PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

School of
Applied Computing

Network Security (NS)

Lab - Cracking WPA2 Encryption using CAINE/Kali Linux

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

The purpose of today's laboratory exercise is to Cracking WPA2 Encryption using CAINE/Kali Linux

WPA2 (Wi-FI Protected Access 2) is a network security technology commonly used on Wi-Fi wireless networks. WPA2 replaced the original WPA technology on all certified Wi-Fi hardware since 2006 and is based on the IEEE 802.11i technology standard for data encryption. WPA2-PSK may not be as safe as you think. There are a few attacks that still work against WAP2-PSK. One of the most common attacks against WPA2 is done by exploiting a weak passphrase. In this Lab exercise, you will learn how to crack WPA2 by exploiting a weak passphrase.

Step 1:

The first step is to verify the router configuration. Normally in a real penetration test we would not have this option, but since this is a lab exercise, you have more flexibility.

Connect the WiFi dongle provided to you by your module leader to your Lab computer. Switch/boot the computer with the CAINE or Kali Linux DVD. After a successful boot-up, click on the network connection icon to make sure that the WiFi networks around the lab is being detected by the WiFi dongle.

Step 2:

The next step is to enable the WiFi wireless interface. This is accomplished by typing the following command at the terminal as shown in figure 1 below:

sudo ifconfig wlan0 up

Following the command, note that nothing appears on the screen. However, a lot has happened at the bacckgrouund.

Figure 1: Command to enable WiFi interface.

Step 3:

Now, you need to know which wireless networks are being detected by your WiFi dongle. To achieve this, you need to type the following command:

sudo iwlist wlan0 scanning

This command forces the wireless card to scan and report on all wireless networks in the vicinity as shown in Figure 2 below.

