

ÍNDICE:

Caso práctico	2
Apartado 1: Revisar el diseño de la red Wi-Fi	2
Apartado 2: Monitorización de datos	7
Apartado 3: Exposición en redes OPEN	8
Apartado 4: Debilidades en las redes inalámbricas.	10
Bibliografía:.....	15

Caso práctico

Una vez han adquirido los conocimientos y las técnicas utilizadas para comprobar la seguridad de las redes Wi-Fi, el equipo quiere realizar una primera revisión.

Es la primera vez que se realizan pruebas de este tipo y deciden dividir la auditoría en tres fases.

La primera fase se centrará en buscar debilidades de diseño de la red Inalámbrica y contemplará las casuísticas en el que se estén utilizando tipologías de redes Wi-Fi que no resulten adecuadas para la funcionalidad que desempeñan.

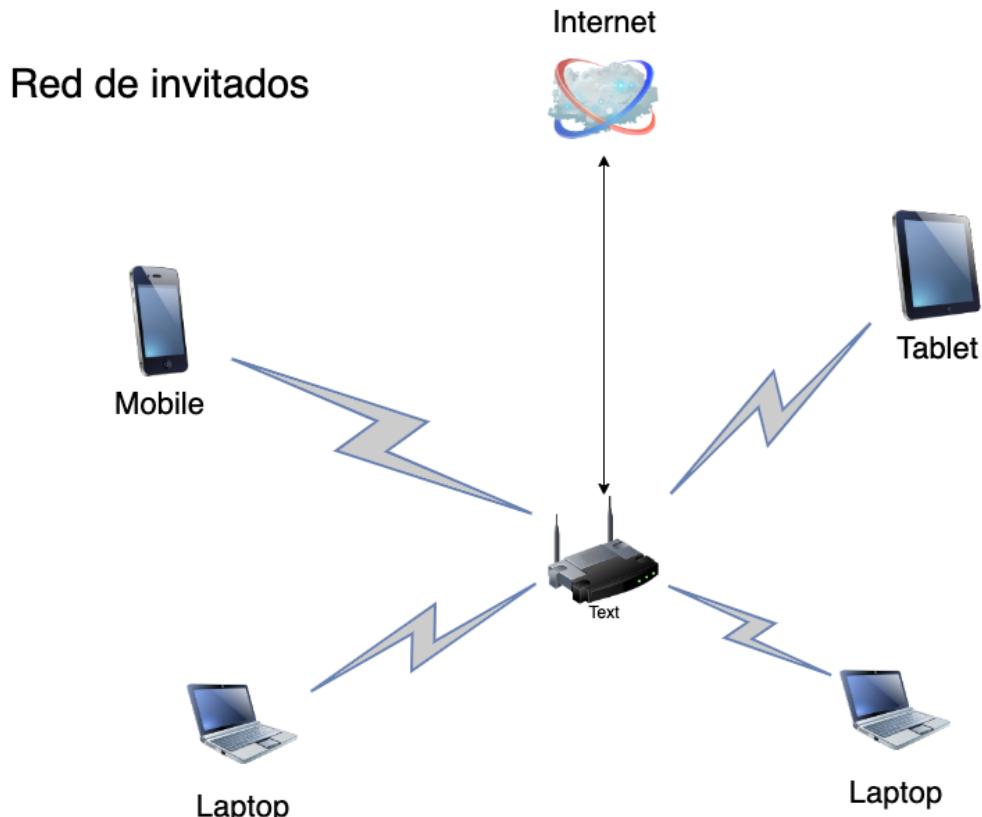
En la segunda fase realizarán una monitorización de las redes de la empresa con la finalidad de disponer de un inventario de Puntos de Acceso, nombre de redes y canales.

Para finalizar, se emplearán las técnicas descritas en los apartados de "Ataques a redes Wi-Fi" para comprobar si sería posible acceder a las redes Wi-Fi analizadas.

Apartado 1: Revisar el diseño de la red Wi-Fi

A continuación se muestran varios diagramas de la red. Teniendo en cuenta los conocimientos adquiridos en esta unidad, comenta para cada una de las redes que se muestran la problemática de diseño existente y cómo sería la infraestructura ideal.

- **Red de invitados:** La compañía dispone de una red Wi-Fi de invitados tipo **OPEN** para dotar de conectividad las salas de reuniones cuando tienen visitas de clientes o proveedores. También es común que en ciertas ocasiones se conecten los propios empleados con sus equipos corporativos dado que la cobertura en las salas de reuniones es mejor. Necesitas resolver las siguientes cuestiones:
 - Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
 - Justificar los tipos de ataque a los que está expuesta.
 - Mejoras que implementarías en la red
- A continuación, se muestra el diagrama de la red de invitados:



Sergio Romero Redondoación ([CC0](#))

En esta red nos encontramos dos problemas esenciales los cuales describo a continuación:

- Red tipo OPEN: este tipo de red no requiere autentificación, lo cual implica que cualquier persona puede conectarse a ella sin necesidad de contraseña, esto expone a la red a cualquier agente malintencionado.
- Uso por empleados: los empleados al hacer un uso de esta red con los dispositivos corporativos exponen los datos de sus dispositivos a cualquiera que tenga acceso a la red y esta al ser open nos indica que cualquiera puede acceder a ella.

