Módulo 3. Autenticación de red y wifi enterprise

CÓRDOBA CREA FUTURO

Unidad 1. 802.1X. Herramientas de seguridad de wireless en LAN

Introducción

En la actualidad, la mayoría de las organizaciones utiliza redes inalámbricas para sus comunicaciones. Sin embargo, esto no implica que se trate de un medio completamente seguro. Las redes inalámbricas son más vulnerables que las conexiones por cable, ya que las ondas de radio que emplean pueden ser interceptadas con mayor facilidad.

Existen, no obstante, medidas y herramientas que permiten mitigar los riesgos asociados a este tipo de conexiones.

Una red inalámbrica puede definirse como aquella en la que dos o más dispositivos electrónicos se conectan sin necesidad de utilizar cables. Esta conexión es posible siempre que los dispositivos se encuentren dentro del área de cobertura de la red.

El funcionamiento de estas redes se basa en el uso de ondas electromagnéticas, cuya frecuencia varía según la tecnología que se utilice.

Un aspecto relevante en el uso de redes inalámbricas es la diferenciación de sus tipos, según el área que abarcan y su propósito. A continuación, se describen las principales categorías:

- **WPAN (*wireless personal area network*)**. Red inalámbrica de área personal. Tiene un alcance reducido y solo cubre unos pocos metros. La tecnología más común en este tipo de redes es *Bluetooth*.
- **WLAN (*wireless local area network*)**: red inalámbrica de área local. Representa la alternativa inalámbrica a las redes cableadas en entornos empresariales y domésticos. Su

alcance promedio ronda los 100 metros. La tecnología más utilizada es *Wi-Fi*, que opera en las bandas de 2,4 GHz y 5 GHz.

- **WMAN (*wireless metropolitan area network*)**: red inalámbrica de área metropolitana. Estas redes cubren distancias mayores, entre 4 y 10 km, y son empleadas, en general, por proveedores de servicios de telecomunicaciones. La tecnología más representativa es *WiMAX*.

- **WWAN (*wireless wide area network*)**: red inalámbrica de área extensa. Diseñada para abarcar grandes zonas geográficas, suele ser utilizada por compañías de telefonía móvil para ofrecer conectividad en áreas amplias.

El presente módulo se enfoca en las redes WLAN (*wireless local area network*), es decir, redes inalámbricas de área local. Estas redes utilizan los estándares 802.11, desarrollados por el IEEE, para definir cómo se comunican los dispositivos dentro de un entorno wifi.

Estos estándares han evolucionado con el tiempo, mejorando aspectos como la velocidad, el alcance, la eficiencia y la utilización de distintas bandas de frecuencia. Cada nueva versión representa un avance técnico respecto a la anterior, lo que permite adaptarse a las crecientes demandas de conectividad.

Las distintas generaciones del protocolo 802.11 (b, g, n, ac, ax, be) introducen mejoras progresivas en términos de rendimiento y funcionalidad. A continuación, se presenta un resumen comparativo de su evolución:

Tabla 1. Evolución de los estándares 802.11

Estándar (nombre comercial)	Frecuencia de banda	Velocidad máxima teórica	Características clave

802.11a (wifi 2)	5 GHz	54 Mbps	Introdujo el uso de la banda de 5 GHz para evitar interferencias comunes en 2,4 GHz. Fue uno de los primeros estándares con velocidades relativamente altas, aunque no era compatible con 802.11b.
802.11b (wifi 1)	2.4 GHz	11 Mbps	Considerado el primer estándar wifi de uso extendido, aunque presentaba velocidades bajas y era susceptible a interferencias debido a su operación en la banda de 2,4 GHz.
802.11g (wifi 3)	2.4 GHz	54 Mbps	Combinó la velocidad de 802.11a con la compatibilidad de 802.11b, ofreciendo mejoras notables en rendimiento sin cambiar de banda.
802.11n (wifi 4)	2.4 GHz y 5 GHz	Hasta 600 Mbps	Introdujo la tecnología MIMO (múltiples flujos espaciales) y canales de 40 MHz, lo que incrementó tanto la velocidad como el alcance. Es retrocompatible con los estándares anteriores.
802.11ac (wifi 5)	5 GHz (principalmente)	Más de 1 Gbps	Conocido como «Wi-Fi Gigabit», se centró exclusivamente en la banda de 5 GHz. Incorporó MU-MIMO, canales más anchos (hasta 160 MHz) y una

			modulación más eficiente, alcanzando velocidades superiores a 1 Gbps.
802.11ax (wifi- 6)	2.4 GHz y 5 GHz	Hasta 10 Gbps	Diseñado para ambientes con alta densidad de dispositivos. Utiliza OFDMA, MU-MIMO en ambas bandas, y mejoras en eficiencia energética, ofreciendo conexiones más rápidas, estables y adaptadas al tráfico concurrente.

Fuente: elaboración propia

Definición de algunos componentes de una red wifi

En una red wifi, intervienen distintos componentes que permiten establecer y mantener la conectividad inalámbrica.

El punto de acceso es el dispositivo encargado de interconectar equipos cableados, como *routers* o *switches*, y crear una red inalámbrica a la que otros dispositivos pueden conectarse de forma remota mediante una tarjeta de red inalámbrica.

