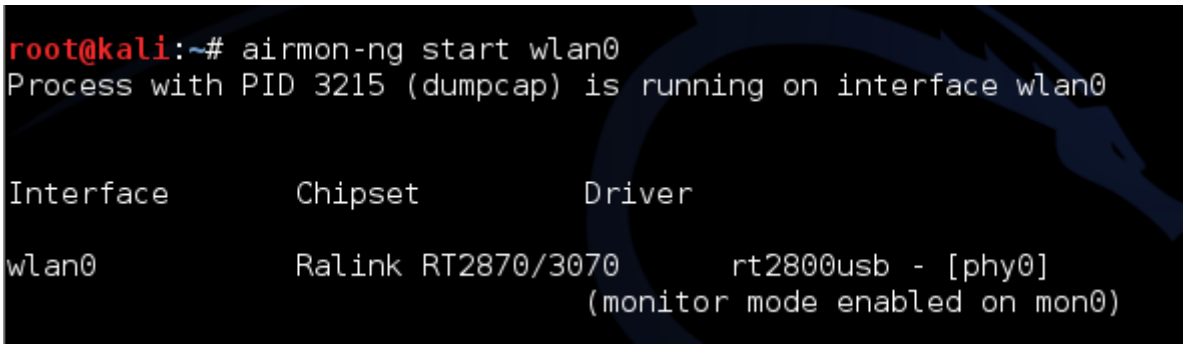
Uncovering Hidden SSIDs

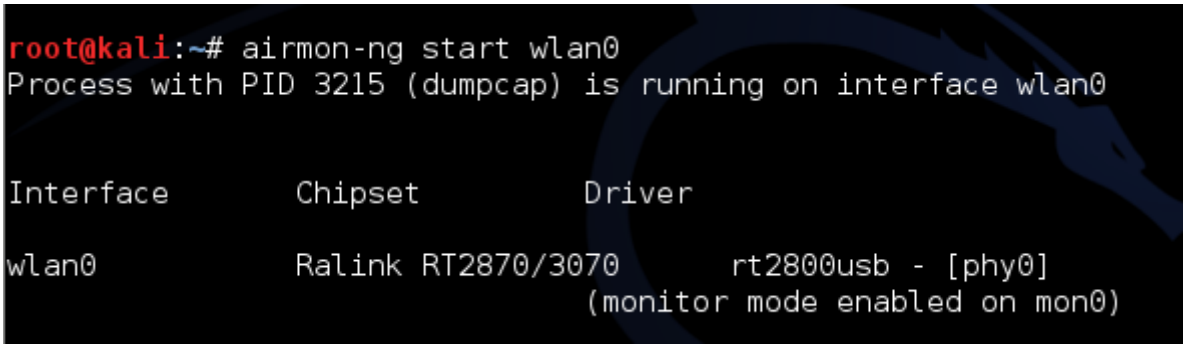
pentestlab.blog/category/wireless/page/2

January 31, 2015



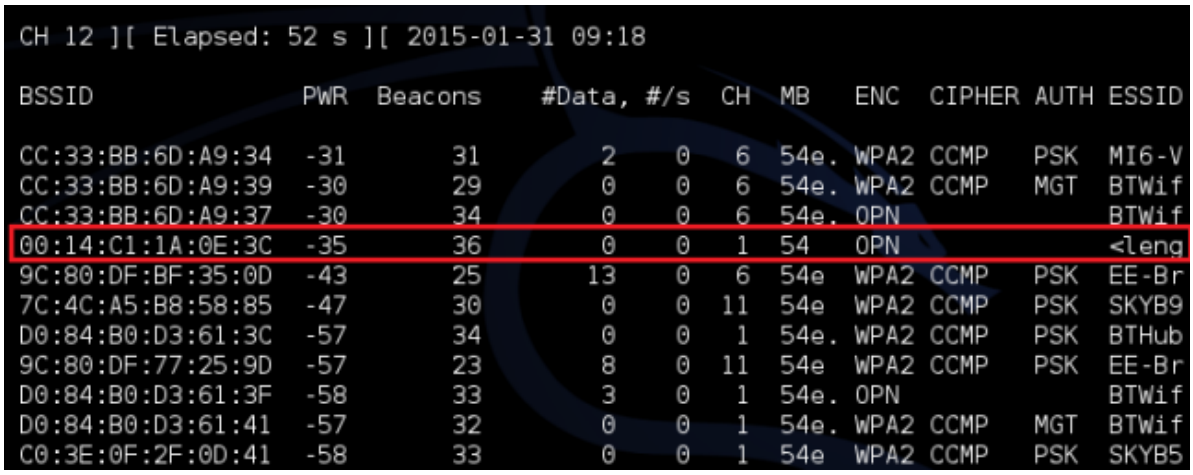
By default every access point is broadcasting the SSID in the beacon frames. Sometimes network administrators might choose to configure the AP not to broadcast the SSID because they are thinking that they will avoid attacks just because if a malicious user doesn't know that a network exist how he is 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.



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.