Los tipos de ataque mas comunes que podemos encontrarnos en este tipo de redes son:

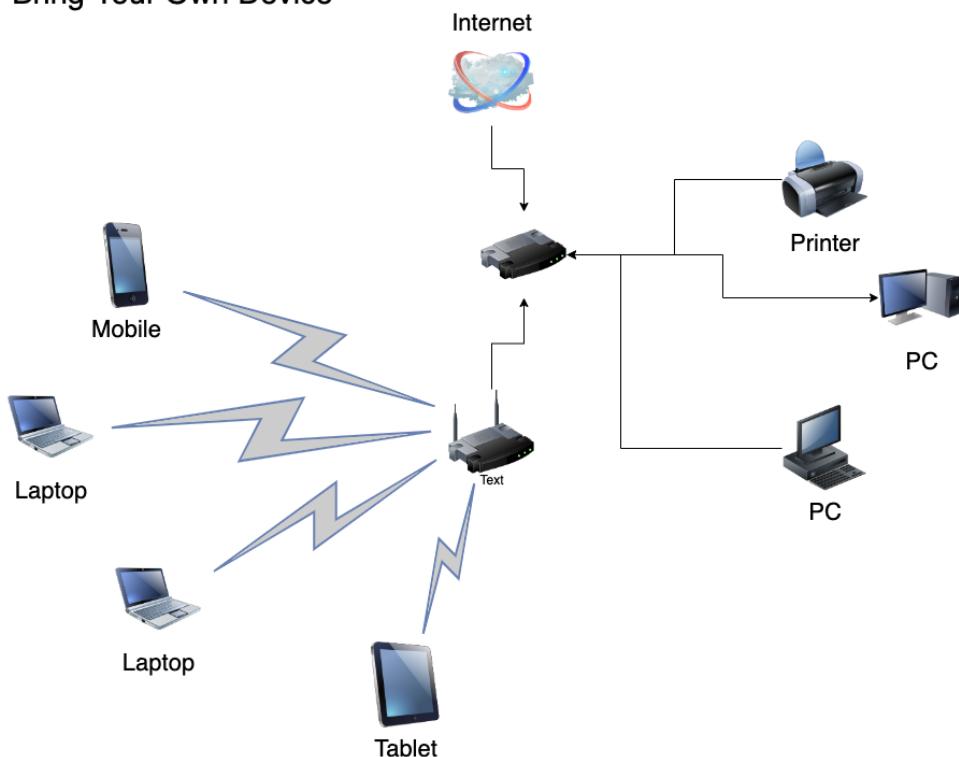
- Ataque MiM (man in the middle): un agente malintencionado puede interceptar y modificar las comunicaciones entre los dispositivos y el punto de acceso.
- Sniffing del tráfico: en este caso podrían interceptar, capturar y analizar el tráfico generado por cualquier dispositivo conectado a esta red y obtener información sensible y relevante.
- Suplantacion: un atacante puede crear pasarelas para obtener credenciales de los que se conecten a ella.

Possibles mejoras a implementar para mejorar la seguridad:

- WPA3: cambiar de red OPEN a una con WPA3 para una mejor seguridad y que requiera autentificación.
- Segmentar la red: crear redes separadas para invitados y para empleados, con ello evitar que los empleados accedan con dispositivos corporativos a la misma red que los invitados.
- Monitorizar: implementar sistemas que monitoricen y generen alertas para la detección de posibles intrusos.
- **Red de dispositivos móviles:** La compañía adoptó hace varios años la filosofía "Bring Your Own Device" mediante la cual dispone de una red específica para que los empleados puedan utilizar sus equipos personales (smartphone, tablet o portátil) para acceder a ciertos servicios en la red de empleados, como acceso al correo electrónico, al servidor de ficheros y a imprimir con las impresoras. La red se encuentra protegida mediante **WPA2-PSK**. Además, en los últimos meses se han ido varios empleados a trabajar a la fábrica de al lado, aunque el administrador de la red no ha notado que la red tenga menos usuarios conectados.
 - Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
 - Justificar los tipos de ataque a los que está expuesta.
 - Mejoras que implementaría en la red
- A continuación, se muestra el diagrama de la red de dispositivos móviles:

**Red dispositivos móviles
/ Bring Your Own Device**

Red LAN Corporativa



Sergio Romero Redondo ([CC0](#))

En este caso nos podemos encontrar con varios problemas de seguridad:

- WPA2-PSK: Es mas seguro que cualquier red abierta, pero puede ser vulnerable a ataques de fuerza bruta con contraseñas mal configuradas.
- BYOD (bring your own device): El que los empleados puedan hacer un uso de sus dispositivos en la red añade un problema de seguridad, estos dispositivos podrían estar comprometidos, lo que haría que trasladaran este problema a la red de la empresa.
- Usuarios de otras empresas conectados: Otro gran problema a tener en cuenta y que debemos considerar es el que no se haya disminuido los usuarios tras la salida de varios empleados a otra empresa cercana.

Los tipos de ataques a considerar en estas redes:

- Ataques de fuerza bruta: En este ataque se intenta adivinar la contraseña mediante la prueba de muchas posibles contraseñas. Depende de la configuración de estas y su complejidad dependerá la posible consecución de este ataque.
- Ataque de suplantación o portal cautivo: mediante este ataque se puede matar la señal original wifi y crear un punto de acceso con un portal cautivo que obligue a los usuarios a introducir la contraseña de la red y con esta tener acceso a ella.
- Ataques insider: Existencia de usuarios que tienen acceso a la red y han dejado la empresa es un gran problema y mas dependiendo de como hayan salido de ella y si han ido a empresas de la competencia.

Posibles mejoras en esta red:

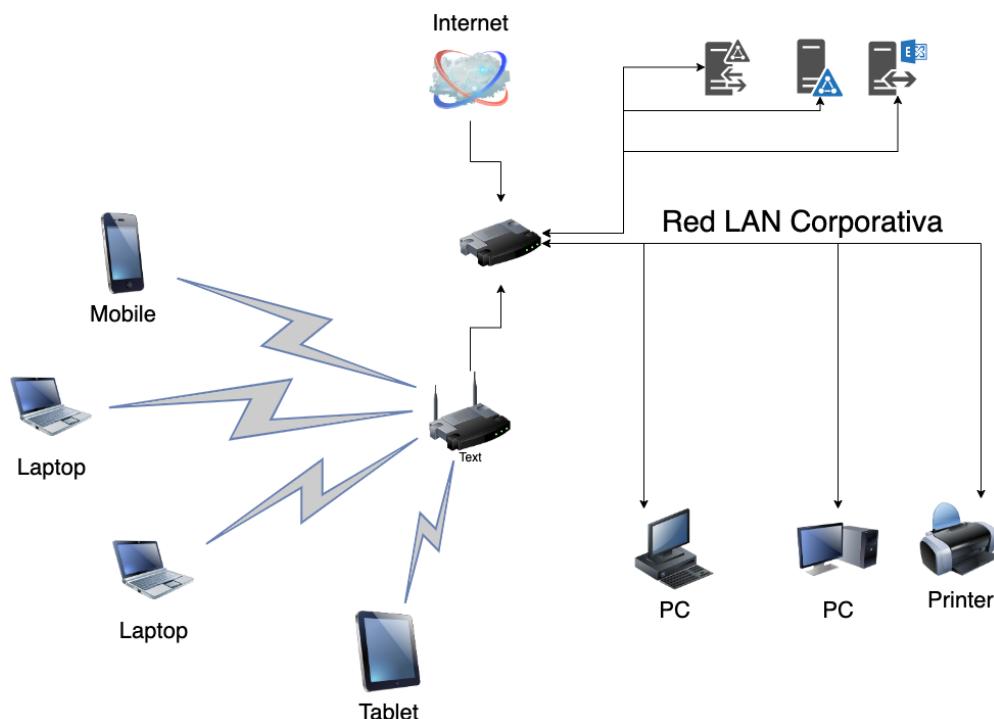
- Implementar WPA3: cambiar a este tipo de red para ofrecer mejoras de seguridad y un medio de autenticación más fuerte.
- Políticas de seguridad para BYOD: implementar unas políticas de seguridad más restrictivas para los dispositivos personales. Incluyendo software de seguridad y políticas de actualización regular de dispositivos.
- Gestión de accesos: revocación de autorización de empleado, realizar cambios de contraseñas regulares.
- Segmentación de la red: es una buena practica en general segmentar la red para que tengan acceso a ella dependiendo del nivel de seguridad de los dispositivos y usuarios.
- **Red corporativa:** Para finalizar, la compañía dispone de una red Wi-Fi en la que sólo está permitido el acceso a los usuarios legítimos de la empresa. La particularidad de esta red es que proporciona el mismo nivel de acceso a la red que cualquier equipo conectado por cable. Para proporcionar este nivel de acceso, la red es de tipo **WPA2-Enterprise** a la cual los empleados acceden **autenticándose con su usuario y contraseña**. En este sentido su proveedor habitual de servicios le ha indicado que necesita desplegar un MDM

para garantizar una mayor protección en la red, este **MDM** está presupuestado pero aún no se ha desplegado.

- Justificar que problemas de seguridad dispone esta red en base al tipo de red Wi-Fi que es, y el uso que se hace de ella.
- Justificar los tipos de ataque a los que está expuesta.
- Mejoras que implementarías en la red
- A continuación, se muestra el diagrama de la red corporativa para su acceso mediante Wi-Fi:

Red WPA2-Enterprise

Red de Servidores



Sergio Romero Redondo ([CC0](#))

Problemas de seguridad que se ven en esta red:

- Acceso completo: la red da el mismo acceso que un dispositivo conectado por cable lo que conlleva que un atacante pueda tener acceso a toda la información de la red y servidores.
- WPA2-Enterprise: aunque es mas seguro, aun puede ser vulnerable con malas políticas de seguridad.
- Falta de MDM: el sistema de gestión de dispositivos móviles no esta disponible aun en la red lo que puede provocar la dificultad en el control de dispositivos que acceden a la red.

Tipos de ataques posibles:

- Ataque por fuerza bruta: intentos de acceder a la red por la fuerza probando credenciales.

- Ataque de insider: empleados o ex empleados con acceso a la red y que tengan malas intenciones, pueden crear este tipo de ataques y en este caso amenaza toda la información de la empresa.
- Ataque MitM: aunque son más difíciles como en el caso anterior que ni los nombré en este caso pues lo nombro a través de un dispositivo comprometido y autorizado.

Mejoras en la red:

- Desplegar MDM: implementar el sistema recomendado para la gestión de dispositivos móviles y con ello asegurar y controlar los dispositivos que acceden a la red.
- Segmentación de la red: como he mencionado con anterioridad, es una buena práctica y se debe considerar siempre, crear subredes con diferentes niveles de acceso y dispositivos.
- Autentificación multifactor. Para añadir una capa de seguridad a la red.
- Auditorias y concienciación a los empleados.

Apartado 2: Monitorización de datos

Dada la siguiente captura de airodump responde a las siguientes cuestiones:

- Indica los BSSID de los Puntos de Acceso de las Redes Skynet y Skynet_Plus.

Skynet: 18:D6:C7:E8:CF:C0

26:57:60:92:DB:F8

34:57:60:92:DB:F0

Skynet_plus: 18:D6:C7:E8:CF:C1

34:57:60:92:DB:F8

- Indica en qué bandas de frecuencia y en qué canales operan las redes Skynet y Skynet_Plus.

Skynet: en los canales 11 (2.462 GHz) (2.4GHz) y 56 (5280MHz) (5GHz)

Skynet_Plus: en los canales 36 (5180MHz) y 56 (5280MHz) ambas son de 5GHz

- Indica a qué red está conectado el dispositivo con MAC 6E:52:AC:9D:B4:87.

86:97:D1:35:E4:3E	6E:52:AC:9D:B4:87	-1	6e- 0	0	2
Esta conectado con 86:97:D1:35:A4:3E					
86:97:D1:35:E4:3E	-86	15	12	0 52 1733	WPA2 CCMP PSK MOVISTAR_E435

La cual corresponde con MOVISTAR_E435

- Indica en que red intenta conectarse el dispositivo 5C:CF:7F:B4:F4:2C.

A la red ONOD79D la cual no esta al alcance en esta captura.