La tarjeta de red inalámbrica, también conocida como tarjeta wifi, es la que permite a un dispositivo conectarse a una red sin necesidad de cables. Está integrada en la mayoría de los dispositivos móviles y portátiles, aunque también existen versiones externas.

El *router*, por su parte, proporciona conectividad a nivel de red (capa 3 del modelo OSI). Su función principal es encaminar paquetes de datos entre redes distintas. Es decir, interconecta subredes —conjuntos de dispositivos con direcciones IP dentro de un mismo rango— permitiendo la comunicación entre ellas mediante el reenvío de paquetes.

Cabe señalar que la seguridad en redes inalámbricas corporativas requiere mucho más que una contraseña compartida. En entornos empresariales o educativos, donde numerosos dispositivos se conectan simultáneamente, resulta fundamental implementar mecanismos de

autenticación que sean robustos, centralizados y escalables. Estos sistemas permiten gestionar de forma segura el acceso a la red, adaptándose a las necesidades de control y trazabilidad propias de organizaciones con múltiples usuarios.

En el contexto de redes inalámbricas, es fundamental identificar cómo las distintas amenazas afectan los principios básicos de la seguridad de la información: autenticación, confidencialidad, integridad, disponibilidad, control de acceso y no repudio. La siguiente tabla muestra una clasificación de diversos tipos de ataques según el principio que comprometen. Esto permite visualizar qué tipo de protección es más relevante frente a cada amenaza:

Tabla 2. Relación entre tipos de amenazas y principios de la seguridad informática

	AUTENTICACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONTROL DE ACCESO	NO REPUDIO
Barrido de Frecuencias	NO	NO	NO	NO	SI	N/A
Sniffing	NO	SI	NO	NO	NO	N/A
Spoofing	SI	NO	NO	NO	NO	N/A
Hijacking	SI	NO	NO	NO	NO	N/A
Ingenieria Social	SI	SI	NO	NO	NO	N/A
Confianza Transitiva	SI	NO	NO	NO	NO	N/A
Creación de un Puente	SI	NO	NO	NO	NO	N/A
Adivinación de contraseñas	SI	NO	NO	NO	NO	N/A
Explotación de errores o fallos de software (bugs)	NO	NO	NO	SI	NO	N/A
Denegación de Servicios	NO	NO	NO	SI	NO	N/A
Mensaje de control de red	NO	NO	NO	SI	NO	N/A
Interferencia/inhibición	NO	NO	NO	SI	NO	N/A
Ataques dirigidos por datos	NO	SI	NO	NO	NO	N/A
Caballo de Troya	NO	SI	NO	NO	NO	N/A
Enrrutamiento Fuente	NO	SI	SI	NO	NO	N/A
Evil Twin	NO	SI	NO	NO	NO	N/A
Man in the Middle	NO	SI	NO	NO	NO	N/A
Modificación de Datos	NO	NO	SI	NO	NO	N/A

Fuente: Cano y Salgado, 2016, https://bit.ly/3rBvey4

El estándar IEEE 802.1X, en conjunto con EAP (protocolo de autenticación extensible), RADIUS y servidores de identidad, permite aplicar controles de acceso basados en la identidad del usuario o del dispositivo, mediante el uso de certificados digitales o credenciales de red.

Esta unidad desarrolla en profundidad los conceptos fundamentales, las herramientas involucradas, los roles de cada componente, la configuración básica, la resolución de problemas frecuentes y recomendaciones prácticas para implementar una red inalámbrica segura con autenticación empresarial basada en 802.1X.

1.1. EAP-TLS / EAP-TTLS: concepto y requisitos

Las redes inalámbricas permiten que dos o más dispositivos se conecten entre sí sin necesidad de utilizar cables, siempre que se encuentren dentro del área de cobertura. Esta tecnología, si bien práctica, requiere mecanismos sólidos de autenticación para garantizar el acceso seguro a los recursos de red, especialmente en entornos empresariales.

El estándar IEEE 802.1X define un mecanismo de control de acceso a la red basado en puertos, aplicable tanto a redes cableadas como inalámbricas. Su función principal es permitir o denegar el acceso a un dispositivo en función de la autenticación de sus credenciales a través de un servidor centralizado.

En este esquema, 802.1X trabaja en conjunto con un servidor de autenticación —habitualmente RADIUS— para validar las credenciales presentadas por el dispositivo que intenta conectarse. Solo si la autenticación es exitosa, el dispositivo obtiene acceso a la red local, ya sea por cable o por wifi.

Los componentes principales de esta arquitectura son los siguientes:

Suplicante. —

El dispositivo cliente que solicita el acceso, como una computadora portátil o un teléfono móvil.

Autenticador: —

el dispositivo que intermedia entre el cliente y el servidor de autenticación. Puede ser un punto de acceso inalámbrico o un *switch*.

Servidor de autenticación: —

generalmente un servidor RADIUS, encargado de validar las credenciales del cliente y determinar si se le concede acceso a la red.

