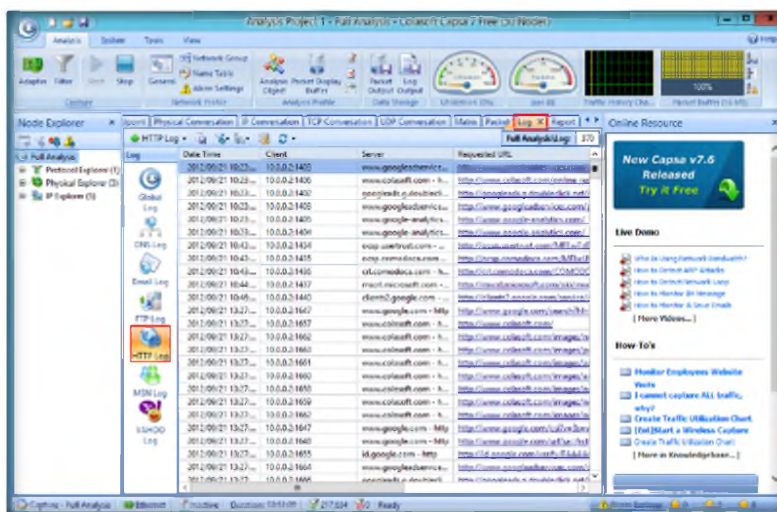


FIGURE 4.26: Colasoft Capsa Network Analyzer HTTP Log view

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

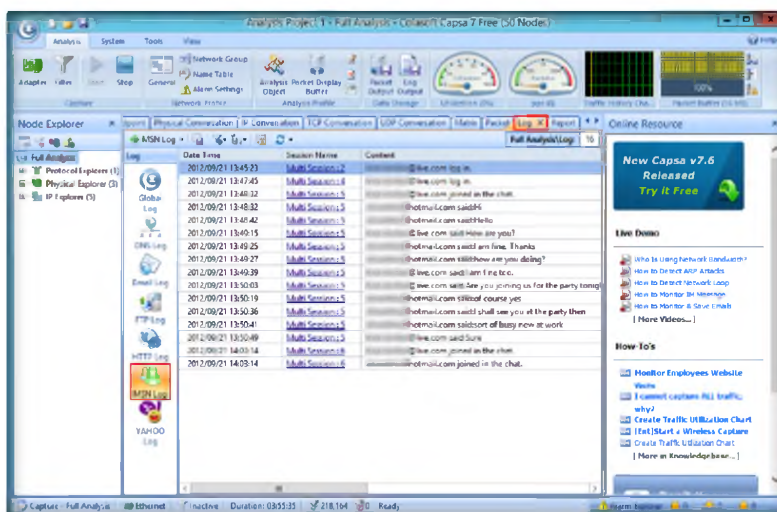


FIGURE 4.27: Colasoft Capsa Network Analyzer MSN Log view

Module 08 – Sniffers

35. The **Report** tab provides 27 statistics reports from the global network to a specific network node.

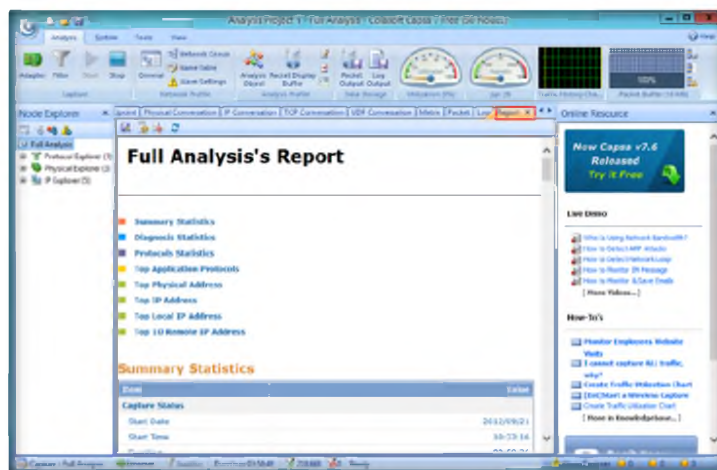


FIGURE 4.28: Colasoft Capsa Network Analyzer Full Analysis's Report

36. You can click the respective hyperlinks for information or you can scroll down to view the 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.

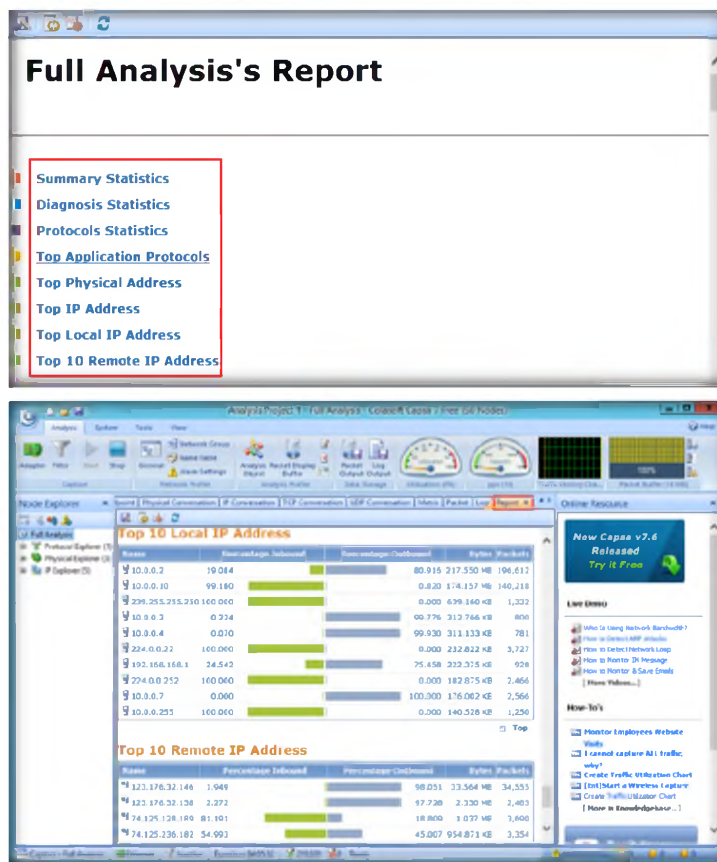


FIGURE 4.29: Colasoft Capsa Network Analyzer Full Analysis's Report

37. Click **Stop** on toolbar after completing your task.

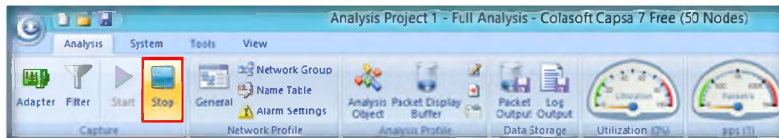


FIGURE 4.30: Colasoft Capsa Network Analyzer Stopping process

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Capsa Network Analyzer	Diagnosis: - Name - Physical Address - IP Address
	Packet Info: - Packet Number - Packet Length - Captured Length
	Ethernet Type: - Destination Address - Source Address - Protocol - Physical Endpoint - IP Endpoint
	Conversations: - Physical Conversation - IP Conversation - TCP Conversation - UDP Conversation
	Logs: - Global Log - DNS Log - Email Log - FTP Log - HTTP Log - MSN Log - Yahoo Log

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

Questions

1. Analyze how Capsa affects your network traffic, while analyzing the network.
2. What types of instant messages does Capsa monitor?
3. Determine if the packet buffer will affect performance. If yes, then what steps can you take to avoid or reduce its effect on software?

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



Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and display packet data in detail.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

As in the previous lab, you are able to capture TCP and UDP conversations; an attacker, too, can collect this information and perform attacks on a network. Attackers listen to the conversation occurring between two hosts and issue packets using the same source IP address. Attackers will first know the IP address and correct sequence number by monitoring the traffic. Once the attacker has control over the connection, he or she then sends counterfeit packets. These sorts of attacks can cause various types of damage, including the injection into an existing TCP connection of data and the premature closure of an existing TCP connection by the injection of counterfeit packets with the FIN bit set.

As an administrator you can configure a firewall or router to prevent the damage caused by such attacks. To be 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. Another use of a packet analyzer is to sniff passwords, which you will learn about in this lab using the Wireshark packet analyzer.

Lab Objectives

The objective of this lab is to demonstrate the **sniffing** technique to capture from **multiple** interfaces and data collection from any network topology.

Lab Environment

In the lab you will need:

- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

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

- You can also download the latest version of **Wireshark** from the link <http://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 (Windows 8 or Windows 2008 Server) as a Victim machine
- A web browser with Internet connection
- Double-click **Wireshark-win64-1.8.2.exe** and follow the wizard-driven installation steps to install Wireshark
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Password Sniffing

Password sniffing uses various techniques to sniff network and get someone's password. Networks use **broadcast** technology to send data. Data **transmits** through the broadcast network, which can be read by anyone on the other computer present on the network. Usually, all the computers except the recipient of the message will notice that the **message** is not meant for them, and ignore it.

Many computers are **programmed** to look at every message on the network. If someone misuses the facility, they can view **message**, which is not intended of others.

Lab Tasks

TASK 1

Capturing Packet

1. Before starting this lab, login to the virtual machine(s).
2. On the host machine, launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

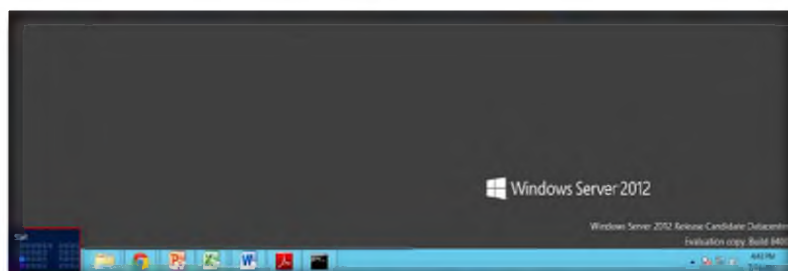


FIGURE 5.1: Windows Server 2012 – Desktop view

3. Click **Wireshark** to launch the application.

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

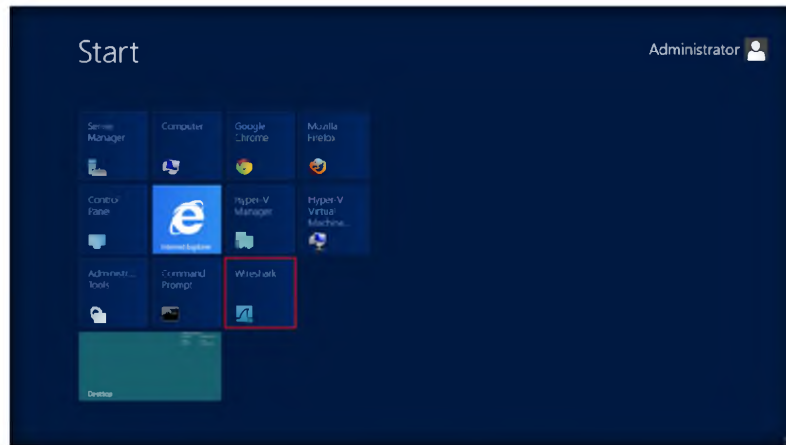


FIGURE 5.2: Windows Server 2012 – Desktop view

 A network packet analyzer is a kind of measuring device used to examine what is going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

