Hacking Wireless Networks

Module 14

Hacking Wireless Networks

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to applications and data throughout a radio network.

ICON KEY

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

Lab Scenario

Wireless network technology is becoming increasingly popular, but at the same time, it has many security issues. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. However, the convenience of WLANs also introduces security concerns that do not exist in a wired world. Connecting to a network no longer requires an Ethernet cable. Instead, data packets are airborne and available to anyone with ability to intercept and decode them. Several reports have explained weaknesses in the Wired Equivalent Privacy (WEP) algorithm by 802.11x standard to encrypt wireless data.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of wireless concepts, wireless encryption, and their related threats. As a security administrator, you must protect your company's wireless network from hacking.

Lab Objectives

The objective of this lab is to protect the wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks

In this lab, you will need a web browser with an Internet connection.

- This lab requires AirPcap adapter installed on your machine for all labs

Lab Duration

Time: 35 Minutes

Overview of Wireless Network

"Wireless network" refers to any type of computer network commonly associated with telecommunications whose interconnections between nodes are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves such as radio waves for the carrier. The implementation usually takes place at the physical level or layer of the network.

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 Wireless Networks are:

- WiFi Packet Sniffing Using AirPcap with **Wireshark**
- Sniffing the Network Using the **OmniPeek Network Analyzer**
- Cracking a WEP Network with **Aircrack-ng** for Windows

Lab Analysis

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

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

Lab 1

WiFi Packet Sniffing Using AirPcap with Wireshark

The AirPcap adapter is a USB device that, when used in tangent with the AirPcap drivers and WinPcap libraries, allows a pen tester to monitor 802.11b/g traffic in monitor mode.

ICON KEY

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

Lab Scenario

Wireless networks can be open to active or passive attacks. These attacks include DoS, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab, we discuss Wireshark, a tool that can sniff s network using a wireless adapter. Because you are the ethical hacker and penetration tester of an organization, you need to check the wireless security, exploit the flaws in WEP, and evaluate weaknesses present in the WEP of your organization.

Lab Objectives

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

- Discover WEP packets

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks

To execute this lab, you will need:

- To install AirPcap adapter drivers: navigate to **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\AirPcap - Enabled Open Source Tools**, and double-click **setup_airpcap_4_1_1.exe** to install
- When you are installing the AirPcap adapter drivers, if any installation error occurs, install the AirPcap adapter drivers in compatibility mode (right-click the **AirPcap adapter driver** exe file, select **Properties → Compatibility**, check **Run this program in compatibility mode for**, and select **Windows 7**)
- Wireshark is located at **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\AirPcap - Enabled Open Source Tools**
- Run this lab in **Windows Server 2012** (host machine)
- An access point configured with WEP on the host machine
- **This lab requires the AirPcap adapter installed on your machine. If you don't have this adapter, please do not proceed with this lab.**
- A standard AirPcap adapter with its drivers installed on your host machine
- WinPcap libraries, Wireshark, and Cain & Abel installed on your host machine
- Administrative privileges to run AirPcap and other tools

- A client connected to a wireless access point

Lab Duration

Time: 10 Minutes

Overview of WEP (Wired Equivalent Privacy)

Several serious **weaknesses** in the protocol have been identified by cryptanalysts with the result that, today, a WEP connection can be easily cracked. Once entered into a network, a skilled hacker can **modify** software, **network settings**, and other **security** settings.

Wired Equivalent Privacy (WEP) is a deprecated security **algorithm** for IEEE 802.11 wireless networks.

Lab Tasks

Download AirPcap drivers from the site and follow the steps to install AirPcap drivers.

TASK 1

Configure AirPcap

1. Plug in the AirPcap device in a USB port and wait for the hardware installation to complete.
2. Launch the **AirPcap Control Panel** application from the **Apps** screen.

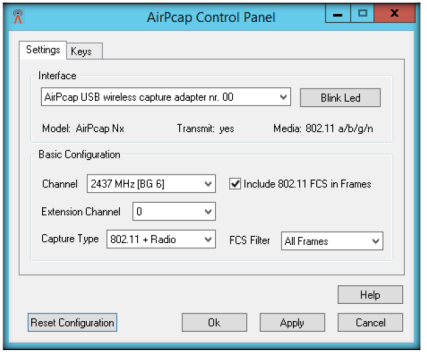
You can download AirPcap drives from http://www.airdemon.net/riverbed.html

FIGURE 1.1: Launching AirPcap Control Panel application from the Apps screen

The AirPcap adapters can work in monitor mode. In this mode, the AirPcap adapter captures all of the frames that are transferred on a channel, not just frames that are addressed to it.

3. The **AirPcap Control Panel** window appears, as shown in the screenshot:

The Multi-Channel Aggregator can be configured like any real AirPcap device, and therefore can have its own decryption, FCS checking and packet filtering settings.