En este contexto, los métodos EAP-TLS y EAP-TTLS se utilizan como mecanismos de autenticación dentro del marco de 802.1X. En las siguientes secciones se detallarán sus características, requisitos y aplicaciones.

EAP (Extensible Authentication Protocol)

EAP es un marco para el transporte de métodos de autenticación, utilizado dentro del estándar 802.1X para encapsular el intercambio de credenciales entre el cliente (suplicante) y el servidor de autenticación. Su principal ventaja es la flexibilidad, ya que admite múltiples formas de autenticación según las necesidades de seguridad e infraestructura de cada red.

EAP (protocolo de autenticación extensible) es un marco flexible para la autenticación de red, que permite el acceso seguro de usuarios y dispositivos mediante distintos métodos, como contraseñas, certificados o *tokens*. Es comúnmente utilizado en redes wifi y conexiones VPN a través del estándar 802.1X.

Funciona como una conversación entre un cliente (par) y un servidor de autenticación (como RADIUS), mediada por un autenticador (punto de acceso o switch), que transmite los mensajes. De este modo, se garantiza que solo los usuarios autorizados accedan mediante una verificación de credenciales, normalmente cifrada.

EAP es un marco que permite múltiples métodos de autenticación. En redes empresariales, los más seguros y comunes son los siguientes:

- **EAP-TLS (Transport Layer Security)**

  EAP-TLS (Transport Layer Security) es un método de autenticación que utiliza certificados digitales tanto en el cliente (suplicante) como en el servidor para verificar la identidad de ambas partes. Al no depender de contraseñas, ofrece un nivel de seguridad muy alto y reduce significativamente el riesgo de ataques por robo o reutilización de credenciales. Su implementación requiere contar con una infraestructura de clave pública (PKI) que permita la emisión, distribución y gestión de los certificados digitales necesarios en los dispositivos y en el servidor de autenticación.

- **EAP-TTLS (Tunneled TLS)**

  EAP-TTLS (Tunneled TLS) es un método de autenticación que establece un túnel TLS mediante la validación del certificado digital del servidor. Una vez creado ese canal cifrado, permite que el cliente se autentique utilizando credenciales tradicionales, como nombre de usuario y contraseña, a través de métodos como PAP o MSCHAPv2. Estas credenciales pueden verificarse contra servicios de directorio como LDAP o Active Directory. Aunque no alcanza el nivel de seguridad de EAP-TLS, EAP-TTLS es más sencillo de implementar, ya que no requiere certificados digitales en el cliente, lo que lo convierte en una opción flexible para organizaciones que buscan reducir la complejidad en la gestión de dispositivos.

Para implementar autenticación mediante EAP-TLS o EAP-TTLS es necesario contar con una infraestructura mínima que incluya varios componentes clave. En primer lugar, se requiere un servidor RADIUS, que será el encargado de validar las credenciales de los usuarios o dispositivos. Entre las opciones más utilizadas se encuentran FreeRADIUS, por ser gratuito y ampliamente adoptado, y Microsoft NPS, incluido en entornos Windows Server.

Además, es indispensable disponer de una infraestructura de clave pública (PKI), que permita emitir y gestionar certificados digitales. Esto puede lograrse mediante herramientas como OpenSSL, XCA o una autoridad certificadora interna según el tamaño y las necesidades de la organización.

El cliente o dispositivo que desea acceder a la red debe ser compatible con EAP y, en el caso de EAP-TLS, con el uso de certificados. Los sistemas operativos más recientes como Windows 10 o superior, Linux con NetworkManager o *wpa_supplicant*, y macOS, ya incluyen compatibilidad con estos métodos. Estos dispositivos actúan como suplicantes en el proceso de autenticación.

También se necesita que los puntos de acceso sean compatibles con 802.1X, lo cual es común en dispositivos de fabricantes como Ubiquiti, MikroTik, Cisco o en soluciones basadas en OpenWRT. En términos de seguridad inalámbrica, es importante que los puntos de acceso soporten WPA2-Enterprise o WPA3-Enterprise, que son los modos necesarios para integrar 802.1X con cifrado adecuado.

Como recomendación práctica, para pequeñas empresas que no desean implementar una PKI completa desde el inicio, EAP-TTLS puede representar una opción viable, ya que reduce la complejidad al no requerir certificados en los dispositivos cliente.

1.2. Suplicantes (Windows/Linux) y certificados

El suplicante es el componente del dispositivo cliente encargado de iniciar el proceso de autenticación 802.1X. Los sistemas operativos modernos ya incorporan clientes compatibles con este protocolo, lo que facilita su implementación en entornos empresariales.

En el caso de Windows, el sistema operativo incluye un suplicante nativo desde la versión XP SP3. Este cliente soporta métodos como EAP-TLS, PEAP y EAP-TTLS, y puede configurarse manualmente desde el administrador de redes o de forma centralizada mediante directivas de

grupo (GPO) en entornos con Active Directory. El soporte para EAP-TLS es nativo, y los certificados digitales utilizados se almacenan en el almacén del sistema operativo.