4. The **Wireshark** main window appears.

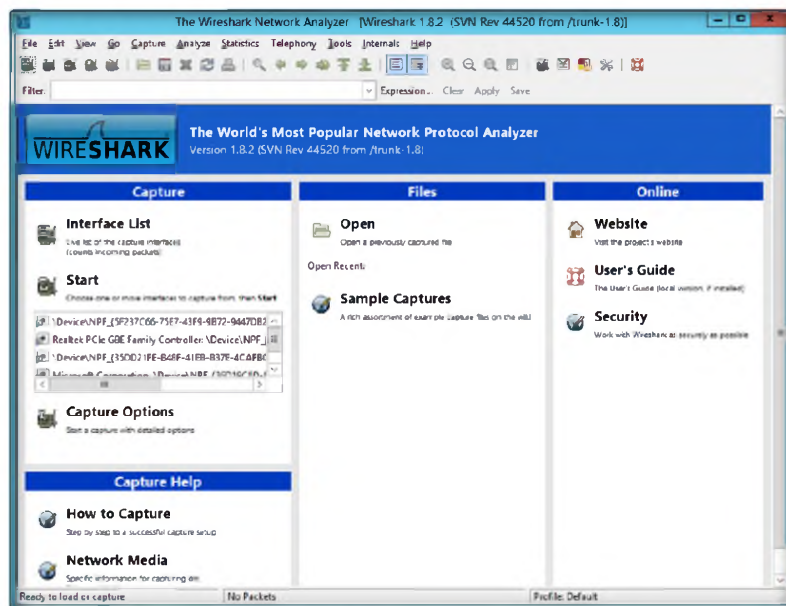


FIGURE 5.3: Wireshark Main Window

FIGURE 5.3: Wireshark Main Window

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

Module 08 – Sniffers

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

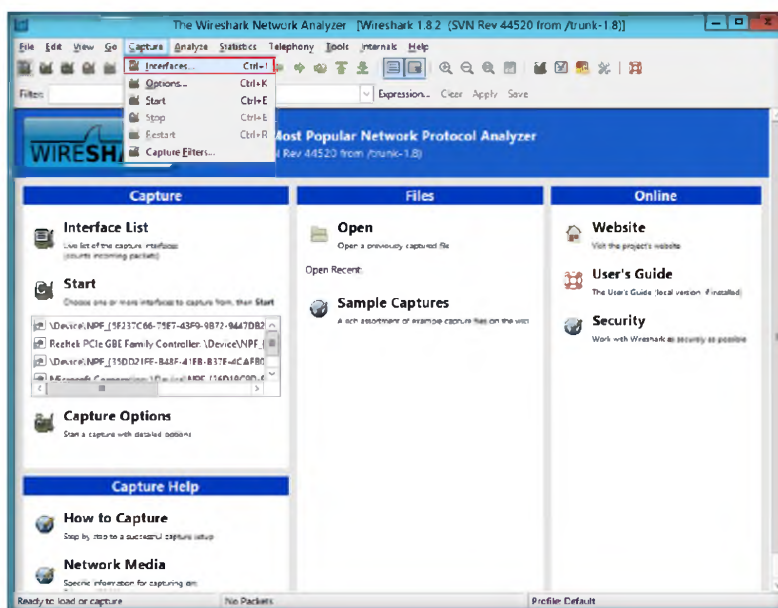


FIGURE 5.4: Wireshark Main Window with Interface Option

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

6. The **Wireshark Capture Interface** window appears.

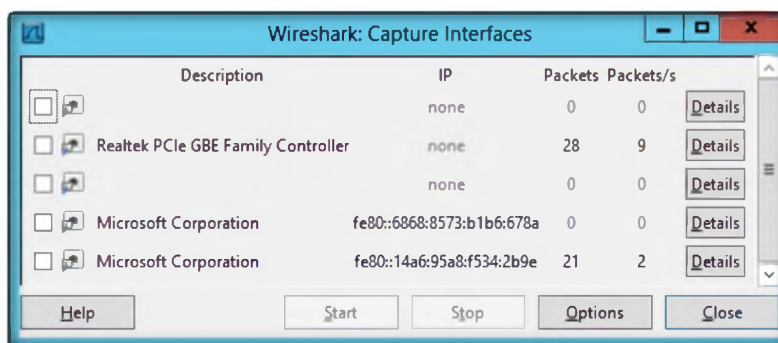


FIGURE 5.5: Wireshark Capture Interfaces Window

7. In the **Wireshark Capture Interfaces** dialog box, find and select the **Ethernet Driver Interface** that is connected to the system.
8. In the previous screenshot, it is the **Realtek PCIe GBE Family Controller**. The interface should show some packets passing through it, as it is connected to the network.
9. Click **Start** in that interface's line.

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

 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.

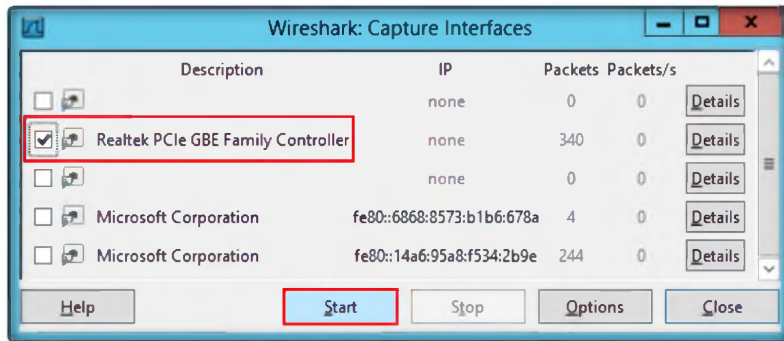


FIGURE 5.6: Wireshark Capture Interfaces Window – Starting Capture

10. Traffic informs of packets generated through the computer while browsing the Internet.

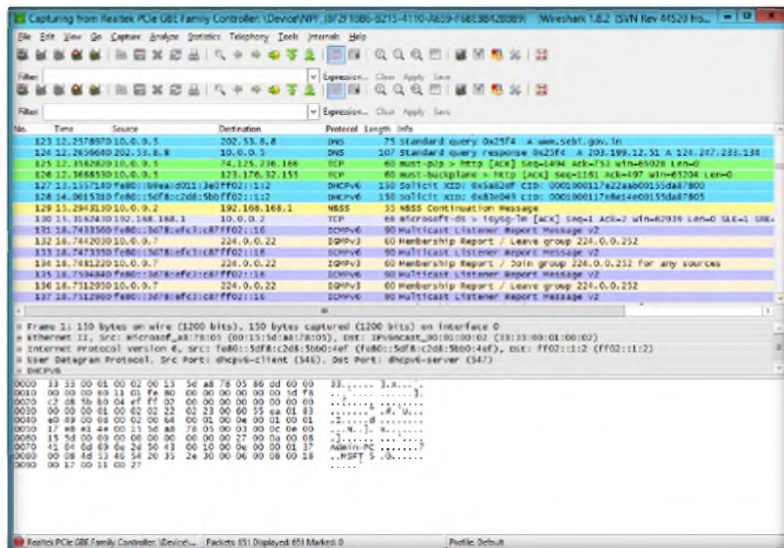


FIGURE 5.7: Wireshark Window with Packets Captured

11. Now, switch to the virtual machine and login to your email ID for which you would like to sniff the password.
12. Stop the running live capture by clicking the icon  on the toolbar.

TASK 2

Stop Live Capturing

Module 08 – Sniffers

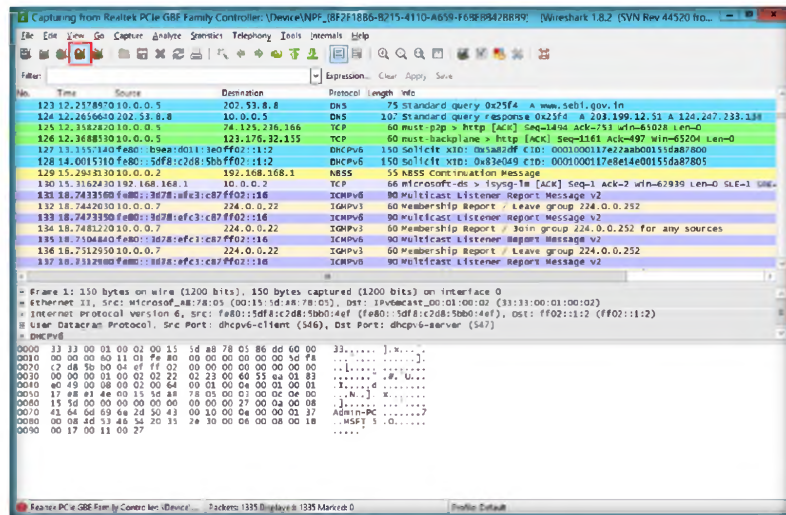


FIGURE 5.8: Wireshark Window – Stopping Live Capture

- You may save the captured packets from **File** → **Save As**, provide a name for the file, and save it in the desired location

TASK 3

Saving Captured Files

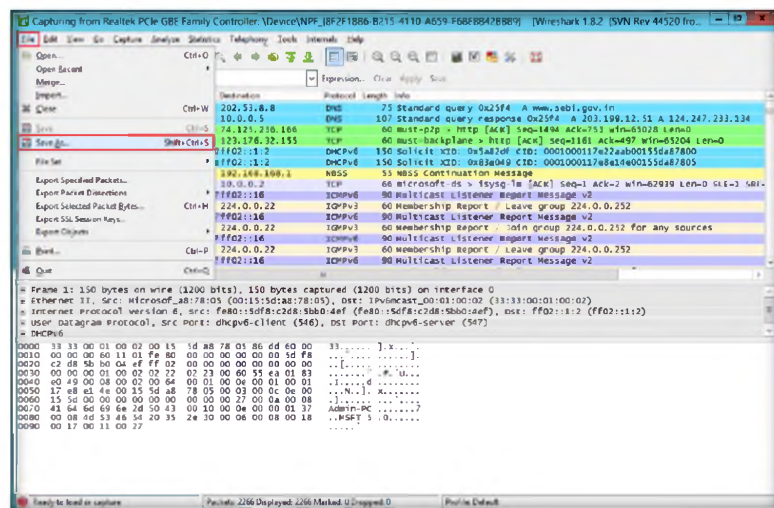


FIGURE 5.9: Wireshark – Saving the Captured Packets

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

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

Module 08 – Sniffers

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.

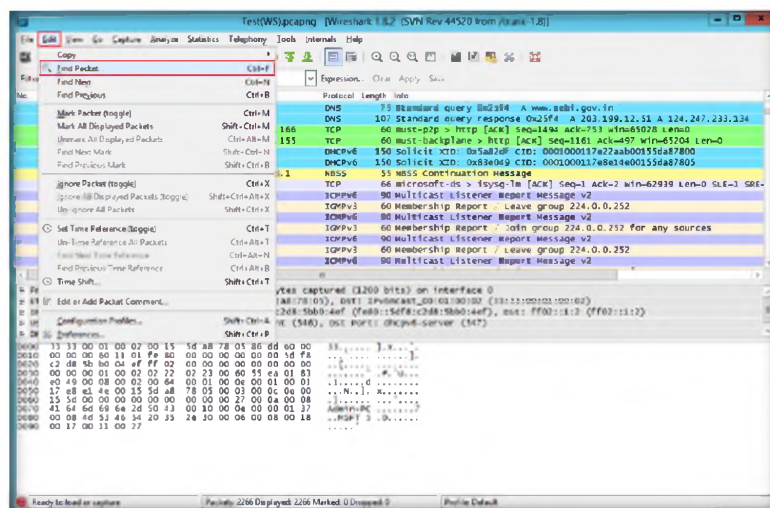


FIGURE 5.10: Wireshark – Finding Packet Option

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

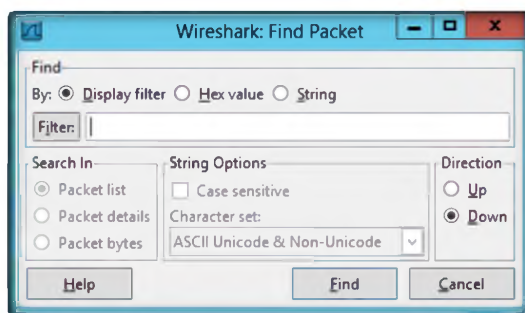


FIGURE 5.11: Wireshark – Find Packet Window

16. In **Find By**, select **String**, type **pwd** in the **Filter** field, select the radio button for **Packet details** under **Search In** and select **ASCII Unicode & Non-Unicode** from the **Character set** drop-down list. 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).

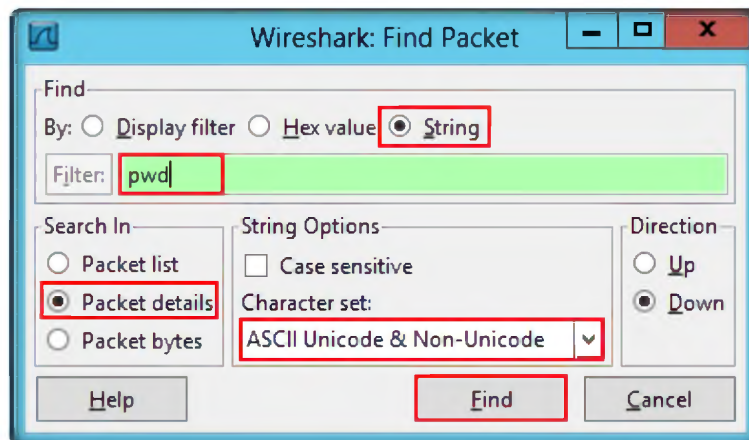


FIGURE 5.12: Wireshark – Selecting Options in Find Packet Window

 Wireshark media types are supported depends on many things like the operating system you are using.

