

# Tarea online HE02.

Título de la tarea: Analizando la red Wi-Fi

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

## ¿Qué contenidos o resultados de aprendizaje trabajaremos?

### Resultados de aprendizaje

#### ✓ RA1.

- ➡ a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.
- ➡ b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.
- ➡ c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.
- ➡ d) Se ha accedido a redes inalámbricas vulnerables.
- ➡ e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.
- ➡ f) Se han utilizado técnicas de “Equipo Rojo y Azul”.
- ➡ g) Se han realizado informes sobre las vulnerabilidades detectadas.

### Contenidos

- 1.- Conceptos generales en hacking ético de entornos inalámbricos.
  - 1.1.- Principales diferencias entre las bandas de frecuencia 2,4GHz y 5GHz.
  - 1.2.- Componentes de una red inalámbrica.
  - 1.3.- Terminología.
  - 1.4.- Tipos de redes inalámbricas.
  - 1.5.- Equipamiento necesario.
  - 1.6.- Modos de operación de las tarjetas inalámbricas.
- 2.- Análisis y recolección de datos en redes inalámbricas.
  - 2.1.- Necesidades técnicas para la monitorización.
  - 2.2.- Estableciendo la tarjeta de red en modo Monitor.
  - 2.3.- Monitorizando la red inalámbrica.
- 3.- Ataques a redes inalámbricas.

- 3.1.- Ataques a redes tipo OPEN.
- 3.2.- Ataques a redes tipo WEP.
- 3.3.- Ataques a redes tipo WPA/WPA2-PSK.
- 3.4.- Ataques a redes tipo WPA/WPA2-Enterprise.
- 4.- Herramientas de seguridad y hacking ético.

# 1.- Descripción de la tarea.



## 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.



[Direct Media](#) (Dominio público)

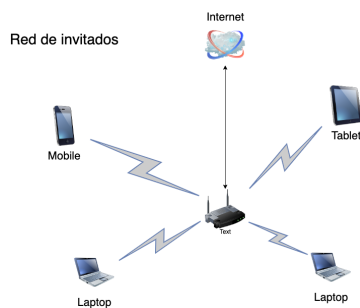
- ✓ La primera fase se centrará en buscar debilidades de diseño de la red inalámbrica y contemplará las casuísticas en el que se estén utilizando tipologías de redes Wi-Fi que no resulten adecuadas para la funcionalidad que desempeñan.
- ✓ En la segunda fase realizarán una monitorización de las redes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

## ¿Qué te pedimos que hagas?

### ✓ 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:

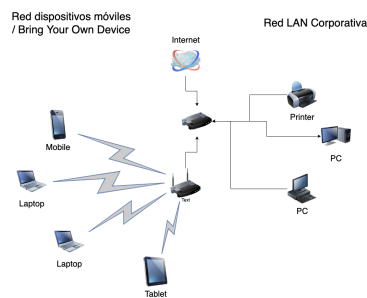


Sergio Romero Redondoación (CC0)

- ➡ **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 implementarías en la red

- ➡ A continuación se muestra el diagrama de la red de dispositivos móviles:

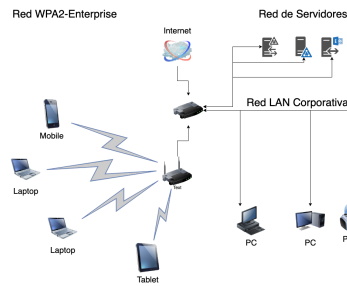


Sergio Romero Redondo (CC0)

- ➡ **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:



Sergio Romero Redondo (CC0)

## ✔ 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.
- Indica en que bandas de frecuencia y en que canales operan las redes Skynet y Skynet\_Plus.
- Indica a qué red está conectado el dispositivo con MAC 6E:52:AC:9D:B4:87.
- Indica en que red intenta conectarse el dispositivo 5C:CF:7F:B4:F4:2C.