En Linux, el suplicante más común es *wpa_supplicant*, que puede configurarse a través de archivos de texto o mediante herramientas gráficas como NetworkManager. Este componente admite tanto EAP-TLS como EAP-TTLS, y se configura editando el archivo */etc/wpa_supplicant.conf*. A modo de ejemplo, una configuración para EAP-TLS podría estructurarse de la siguiente manera:

```
network={
  ssid="RedSegura"
  key_mgmt=WPA-EAP
  eap=TLS
  identity="usuario@empresa.com"
  ca_cert="/etc/certs/ca.pem"
  client_cert="/etc/certs/user.pem"
  private_key="/etc/certs/user.key"
}
```

En cuanto al uso de certificados digitales, es necesario contar con una autoridad certificadora (CA) interna que permita emitir los certificados requeridos para la autenticación. El certificado del servidor RADIUS es obligatorio, ya que los dispositivos cliente lo utilizan para verificar la autenticidad del servidor. En el caso de EAP-TLS, también se requiere un certificado por cada cliente, emitido por la CA corporativa e instalado en los dispositivos correspondientes.

Entre las herramientas recomendadas para la generación y gestión de certificados se encuentran:

- OpenSSL, una solución de consola potente y ampliamente utilizada;
- XCA, una opción gráfica multiplataforma fácil de usar;
- TinyCA, una alternativa más simple orientada a entornos GNU/Linux.

Se recomienda utilizar certificados con expiración corta y aplicar mecanismos de renovación automática, ya sea mediante SCEP (Simple Certificate Enrollment Protocol) o scripts personalizados. Como buenas prácticas, se sugiere automatizar la inscripción de certificados (por ejemplo, mediante GPO, Intune o *scripts* de instalación), emplear nombres comunes (CN) descriptivos en los certificados para facilitar su identificación y auditoría, y revocar los certificados asociados a dispositivos o usuarios que ya no estén autorizados.

1.3. Listas de acceso dinámicas

Una de las principales ventajas del uso de 802.1X es la posibilidad de aplicar políticas de red de forma dinámica, en función del usuario o dispositivo autenticado. Esto se logra mediante la capacidad del servidor RADIUS de enviar atributos específicos a los *switches* o puntos de acceso, que luego aplican configuraciones como la asignación a una VLAN determinada o el establecimiento de reglas de calidad de servicio (QoS) o control de acceso (ACL).

El proceso funciona de la siguiente manera: cuando un usuario se autentica mediante 802.1X, el servidor RADIUS no solo valida las credenciales, sino que puede responder con atributos adicionales, como la VLAN a la que debe asignarse el dispositivo. El *switch* o punto de acceso interpreta esta respuesta y aplica la configuración correspondiente. De este modo, es posible segmentar la red automáticamente según el perfil del usuario autenticado.

Esta funcionalidad permite, por ejemplo, separar el tráfico de empleados del de invitados, restringir el acceso a ciertos servidores o servicios internos según los privilegios del usuario, o bien aplicar filtros de contenido y limitaciones de ancho de banda adaptadas al rol de cada dispositivo en la red.

Para implementar este tipo de políticas, se requieren *switches* o puntos de acceso compatibles con 802.1X, como los que ofrecen soluciones basadas en OpenWRT, DD-WRT, pfSense, MikroTik o Unifi. Asimismo, es necesario contar con un servidor RADIUS como FreeRADIUS, que permite definir reglas complejas basadas en atributos como la dirección MAC, el grupo LDAP al que pertenece el usuario o el tipo de dispositivo.

VLAN dinámicas

Las VLAN dinámicas permiten asignar de forma automática a cada usuario una red virtual específica una vez completado el proceso de autenticación mediante 802.1X. Esta asignación es gestionada por el servidor RADIUS, que envía atributos al switch o punto de acceso para indicar la VLAN correspondiente según el perfil del usuario.

Por ejemplo, es posible configurar que los usuarios administrativos sean asignados a la VLAN 10, mientras que los visitantes sean redirigidos a la VLAN 99. Esta segmentación mejora la seguridad y permite aplicar políticas diferenciadas de acceso, monitoreo o priorización de tráfico.

Entre los atributos más comunes utilizados por el servidor RADIUS para este fin se encuentran *Tunnel-Type* (por ejemplo, VLAN), *Tunnel-Medium-Type* (como IEEE-802) y *Tunnel-Private-Group-ID*, que indica el identificador numérico de la VLAN a aplicar.

Para que este mecanismo funcione correctamente, es necesario que los switches o puntos de acceso utilizados soporten VLAN dinámicas, como es el caso de dispositivos de fabricantes como Cisco, Aruba o MikroTik. Además, se requiere una configuración adecuada del servidor RADIUS, donde se definan correctamente los atributos y condiciones para cada perfil de usuario.

1.4. *Troubleshooting* y registros

La implementación de 802.1X puede presentar dificultades si no se cuenta con mecanismos adecuados para la supervisión y el diagnóstico. La disponibilidad de registros detallados resulta fundamental para identificar y resolver problemas en el proceso de autenticación.

En el caso de FreeRADIUS, los registros suelen ubicarse en */var/log/freeradius/radius.log*. Para obtener mayor visibilidad, se recomienda activar el modo de depuración desde el archivo de

configuración *radiusd.conf* o dentro de la carpeta *mods-enabled/logging*. También es posible iniciar el servidor en modo de depuración con el comando **radiusd -X**, lo que permite observar en tiempo real cada paso del proceso de autenticación.