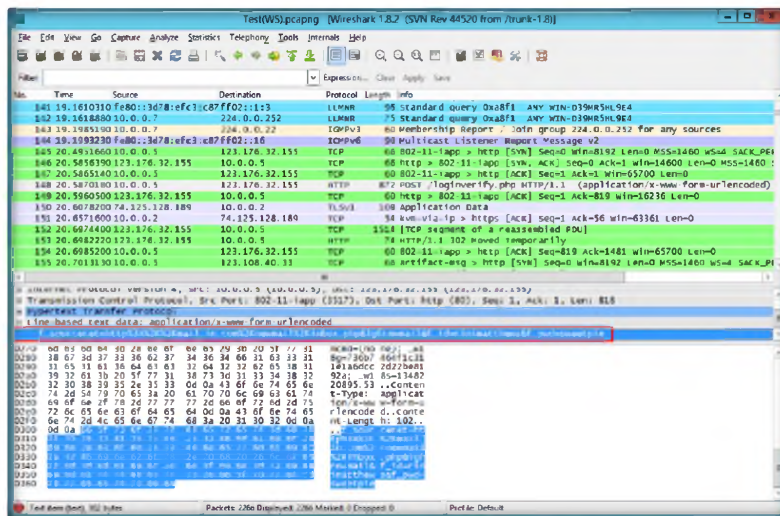


FIGURE 5.13: Wireshark – Sniffed Password in Captured Packet

18. If you are working on **iLabs** environment, then use the **Test(WS)** sample captured file located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark\Wireshark Sample Capture files** to sniff the password.

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

Tool/Utility	Information Collected/Objectives Achieved
Wireshark	- Time - Source - Destination - Protocol - Length - Info - Internet Protocol - TCP, Source Port Info - User ID and Password

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

Questions

1. Evaluate the protocols that are supported by Wireshark.
2. Determine the devices Wireshark uses to capture packets.

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



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, cracking encrypted passwords.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

You have learned in the previous lab how you can get user name and password information using Wireshark. By merely capturing enough packets, attackers can extract the user name and password if the victim authenticates themselves in a public network especially into a website without an HTTPS connection. Once the password is hacked, an attacker can simply log into the victim's email account or use that password to log in to their PayPal and drain their 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 preventive measures an administrator in an organization should always advise employees not provide sensitive information in public networks without an HTTPS connection. 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 user name and password information is by using Cain & Abel to perform a man-in-the-middle attack.

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 a man-in-the-middle attack
- Sniff the network for the password

Lab Environment

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

To carry-out the lab, you need:

- **Cain & Abel** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\Cain & 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** running on virtual machine as attacker machine
- **Windows 2008 Server** running on virtual machine as the victim machine
- A web browser with Internet connection
- Double-click **ca_setup.exe** and follow the wizard-driven installation steps to install Cain & Abel
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Man-In-The-Middle Attack

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

A man-in-the-middle attack (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.

Man-in-the-middle attacks come in many **variations** and can be carried out on a **switched LAN**.

Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Launch your **Windows 2008 Server** virtual machine (**Victim Machine**).
2. Launch your **Windows 8** virtual machine (**Attacker Machine**).
3. On the host machine (Windows Server 2012), launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Module 08 – Sniffers

 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.

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

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

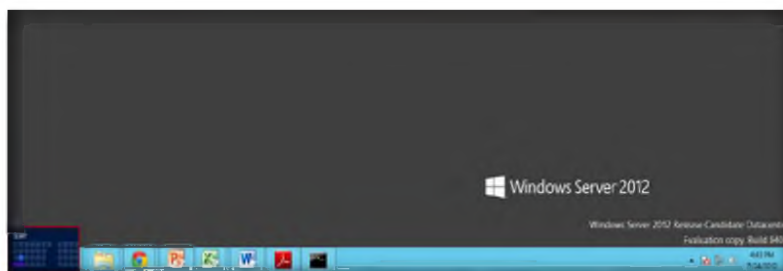


FIGURE 6.1: Windows Server 2012 – Desktop view

4. Click **Cain** in the **Start** menu to launch Cain& Abel.

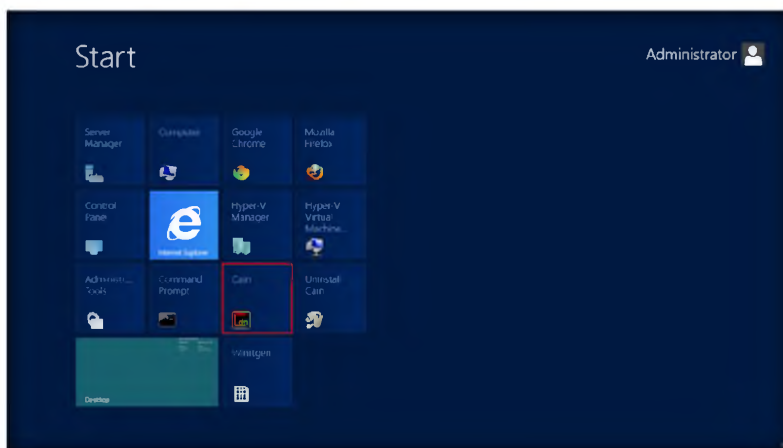


FIGURE 6.2: Windows Server 2012 – Desktop view

5. The main window of Cain & Abel appears.

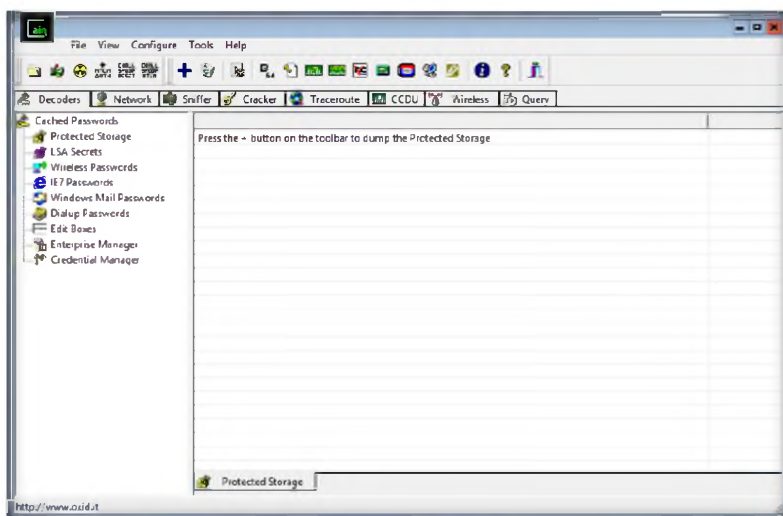


FIGURE 6.3: Cain & Abel Main Window

6. When you first open Cain & Abel, you will notice a series of tabs near the top of the window.
7. To configure the **Ethernet card**, click **Configure** from the 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.

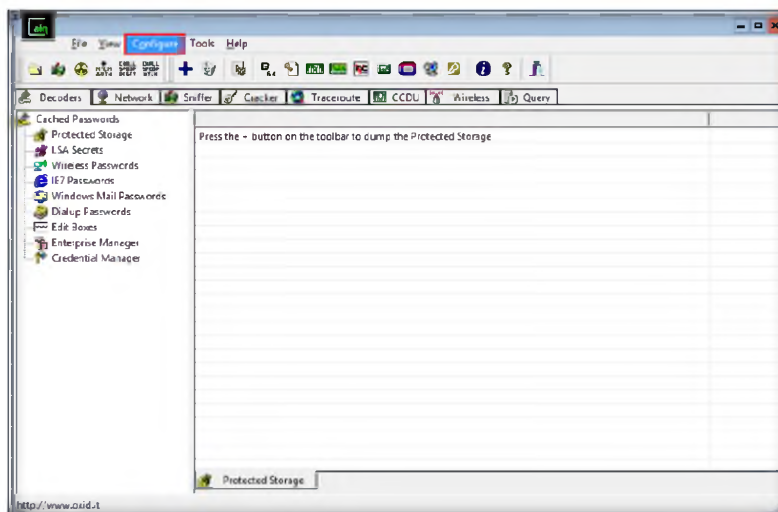


FIGURE 6.4: Cain & Abel Configuration Option

FIGURE 6.4: Cain & Abel Configuration Option

8. The **Configuration Dialog** window appears.
9. The **Configuration Dialog** window consists of several tabs. Click the **Sniffer** tab to select the sniffing adapter.
10. Select **Adapter** and click **Apply** and then **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.

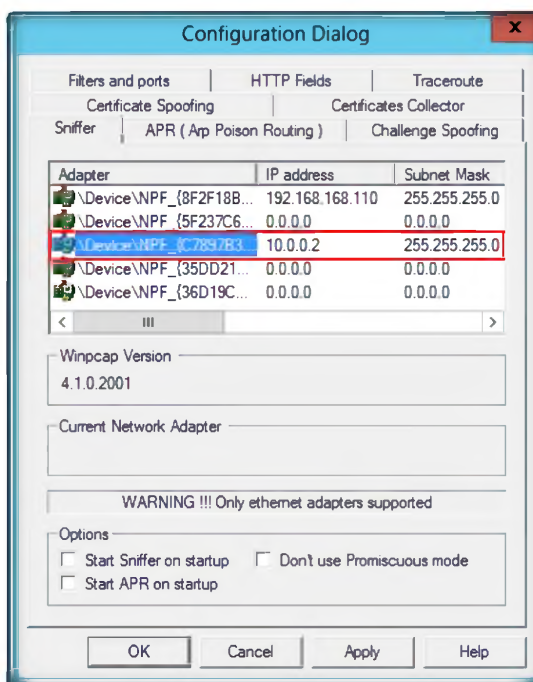


FIGURE 6.5: Cain & Abel Configuration Dialog Window

11. Click the **Start/Stop Sniffer** icon on the toolbar.

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

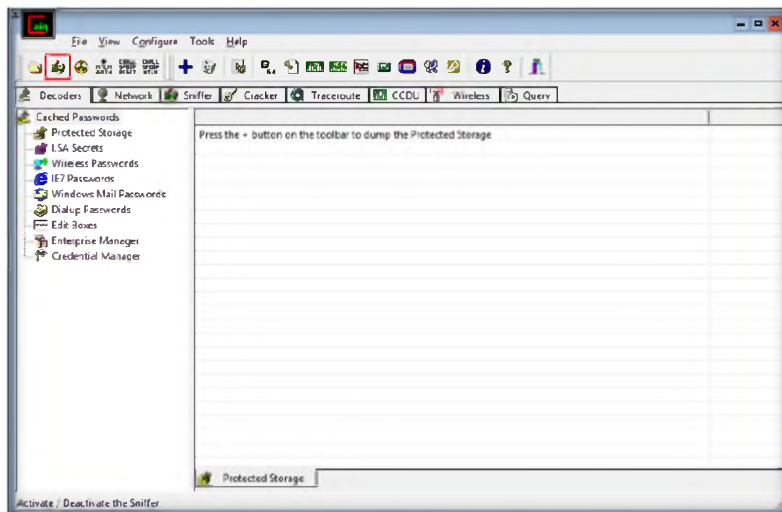


FIGURE 6.6: Cain & Abel Configuration Dialog Window

FIGURE 6.6: Cain & Abel Configuration Dialog Window

Note: If you get Cain Warning pop-up, click **OK**.

12. Now click the **Sniffer** tab.

● 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.

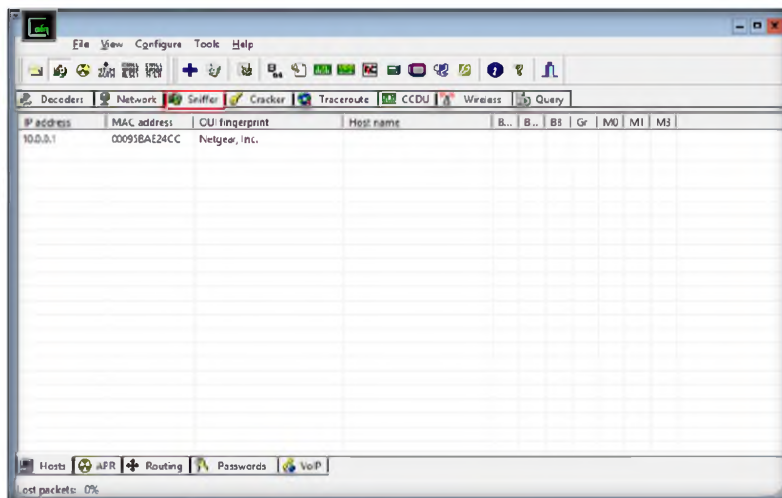


FIGURE 6.7: Sniffer tab

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

14. The **MAC Address Scanner** window appears. Select **All hosts in my subnet** and check the **All Tests** check box. Click **OK**.

