Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 8

Auditing a Wireless Network and Planning for a Secure WLAN Implementation

**Section 1: Hands-On Demonstration**

Part 1: Explore the Aircrack-ng Suite

On the vWorkstation desktop, double-click the Connections folder.

In the Connections folder, double-click the Kali shortcut to open a remote PuTTY session to the Kali machine.

This connection is using SSH (Secure Shell) to log in as root.

At the command prompt, type man airmon-ng and press Enter to review the online manual for the airmon-ng tool.

Text

Description automatically generated

The airmon-ng tool is used to enable the monitor mode on wireless LAN interfaces. It may also be used to toggle between the monitor mode and the managed mode. Entering the airmon-ng command without parameters will show the interface’s status on the WLAN.

In the PuTTY window, press Enter and press the spacebar until you reach the bottom of the airmon-ng online manual, then use the scrollbar to return to the top of the manual and explore the various functions and switches for this tool.

At the command prompt, type cd /usr/sbin and press Enter to change the current directory to /usr/sbin.

At the command prompt, type ./airodump-ng --help and press Enter to review the online manual for the airodump-ng tool.

Text

Description automatically generated

The airodump-ng tool is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP initialization vectors with the intent of using them with aircrack-ng. With a GPS receiver connected to the computer, airodump-ng is also capable of logging the coordinates of the access points that have been found. Additionally, airodump-ng creates files containing the details of all access points and clients found on that WLAN, similar to an IP discovery after an Nmap scan.

In the PuTTY window, use the scrollbar to explore the functions and switches for this tool. You will need this information as part of your deliverables for this lab.

In the PuTTY window, type clear and press Enter to clear the screen and return to the command prompt.

At the command prompt, type ./aireplay-ng --help and press Enter to review the online manual for the aireplay-ng tool.

Text

Description automatically generated

The aireplay-ng tool is used to inject frames. The primary function of this injection is to generate traffic that aircrack-ng will use later for cracking the WEP and WPA-PSK keys. There are different attacks that can cause de-authentications for capturing WPA handshake data, fake authentications, interactive packet replay, handcrafted ARP request injection, and ARP-request reinjection.

In the PuTTY window, use the scrollbar to explore the functions and switches for this tool.

In the PuTTY window, type clear and press Enter to clear the screen and return to the command prompt.

At the command prompt, type aircrack-ng --help and press Enter to open the online manual for the aircrack-ng tool.

Text

Description automatically generated

The aircrack-ng tool is an 802.11 WEP and WPA-PSK key cracking program that can recover keys when enough data packets have been captured.

In the PuTTY window, use the scrollbar to explore the functions and switches for this tool.

Minimize the PuTTY window to return to the vWorkstation desktop.

Part 2: View a Demonstration of an Actual Aircrack-ng Hack

On your local machine, open a new browser window, then type http://www.vlabsondemand.com/video/hacking\_lab08 in the address box and press Enter to play a video demonstrating how the hacking tools you explored earlier in this lab can be used to penetrate a vulnerable system.

The information in this video, which includes closed captions, is required to complete the deliverables for this lab, so you may have to review the video multiple times. If necessary, you

can increase the video size by clicking the full screen button or using the zoom feature in the browser window.

Please note that you will not be able to replicate the steps in the video in the lab environment. These steps require a live wireless connection, which is not available in the virtual lab environment.

In your Lab Report file, summarize the steps used in the video to crack the WPA key.

1. Logged into Kali Linux

2. They used airmon-ng start wlan0 command to use to monitor all wireless traffic and verified that mon0 interface was created.

3. Used aireplay –ng -0 5 –a “target MAC address” –h “host MAC address” –ignore -negative –on mon0 and this will inject 5 de-authorization attack to force clients of the network.

4. Used Airodump-ng –channel 11 –bassid “”MAC address of target” –wire Capture mon0 and Pressed ctrl c to stop the dump process.

5. Entered command aircrack-ng –w wordlist Capture01.cap which allows the wordlist to crack the WAP key

6. Entered the wireless network to crack and wait for aircrack to crack the passkey for the network selected.

7. Tested results by logging into the selected network with the cracked passkey.

**Section 2: Applied Learning**

Part 1: Crack a WLAN WPA Key

Open a PuTTY session with the Kali machine.

Note: Now that you are ready to monitor WiFi traffic on the Kali system, you will need to see what is broadcasting in the area. This is a standard WiFi command used in virtually every Linux distribution. Items you will want to pay close attention to are outlined in the following steps:

BSS (Basic Service Set): Used for listing all stations that communicate with each other at the Physical level

BSSID (Basic Service Set Identifier): Used to Identify Access Points, MAC (Machine Access Code)

ESSID (Extended Service Set Identifier): Much like a Radio station call sign

SSID (Service Set Identifier): The name assigned to the AP unit

MAC (Machine Address Code): This is generally the physical hardware address of the WiFi network

Group Ciphers: TKIP AES PSK

Authentication suites: This will be PSK TKIP versions

WPA/WPS: Review which version is used on the WiFi device

Model: Knowing the model number will allow a hacker to research additional vulnerabilities

Device name is useful in two manners: First, it allows you to keep track of the WiFi; secondly, if the hacker were to create its own WiFi with the same name and boost his/her broadcast signal and keep the AP as Open access, the hacker would be able to get your authentication key or passphrase.

Other information that might be useful for you to know is included in the following list. A seasoned hacker will concentrate on the items in the previous list.

BSSID (MAC Address of each AP unit listed)

PWR (Antenna Power output) if -1 the driver doesn’t support signal level reporting

BEACON (Number of announcements sent out by the AP unit)

#DATA (Number of packets captured)

#/S (Number of packets per second over a period of 10 seconds)

CH (Channel the AP unit is broadcasting on)

MB (Maximum Speed, If MB=11 it’s 802.11b, MB=22 it’s 802.11b+ )

ENC (Encryption algorithm currently in use)

CIPHER (Cipher detected, CCMP=WPA2, TKIP=WPA)

AUTH (Authentication protocol used)

ESSID (Name of the AP unit)

LOST (Number of packets lost in 10 seconds, based on the sequence number)

PACKETS (Number of data packets sent by the clients)

PROBE (Clients connected to or trying to get connection)

At the command prompt, execute aircrack-ng -w /WLAN/wordlist/wordlist.txt /WLAN/wordlist/WLAN/Capture-01.cap to open a wordlist dictionary file and capture file in aircrack-ng.

Graphical user interface, text

Description automatically generated

Notice that both the wordlist dictionary file and the sub-directory containing the Capture-01.cap capture file are in the same directory (WLAN). The aircrack-ng tool will display a list of the captured networks.

At the Index number of target network? prompt, type 18 and press Enter to select the Silentvalor WLAN network.

Text

Description automatically generated with medium confidence

Aircrack-ng will run the wordlist dictionary file against the capture file to try to crack the WPA key. This process will take several minutes to complete.

When the Aircrack-ng tool has successfully identified the WPA key, make a screen capture showing the WPA key and paste it into your Lab Report file.

In your Lab Report file, document the time aircrack-ng took to identify the key and the number of keys tested.

Aircrack-ng displays a time clock in the status line just before the number of keys tested.

At the command prompt, execute exit to close the PuTTY window.