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

FIGURE 1.2: AirPcap Control Panel window

4. In the **Basic Configuration** section, select a suitable **channel** from the **Channel** drop-down list, and set a frequency you want to capture from the **Capture Type** drop-down list.

In Basic Configuration box settings: Channel: The channels available in the Channel list box depend upon the selected adapter. Since channel numbers 14 in the 2.4 GHz and 5 GHz bands overlap and there are center frequencies (channels) that do not have channel numbers., Each available channel is given by its center frequency.

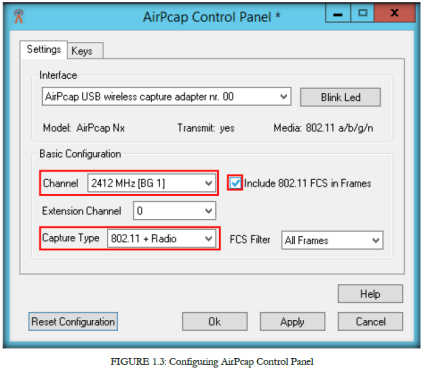


FIGURE 1.3: Configuring AirPcap Control Panel

5. Click the **Keys** tab. Ensure that the **Enable WEP Decryption** check box is selected. This enables the WEP decryption algorithm. You can **Add New Key**, **Remove Key**, **Edit Key**, and **Move Key UP or Down**.
6. After configuring settings and keys, click **OK**.

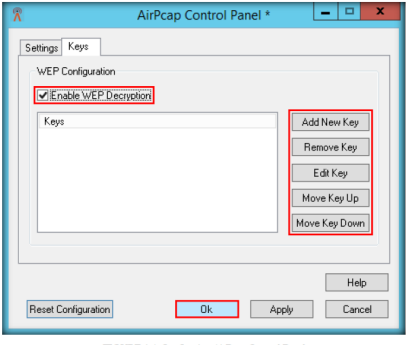


FIGURE 1.4: Configuring AirPcap Control Panel

In Basic Configuration Settings: Extension Channel: For 802.11n adapters, one can use the Extension Channel list to create a "wide" channel. The choices are -1 (the preceding 20 MHz frequency band), 0 (no extension channel), or +1 (the succeeding 20 MHz frequency band). The channel of the additional frequency band is called the extension channel.

TASK 2

Configure Wireshark

7. Launch **Wireshark Network Analyzer** from the **Apps** screen. The **Wireshark** main window appears, as shown in the following screenshot:

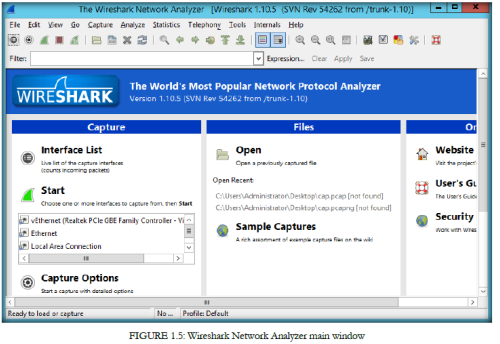


FIGURE 1.5: Wireshark Network Analyzer main window

8. Configure AirPcap as an interface to Wireshark. To do this, select **Capture → Interfaces...**.

The following are some of the many features Wireshark provides 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.
- **Filter** packets on many criteria.
- **Search** for packets on many criteria.
- **Colorize** packet display based on filters.
- Create various **statistics**

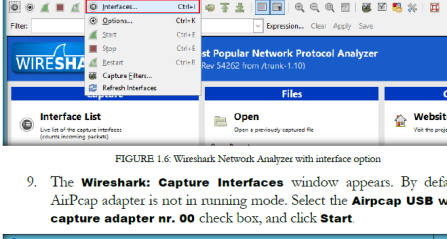


FIGURE 1.6: Wireshark Network Analyzer with interface option

9. The **Wireshark: Capture Interfaces** window appears. By default, the AirPcap adapter is not in running mode. Select the **Airpcap USB wireless capture adapter nr. 00** check box, and click **Start**.

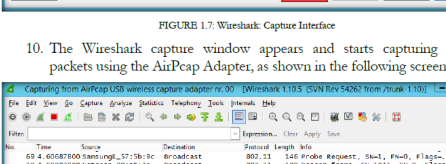


FIGURE 1.7: Wireshark: Capture Interface

TASK 3

Capture Packets

10. The Wireshark capture window appears and starts capturing wireless packets using the AirPcap Adapter, as shown in the following screenshot:

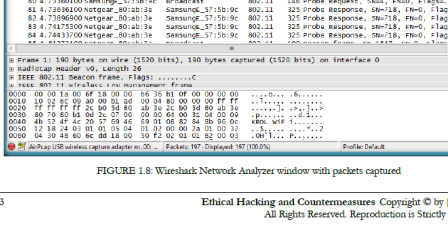


FIGURE 1.8: Wireshark Network Analyzer window with packets captured

Note: Wireshark isn't an intrusion detection system. It does not warn you when someone does 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.