Module 08 – Sniffers

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

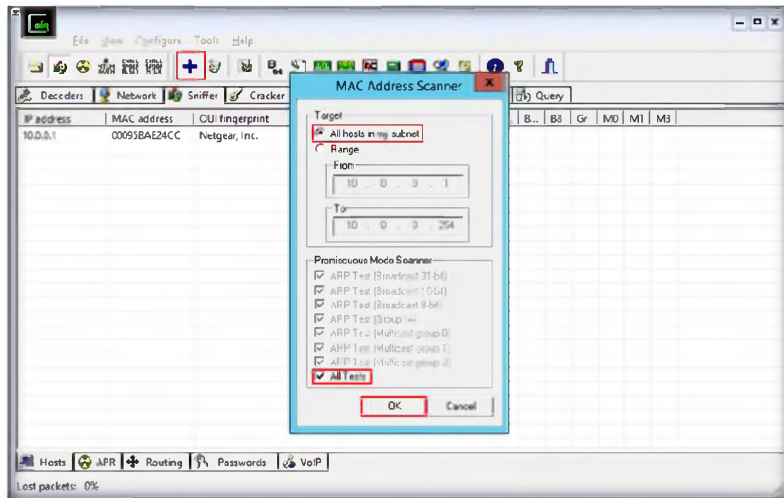


FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

- Cain & Abel starts scanning for MAC addresses and lists all found MAC address.

Speeding up packet capture speed by wireless packet injection

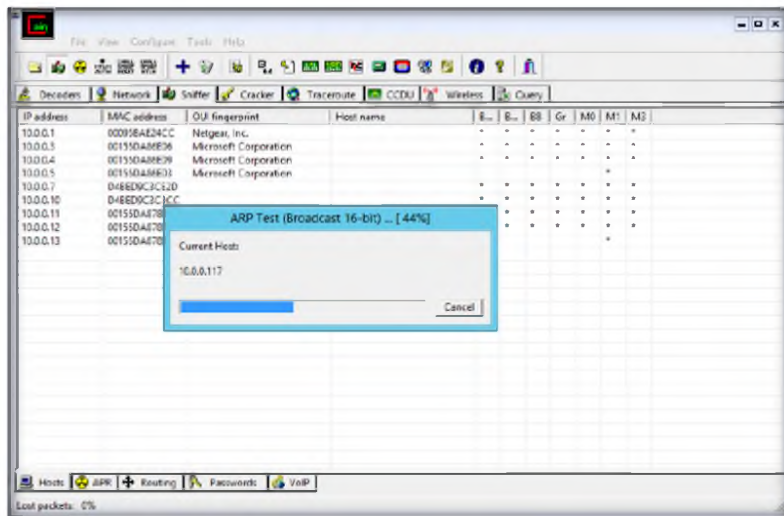


FIGURE 6.9: Cain & Abel – Scanning MAC Addresses Window

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

- After scanning is **completed**, a list of detected **MAC addresses** is displayed.
- Click the **APR** tab at the bottom of the main window.

Module 08 – Sniffers

 **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.

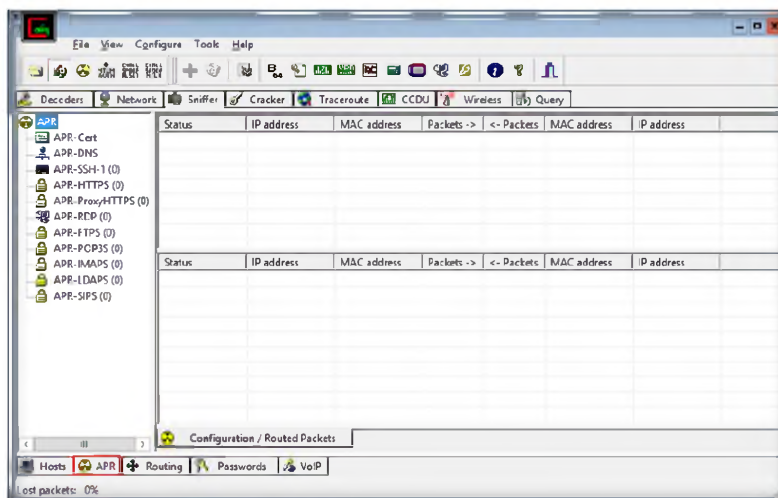


FIGURE 6.10: Cain & Abel ARP Tab

FIGURE 6.10: Cain & Abel ARP Tab

18. Click anywhere in the **Configuration/Routed Packets** window of APR to activate the **Plus** icon.

 **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.

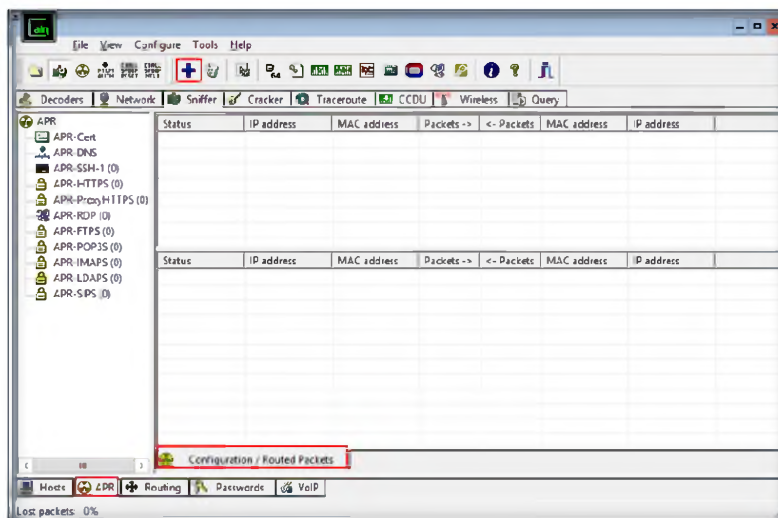


FIGURE 6.11: Cain & Abel ARP Tab

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

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.

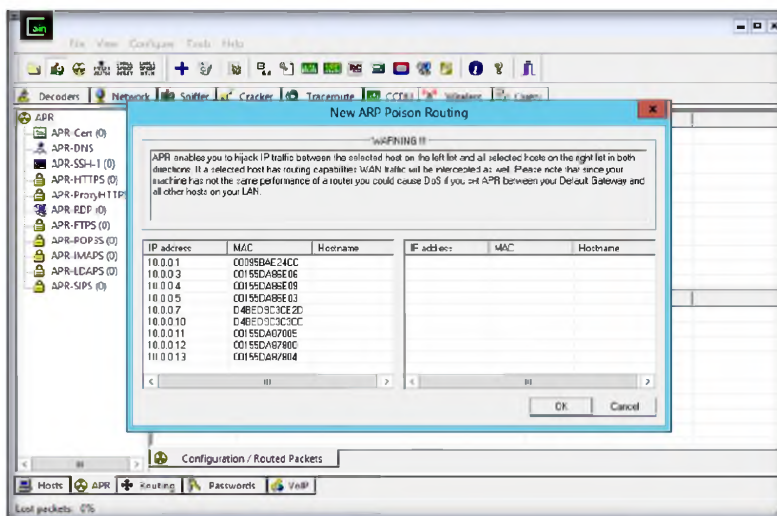


FIGURE 6.12: Cain & Abel ARP Tab

FIGURE 6.12: Cain & Abel ARP Tab

- To monitor the traffic between two computers, select **10.0.0.3** (Windows 8 virtual machine) and **10.0.0.5** (Windows 2008 Server virtual machine). Click **OK**.

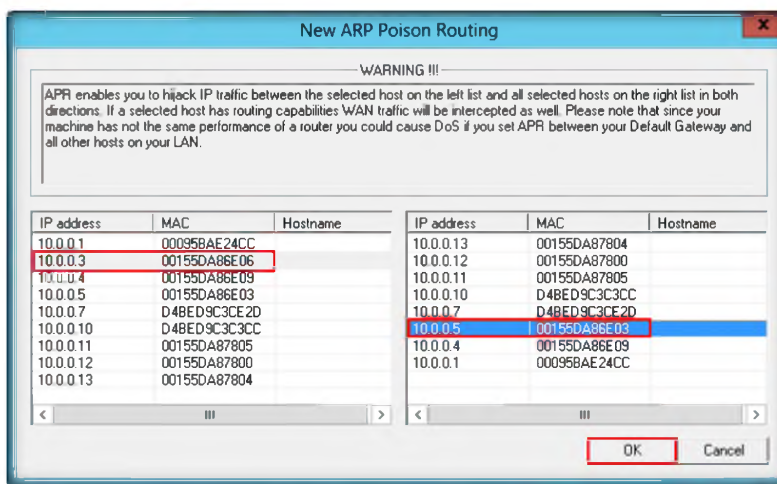


FIGURE 6.13: Cain & Abel ARP Tab

FIGURE 6.13: Cain & Abel ARP Tab

- Select the added IP address in the **Configuration/Routed** packets and click the **Start/Stop ARP** icon.

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

Module 08 – Sniffers

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

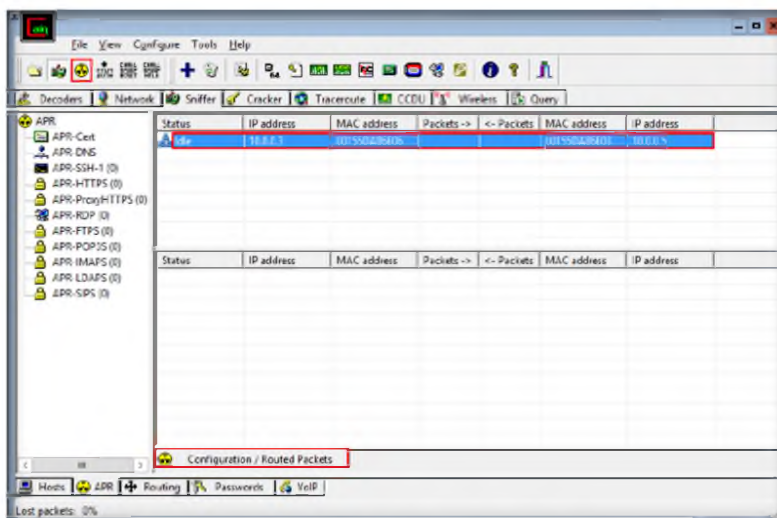


FIGURE 6.14: Cain & Abel ARP Poisoning

FIGURE 6.14: Cain & Abel ARP Poisoning

22. Now launch the command prompt in Windows 2008 Server and type **ftp 10.0.0.3** (IP address of Windows 8 machine) and press **Enter**.
23. When prompted for Username type **"Martin"** and press **Enter** and for 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