Además, se pueden utilizar herramientas como *tcpdump* o Wireshark para capturar e inspeccionar el intercambio EAP y TLS, lo que facilita el análisis de errores en la negociación de credenciales. Para probar la conectividad con el servidor RADIUS, comandos como *radtest* o herramientas gráficas como NTRadPing son útiles para validar usuarios y atributos.

En sistemas Windows que utilizan NPS como servidor RADIUS, los registros relevantes se encuentran en el visor de eventos, dentro de la categoría «Seguridad». Para facilitar la revisión y correlación de incidentes, se pueden integrar herramientas de análisis de registros como Logwatch, Graylog o Wazuh, especialmente si se cuenta con una solución SIEM en el entorno.

Entre los problemas más frecuentes en la autenticación 802.1X se destacan los certificados expirados, errores en la configuración del suplicante, desincronización horaria entre dispositivos (es recomendable utilizar NTP), y errores en la asignación de VLAN o en los atributos enviados por el servidor RADIUS.

Tabla 3. Problemas comunes en la autenticación 802.1X y sus posibles causas

Problema	Posible causa
Timeout del cliente	AP no reenvía correctamente EAP
Fallo TLS	Certificado no confiable o expirado
Rechazo en servidor	Credenciales inválidas o política errónea
VLAN incorrecta	Atributos mal definidos en RADIUS

Fuente: elaboración propia

Actividad práctica complementaria: implementación de autenticación 802.1X con EAP-TTLS

Esta actividad propone configurar una red wifi corporativa segura mediante autenticación 802.1X con EAP-TTLS, utilizando FreeRADIUS como servidor de autenticación. El objetivo es simular un entorno empresarial básico y comprobar el funcionamiento del proceso de autenticación en una red inalámbrica.

Objetivo: configurar una red wifi corporativa en un entorno de laboratorio virtual, utilizando FreeRADIUS y EAP-TTLS como método de autenticación.

Entorno sugerido:

- Una máquina virtual con Ubuntu Server donde se instalará FreeRADIUS.
- Una máquina cliente con Linux o Windows.
- Un punto de acceso virtual utilizando *hostapd* o un dispositivo físico compatible con WPA2-Enterprise.

Pasos sugeridos:

1. Instalar una autoridad certificadora (CA) y emitir los certificados para el servidor y el cliente. Instalar FreeRADIUS con el comando sudo apt install freeradius.
2. Configurar FreeRADIUS para usar EAP-TTLS.
3. Generar el certificado para el servidor.
4. Crear un usuario de prueba en el archivo */etc/freeradius/3.0/users*, por ejemplo, *juan Cleartext-Password := "clave123"*.

5. Configurar el punto de acceso para usar WPA2-Enterprise y conectar con el servidor RADIUS.

6. Activar el método EAP-TTLS en el archivo *mods-enabled/eap*.

7. En el cliente Linux, configurar *wpa_supplicant* con los parámetros adecuados; en Windows, instalar el certificado del cliente y configurar manualmente el método de autenticación en el panel de red.

8. Verificar la conexión del cliente y validar el proceso de autenticación revisando los registros del servidor RADIUS.

9. Utilizar Wireshark para observar el *handshake* TLS y el intercambio EAP.

Como alternativa, se puede implementar este entorno en VirtualBox utilizando pfSense con el paquete FreeRADIUS, lo que ofrece una interfaz más visual y facilita la persistencia de la configuración.

CONTINUAR

Unidad 2. Wifi WPA3 – Enterprise

Introducción

La movilidad en entornos corporativos y residenciales es una práctica cada vez más común, impulsada por los avances continuos en tecnologías inalámbricas, que ofrecen mayores velocidades de conexión, más funcionalidades y costos cada vez más accesibles.

Sin embargo, esta facilidad de conexión sin cables, disponible en cualquier lugar con cobertura, también genera necesidades específicas de seguridad. Las redes wifi están expuestas a diversos riesgos, ya que actores malintencionados pueden utilizar herramientas de análisis de paquetes para capturar el tráfico de red, accediendo potencialmente a información confidencial como credenciales, contraseñas o datos financieros.

Los analizadores de protocolos permiten monitorear y registrar la información transmitida en una red. Algunos atacantes incluso utilizan puntos de acceso falsos, configurados en zonas públicas como cafeterías, para engañar a los usuarios y capturar sus datos personales mediante estos dispositivos.

Esta unidad aborda los mecanismos de defensa disponibles ante las amenazas presentes en redes wifi corporativas, haciendo especial foco en las capacidades de seguridad que ofrece el estándar WPA3-Enterprise.

Los protocolos de redes inalámbricas se basan principalmente en el estándar IEEE 802.11, que define los mecanismos para la comunicación sin cables y las medidas de seguridad asociadas.

La primera generación del estándar 802.11 incorporaba como protocolo de seguridad a WEP (*Wired Equivalent Privacy*), diseñado para ofrecer un nivel de privacidad similar al de las redes cableadas. Sin embargo, se descubrieron múltiples vulnerabilidades en su diseño, especialmente en el algoritmo de cifrado utilizado para codificar los datos transmitidos en redes WLAN.