11. You will be able to view the **source** and **destination** of the packets captured by Wireshark.

One possible alternative is to run tcpdump, or the dumpcap utility that comes with Wireshark, with superuser privileges to capture packets into a file, and later analyze these packets by running Wireshark with restricted privileges on the packet capture dump file.

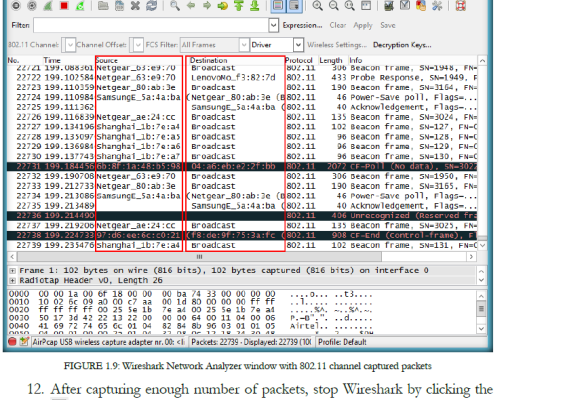


FIGURE 1.9: Wireshark Network Analyzer window with 802.11 channel captured packets

Wireshark is a network packet analyzer that captures network packets and tries to display that packet data as detailed as possible.

12. After capturing enough number of packets, stop Wireshark by clicking the icon in the Wireshark toolbar.

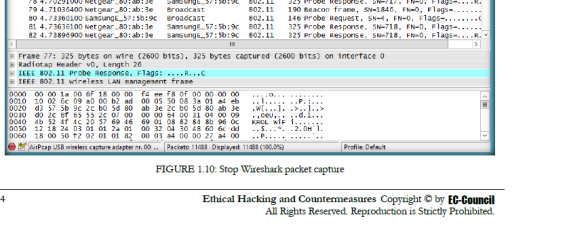


FIGURE 1.10: Stop Wireshark packet capture

Wireshark can open packets captured from a large number of other capture programs.

13. Go to **File** in the menu bar, and select **Save**.

The latest version is faster and contains a lot of new features, like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

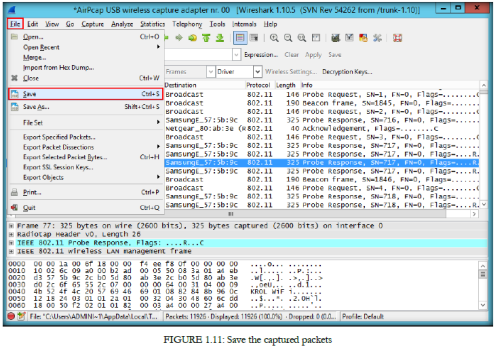


FIGURE 1.11: Save the captured packets

14. Enter the **File name**, and click **Save**.

Wireshark can capture traffic from many different network media types—and despite its name—including wireless LAN as well. Which media types are supported, depends on many things, such as the operating system you are using.

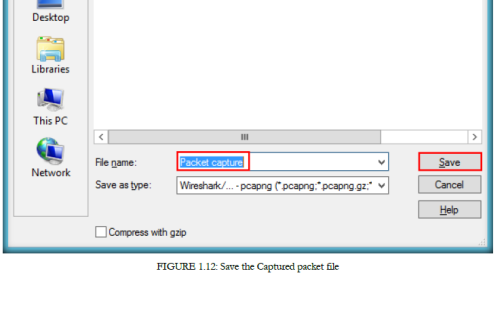


FIGURE 1.12: Save the Captured packet file

15. You can access the saved packet capture file anytime, and by issuing packet filtering commands in the Filter field, you can narrow down the packet search in an attempt to find packets containing sensible information.
16. In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Lab Analysis

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

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

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

Lab 2

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

Packet sniffing is a form of wire-tapping applied to computer networks. It came into vogue with the Ethernet, and as such, this means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic address to other stations. Sniffing programs turn off the filter, and thus see everyone traffic. Most of the hubs/switches allow the inducer to sniff remotely using SNMP, which has weak authentication. Using POP, IMAP, HTTP Basic, and talent authentication, an intruder can read the password off the wire in cleartext.

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. OmniPeek network analysis performs deep packet inspection, network forensics, troubleshooting, and packet and protocol analysis of wired and wireless networks. In this lab, we discuss wireless packet analysis of captured packets.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks

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 will need:

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

Lab Duration

Time: 10 Minutes

Overview of OmniPeek Network Analyzer

You can download OmniPeek Network Analyzer from www.wildpackets.com.

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 802.11 a/b/g/n.

Lab Tasks

TASK 1

Install OmniPeek Network Analyzer

Note: If you have already installed the tool, launch it from the **Apps** screen and skip to **step 22**.