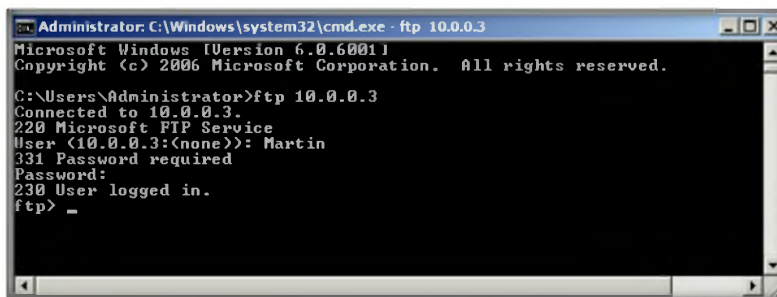


FIGURE 6.15: Start ftp://10.0.0.3

24. Now, on the host machine, observe the tool listing some packets exchange.

Module 08 – Sniffers

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

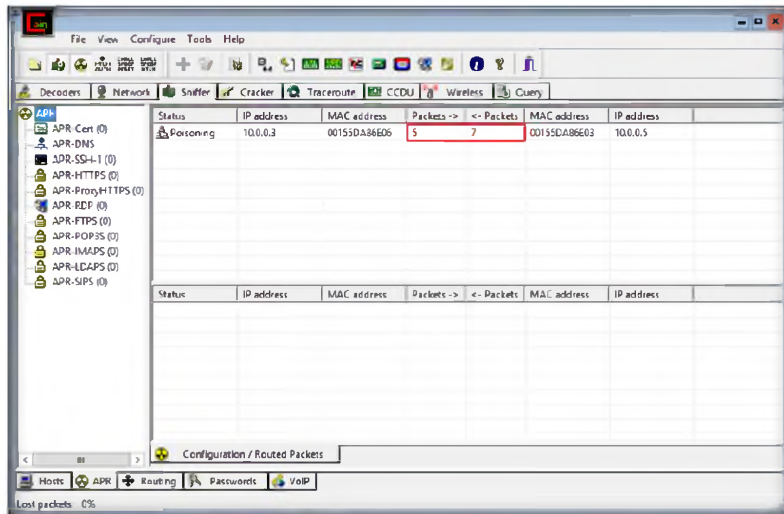


FIGURE 6.16: Sniffer window with more packets exchanged

FIGURE 6.16: Sniffer window with more packets exchanged

25. Click the **Passwords** tab as shown in the following screenshot to view the sniffed password for **ftp 10.0.0.3**.

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

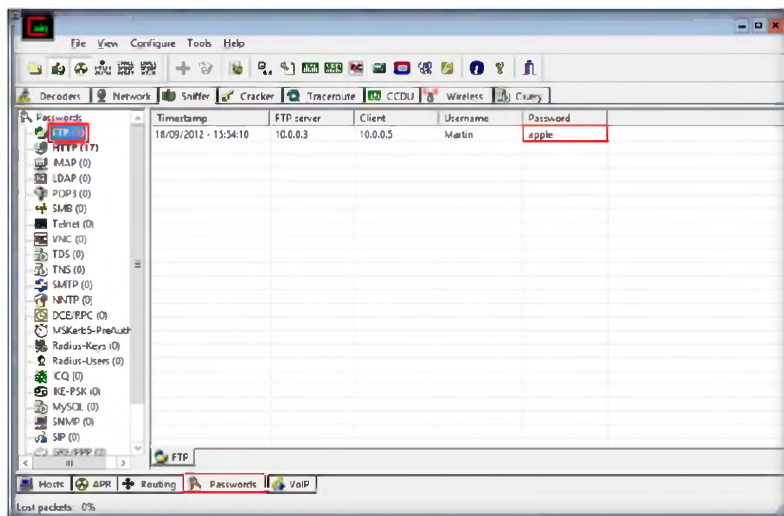


FIGURE 6.17: Sniffer window with more packets exchanged

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Cain & Abel	IP Address – 10.0.0.3 MAC Address – 00155DA86E06 Packets Sent – 5 Packets Received – 7 FTP Server – 10.0.0.3 Username – Martin Password – apple

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.
2. How can you easily find the password captured in an EDP MITM attack using only Notepad or some other text editor?
3. How can one protect a Windows Server against RDP MITM attacks?

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



Detecting ARP Attacks with the 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

Lab Scenario

You have already learned in the previous lab to capture user name and password information using Cain & Abel. Similarly, attackers, too, can sniff the username and password of a user. Once attackers have a user name and password, they can simply gain access to a network's database and perform illegitimate activities. If that account has administrator permissions, attackers can disable firewalls and load fatal viruses and worms on the computer and spread that onto the network. They can also perform different types of attacks such as denial-of-service attacks, spoofing, buffer overflow, heap overflow, etc.

When using a wireless connection, as an administrator you must use the strongest security supported by your wireless devices and also advise other employees to use a strong password. The passwords must be changed weekly or monthly.

Another method attackers can implement is ARP attacks through which they can snoop or manipulate all your data passing over the network. This includes documents, emails, and VoiceIP conversations. ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use the XArp tool, which provides advanced techniques to detect ARP attacks to prevent your data.

Lab Objectives

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

- To detect ARP attacks

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

Lab Environment

To carry-out the lab, you need:

- **XArp** is located at **D:\CEH-Tools\CEHv8 Module 08 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
- Double-click **xarp-2.2.2-win.exe** and follow the wizard-driven installation steps to install **XArp**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of XArp

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

Lab Tasks

TASK 1

Launching the XArp tool

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

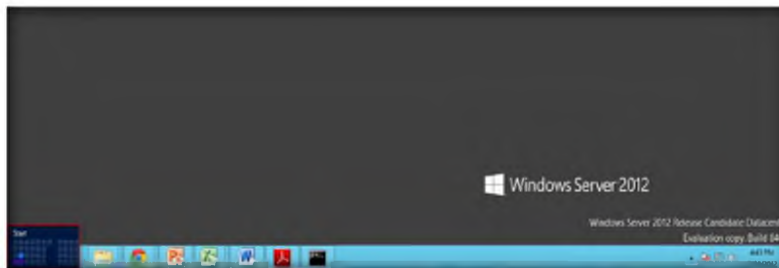


FIGURE 7.1: Windows Server 2012 – Desktop view

2. Click **XArp** in the **Start** menu to launch the XArp tool.

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

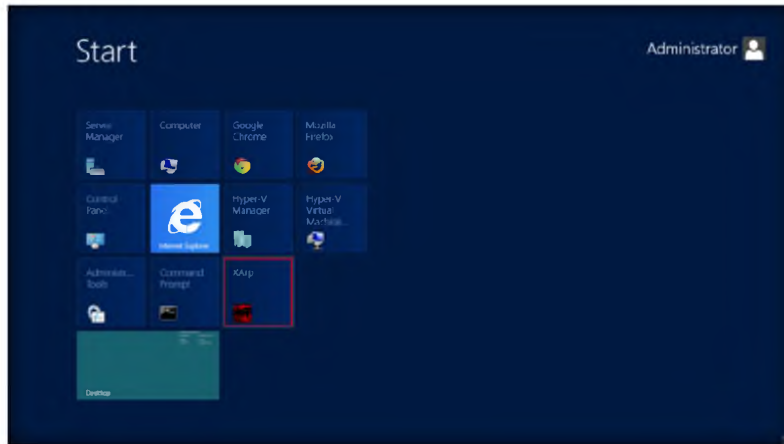


FIGURE 7.2: Windows Server 2012 – Apps

3. The main Window of XArp appears with 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.

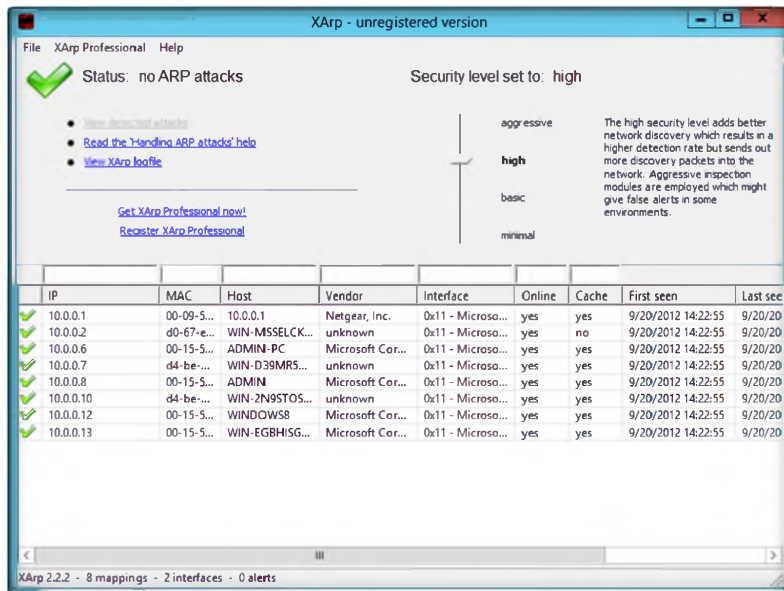


FIGURE 7.3: XArp status when security level set to high

4. On the host machine, XArp displays no ARP attacks.

Note: If you observe the same results, log in to a virtual machine and run Cain & Abel to initiate ARP poisoning to the host machine.

5. By default the security level is set to high. Set the **Security level** to **aggressive** on the XArp screen.

Module 08 – Sniffers

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.

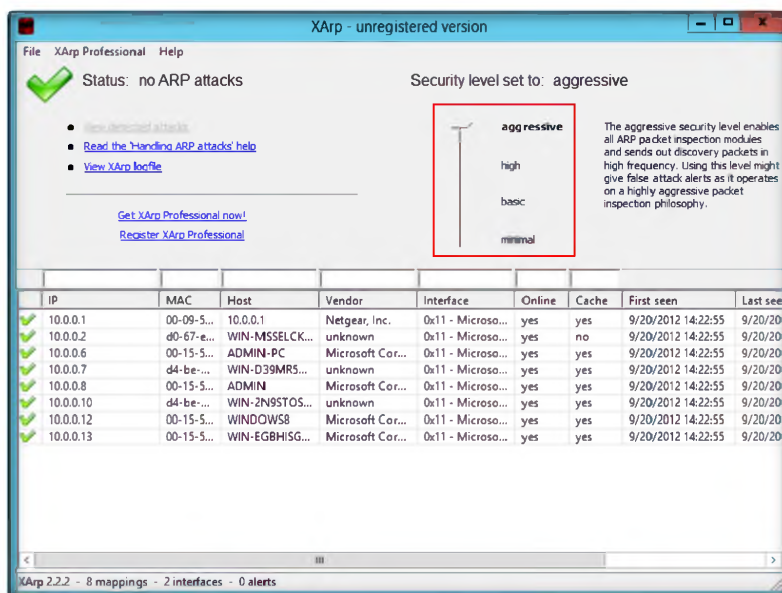


FIGURE 7.4: XArp status when security level set to aggressive

- Log in to Windows 2008 Server, and run Cain & Abel to initiate an ARP attack on a Windows 2012 host machine.
- 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.

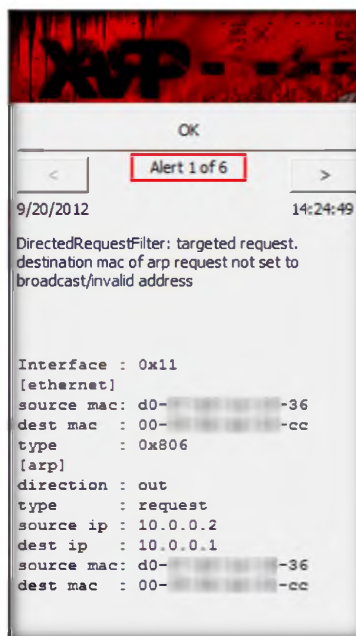


FIGURE 7.5: XArp displaying Alerts

- Now, the XArp **Status** changes to **ARP attacks detected**.

Module 08 – Sniffers

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.

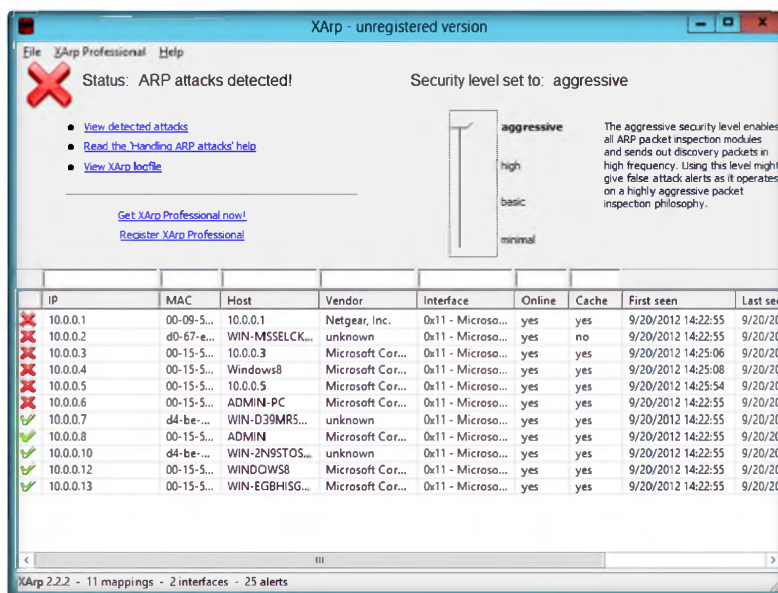


FIGURE 7.6: XArp – ARP attacks detected

Lab Analysis

Analyze and document the results related to the lab exercise.