(not associated)	5C:CF:7F:B4:F4:2C	-86	0 - 1	0	2	ONOD79D
------------------	-------------------	-----	-------	---	---	---------

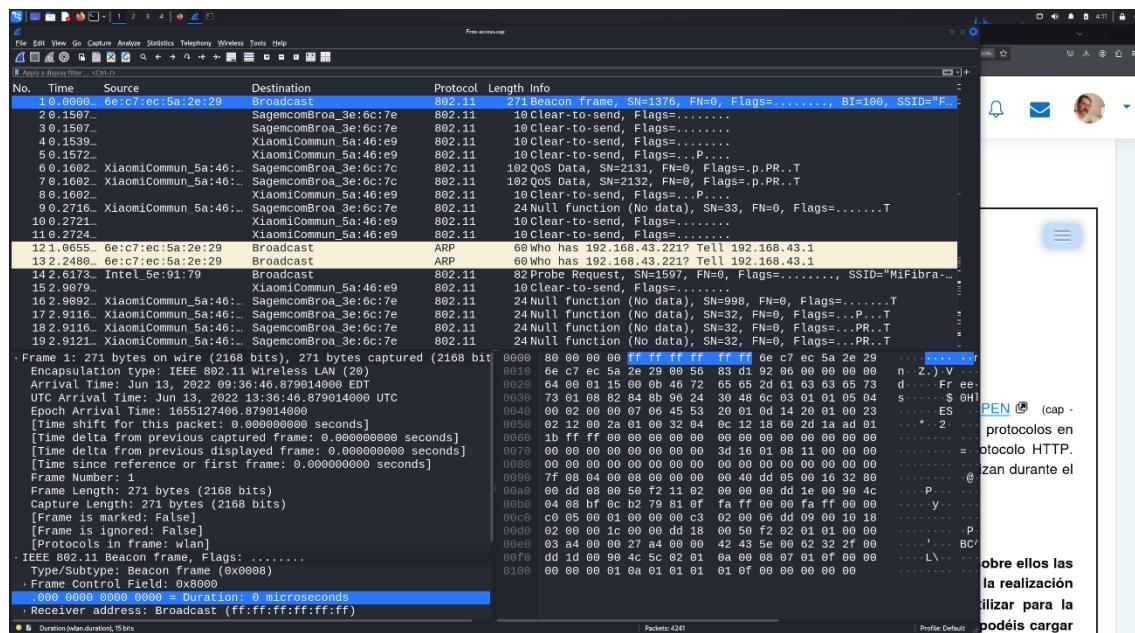
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:D6:C7:E8:CF:C0	-33	18	5	0	36 1170	WPA2	CCMP	PSK	Skynet_plus
18:D6:C7:E8:CF:C1	-43	17	2	0	11 195	WPA2	CCMP	PSK	Skynet
98:00:6A:A0:9B:C4	-73	11	4	0	5 130	WPA2	CCMP	PSK	DIGIFIBRA_gima
DC:53:7C:14:71:E4	-76	9	0	0	7 130	WPA2	CCMP	PSK	Delfin
A4:97:33:4A:82:1E	-77	15	0	0	52 1733	OPN			MOVISTAR_PLUS_8210
DC:53:7C:59:55:3F	-78	16	0	0	108 1170	WPA2	CCMP	PSK	ONO6CG3-5G
DC:53:7C:59:55:3E	-79	10	0	0	11 195	WPA2	CCMP	PSK	ONO6CG3
16:66:78:72:A8:EF	-82	11	0	0	6 130	WPA2	CCMP	PSK	iPhone de Melisa
DC:F8:B9:A1:50:83	-82	12	0	0	7 130	WPA2	CCMP	PSK	DIGIFIBRA-tdTS
DC:F8:B9:A1:50:84	-84	15	0	0	44 780	WPA2	CCMP	PSK	DIGIFIBRA-PLUS-tdTS
10:5D:DC:72:F2:10	-84	7	0	0	1 360	WPA2	CCMP	PSK	PATRALEX
98:97:D1:35:E4:36	-84	9	3	0	1 130	WPA2	CCMP	PSK	MOVISTAR_E435
98:00:6A:A0:9B:C5	-85	15	0	0	44 780	WPA2	CCMP	PSK	DIGIFIBRA-PLUS-gima
CC:D4:A1:E1:7B:B4	-85	4	0	0	6 130	WPA2	CCMP	PSK	MOVISTAR_7BB3
10:5D:DC:72:F2:15	-85	7	0	0	1 360	WPA2	CCMP	PSK	<length: 0>
86:97:D1:35:E4:3E	-86	15	12	0	52 1733	WPA2	CCMP	PSK	MOVISTAR_E435
98:97:D1:35:E4:3E	-86	15	32	0	52 1733	WPA2	CCMP	PSK	MOVISTAR_PLUS_E435
CC:ED:DC:C9:03:58	-86	3	0	0	1 130	WPA2	CCMP	PSK	MOVISTAR_0358
26:57:60:92:DB:F8	-87	13	0	0	56 1733	WPA2	CCMP	PSK	Skynet
34:57:60:92:DB:F8	-87	13	7	0	56 1733	WPA2	CCMP	PSK	Skynet_plus
DC:53:7C:14:71:E5	-87	12	0	0	44 270	WPA2	CCMP	PSK	ONOABA-5G
6A:CE:DA:7D:FA:47	-89	3	0	0	100 1733	WPA2	CCMP	PSK	MiFibra-FA43
A4:CE:DA:7D:FA:46	-89	5	0	0	100 1733	WPA2	CCMP	PSK	<length: 0>
44:48:B9:29:3D:C0	-1	0	0	0	11 -1				<length: 0>
A4:CE:DA:7D:FA:45	-84	1	0	0	6 130	WPA2	CCMP	PSK	MiFibra-FA43
A4:2B:B0:A8:70:5E	-85	3	0	0	1 270	WPA2	CCMP	PSK	TP-LINK_A8705E
C6:D4:A1:E1:7B:BC	-1	0	0	0	36 -1				<length: 0>
62:1E:A3:67:32:47	-86	1	0	0	6 130	WPA2	CCMP	PSK	vodafone1BE0
34:57:60:92:DB:F0	-88	3	0	0	11 130	WPA2	CCMP	PSK	Skynet
62:1E:A3:67:32:44	-88	3	0	0	6 130	WPA2	CCMP	PSK	<length: 10>
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes		
(not associated)	1A:57:5D:CC:D0:20	-81	0 - 1	0	4				
(not associated)	5C:CF:7F:B4:F4:2C	-86	0 - 1	0	2				ONOD79D
(not associated)	FE:67:59:20:66:3A	-87	0 - 6	0	2				
(not associated)	C6:AA:99:2F:47:00	-87	0 - 1	0	2				MiFibra-0B4B
(not associated)	62:A8:65:A0:8D:D5	-88	0 - 6	0	2				
16:66:78:72:A8:EF	48:D2:24:BA:04:43	-84	0 - 6	0	1				
DC:F8:B9:A1:50:83	CE:EA:84:22:53:46	-87	0 -11	0	1				
86:97:D1:35:E4:3E	6E:52:AC:9D:B4:87	-1	6e- 0	0	2				
86:97:D1:35:E4:3E	D0:B1:28:14:A7:AD	-1	6e- 0	0	5				
98:97:D1:35:E4:3E	04:54:53:EB:26:F6	-1	6e- 0	0	26				