WEP emplea el algoritmo de cifrado de flujo RC4, junto con un vector de inicialización (IV) de solo 24 bits, lo que genera colisiones frecuentes entre IVs y facilita el criptoanálisis. Uno de los ataques más conocidos fue el ataque de repetición ARP, que redujo considerablemente el tiempo necesario para comprometer la red. Herramientas como *Aircrack-ng* se popularizaron por su capacidad para explotar estas debilidades y descifrar claves WEP.

Posteriormente, se desarrollaron métodos más eficientes como el ataque Pyshkin–Tews–Weinmann (PTW), que disminuyó la cantidad de paquetes necesarios para romper una clave WEP a entre 20 000 y 50 000. Con la ayuda de ataques de repetición ARP, este proceso podía completarse en menos de un minuto.

El acceso protegido wifi (WPA) fue introducido como una solución intermedia para mitigar las vulnerabilidades de WEP. Aunque representa un método de autenticación más robusto, su nivel de seguridad depende en gran medida de la calidad de la contraseña utilizada, ya que contraseñas débiles pueden ser comprometidas mediante ataques de diccionario.

WPA2 mejoró significativamente este esquema al incorporar el estándar de cifrado avanzado (AES) y el protocolo de código de autenticación de mensajes en modo contador (CCMP), que proporciona integridad de los mensajes. Estas mejoras colocaron a WPA2 por encima de sus predecesores en términos de protección criptográfica.

Posteriormente, WPA3, presentado en 2018, introdujo mecanismos de seguridad más avanzados. En el modo personal, implementa cifrado de 128 bits, mientras que en el modo empresarial alcanza los 192 bits. Además de mejorar la resistencia frente a ataques de fuerza bruta, WPA3 incorpora funciones como autenticación simultánea de iguales (SAE), que reemplaza el intercambio de claves precompartidas por un proceso más seguro.

En el ámbito de la seguridad inalámbrica, se utilizan prácticas como la difusión del identificador de conjunto de servicios (SSID), que permite que el nombre de la red sea visible para los dispositivos cercanos, y el filtrado por dirección MAC, que restringe el acceso a la red

según la dirección de hardware del dispositivo. Sin embargo, estas medidas proporcionan una protección limitada, ya que los SSID pueden extraerse fácilmente del tráfico de red y las direcciones MAC pueden falsificarse sin dificultad.

Así, la seguridad wifi ha evolucionado considerablemente desde sus primeras versiones hasta los estándares actuales.

Tabla 4. Estado actual de los principales protocolos de seguridad wifi

Protocolo	Seguridad	Estado actual
WEP	Muy débil	Roto, no debe usarse
WPA	Medio	Inseguro ante ataques modernos
WPA2-PSK	Fuerte	Seguro si usa contraseñas robustas

Fuente: elaboración propia

2.1. Diseño de SSID y segmentación

La seguridad es uno de los aspectos más relevantes al tratar redes inalámbricas. Desde su aparición, se han desarrollado distintos protocolos orientados a proteger las comunicaciones, aunque con resultados limitados en las primeras generaciones.

Por esta razón, es fundamental seguir una serie de parámetros que permitan asegurar y controlar el acceso a la red de forma efectiva. Tras la publicación de los primeros estándares que dieron origen a las redes *Wireless Ethernet* (IEEE 802.11a y 802.11b), también conocidas como wifi por el consorcio encargado de su interoperabilidad, surgió la necesidad inmediata de definir mecanismos de seguridad que protegieran las transmisiones frente a accesos no autorizados. Como respuesta inicial, se diseñó el protocolo WEP (*Wired Equivalent Privacy*), que ofrecía tres mecanismos básicos de protección:

- control por nombre de red (SSID);
- clave compartida estática;
- autenticación por dirección MAC.

En principio, se recomendaba utilizar estos mecanismos de forma combinada para reforzar la seguridad. Sin embargo, pronto se descubrió que podían ser vulnerados fácilmente en poco tiempo mediante herramientas de análisis de tráfico (*sniffers*), incluso por usuarios con conocimientos técnicos limitados.

Para mitigar esta debilidad, comenzaron a desarrollarse soluciones no estandarizadas que abordaban el problema desde distintas áreas, enfocándose tanto en la mejora del cifrado como en nuevas formas de autenticación y control de acceso.

El diseño de SSID (*service set identifier*) en entornos empresariales resulta clave para garantizar un acceso seguro y ordenado a la red inalámbrica. A continuación, se detallan algunas buenas prácticas aplicables a redes wifi empresariales:

- **Separar por perfil de usuario o función**. Por ejemplo, crear un SSID para empleados, otro para invitados y otro para dispositivos *IoT*. Esto permite aplicar políticas diferenciadas según el tipo de conexión.
- **Usar nombres descriptivos, pero sin revelar información sensible**: por ejemplo, «Empresa-Staff» es un nombre adecuado, mientras que «Contabilidad-RedWiFi» puede representar un riesgo desde el punto de vista de la ingeniería social.
- **VLAN por SSID**: asociar cada SSID a una VLAN distinta permite segmentar el tráfico de red y aplicar políticas específicas según el grupo o función del usuario conectado.