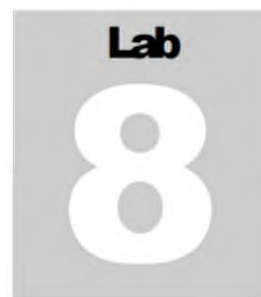
Tool/Utility	Information Collected/Objectives Achieved
XArp	Interface [Ethernet]: 0x11 Source Mac: d0-xx-xx-xx-xx-36 Destination Mac: 00-xx-xx-xx-xx-cc Type [arp]: 0x806 Direction: Out Source IP: 10.0.0.2 Destination IP: 10.0.0.1 Host: 10.0.0.1 Vendor: Netgear, Inc.

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

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



Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI

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

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

With an ARP storm attack, an attacker collects the IP address and MAC address of the machines in a network for future attacks. An attacker can send ARP packets to attack a network. If an ARP packet with a 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 the network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific technique with a protocol analyzer you should be able to identify the cause of the broadcast storm and a method to resolve the storm. Identify susceptible points on the network and protect them before attackers discover and exploit the vulnerabilities, especially on ARP-enabled LAN systems, a protocol with known security loopholes that allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all the packets that pass over a network. As an expert **ethical hacker** and **penetration tester** you must be aware of the tools to detect network interfaces running in promiscuous mode as it might be a network sniffer. In this lab you will learn to use the tool PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab to accomplish:

- To detect promiscuous systems in a network

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

Lab Environment

To carry-out the lab, you need:

- **PromqryUI** is located at **D:\CEH-Tools\CEHv8 Module 08 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 2008 Server**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

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

Lab Tasks

TASK 1

Running PromqryUI

1. Go to the tool location at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.
2. Double-click **promqryui.exe**, and click **Run**.

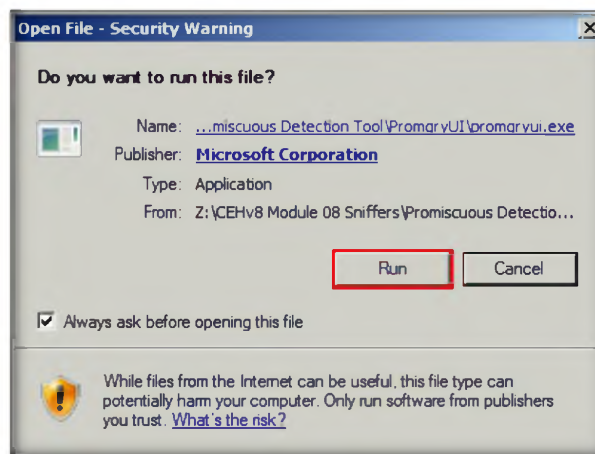


FIGURE 8.1: PromqryUI – Run prompt

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

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

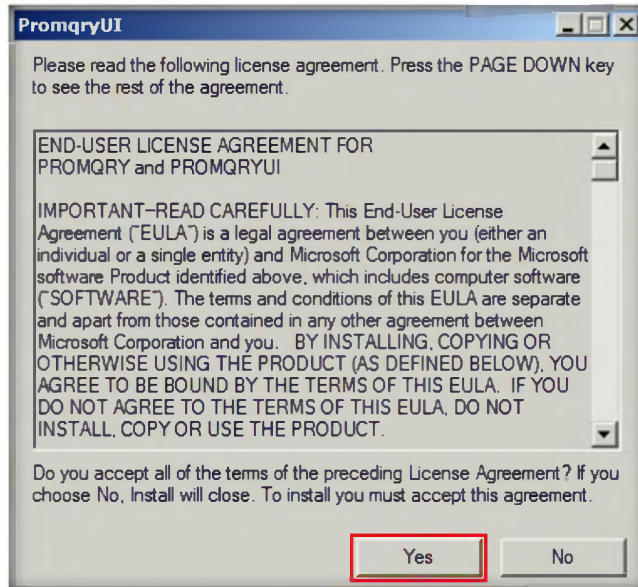


FIGURE 8.2: PromqryUI – License Agreement dialog box

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

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

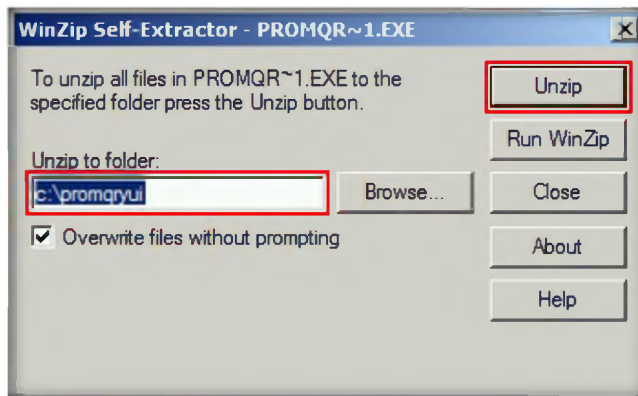


FIGURE 8.3: PromqryUI – WinZip Self-Extractor dialog box

- Click **OK** after the unzip is successful.



FIGURE 8.4: WinZip Self-Extractor dialog box

6. 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.

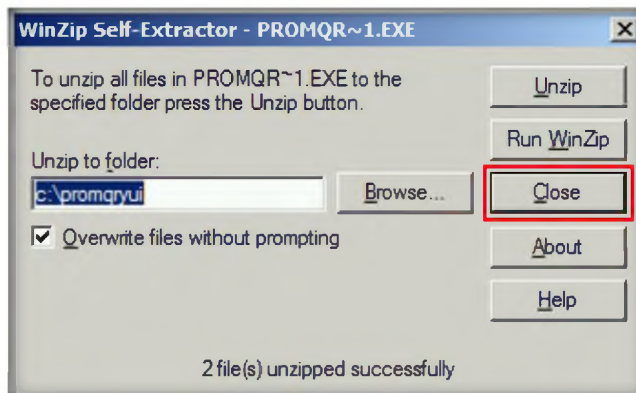


FIGURE 8.5: PromqryUI – WinZip Self-Extractor dialog box

7. Now, install **.NET Framework 1.1** by double-clicking the **dotnetfx.exe** file located at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.

8. Click **Run** in the **Open File - Security Warning** dialog box.

TASK 2

Running .NET Framework 1.1

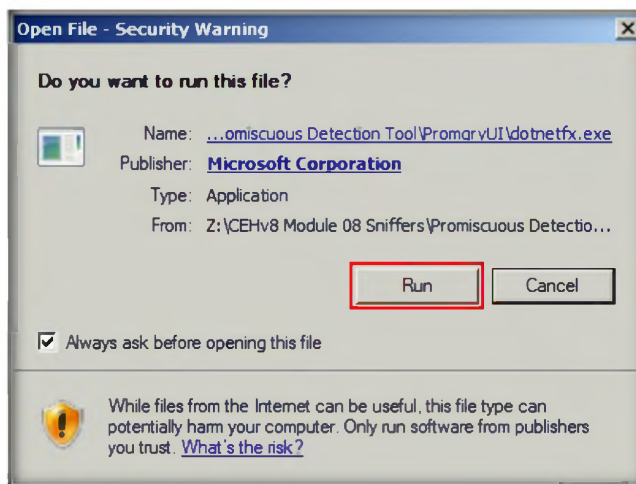


FIGURE 8.6: .NET Framework – Run dialog box

9. Click **Yes** to initiate the **.NET Framework** installation in the **Setup** dialog box.

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

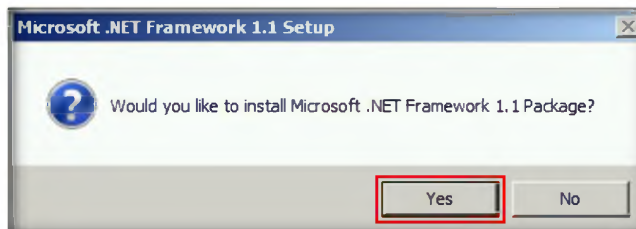


FIGURE 8.7: .NET Framework – Install dialog box

10. While attempting to install .NET Framework 1.1, you will get a **Program Compatibility Assistant** dialog box. Click **Run Program**.

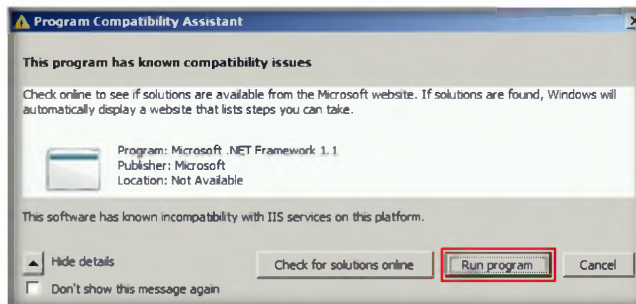


FIGURE 8.8: .NET Framework – Program Compatibility Assistant dialog box

TASK 3

Installing .NET Framework 1.1

11. Select the radio button for **I agree** and click **Install** in the **License Agreement** dialog box.

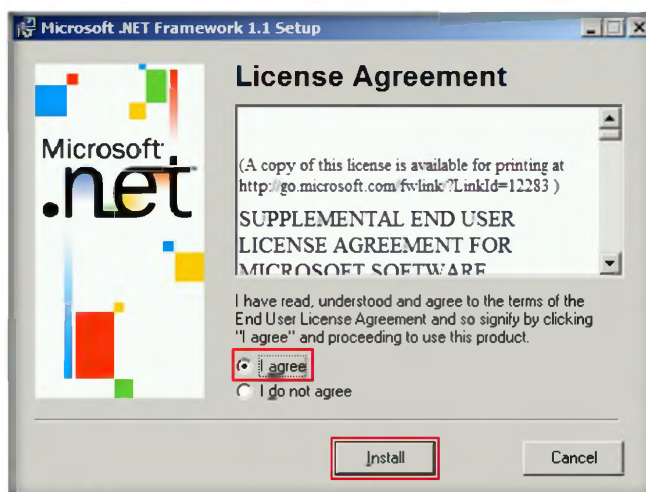


FIGURE 8.9: .NET Framework – License Agreement dialog box

12. Once the installation is complete, click **OK** in the **Microsoft .NET Framework 1.1 Setup** dialog box.

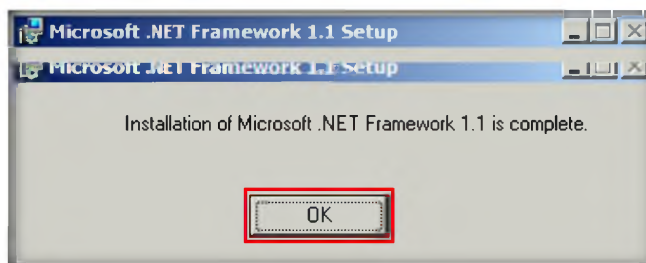


FIGURE 8.10: .NET Framework – Installation complete message box

TASK 3

Installing PromqryUI

13. Now, go to **C:\promqryui** and double-click **pqsetup.msi** and follow the installation wizard to install PromqryUI.

14. Once installation is complete, go to **Start** and click **Promqry** to launch the program.

✎ 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.