Sergio Romero Redondo ([CC0](#))

Apartado 3: Exposición en redes OPEN

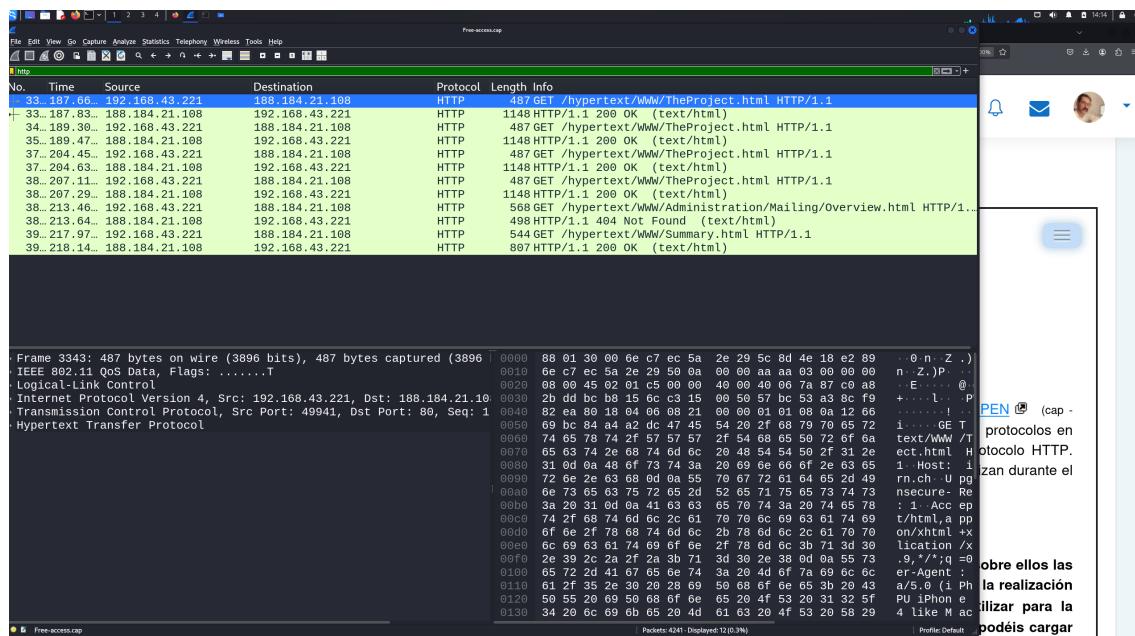
En este apartado se proporciona una [Captura de red de la monitorización de una red OPEN](#) (cap - 383,21 KB). Entre las tramas de gestión capturadas podréis ver cómo se exponen ciertos protocolos en claro, localizarlos con wireshark y mostrar la comunicación que se establece en el protocolo HTTP. Recordad documentar todo el proceso mediante capturas y detallar los pasos que se realizan durante el proceso.

Al abrir el archivo Free-access.cap se abre directamente Wireshark.

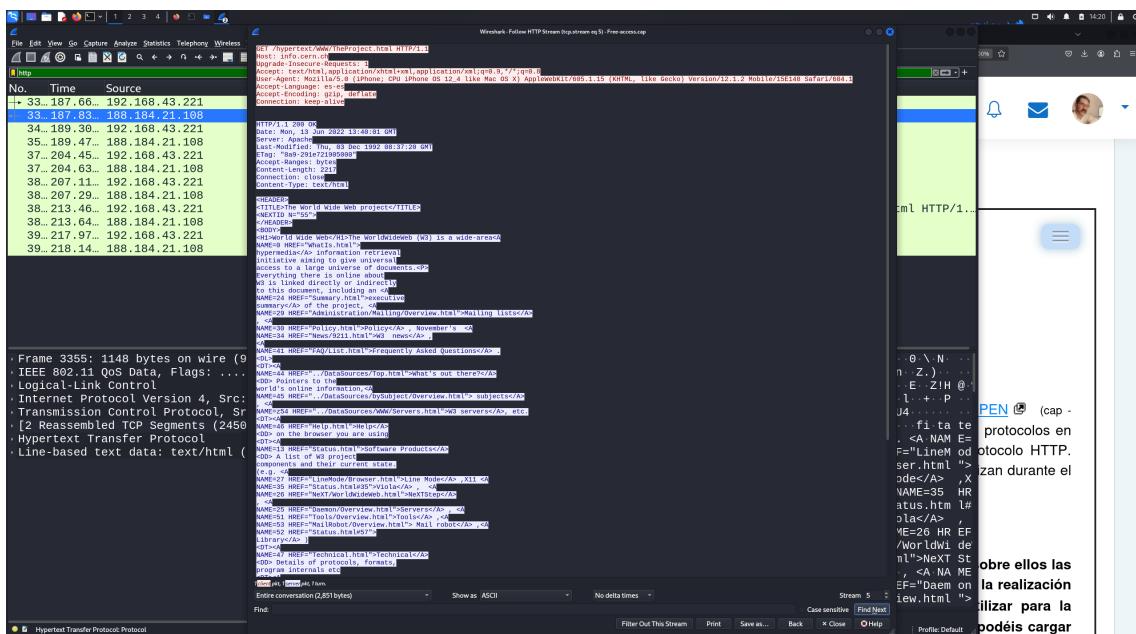


Podemos observar los protocolos en la barra de protocolos de cada comunicación, donde podemos observar los diferentes protocolos, ARP, DHCP, DNS, HTTP, ICMPV6, TLS.

