Lab 9: Wireless Security

Introduction

In this lab students will explore ways to perform wireless attacks and understand potential defenses. The attacks that will be covered are inspecting & modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WPA2 protected networks.

Software Requirements

All required files are packed and configured in the provided virtual machine image.

- The Virtual Machine running Ubuntu 16.04
- Wireshark: Network protocol analyzer
- Aircrack- ng: a suite of tools to assess WiFi network security http://aircrack-ng.en.softonic.com/

Task 1: Setup an Access Point

Step 1: Setup an access point by using a home router or some software to turn your laptop into a hotspot like connectify hotspot

Step 2: Configure the SSID, username, and password. For example:

a. SSID: TestCrack
b. Username: user
c. Password: passwd

Step 3: Configure the security protocol to be WPA2.

Task 2: Capturing Wireless Packets

To capture wireless packets, you need to have a wireless network card installed on your machine. There are two kinds of wireless network interface: One is the internal NIC. Most of the laptops will have an internal NIC; the other one is the external NIC. You can use either **Wireshark** or **Aircrack-ng** to capture wireless packets.

Wireshark

Step 1: Start the Wireshark program.
In order to sniff the packets, you may need to grant Wireshark root privilege by typing *$ sudo wireshark* in a terminal.

Step 2: Select the WiFi Interface
Click the Capture -> Options in the Wireshark program. Look for the interface for WiFi. Normally, the interface name is wlan0, but it may be a different name that depends on your configuration. For instance, the name of the WiFi interface on my MacBook is “Wi-Fi:en1”.

Step 3: Enable the Monitor Mode
In Monitor Mode, it captures all packets from all SSID in its distance range. Please note that Monitor Mode is different from Promiscuous Mode. For the purpose of this lab, we need to capture all the traffic so that we need to enable the monitor mode.

Step 4: Start Capturing
Click on start in the capture interfaces window and start the capture.

Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

MAC: https://martinsjean256.wordpress.com/2018/02/12/hacking-aircrack-ng-on-mac-cracking-wi-fi-without-kali-in-parallels/
Linux: https://linuxhint.com/install_aircrack-ng_ubuntu/
Windows: https://www.aircrack-ng.org/doku.php?id=aircrack-ng_suite-under-windows_for_dummies

Task 3: Capturing the Four-way Handshake

To crack the WPA/WPA2 passphrase, we first need to capture the four-way handshake that contains

Step 1: Start to capture all the traffic
This is what we just did in our previous step. Just the Wireshark program into Monitor Mode and run.

Step 2: Connect to the access point using its passphrase
Use your cell phone or laptop connects to the access point.

Step 3: Stop Wireshark program and identify the four-way handsake
Press the stop button to stop capturing in Wireshark; type keyword "EAPOL" in the filter to identify the four-way handshake.

Task 4: Cracking WPA2 WiFi Passphrase Using Aircrack-ng

Step 1: Copy the cap/pcap file into the VM

Step 2: Use aircrack-ng to crack the passphrase
You may use the following command to see the manual.

```
$ man aircrack-ng
```

Run the following command to crack the passphrase

```
$ aircrack-ng -w <word list>  <pcap file>
 -w: specify the path to the wordlist, you are free to add your password into it.
```

Assignment:

1. Read the instructions above and finish all the tasks. Demonstrate with snapshots of Wireshark captured packets that

    a. You have successfully set the laptop to be monitor mode and captured the 4-way handshake packets (Task 3)

    b. You have cracked a simple password encrypted by the WPA2 with a word list. (Task 4)

2. Answer the following questions and justify your answers

    a. What is the difference between Monitor Mode and Promiscuous Mode

    b. If the WiFi traffic is on-going, how to crack the WiFi password?