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

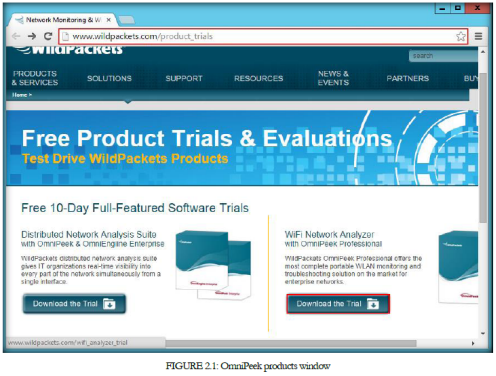


FIGURE 2.1: OmniPeek products window

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

Note: You need to specify a non-personal business email ID at the time of registration.

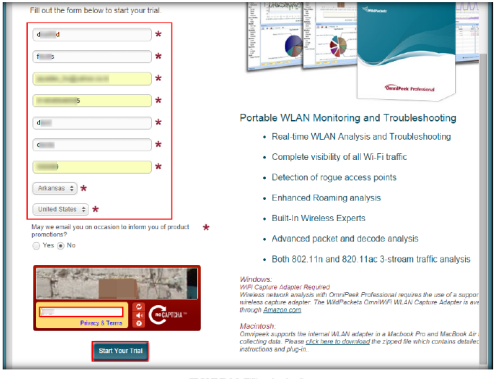


FIGURE 2.2: Filling the details

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

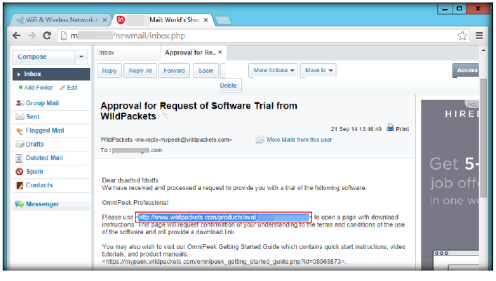


FIGURE 2.3: Email account containing the download link

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

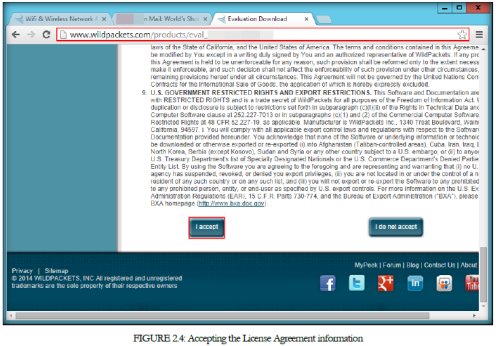


FIGURE 2.4: Accepting the License Agreement information

7. The OmniPeek download page appears containing the serial number as well as the download link. Copy the serial number, and click the download button.