Utilizo la barra de filtrado para filtrar el protocolo HTTP y saco las tramas capturadas con este protocolo.



Abro con botón derecho follow/ http stream y se puede observar en detalle la estructura y los datos de la web consultada.



Apartado 4: Debilidades en las redes inalámbricas.

En este apartado se entregan varios ficheros de captura para que podáis realizar sobre ellos las técnicas de cracking descritas durante el módulo. Para no extendernos mucho en la realización de la tarea se ha configurado un [diccionario](#)

(txt - 16,25 KB) que podéis utilizar para la resolución de la tarea. Cabe destacar que si queréis ver el proceso de la captura podéis cargar el fichero de captura en airodump-ng con el operador -r

```
$ airodump-ng -r fichero_de_captura
```

Recordad que tendréis que documentar todo el proceso con capturas indicando los pasos realizados.

- A continuación se presenta un paquete de captura de red que contiene la [captura de un 4-way-handsake](#) (pcap - 175,76 KB) de una red WPA2-PSK para aplicarle una técnica de cracking offline. Podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

Me sitúo en la carpeta Downloads donde tengo los archivos descargados y ejecuto aircrack-ng -w diccionario.txt wpa2-psk.pcap, me solicita el numero de la red e indicamos el 1, ya que es de la que tenemos el handshake.

```
(kali㉿kali)-[~/Downloads]
└─$ aircrack-ng -w diccionario.txt wpa2-psk.pcap
Reading packets, please wait ...
Opening wpa2-psk.pcap
Read 1093 packets.

#   BSSID           ESSID
1  00:0C:41:82:B2:55  Coherer
2  65:78:F7:B7:30:84
3  65:78:F7:B7:60:A9
4  81:F8:47:33:56:BB
5  92:F3:65:74:D2:DB
6  98:D3:04:64:FA:55
7  F4:9F:8F:EA:7B:E6
8  FF:FF:FF:FF:FF:3F

Index number of target network ? 1
Reading packets, please wait ...
Opening wpa2-psk.pcap
Read 1093 packets.

1 potential targets
```

Recordad que tendréis que documentar todo el proceso con capturas indicando los pasos realizados.

- A continuación se presenta un paquete de captura de red que contiene la [captura de un WPA2-way-handshake](#) (pcap - 175,76 KB) de una red WPA2-PSK para aplicarle una técnica de cracking offline. Podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.
- A continuación se presenta un paquete de captura de red que contiene la [captura de un PMKID](#) (pcap - 27,71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en

Tras ello lee los paquetes y empieza a comprobar las contraseñas con el archivo diccionario.txt facilitado.

En poco tiempo nos indica que una contraseña encontrada.

KEY FOUND! [Induction]

```
Aircrack-ng 1.7
[00:00:01] 2237/2302 keys tested (2695.60 k/s)

Time left: 0 seconds          97.18%
En este apartado se entregan varios ficheros de captura para que podáis realizar sobre ellos las técnicas de cracking descritas durante el módulo. Para no extendernos mucho en la realización de la tarea se ha configurado un diccionario (txt - 16,25 KB) que podéis utilizar para la prueba de fuerza bruta. Cabe destacar que si queréis ver el proceso de la captura podéis cargar el fichero de captura en airodump-ng con el operador -r.

KEY FOUND! [ Induction ]
Tarea online HE02

Master Key   : 07 68 18 AD 63 4C 1A 9A D7 C2 F0 81 17 98 2A D5 80
               62 F8 8F 3F 2C F3 C2 23 54 D6 CF AF 7E 2E E7 43
Transient Key : CF 53 2A 9E CE 72 B5 D3 15 9B 18 6C 6C A3 7D FC
               D4 45 8C 5D 40 2C 6B FC C9 C3 1D 1E 5B 2A 66 5F
               8B 7F B1 AA 17 E8 81 7E 78 C9 F1 26 4F C9 35 04
               C4 E7 60 DC 16 69 2F 42 64 FB BB DB 28 79 BF 9F

EAPOL HMAC   : 63 EA 18 75 C9 5B BD B4 B7 72 4E 62 71 D9 BF 03

Recordad que tendréis que documentar todo el proceso con capturas indicando los pasos realizados.

(kali㉿kali)-[~/Downloads]
└─$
```

A continuación se presenta un paquete de captura de red que contiene la [captura de un WPA2-way-handshake](#) (pcap - 175,76 KB) de una red WPA2-PSK para aplicarle una técnica de cracking offline. Podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

A continuación se presenta un paquete de captura de red que contiene la [captura de un PMKID](#) (pcap - 27,71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en

- A continuación se presenta un paquete de captura de red que contiene la [captura de un PMKID](#) (pcap - 27,71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