BSSID	Power	Source	#Data	R/s	Ch	MB	ENC	CIPHER	Auth	ESSID
18:06:C7:18:C7:C5	-31	18	5	0	16	1178	WPA2	CCMP	PSK	Skynet_plus
18:06:C7:18:C7:C5	-43	17	2	0	11	105	WPA2	CCMP	PSK	Skynet
38:80:6A:A8:38:C4	-73	11	4	0	5	138	WPA2	CCMP	PSK	DISCIBRA_plus
DC:53:7C:14:71:04	-76	9	0	0	7	138	WPA2	CCMP	PSK	Salto
AA:97:33:AA:42:1E	-77	15	0	0	12	1733	WPA2	CCMP	PSK	MOVISTAR_PLUS_8210
DC:53:7C:59:55:3E	-79	18	0	0	11	105	WPA2	CCMP	PSK	OWG63
18:06:78:72:AA:07	-82	11	0	0	6	138	WPA2	CCMP	PSK	iPhone de Mollia
DC:F4:89:A1:58:83	-82	12	0	0	7	138	WPA2	CCMP	PSK	DISCIBRA-LUTS
DC:F4:89:A1:58:84	-84	15	0	0	44	788	WPA2	CCMP	PSK	DISCIBRA_PLUS-LUTS
18:50:DE:72:72:18	-84	7	0	0	1	368	WPA2	CCMP	PSK	PATALLER
18:50:DE:72:72:18	-84	8	0	0	1	138	WPA2	CCMP	PSK	MOVISTAR_8435
38:80:6A:A8:38:C5	-85	15	0	0	44	788	WPA2	CCMP	PSK	DISCIBRA_PLUS-gino
C0:0A:03:13:78:04	-85	4	0	0	6	138	WPA2	CCMP	PSK	MOVISTAR_7803
18:50:DE:72:72:15	-85	7	0	0	1	368	WPA2	CCMP	PSK	-length: 8-
18:50:DE:72:72:15	-85	7	0	0	1	368	WPA2	CCMP	PSK	-length: 8-
18:50:DE:72:72:15	-85	15	12	0	52	1733	WPA2	CCMP	PSK	MOVISTAR_8435
18:50:DE:72:72:15	-85	15	12	0	52	1733	WPA2	CCMP	PSK	MOVISTAR_PLUS_8435
C0:0A:03:13:78:04	-86	3	0	0	1	138	WPA2	CCMP	PSK	MOVISTAR_8104
26:57:08:92:08:F8	-87	13	0	0	55	1733	WPA2	CCMP	PSK	Skynet
5C:CF:7F:14:71:03	-87	12	0	0	55	1733	WPA2	CCMP	PSK	Skynet_plus
DC:53:7C:14:71:03	-87	12	0	0	44	278	WPA2	CCMP	PSK	ONDARA_SG
0A:CE:0A:70:3A:45	-89	5	0	0	180	1733	WPA2	CCMP	PSK	WiFiFibra-F43
AA:CE:0A:70:3A:46	-89	5	0	0	180	1733	WPA2	CCMP	PSK	-length: 8-
AA:CE:0A:70:3A:46	-89	5	0	0	11	1	WPA2	CCMP	PSK	-length: 8-
AA:CE:0A:70:3A:45	-84	1	0	0	6	138	WPA2	CCMP	PSK	WiFiFibra-F43
AA:CE:0A:70:3A:45	-85	3	0	0	2	278	WPA2	CCMP	PSK	TP-LINK-AR55E
CE:04:A1:E1:78:BC	-81	0	0	0	36	-1	WPA2	CCMP	PSK	-length: 8-
62:1E:83:67:72:47	-80	1	0	0	6	138	WPA2	CCMP	PSK	Voicemaster800
34:57:08:92:08:F8	-88	3	0	0	11	138	WPA2	CCMP	PSK	Skynet
62:1E:83:67:72:44	-88	3	0	0	6	138	WPA2	CCMP	PSK	-length: 18-

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.

## ✔ 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.
- 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.
- 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.

#### **NOTA IMPORTANTE**

**Para los apartados en los que se solicita realizar una captura de pantalla hay que tener en cuenta que las capturas realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.**

## 2.- Información de interés.

### Recursos necesarios y recomendaciones

#### Recursos necesarios

- ✓ Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- ✓ Conexión a Internet para consultar ejemplos de la Unidad 2.
- ✓ Sistemas Operativos preferidos Kali Linux, Parrot Linux, Debian Linux, Ubuntu Linux
- ✓ Navegador web.
- ✓ Software para comprimir los archivos de la tarea.

#### Recomendaciones

- ✓ Antes de abordar la tarea:
  - ➔ lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - ➔ Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- ✓ No olvides elaborar el documento explicativo.



### Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

**Apellido1\_Apellido2\_Nombre\_HE02\_Tarea**

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la segunda unidad del MP de HE**, debería nombrar esta tarea como...

**sanchez\_manas\_begona\_HE02\_Tarea**

### 3.- Evaluación de la tarea.

#### Criterios de evaluación RA1

- ✓ a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.
- ✓ b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.
- ✓ c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.
- ✓ d) Se ha accedido a redes inalámbricas vulnerables.
- ✓ e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.
- ✓ f) Se han utilizado técnicas de “Equipo Rojo y Azul”.
- ✓ g) Se han realizado informes sobre las vulnerabilidades detectadas.

#### ¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
<b>Apartado 1:</b> Indica y justifica de manera correcta los problemas de seguridad y posibles ataques a la red Wi-Fi de invitados. Indica y Justifica adecuadamente mejoras en el diseño de la red	1 punto
<b>Apartado 1:</b> Indica y justifica de manera correcta los problemas de seguridad y posibles ataques a la red Wi-Fi de dispositivos móviles. Indica y Justifica adecuadamente mejoras en el diseño de la red	1 punto
<b>Apartado 1:</b> Indica y justifica de manera correcta los problemas de seguridad y posibles ataques a la red Wi-fi corporativa. Indica y Justifica adecuadamente mejoras en el diseño de la red	1 punto
<b>Apartado 2:</b> Responde de manera adecuada a todas las cuestiones que se plantean sobre la captura de la monitorización.	1 punto (0,25 por subapartado)
<b>Apartado 3:</b> Muestra de manera correcta los datos en texto plano capturados en la red de tipo open. El alumno puede utilizar la herramienta wireshark para mostrar los datos u otra de su elección	1,5 puntos



<b>Apartado 4:</b> Muestra y detalla de manera correcta todos el proceso de cracking del 4-way-handshake.	1,5 puntos
<b>Apartado 4:</b> Muestra y detalla de manera correcta todos el proceso de cracking del PMKID capturado.	1,5 puntos
<b>Apartado 4:</b> Muestra y detalla de manera correcta todos el proceso de cracking del hash NETNTLMv1 capturado.	1,5 puntos
Redacción clara y correcta, sin errores ortográficos	<b>Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.</b>

#### NOTA IMPORTANTE

**Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.**