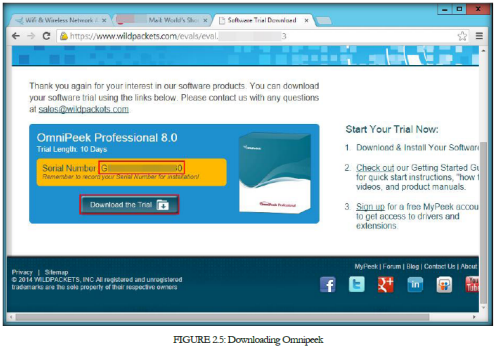


FIGURE 2.5: Downloading Omnipeek

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

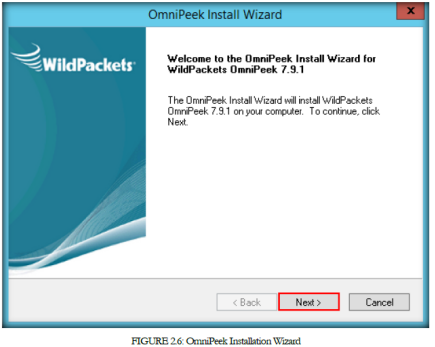


FIGURE 2.6: OmniPeek Installation Wizard

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

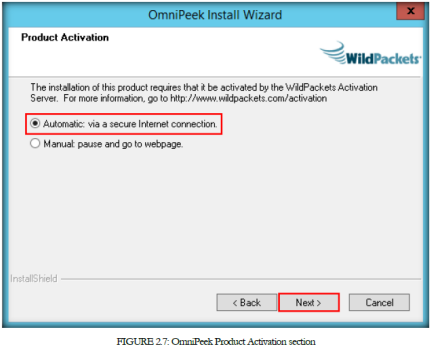


FIGURE 2.7: OmniPeek Product Activation section

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

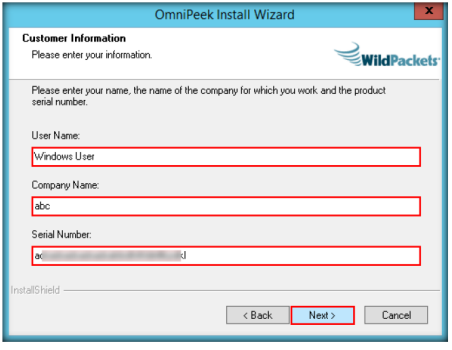


FIGURE 2.8: OmniPeek Customer Information section

14. The **Automatic Activation** step appears; enter your **Email ID,** and click **Next**.

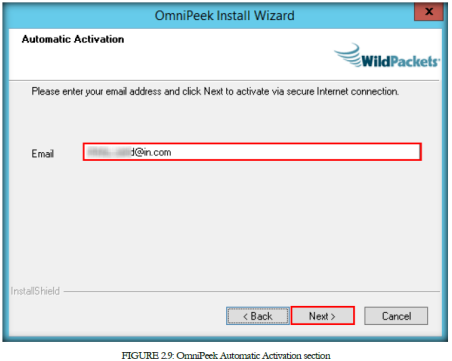


FIGURE 2.9: OmniPeek Automatic Activation section

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

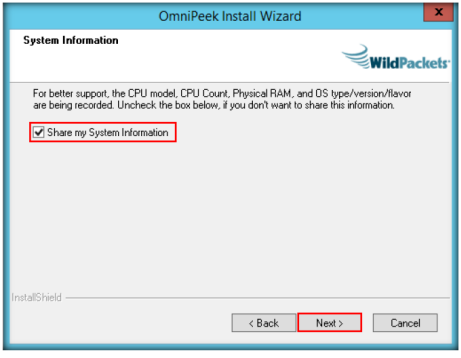


FIGURE 2.10: OmniPeek System Information section

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

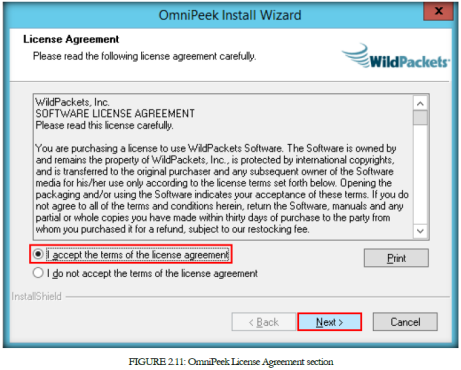


FIGURE 2.11: OmniPeek License Agreement section

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

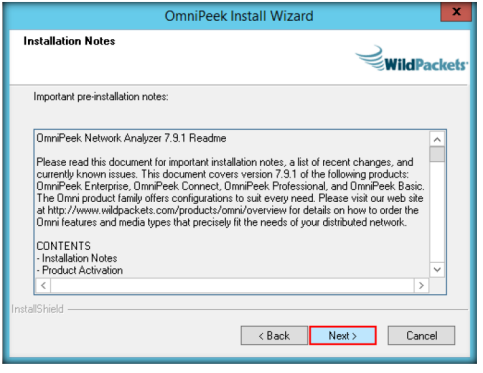


FIGURE 2.12: OmniPeek Installation Notes section

18. The **Setup Type** step appears; select the **Complete** radio button, and click **Next**.

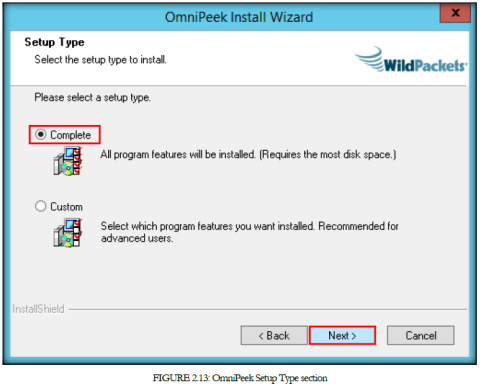
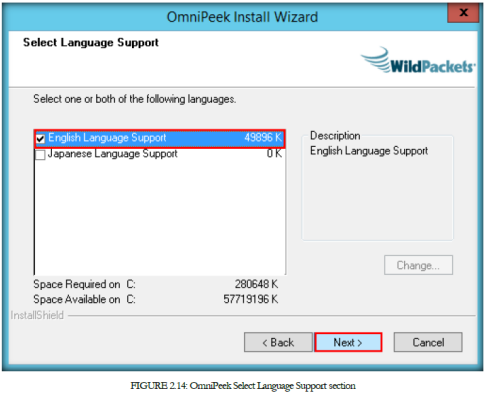


FIGURE 2.13: OmniPeek Setup Type section

19. The **Select Language Support** step appears; select the language support and click **Next**. The selected **English Language Support** is shown below.



