How To Uncover Hidden SSID With Kali Linux

In this quick lab we will go trough how to Uncover hidden SSID with Kali Linux and a wireless card that can be set to monitor mode.

SSID is short for service set identifier (SSID), SSID is the sequence of characters that uniquely identify a wireless local area network, the name can be up to 32 alphanumeric character and is case sensitive .

By default the configuration mode for a access point is to broadcast the SSID in a beacon frame, this allows clients to discover them easily.

Some network administrators disables the broadcasting of SSID in the configuration file, this tells the access point to not broadcast the SSID in the beacon frame, it is done in believe that it will add one more security layer to the network, the effect of not sending out the SSID is that only devices that knows the name of the SSID can connect to

the network.

Unfortunately hiding the SSID will not add any extra security layer to the WLAN, there are lots of different method to uncover a hidden SSID, you can use windows and android tools to automatically discover SSIDs, hiding the SSID should not be considered as a extra security layer.

Requirements

- Kali Linux
- Wireless card capable of monitor mode and packet injection, like the ALFA AWUS1900
- Your wireless card name

I am using a old D-link router with disabled SSID, for wireless card i am using is my 8 year old AWUS036H-

DISCLAIMER: This software/tutorial is for educational purposes only. Please don't use for illegal activity. The author is not responsible for the use of the application or the users action.

Step 1: Set Wireless card in monitor mode

1.1 Display wireless card name

```
sudo iwconfig
```

```
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
```

```
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Here we can see that my wireless card name is called wlan0.

1.2 Kill interfering processes

```
sudo airmon-ng check kill
```

1.3 Put the interface into monitor mode, this can be archived in different ways, i am using airmon-ng to start the card in monitor mode.

```
sudo airmon-ng start wlan0
```

NOTE: The command will create a new virtual interface with the same name as your old interface plus the word mon.

1.4 Display wireless card to confirm the new interface

```
sudo iwconfig
```

```
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
eth0      no wireless extensions.
```

```
lo        no wireless extensions.

root@iPhone:~#
```

Step 2: Scan for available networks

2.1 Use airodump-ng to scan for nearby networks and look for your router. i know that my BSSID is 84:C9:B2:6A:9E:90 and i am using channel 6.

```
sudo airodump-ng wlan0mon
```

```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -29      144       11    0   6  130  WPA2 CCMP   PSK  <length:
0>
 F0:9F:C2:AA:6C:B9  -47       45        0    0   1  195  WPA2 CCMP   PSK  Perham
 32:CD:A7:15:AD:49  -49       29        0    0   6  54e  WPA2 CCMP   PSK  DIRECT-
SoM2020 Series
 BC:EE:7B:7E:18:90  -49      124       12    0   9  195  WPA2 CCMP   PSK  nocco1
 80:2A:A8:44:C5:B1  -51       76        3    0   1  195  WPA2 CCMP   PSK  PontuS
 82:2A:A8:44:C5:B1  -51       63        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 F2:9F:C2:AA:6C:B9  -47       51        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 08:86:3B:DD:2C:95  -54       20        4    0   1  130  WPA2 CCMP   PSK
belkin.24d
```

I can see that the first SSID network have no SSID “<length: 0>” and it matches my BSSID and channel.

Now type down the BSSID and the channel of your access point and cancel the current command and rerun it specifying the BSSID and channel of the hidden SSID.

```
sudo airodump-ng -c 6 --bssid 84:C9:B2:6A:9E:90 wlan0mon
```

```
CH  6 ][ Elapsed: 18 s ][ 2019-07-15 20:21 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -25  87      185       35    0   6  130  WPA2 CCMP   PSK
<length:  0>
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0       21
```

We have two options while scanning the network, we can either wait for a new device to connect. The new device will send out a beacon frame, airodump-ng will immediately populate the SSID in the terminal output.

I will now connect a device to the network to demonstrate how it will show up in the output.

```
CH  6 ][ Elapsed: 6 mins ][ 2019-07-15 20:27 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -24 100     3247      416    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      262
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1      2        6
```

Observer that the ESSID is now showing the name HoneyP01

Second options is to force disconnect one or all of devices that are associated with the AP. We can use aireplay-ng to disconnect devices by flooding them with de-authentication packets.

2.2 Open a new terminal and send de authentication packets to all connected devices on

the router. The command will send out 5 de-authentication packets to the access point.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 --ignore-negative wlan0mon
```

```
20:38:49  Waiting for beacon frame (BSSID: 84:C9:B2:6A:9E:90) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:38:49  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
root@iPhone:~#
```

2.3 Go back to terminal one, now you should see the ESSID of the hidden WLAN.

```
CH  6 ][ Elapsed: 7 mins ][ 2019-07-15 20:39 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -16  96     4204      608    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      322
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1e     0       37
```

We can refine our scan and just target one associated device, modify the command by adding a target station.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 -c 00:C0:CA:95:EA:8B --ignore-negative
wlan0mon
```

Conclusion

Uncovering a hidden SSID is easy, due to when a device connects to an access point. The device and the access point exchanges probe requests and response packets.

We have covered some basic terminal commands to uncover a hidden SSID. All equipment used on the lab is mine. Please don’t preform the commands on unauthorized networks.