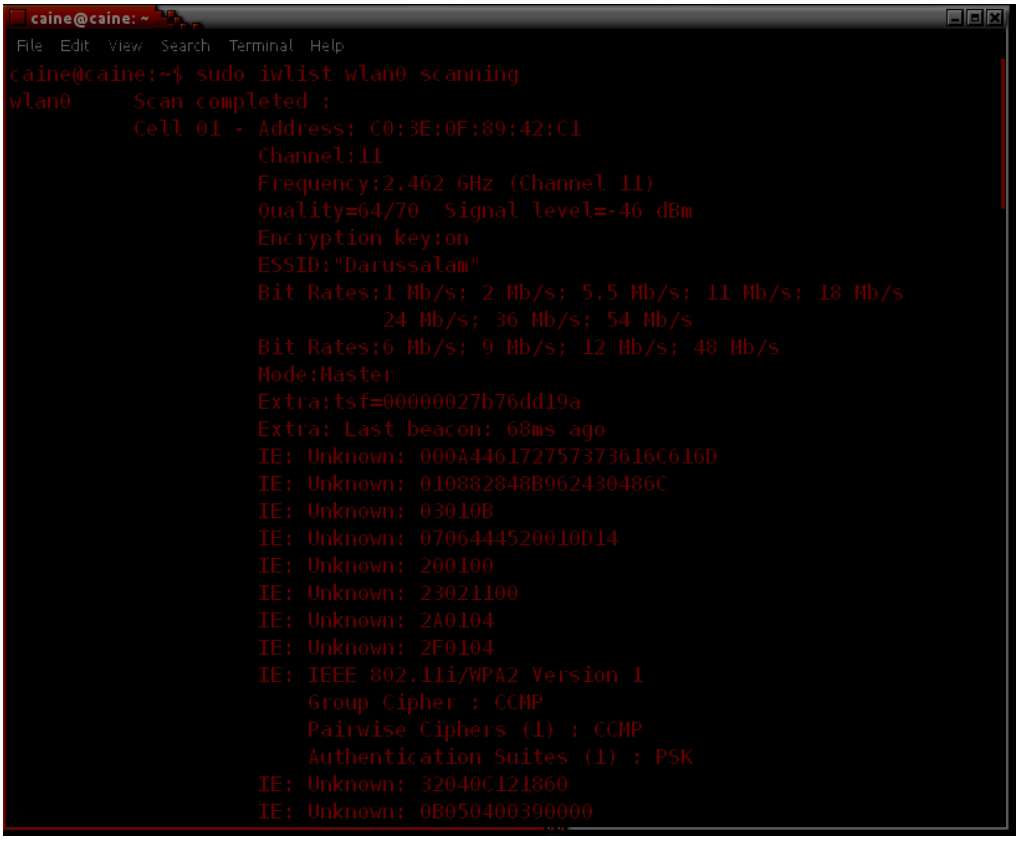

Figure 2: Detecting wireless networks

Take time to study the information shown in your Figure 2. Try to identify the wireless network your WiFi dongle needs to target for attackingg. Try to identify its name, MAC address, channel, frequency, quality of signal and the encryption system used.

In the above example, the first network detected is called “Darussalam”. The router's MAC address is C0:3E:0F:89:42:C1. The network is operating on channel 11. The signal quality is 64/70 (very good). The encryption system used is CCMP (Counter Mode with Cipher Block Chain Message Authentication Protocol).

Step 5:

In this step you need to change your wireless card into ***monitoring mode***. This will allow the wireless card to examine all the data packets in the air.

You do this by creating a ***monitor interface*** using the following command:

sudo airmon-ng

If you get an error message running the above command, it means that **aircrack-ng** package in your your distribution of CAINE or Kali DVD is corrupted and you need to manually install it. To do this, type the following command:

sudo apt-get install aircrack-ng

Upon a successful installation, you should get a result similar to Figure 3 below.

```
caine@caine: ~
File  Edit  View  Search  Terminal  Help
caine@caine:~$ sudo apt-get install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  aircrack-ng
0 upgraded, 1 newly installed, 0 to remove and 571 not upgraded.
Need to get 867 kB of archives.
After this operation, 2,219 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu/ trusty/universe aircrack-ng amd64 1:1.1-
6 [867 kB]
Fetched 867 kB in 2s (411 kB/s)
Selecting previously unselected package aircrack-ng.
(Reading database ... 271071 files and directories currently installed.)
Preparing to unpack .../aircrack-ng_1%3a1.1-6_amd64.deb ...
Unpacking aircrack-ng (1:1.1-6) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up aircrack-ng (1:1.1-6) ...
caine@caine:~$
```

Figure 3: Installing aircrack-ng

Now, try running the **airmon-ng** command to verify airmon-ng sees your wireless card. From this point create the monitor interface by issuing the following command:

sudo airmon-ng start wlan0

A successful running of the airmon-ng command should give result as shown in Figure 4 below.

```
Interface       Chipset         Driver

wlan0           Atheros         ath5k - [phy0]
                                (monitor mode enabled on mon0)

caine@caine:~$
```

Figure 4: Verifying that airmon-ng sees the WiFi card.

Next, run the **ifconfig** command to verify the monitor interface is created.

sudo ifconfig

Following the above command, we can see that **mon0** is created. **Y**ou should get a window similar to figure 5 below.