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 2.14: OmniPeek Select Language Support section

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

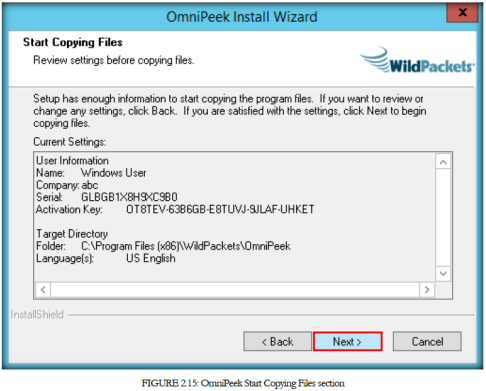


FIGURE 2.15: OmniPeek Start Copying Files section

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

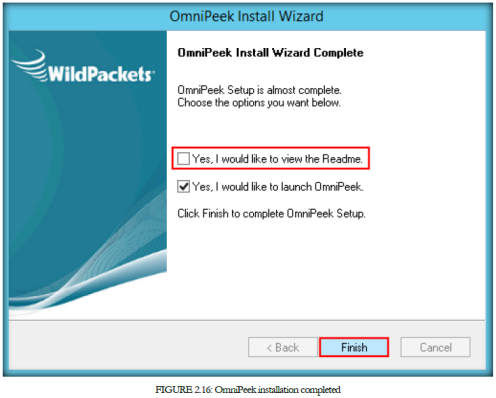


FIGURE 2.16: OmniPeek installation completed

22. The **OmniPeek** dialog box appears; click **OK**.

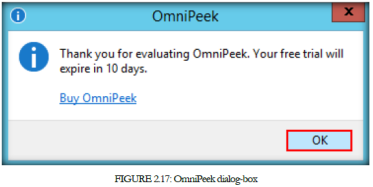


FIGURE 2.17: OmniPeek dialog-box

23. The main window of WildPackets OmniPeek appears; click **View sample files** link, under **Resources**.

Note: For demonstration purpose, in this lab, we are examining a sample capture file instead of actually capturing wireless traffic.

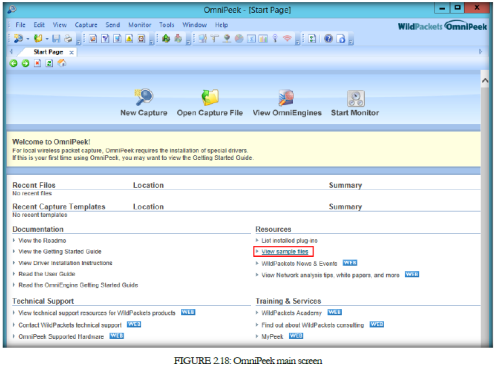


FIGURE 2.18: OmniPeek main screen

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.

24. The **Sample Files** step appears; click the **WPA2.wpz** link to load the sample capture file containing WPA2 encrypted traffic.

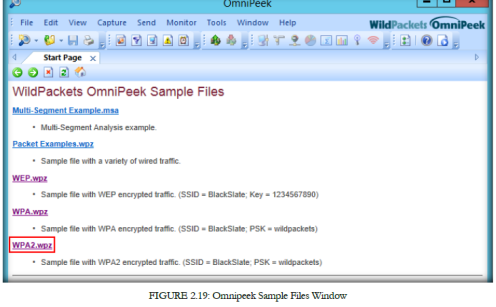


FIGURE 2.19: Omnipeek Sample Files Window

OmniPeek gives network engineers real-time visibility and Expert Analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices.

25. **WPA2.wpz** opens in the window. Select **Packets** under **Dashboards** section in the left pane. The capture window appears, displaying WPA2 encrypted traffic.

26. Double-click any of the packets in the right pane.

Comprehensive network performance management and monitoring of entire enterprise networks, including network segments at remote offices.

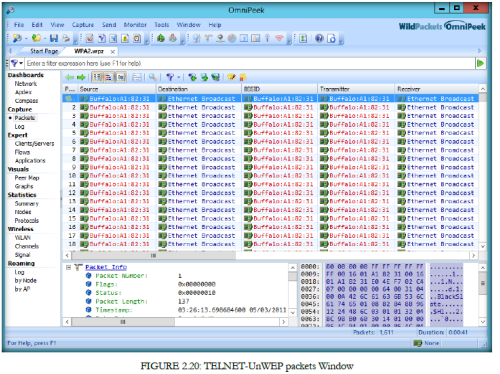


FIGURE 2.20: TELNET-UnWEP packets Window

27. Click the right arrow to view the next packet.

OmniPeek Connect manages an organization's Omnipliance and TimeLine network recorders, and provides all the console capabilities of OmniPeek Enterprise with the exception of local capture and VoIP call playback.

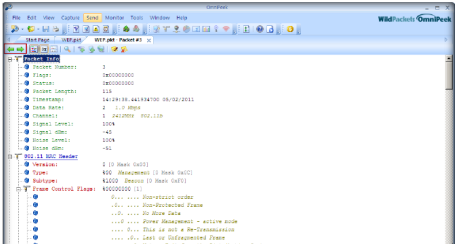


FIGURE 2.21: TELNET-UnWEP packets frame window

28. Close the tab from the top and select different options from the right pane, and click **Graphs**.

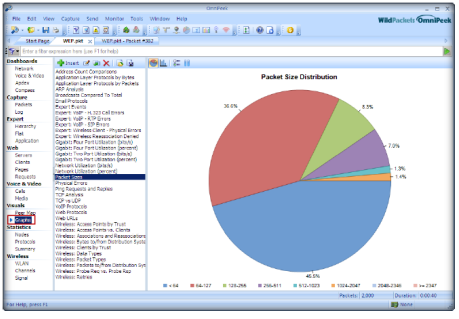


FIGURE 2.22: WEP Graphs window

29. Now, experiment with all the options in the left pane.

OmniPeek Enterprise also provides advanced Voice and Video over IP functionality including signaling and Media analyses of voice and video, VoIP playback, voice and video Expert Analysis, Visual Expert, and more.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data-packet generation rates.