En este caso actuó como en el apartado anterior situándonos en la carpeta donde tenemos los archivos descargados y ejecutamos en la terminal el comando aircrack-ng -w diccionario.txt pmkid.pcap

```
(kali㉿kali)-[~/Downloads]
$ aircrack-ng -w diccionario.txt pmkid.pcap
Reading packets, please wait ...
Opening pmkid.pcap
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Read 192 packets. 3 - Evaluación de la tarea.

#          BSSID                ESSID
1  00:0D:58:EF:88:09  tmpAP
2  00:0D:58:EF:88:0A  Vodafone
3  00:0D:58:EF:88:0B  veles3
4  14:CC:20:C1:CB:2C  Lekonora
5  24:A4:3C:FF:22:36  Intertelcom_FREE
6  28:10:7B:94:BB:29  ogogo
7  F4:EC:38:A6:2F:EA  TPILIN
8  F8:1A:67:E5:05:62  Smile)

Index number of target network ? 6

Recordad que tendréis que documentar todo el proceso con capturas indicando los pasos realizados.

A continuación se presenta un paquete de captura de red que contiene la captura de un WPA2-way-handshake (pcap - 175.76 KB) de una red WPA2-PSK para aplicarle una técnica de cracking offline. Podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

Encryption
A continuación se presenta un paquete de captura de red que contiene la captura de un PMKID (pcap - 27.71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este apartado.
Unknown (pcap - 27.71 KB) de una red WPA2-PSK (Tenéis que realizar esta técnica sobre la red que contiene el PMKID) para aplicarle una técnica de cracking offline. En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este apartado.
Unknown (pcap - 4.92 KB) -> Log autenticación capturada (log - 1.52 KB) mediante un punto de acceso falso, en este caso también podréis aplicar una técnica de cracking offline. En este caso podéis utilizar hashcat o "johntheripper" junto con el diccionario de
```

Selecciono el numero 6 ya que es el que tiene PMKID. ¡Y en poco tiempo nos indica que ha encontrado la clave! KEY FOUND [15211521]

- A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA2-Enterprise ([Log ejecución hostapd-wpe](#) (log - 4,92 KB) - [Log autenticación capturada](#) (log - 1,52 KB)) mediante un punto de acceso falso, en este caso también podréis aplicar una técnica de cracking offline. En este caso podéis utilizar hashcat o "johntheripper" junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

Tras la descarga de los archivos y con ayuda del comando cat compruebo el contenido del log de hostapd con cat hostapd-wpe.log

File Actions Edit View Help

(kali㉿kali)-[~/Downloads]

```
$ cat hostapd-wpe.log
```

mschapv2: Mon Jun 13 15:54:50 2022
username: user_test
challenge: da:5b:ca:fe:3d:97:f1:de
response: ea:a9:b0:16:e8:d2:bd:ee:57:e1:0b:7a:06:3d:a8:dc:5e:92:40:36:ff:66:b4:a0
jtr NETNTLM: user_test:\$NETNTLM\$da5bcacf3d9f1de\$ea9b016e8d2bddee57e10b7a063da8dc5e924036ff66b4a0
hashcat NETNTLM: user_test:::ea9b016e8d2bddee57e10b7a063da8dc5e924036ff66b4a0::da5bcacf3d9f1de

mschapv2: Mon Jun 13 15:59:30 2022
username: user_test
challenge: 6d:c9:06:33:d7:28:45:f1
response: 5b:29:b5:6b:08:b7:3c:f2:a0:90:bd:94:a2:31:9b:77:96:0:c:43:e0:ac:a3:d6:1c
jtr NETNTLM: user_test:\$NETNTLM\$6dc90633d72845f1\$5b29b56b08b73cf2a090bd9442319b7796043e0aca3d61c
hashcat NETNTLM: user_test:::5b29b56b08b73cf2a090bd9442319b7796043e0aca3d61c:6dc90633d72845f1

mschapv2: Mon Jun 13 15:59:42 2022
username: user_test
challenge: 18:37:73:1c:f6:ef:26:f5
response: d0:b0:54:f0:f6:c8:a7:a3:6:fce:2e:b7:a0:08:fef8:8d:c1:82:68:05:f0:f3
jtr NETNTLM: user_test:\$NETNTLM\$1837731cfe26f5\$d0b054f0f6c8a7a36fce2eb7f0a8fe8e8d1826805f0f3
hashcat NETNTLM: user_test:::d0b054f0f6c8a7a36fce2eb7f0a8fe8e8d1826805f0f3:1837731cfe26f5

mschapv2: Mon Jun 13 15:59:45 2022
username: user_test
challenge: ec:02:41:bb:ba:b8:ee:ba
response: c7:a3:58:aa:97:a5:c5:f3:62:e2:df:04:48:f0:29:d7:37:03:0:17:fa:57:d8:15
jtr NETNTLM: user_test:\$NETNTLM\$ec0241bbab8eeba\$c7a358aa97af5f362e2df0448f029d73703e017fa57d815
hashcat NETNTLM: user_test:::c7a358aa97af5f362e2df0448f029d73703e017fa57d815:ec0241bbab8eeba

Recordad que tendrás que documentar todo el proceso con capturas indicando los pasos realizados.

Continuación de la captura de red que contiene la [captura de un PMKID](#). A continuación se presenta un paquete de captura de red que contiene la [captura técnica sobre la red que contiene el PMKID](#). En este caso podéis utilizar el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA-Enterprise (Log ejecución hostapd-wpe) (log - 4.92 KB) - Log autenticación capturada (log - 4.92 KB). En este caso también podréis aplicar una técnica de "cracking offline" utilizando el propio aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.