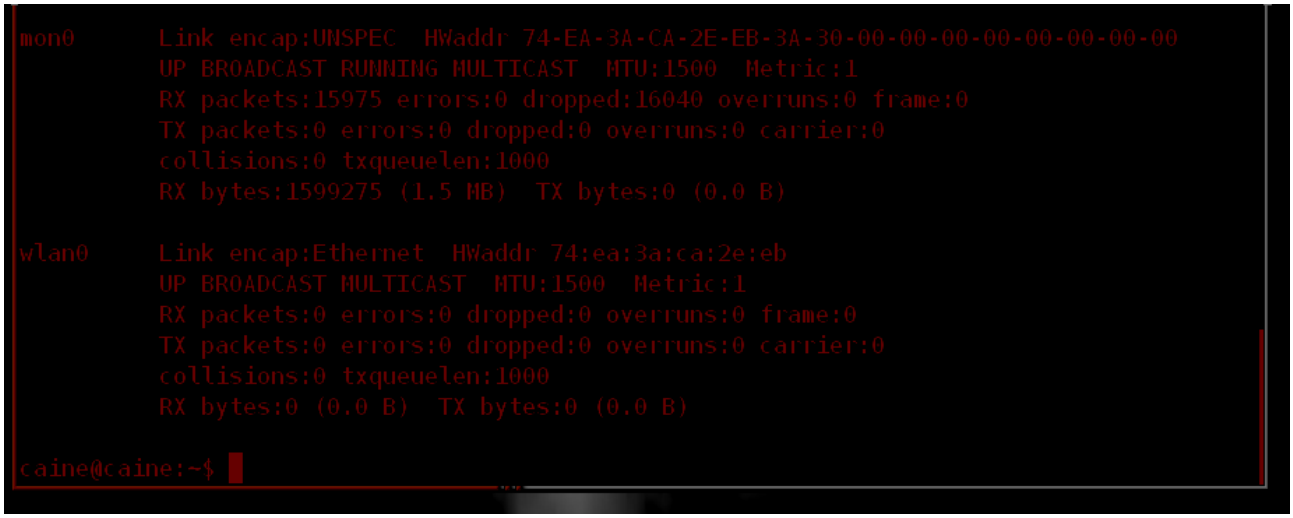

Figure 5: Showing that mon0 interface created.

Step 6:

Now, it is time to use **airodump-ng** to capture the WPA2 handshake. You as the attacker will have to catch someone in the act of authenticating to get a valid capture. To guarantee getting good result in this Lab exercise, try to connect to the targeted university WiFi network using your mobile device while mon0 is running. Alternatively, ask your colleague to connect their Lab PC to the university network using the WiFi dongle connected and the wired Ethernet cable disconnected.

Now, run the following command:

sudo airodump-ng mon0 – -bssid C0:3E:0F:89:42:C1 – –channel 11 – –write BreakingWPA2

(make sure there is no space between "- -")

Explaining the aairbove command:

airodump-ng mon0– –bssid 20:aa:4b:1f:b0:10 (to capture packets from your target Access Point).

– –**channel 11** (to limit channel hopping).

– –**write BreakingWPA2** (the name of the file where to save the captured handshake)

The a**irodump-ng command** will display a valid handshake when it captures it. It will display the handshake confirmation in the upper right hand corner of the screen.

To capture the handshake you are depending on monitoring a legitimate client who is trying authenticate to the targeted network. However, this does not mean you have to wait for a client to legitimately authenticate. You can force a client to re-authenticate, which will happen automatically with most clients when you force a de-authorisation. This technique will be covered in the next Lab exercise.

Step 7:

In this step, you will use **aircrack-ng** with a password dictionary file to crack the password of the wireless network you targeted. Your chances of breaking the password are dependent on the password dictionary file provided to you earlier by your module leader.

Run the following command:

sudo aircrack-ng BreakingWPA2-01.cap -w "*name of your dictionary file"*

The **BreakingWPA2-01.cap** file was created when you ran the **airodump-ng** command. The valid WPA2 handshake airodump captured is stored in the **BreakingWPA2-01.cap** file.
Many attackers use large dictionaries that increase their chances of cracking a passwords. Many dictionaries contain passwords from real users and websites that have been cracked and posted on the Internet. Some sophisticated dictionaries combine multiple languages, permutations of each word, and key words and phrases from social media sites such as Twitter and Facebook.
Note: In the event that you are not able to complete this exercise in the Lab within the time allocated, try to do it at home targeting your home wireless network.

Conclusion
Even though WPA2 as protected by CCMP is a reasonably secure wireless infrastructure, it is possible to break the system and crack the password if it is not strong enough. As a matter of policy, use online resources like http://passwordsgenerator.net/ to generate strong passwords.

Credit: This Lab exercise is based on a concept by Dr Chaos.