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

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

Lab 3

Cracking a WEP Network with Aircrack-ng for Windows

Aircrack-ng is an 802.11 WEP and WPA-PSK keys–cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, and the all-new PTW attack, thus making this attack much faster than those using other WEP cracking tools.

ICON KEY

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

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, attackers will descend in droves to test your wireless network with it.

WEP is used for wireless networks; always change your SSID from the default, before you actually connect the wireless router for the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used, because war-driving tools can easily detect your internal IP addressing if the SSID broadcasts are enabled and the DHCP is being used.

Tools demonstrated in this lab are available on D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in your organization's WEP. In this lab, we discuss how WPA keys are cracked using standard attacks such as KoreK and PTW.

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

To execute this lab, you will need:

- **Aircrack-ng** located at **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng**
- You can also download the latest version of **Aircrack-ng** from the link http://www.aircrack-ng.org/downloads.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in Windows Server 2012
- Administrative privileges to run the tool
- A client connected to a wireless access point
- **This lab requires AirPcap adapter installed on your machine. If you don't have this adapter please do not proceed with the lab.**

Lab Duration

Time: 15 Minutes

Overview of Aircrack-ng

A "wireless network" is any type of computer telecommunications network, the interconnections between the nodes of which are made without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier, and this implementation usually takes place at the physical level, or layer, of the network.

Lab Task

TASK 1

Launch airodump-ng

1. Launch **airodump-ng** (a subset of aircrack-ng suite) **GUI** from **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin** by double-clicking **airodump-ng-airpcap.exe**.
2. If the **Open-File Security Warning** pop-up appears, click **Run**.

3. The **airodump-ng** GUI appears, as shown in the following screenshot:

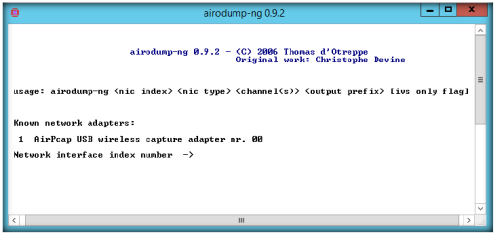
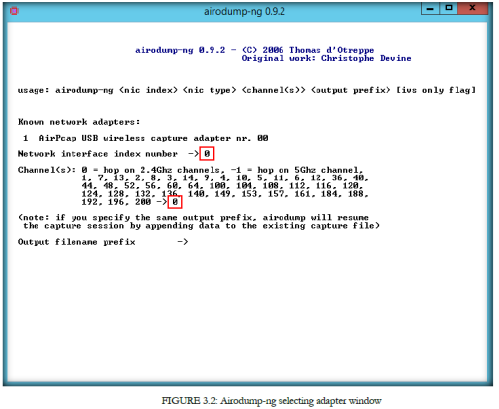


FIGURE 3.1: Airodump-ng selecting adapter window

Aircrack-ng option: -b bssid Long version – bssid. Select the target network based on the access point's MAC address.

4. Type the Airpcap adapter index number **0** and select channel number **0**. Then press **Enter**.
5. Channel 0 refers to all the 2.4 GHz channels. In this lab, we are configuring airodump-ng to capture 2.4 GHz channels.



For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. SSE2 support is included to dramatically speed up WPA/WPA2 key processing.

FIGURE 3.2: Airodump-ng selecting adapter window

6. It will prompt you for a file name. Specify the name as **capture** and press **Enter**.
7. Type **y** in **Only write WEP IVs**. Press **Enter**.

Airodump option: -f <msec> : Time in ms between hopping channels.

Airplay filter option: -d dmac : MAC address, Destination.

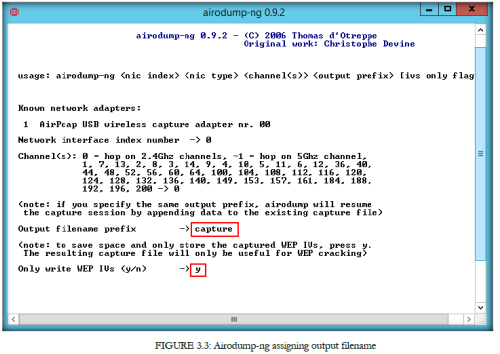


FIGURE 3.3: Airodump-ng assigning output filename

8. Airodump-ng begins to capture the wireless traffic, as shown in the following screenshot.
9. Allow airodump-ng to capture a large number of packets (above 2,000,000).