(kali㉿kali)-[~/Downloads]

Se puede observar que contiene los hashes. Tras ello copio los hashes y los copio en un archivo de texto creado para el efecto con nano hashesnetntlm.txt

```
File Actions Edit View Help
GNU nano 8.2
hashesnetntlm.txt

user_test:::ea9b016e8d2bde57e10b7a063da8dc5e9242036fF66b4a0:da5bcfafe3d97f1de
user_test:::5b29b56bd8b73cF20a90d94a2319b7960c430ca3d61c:6d96e3d3d72845f
user_test:::d0b54f0f6c8a7a3fcfe2b70f0a8feff8e8d1826805f0f3:1837731cf6ef26f5
user_test:::c7a358aa97acf5f3622df0448f029d73703e017f7a57d815:ec0241bbbab8ebea

username: user_test
challenge: da5bcfafe3d97f1de
response: ea9b016e8d2bde57e10b7a063da8dc5e9242036fF66b4a0
jtr NETNTLM: user_test:$NETNTLM$da5bcfafe3d97f1de$ea9b016e8d2bde57e10b7a063da8dc5e9242036fF66b4a0
hashcat NETNTLM: user_test:::ea9b016e8d2bde57e10b7a063da8dc5e9242036fF66b4a0:da5bcfafe3d97f1de

mschapv2: Mon Jun 13 15:59:10 2022
username: user_test
challenge: d0:b9:09:33:d7:28:45:f3
response: 5b:39:b5:6b:d8:87:3c:f7:20:90:bd:94:42:31:9b:77:96:0:c4:3:e0:a:c:a3:d6:1c
jtr NETNTLM: user_test:$NETNTLM$0dc9063d72845f15$b29b56bd8b73cF20a90d942319b77960c430ca3d61c
hashcat NETNTLM: user_test:::5b:29b56bd8b73cF20a90d942319b77960c430ca3d61c:6d96e3d3d72845f

mschapv2: Mon Jun 13 15:59:42 2022
username: user_test
challenge: 18137733:cf6:ef:26:f5
response: d0:b0:54:f0:fb:ca:7a:31:6:ce:2e:87:0:f:0:a:8:f:ef:8e:8d:c1:82:08:05:f0:13
jtr NETNTLM: user_test:$NETNTLM$1837731cf6ef26f5$0b054f0fc8a7a36fce2ebf0f0a8feff8e8dc1826805f0f3
hashcat NETNTLM: user_test:::d0:b0:54:f0:fb:ca:7a:31:6:ce:2ebf0f0a8feff8e8dc1826805f0f3:1837731cf6ef26f5

mschapv2: Mon Jun 13 15:59:45 2022
username: user_test
challenge: ec:82:bb:ba:b8:ee:ba
response: 67:ca:58:aa:97:af:c5:73:62:e2:df:04:48:f9:29:d7:37:0:3:e0:17:fa:57:d8:15
jtr NETNTLM: user_test:$NETNTLM$8c0242bbab8ebea:f7:35:9a:97:fc5:13:0:2:df0:48:f0:29d73703e017fz57d815
hashcat NETNTLM: user_test:::c7:43:8d:80:7d:0:3:0:2:ed:0:9:48:0:9:0:75:70:0:e017f0:29d73703e017fz57d815

[ Read 4 lines ]
[F Help      [ F Where Is      [ K Cut      [ K Execute      [ C Location      M-U Undo      M-A Set Mark      M-J To Bracket
[F Exit      [ O Write Out      [ R Replace      [ U Paste      [ J Justify      [ V Go To Line      M-E Redo      M-B Copy      M-B Where Was
```

Tras ello uso johhtheripper y ejecuto seleccionando el diccionario.txt y el archivo que hemos creado con los hashes capturados.

```
john --wordlist=diccionario.txt hashesnetntlm.txt

File Actions Edit View Help
jtr NETNTLM: user_test:$NETNTLM$6dc90633d72845f1b5b29b56bd8b73cf20a90bd9442319b77960c43e0aca3d61c
hascat NETNTLM: user_test:::5b29b56bd8b73cf20a90bd9442319b77960c43e0aca3d61c6dc90633d72845f1

mschapv2: Mon Jun 13 15:59:42 2022
username: user_test
challenge: 18:37:73:1c:f6:ef:26:f5
response: d0:b0:54:f0:f6:c8:a7:a3:6f:ce:2e:b7:0f:0a:8f:ef:8e:d1:c1:82:68:05:f0:f3
jtr NETNTLM: user_test:$NETNTLM$1837731c6ef26f5$0b054f0f6ca87a36fce2eb70f0a8feff8e8dc1826805f0f3
hascat NETNTLM: user_test:::d0b054f0f6ca87a36fce2eb70f0a8feff8e8dc1826805f0f3:1837731c6ef26f5

mschapv2: Mon Jun 13 15:59:45 2022
username: user_test
challenge: ec:02:41:bb:ba:b8:ee:ba
response: c7:a3:58:aa:97:a7:c5:f3:62:e2:d0:04:48:f0:29:d7:37:03:e0:17:fa:57:d8:15
jtr NETNTLM: user_test:$NETNTLM$ec0241bbbabb8eaba$c7a358aa97afcc5f362e2df0448f029d73703e017fa57d815
hascat NETNTLM: user_test:::c7a358aa97afcc5f362e2df0448f029d73703e017fa57d815:ec0241bbbabb8eaba

[kali㉿kali] - [~/Downloads]
$ john --wordlist=diccionario.txt hashesnetntlm.txt
Created directory: /home/kali/.john
Warning: detected hash type "netntlm", but the string is also recognized as "netntlm-naive" de captura de red que contiene la captura de un PMKID
Use the "--format=netntlm-naive" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=3 aircrack-ng junto con el diccionario de posibles contraseñas que os hemos indicado en este mismo apartado.
Press 'q' or Ctrl-C to abort, almost any other key for status
test1234          (user_test)
test1234          (user_test)
test1234          (user_test)
test1234          (user_test)
4g 0:00:00:00 DONE (2025-01-06 17:40) 200.0g/s 115100p/s 460400c/s 460400c/s impala..induction
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably
Session completed.

[kali㉿kali] - [~/Downloads]
$
```

Gracias a ello obtenemos que la contraseña para user test es test1234

Compruebo el otro archivo de log suministrado y veo el contenido con cat

```
cat hostapd-wpe-run.log
```

Como podemos observar nos arroja información más completa, pero con el anterior archivo ha sido más que suficiente.

Bibliografía:

- Temario de la asignatura.
- Consulta de frecuencias <https://www.redeszone.net/tutoriales/redes-wifi/bandas-frecuencias-wi-fi/>
- Documentación aircrack-ng <https://www.aircrack-ng.org/>