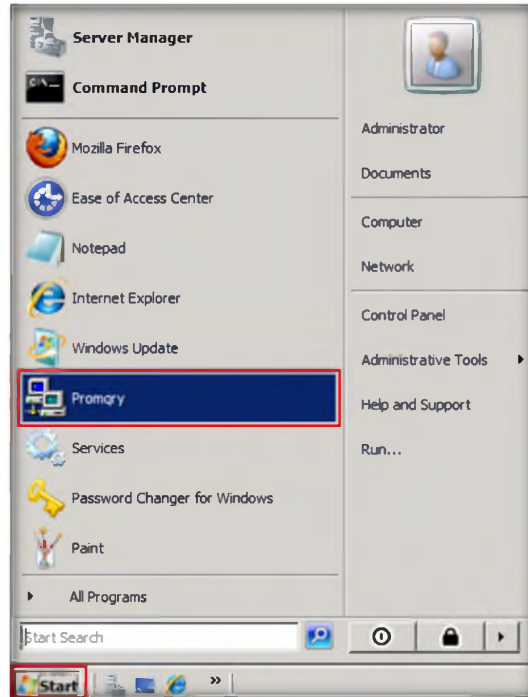


FIGURE 8.11: Windows 2008 Server – Start menu

15. The main window of PromqryUI appears. Click **Add**.

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

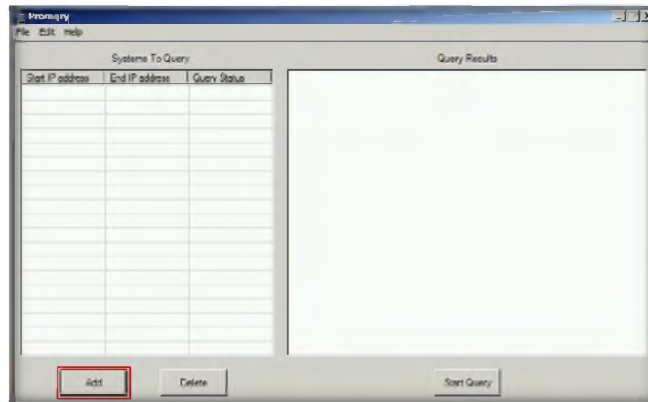


FIGURE 8.12: PromqryUI – Main window

16. The **Select Addition Type** dialog box will appear. Click **Add Single System**.

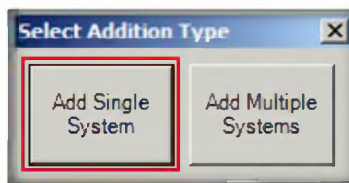


FIGURE 8.13: PromqryUI – Adding system

17. Type the IP address of the system you want to check for promiscuous mode in the **IP Address** field in the **Add System to Query** dialog box and click **Save**.

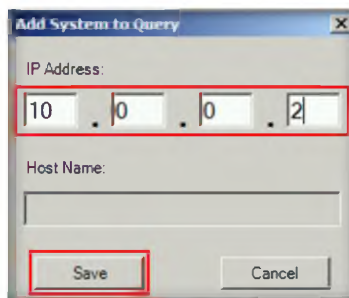


FIGURE 8.14: PromqryUI – Add System to Query

18. Select the added IP address in the **Systems To Query** section and click **Start Query**.

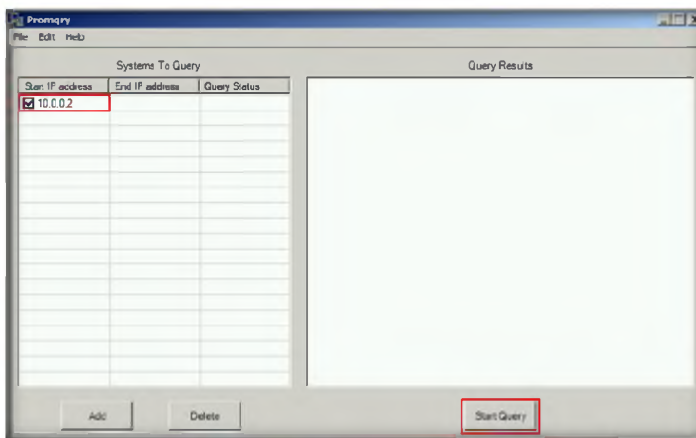


FIGURE 8.15: PromqryUI – Querying system

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.

19. Results will be displayed in **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, etc.

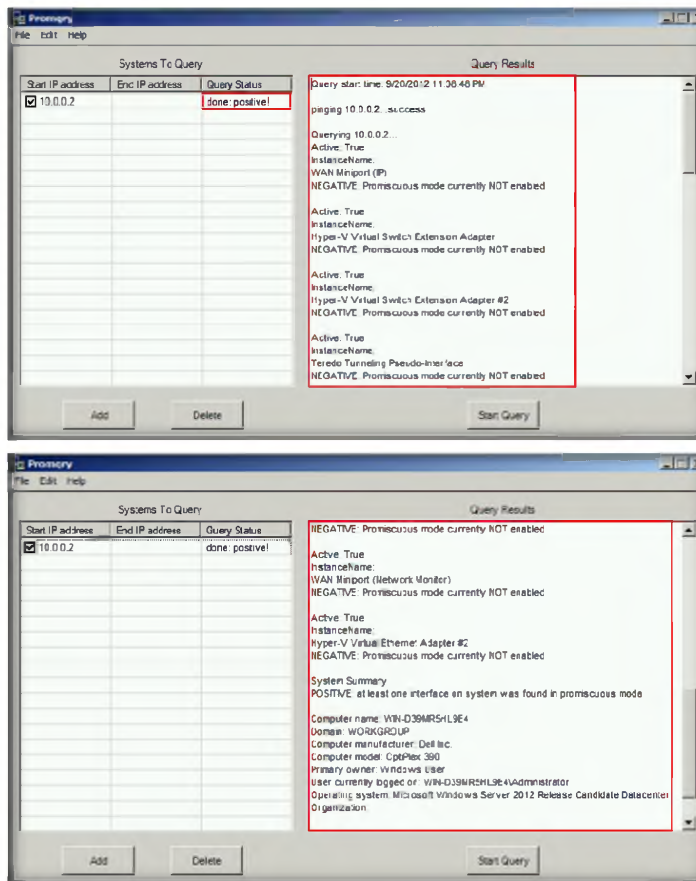


FIGURE 8.16: PromqyUI – Query Results

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
PromqyUI	Computer name: WIN-D39MR5HL9E4 Domain: WORKGROUP Computer manufacturer: Dell Inc. Computer model: OptiPlex 390 Primary owner: Windows User User currently logged on: WIN-D39MR5HL9E4\Administrator Operating system: Microsoft Windows Server 2012 Release Candidate Datacenter

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network

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



Sniffing Password from Captured Packets using Sniff – O – Matic

Sniff – O – Matic is a network protocol analyzer and packet sniffer with a clear and intuitive interface.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Attackers may install a sniffer in a trusted network to capture packets and will be able to view every single packet that is going across the network, if the network uses a hub or a router for data transmission. With the captured packets, attackers can learn about vulnerabilities and sniff the user name and password and log in to the network as an authenticated user. Once logged in successfully to a network, the hacker can easily install viruses and Trojans to steal data, sensitive information, and cause serious damage to that network.

As an expert **ethical hacker** and **penetration tester** you should have sound knowledge of sniffing, network protocols, and authentication mechanisms and encryption techniques. You should also regularly check your network and close the unnecessary ports that are open. Always ensure that if any sensitive data is required to be sent over the network, you use an encrypted protocol to minimize the data leakage.

Lab Objectives

The objective of this lab to sniff passwords using the tool Sniff – O – Matic through captured packets.

Lab Environment

To carry-out the lab, you need:

- **Sniff – O – Matic** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Sniff-O-Matic**
- You can also download the latest version of **Sniff – O – Matic** from <http://www.kwakkellap.com/sniffer.html>

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

- 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
- Double-click **snifftrial.exe** and follow the wizard-driven installation steps to install **Sniff – O – Matic**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Sniff – O – Matic

Sniff – O – Matic captures network traffic and enables you to analyze the data. Detailed packet information is available in a tree structure or a raw data view of the packet data. Sniff – O – Matic's button and columnar data display logically and succinctly presents the collected network traffic data.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.



FIGURE 9.1: Windows Server 2012 – Desktop view

2. Click **Sniff – O – Matic** in the **Start** menu to launch the Sniff – O – Matic tool.

TASK 1

Launching the Sniff-O-Matic tool

Sniff-O-Matic a packet sniffer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network.

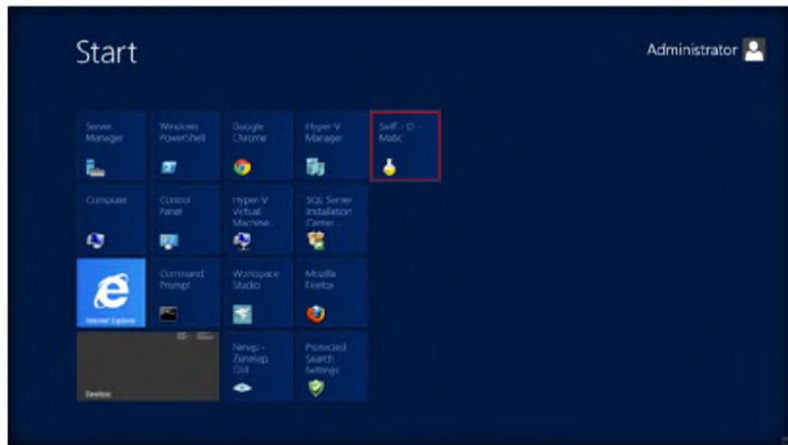


FIGURE 9.2: Windows Server 2012 – Desktop view

3. The main **Sniff – O – Matic** window appears; select the adapter from the drop-down list and click the **Start Capture**  button.

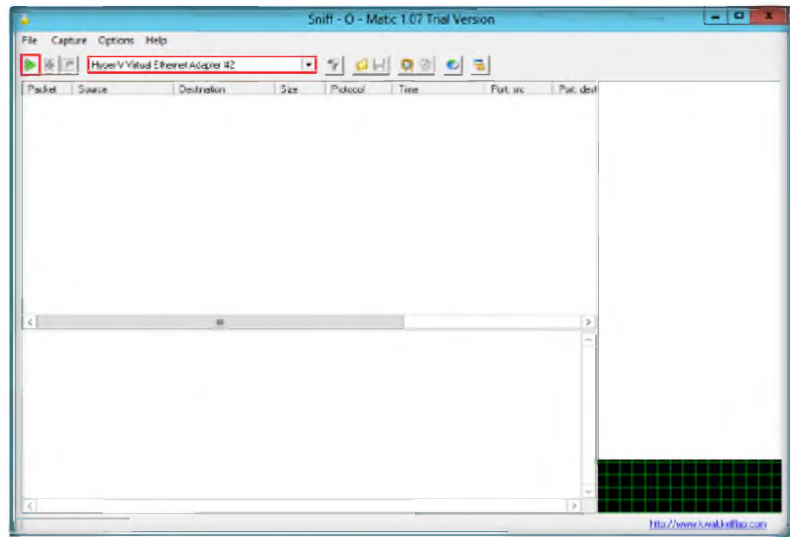


FIGURE 9.3: Sniff-O-Matic – Start capture

4. When the tool starts capturing the packets, launch a browser and log in to your email account.
5. Then, click the **Stop Capture**  button to view the captured packets.

TASK 2

Sniff-O-Matic: Start Packet Capture

Module 08 – Sniffers

Packet capture is the act of capturing data packets crossing a computer network.

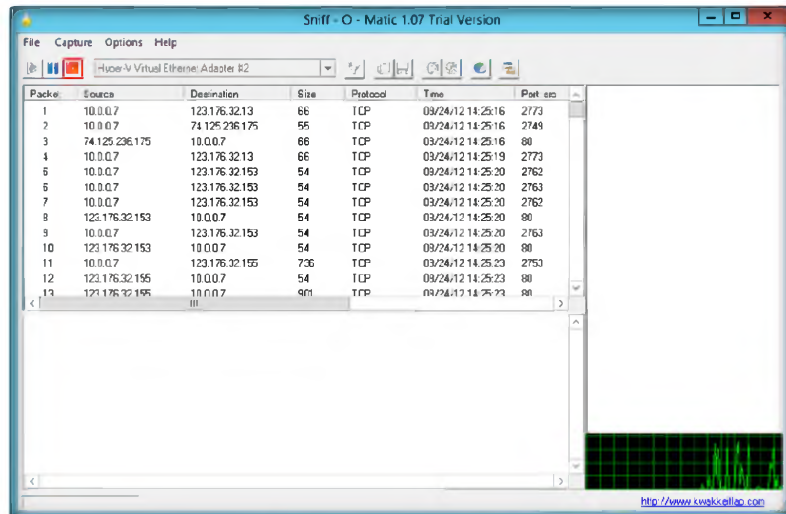


FIGURE 9.4: Sniff-O-Matic – Stop capture

FIGURE 9.4: Sniff-O-Matic – Stop capture

- In the list of captured packets, select a packet to view detailed information.

From the captured packets, detailed information such as Header Length, Protocol, Header Checksum, Source IP, Destination IP, etc. can be viewed by selecting a particular packet.