To confirm that the card is in monitor mode, run the command "iwconfig." You can then confirm the mode is "monitor" and the interface name.

To stop wlan0 type: airmon-ng stop wlan0.

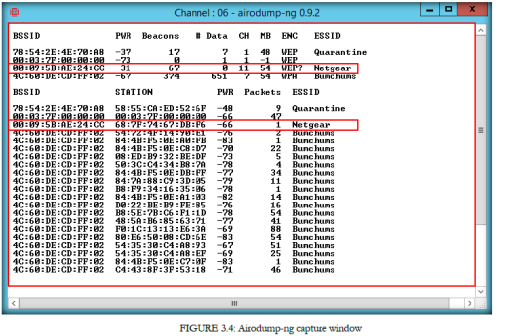


FIGURE 3.4: Airodump-ng capture window

10. Because airodump-ng requires a lot of time to capture enough number of packets and IVs, we are providing a sample capture file that contains the required number of packets and IVs in order to save time. Close the capture window by pressing **Ctrl+C**.
11. Navigate to **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin** and double-click **Aircrack-ng GUI.exe** to launch **Aircrack-ng**. Then click **Choose...**.

airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and run the right commands.

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

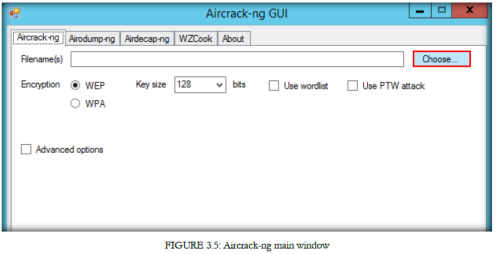


FIGURE 3.5: Aircrack-ng main window

12. The **Open** window appears; navigate to **D:\CEH-Tools\CEHv9 Module 14 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng**, select **wepcapture.cap**, and click **Open**.

Note: This is a different file from the one you recorded; this file contains pre-captured IVS keys.

You may use this key without the "-y" in your wireless client connection prompt and specify that the key is in hexadecimal format to connect to the wireless network.

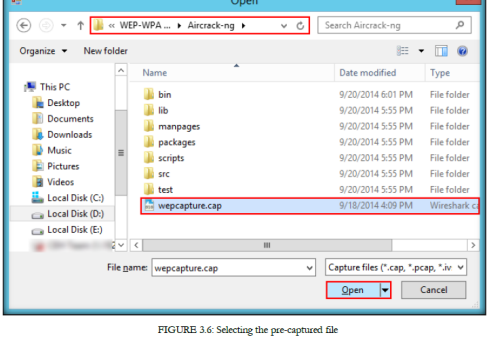


FIGURE 3.6: Selecting the pre-captured file

13. After selecting the file, click **Launch**.

To put your wireless card into monitor mode: airmon-ng start rausb0.

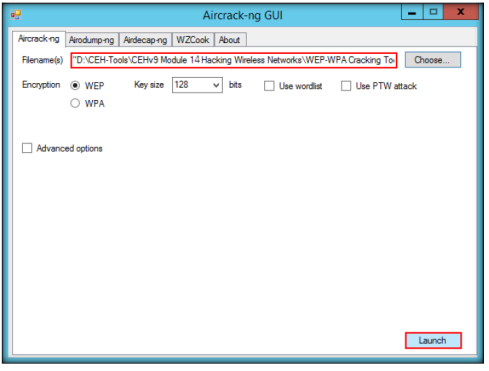


FIGURE 3.7: Aircrack-ng launch window

Airplay filter options: -b bssid: MAC address, access point.

14. Aircrack-ng begins to decode the capture file, as shown in the following screenshot:

To start wlan0 in monitor mode type: airmon-ng start wlan0.

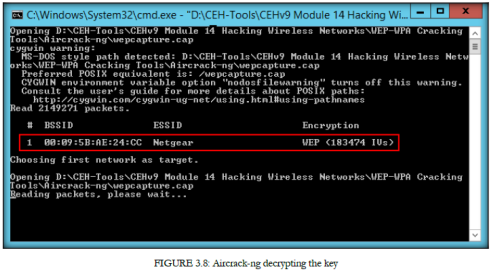


FIGURE 3.8: Aircrack-ng decrypting the key

15. On successfully decoding the file, it displays the key shown in the following screenshot:

Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.

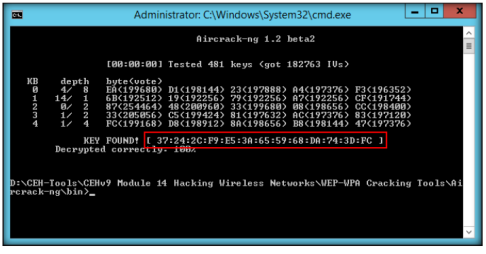


FIGURE 3.9: aircrack-ng with WEP crack key

16. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for open devices, perform vulnerability analysis, and then start exploiting them.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data packet generation rate.

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

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