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

017 TU AYUDA EN CIBERSEGURIDAD
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

FIGURE INDEX

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.

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.

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 hansdhake_aireplay.cap.

In the example above of the file " hansdhake_aireplay.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.