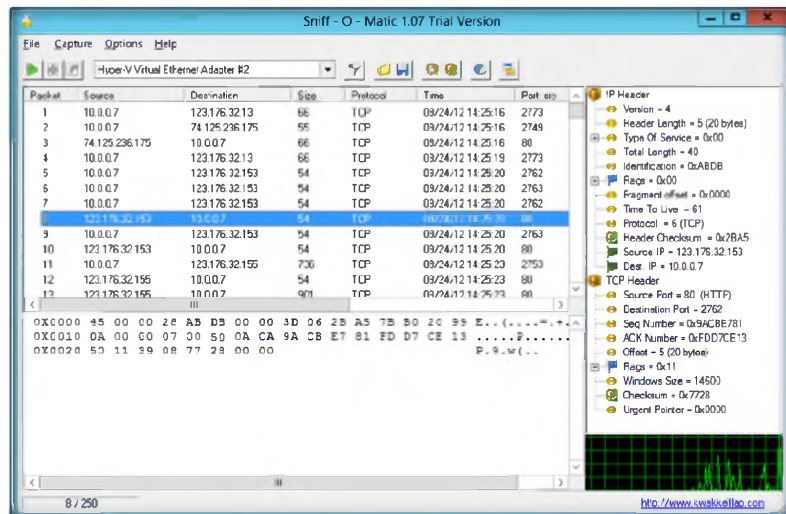


FIGURE 9.5: Sniff-O-Matic – Viewing packet information

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

- In the right pane, select items from the tree and the data for the respective item will be highlighted in red.

Module 08 – Sniffers

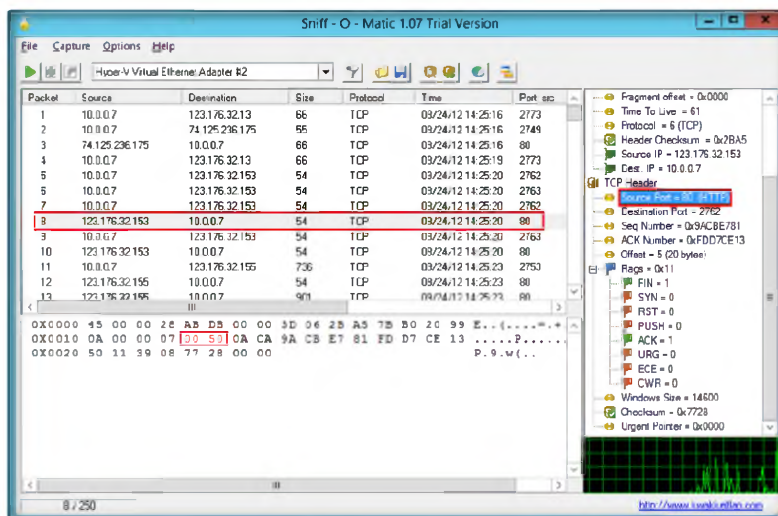


FIGURE 9.6: Sniff-O-Matic – Viewing packet information

Port numbers can occasionally be seen in a web or other service. By default, HTTP uses port 80 and HTTPS uses port 443, but a URL - `http://www.example.com:8080/path/` specifies that the web resource be served by the HTTP server on port 8080

- Now, perform a search for the data in captured frames. Select **Options** → **Find**.

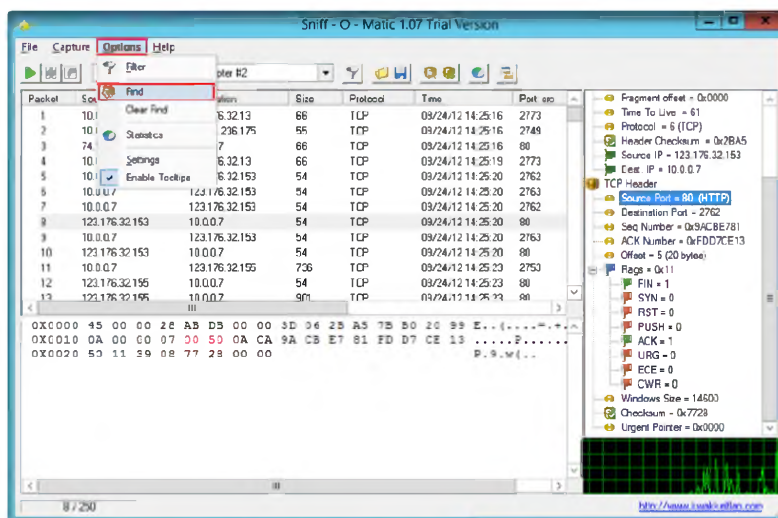


FIGURE 9.7: Sniff-O-Matic – Performing search

FIGURE 9.7: Sniff-O-Matic – Performing search

- The **Find** pop-up box appears; type **pwd** to search for the password information.

Module 08 – Sniffers

Detailed packet information is available in a tree structure or a raw data view of the packet data.

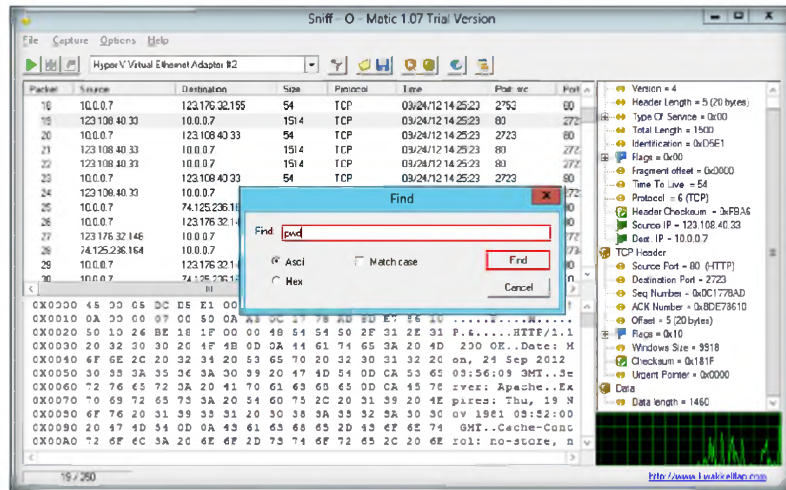


FIGURE 9.8: Sniff-O-Matic – Performing password search

FIGURE 9.8: Sniff-O-Matic – Performing password search

- An icon (packets with binoculars) will appear for the found packets, as shown in the following screenshot.

- Sniff-O-Matic's key features include:
- Capture IP packets on your LAN without packet loss
 - Monitor network activity in real time
 - Filters to show only the packets you want
 - Real-time checksum calculation
 - Save and load captured packets
 - Auto start capturing and continuous capture
 - Traffic charts with filter info

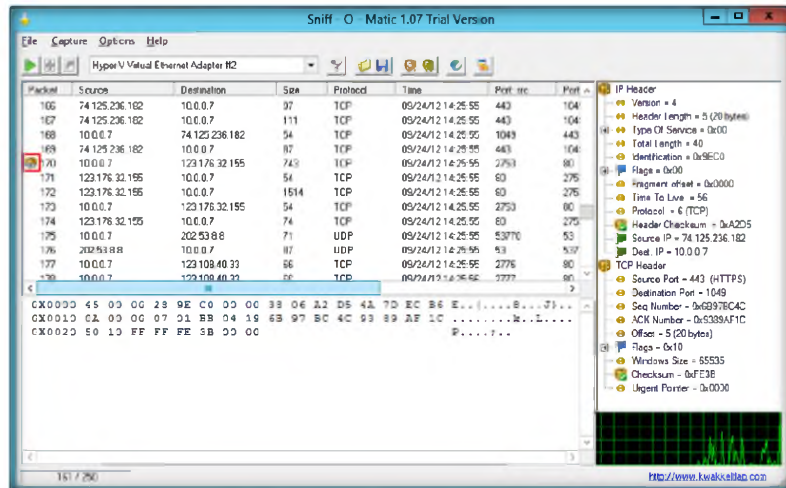


FIGURE 9.9: Sniff-O-Matic – Password search results

- Select the found packet and scroll down the data list for the information, which will be indicated in blue.

Module 08 – Sniffers

Packets captured using Sniff-O-Matic allows you to sniff the password available in cleartext format. If an attacker is able to capture these packets, he can easily identify the password and login to the network as an authenticated user. Attackers will have an advantage if they discover the same password is being used for all the computers.

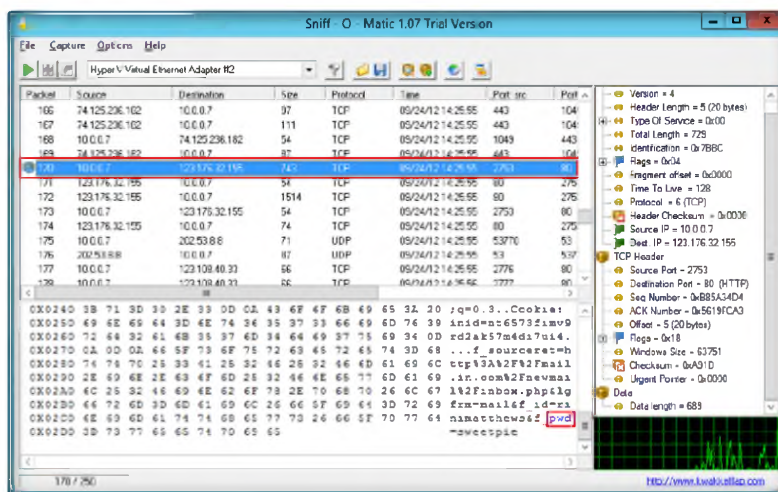


FIGURE 9.10: Sniff-O-Matic – Password search results

12. To mark the packets, right-click the selected packet and click **Mark**.

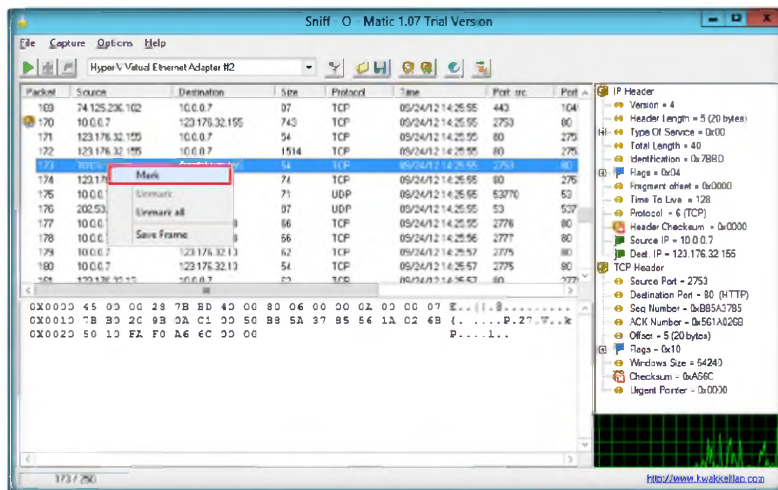


FIGURE 9.11: Sniff-O-Matic – Marking a packet

13. Once the packets are marked, they will have a different icon.

One of the features of the tool includes, protocol and port data, the program displays source and destination IP addresses, and raw packet information. The program offers no IP address to domain name conversion..

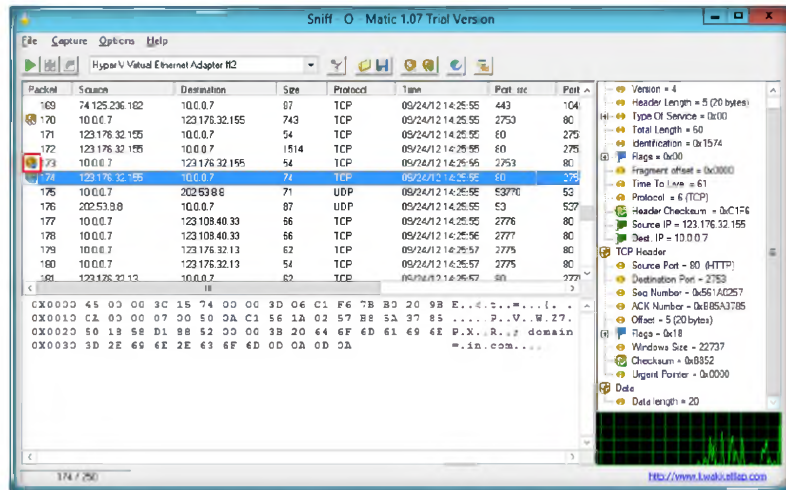


FIGURE 9.12: Sniff-O-Matic – Marked packets

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Sniff-O-Matic	Header Length: 5 Time To Live: 61 Protocol: 6 Header Checksum: 0xC1F6 Source IP: 123.176.32.155 Dest. IP: 10.0.0.7 Source Port: 80 (HTTP) Destination Port: 2753 Username and password

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

Module 08 – Sniffers

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