- **Limitar la cantidad de SSID activos simultáneamente**: mantener demasiados SSID en emisión simultánea incrementa la interferencia en el espectro radioeléctrico y puede degradar el rendimiento general de la red.

Otras soluciones que pueden implementarse para reforzar la seguridad en redes wifi incluyen las siguientes:

- **Autenticación por dirección MAC**: consiste en configurar el punto de acceso con una lista de direcciones MAC autorizadas, permitiendo únicamente la conexión de dispositivos que coincidan con dicha lista. Aunque este método puede ser vulnerado mediante suplantación de direcciones, requiere conocimientos técnicos avanzados. Esta medida contribuye a reforzar los mecanismos de autenticación y control de acceso.

- **Protección mediante *firewall***: algunos sistemas permiten identificar intentos de ataque, como la propagación de *malware*, y ordenar al punto de acceso la desconexión inmediata del dispositivo atacante. El *firewall* actúa como un filtro activo que supervisa y bloquea actividades sospechosas.

- **Uso de NAC (network access control)**: estos sistemas no solo validan la identidad del usuario, sino también el cumplimiento de políticas de seguridad por parte del dispositivo desde el cual se realiza la conexión. Si un equipo autorizado no cumple los requisitos definidos por la organización, puede denegarse el acceso, incluso si las credenciales del usuario son válidas.

- **Implementación de una red privada virtual (VPN)**: una VPN permite extender la red local sobre una red pública, como Internet, asegurando que solo usuarios y dispositivos autorizados puedan establecer conexión y acceder a los recursos internos. Además de controlar el acceso, protege la integridad y confidencialidad de la información transmitida. Para ello, emplea funciones *hash* como MD2, MD5 o SHA, y algoritmos de cifrado como DES, triple DES (3DES) o AES.

Herramientas útiles

Para implementar y gestionar estas soluciones, pueden utilizarse plataformas como Ubiquiti UniFi Controller, pfSense con el módulo de portal cautivo, o las controladoras TP-Link Omada, que ofrecen versiones gratuitas adecuadas para redes pequeñas.

2.2. Políticas de potencia y cobertura

El control de la potencia de emisión de los puntos de acceso (AP) influye directamente en la seguridad, la cobertura y el rendimiento de la red inalámbrica. A continuación, se detallan algunas consideraciones clave:

- **Evitar la sobrecobertura**. Una señal excesivamente potente puede atravesar muros y extenderse más allá del perímetro físico deseado, lo que incrementa el riesgo de accesos no autorizados desde el exterior.

- **Mitigar zonas muertas**: el uso de herramientas como Ekahau HeatMapper (versión gratuita con funciones limitadas) o NetSpot permite generar mapas de calor para detectar áreas sin cobertura y ajustar la distribución o potencia de los AP.

- **Balanceo de carga**: la configuración de umbrales de RSSI (received signal strength indicator) ayuda a que los dispositivos se conecten automáticamente al punto de acceso más cercano, mejorando la distribución de la carga entre los AP disponibles.

- **Práctica recomendada**: aplicar niveles de potencia más bajos en los SSID corporativos, de modo que la red solo sea accesible desde el interior del edificio o del área autorizada

2.3 Amenazas comunes y mitigación

Las redes inalámbricas están expuestas a distintos tipos de ataques, incluso cuando se implementan estándares modernos como WPA3-Enterprise. A continuación, se describe uno de los ataques más frecuentes y las estrategias recomendadas para mitigarlo.

- ***Evil twin* AP**

Un *evil twin* es un tipo particular de punto de acceso falso (*rogue AP*) en el que un atacante crea un AP malicioso que replica el mismo nombre de red (SSID) y las configuraciones de seguridad de una red legítima. El objetivo es engañar a los dispositivos para que se conecten automáticamente a este AP falso, al reconocer un nombre familiar y no distinguirlo del original.

En la práctica, un ataque *evil twin* se desarrolla en varias etapas:

- **Reconocimiento**. El atacante escanea el entorno para identificar redes wifi activas, utilizando herramientas como airodump-ng o Kismet, a fin de obtener el SSID, canal y dirección MAC del AP objetivo.
- **Configuración del AP falso**: una vez recopilada la información, se levanta un punto de acceso falso usando herramientas como hostapd, airbase-ng o dispositivos especializados como Wi-Fi Pineapple. El atacante puede incluso clonar la dirección MAC del AP legítimo, lo que dificulta aún más su detección.

- **Atracción de clientes**: para lograr que los dispositivos se conecten al AP falso, el atacante puede aumentar la potencia de la señal o enviar tramas de desautenticación al AP original (ver tema 4.2.), forzando así la desconexión temporal de los clientes. Muchos dispositivos intentan reconectarse automáticamente al SSID conocido, eligiendo la señal más fuerte, lo que los lleva a vincularse con el AP malicioso.
- **Intercepción y manipulación del tráfico**: una vez conectados al AP falso, el tráfico de los dispositivos pasa a través del atacante. Con herramientas como Bettercap, Wireshark o mitmproxy, es posible capturar credenciales, realizar inspección profunda de paquetes o inyectar contenido malicioso. En algunos casos, el atacante puede presentar un portal cautivo falsificado para robar contraseñas u obtener otros datos sensibles.