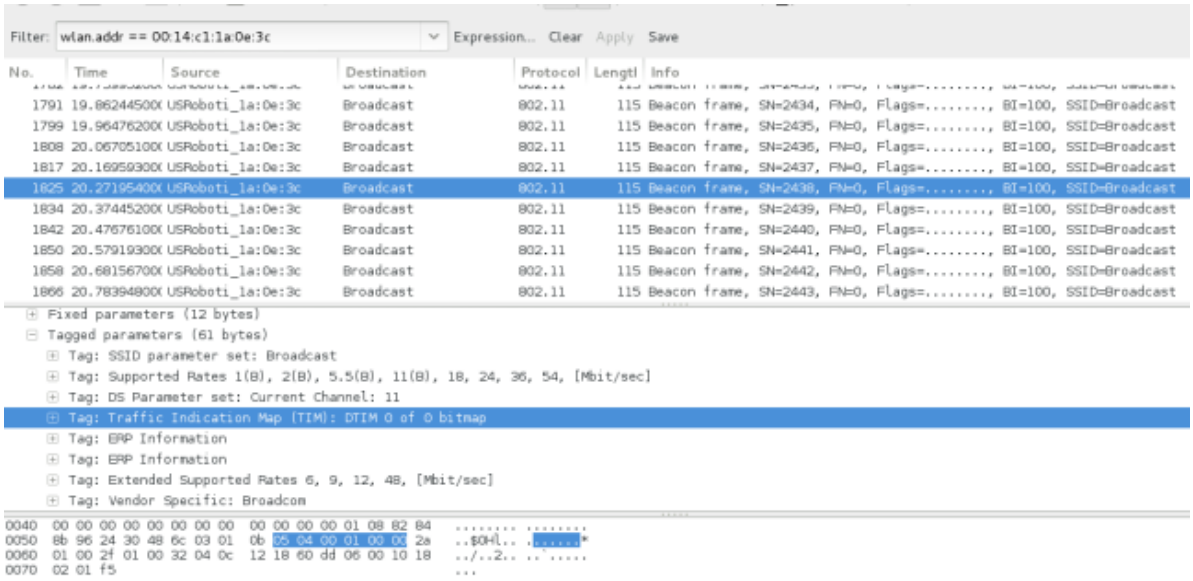
```
CH 12 ][ Elapsed: 52 s ][ 2015-01-31 09:18

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              <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        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.

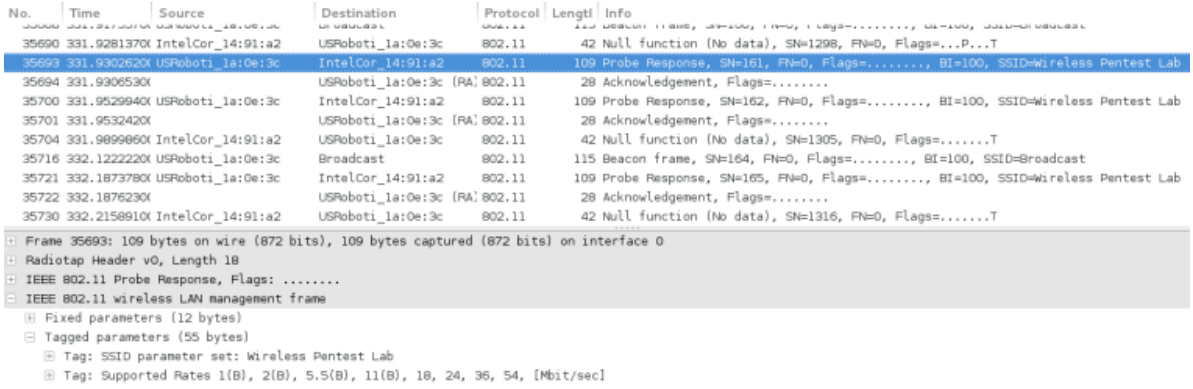


Beacon Frames – Hidden Wireless SSID

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.

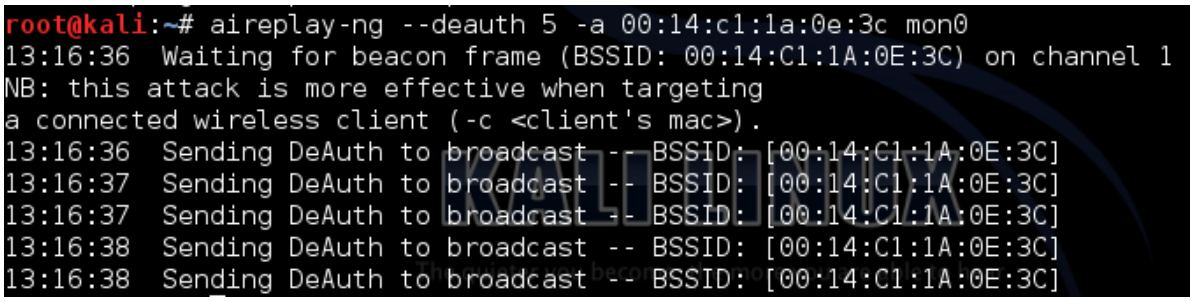


Probe Response Packet contains the SSID

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.

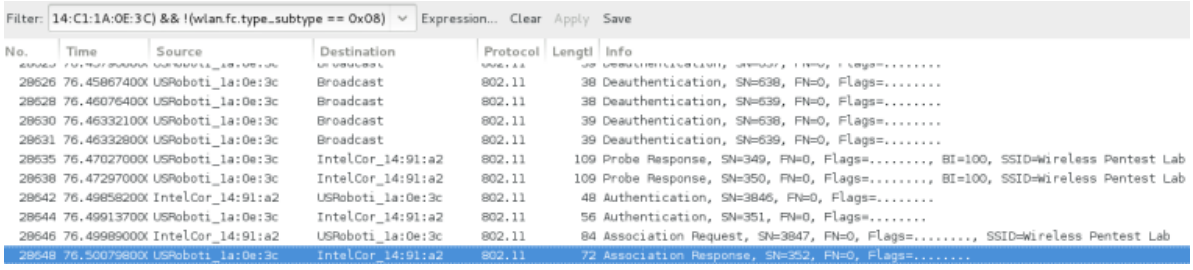
The other method is to send directly deauthentication packets to all the clients on behalf of the access point which in this case is the Wireless Pentest Lab. This will force all the devices that are connected to the access point to disconnect and reconnect which again Probe response packets will be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



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