Este tipo de ataques puede prevenirse mediante el uso de EAP-TLS como método de autenticación, que permite validar la identidad del servidor mediante certificados digitales. De esta forma, aunque un dispositivo detecte un SSID conocido, la conexión no se completará si el servidor RADIUS no presenta un certificado válido y confiable, lo que impide el establecimiento de sesiones con puntos de acceso no autorizados.

- **Ataques de desautenticación (DoS)**

Los ataques de desautenticación explotan las tramas de gestión definidas por el estándar IEEE 802.11, particularmente las tramas *disassociation* y *deauthentication*, que se utilizan legítimamente para finalizar conexiones wifi. Sin embargo, en versiones anteriores al estándar WPA3, estas tramas no están cifradas ni autenticadas, lo que permite que un atacante las falsifique y las envíe simulando ser el punto de acceso o el cliente.

Al recibir una trama de desautenticación, el dispositivo de la víctima no puede verificar su origen ni rechazarla, por lo que finaliza inmediatamente la conexión. De esta forma, un atacante puede interrumpir de forma continua la conectividad wifi de uno o varios usuarios, generando una denegación de servicio (DoS). Este tipo de ataque puede repetirse en bucle, impidiendo la navegación e impactando directamente en la disponibilidad del servicio.

Herramientas como *aireplay-ng*, incluida en la suite *aircrack-ng*, permiten ejecutar este ataque fácilmente. Por ejemplo, el siguiente comando envía 20 tramas falsificadas de desautenticación a un cliente específico:

aireplay-ng --deauth 20 -a <BSSID> -c <MAC_cliente>

También existen herramientas como MDK3 que permiten desautenticación continua o la emisión masiva de tramas en un canal determinado, provocando interrupciones generalizadas en la red inalámbrica.

Este tipo de ataque suele combinarse con *evil twin*, ya que al forzar la desconexión del usuario del AP legítimo, se incrementa la probabilidad de que su dispositivo se reconecte automáticamente a un punto de acceso falso gestionado por el atacante.

En contextos más amplios, los ataques de denegación de servicio pueden incluir la degradación deliberada de la señal wifi, la transmisión de *beacons* falsos o técnicas de *jamming*, aunque estas requieren hardware más específico.

Para mitigar estos ataques, WPA3 incorpora de forma obligatoria los *protected management frames* (PMF), definidos en la enmienda IEEE 802.11w. PMF añade un comprobador de integridad (MIC) a las tramas de gestión críticas, como las de desautenticación, lo que permite a los clientes verificar su autenticidad. Si la firma de una trama no es válida, esta se descarta y no provoca desconexión.

En entornos corporativos, se recomienda habilitar PMF en los puntos de acceso compatibles con WPA2 o WPA3, mediante la opción «802.11w Required» o «Capable», según el dispositivo. Esta medida previene eficazmente los ataques de desautenticación ejecutados por terceros.

Adicionalmente, los sistemas de detección y prevención de intrusiones inalámbricas (WIDS/WIPS) permiten identificar patrones sospechosos, como ráfagas de tramas de gestión, y activar respuestas automáticas, como el bloqueo del origen del ataque o la notificación al administrador de red.

- ***Rogue access points***

Los *rogue AP* son dispositivos wifi instalados sin autorización dentro de una red corporativa. Pueden ser colocados por empleados inadvertidamente o por atacantes con acceso físico, con el objetivo de crear un canal alternativo de conexión. Al no estar controlados por la organización, permiten interceptar o manipular el tráfico que pasa a través de ellos, representando una amenaza directa para la confidencialidad y la integridad de la red.

Este riesgo puede mitigarse activando funciones de detección de AP no autorizados en los controladores wifi y realizando escaneos regulares del entorno inalámbrico.

- ***Cracking* de contraseñas**

Este ataque consiste en capturar el *handshake* de una red protegida con WPA2-Personal y aplicar diccionarios o fuerza bruta para obtener la clave. Es efectivo cuando se utilizan contraseñas débiles, ya que el sistema se basa en una clave precompartida (PSK). WPA3 mejora este aspecto mediante el uso de SAE (*simultaneous authentication of equals*), un método más robusto que dificulta el descifrado sin interacción directa con el punto de acceso, reduciendo la eficacia de los ataques pasivos.

- **Ataque de *man in the middle* (MitM) sobre redes inalámbricas**

Cuando un atacante logra posicionarse entre el cliente y la red inalámbrica (por ejemplo, mediante un *evil twin* o *ARP spoofing* en la LAN), puede llevar a cabo un ataque de tipo *man-in-the-middle* (MitM), interceptando el tráfico para robar información sensible o modificar datos en tránsito. Entre las técnicas más comunes utilizadas se encuentran las siguientes:

- **SSLStrip**. Es una técnica donde el atacante fuerza que el cliente use conexiones HTTP en lugar de HTTPS. Por ejemplo, cuando la víctima intenta abrir un sitio web seguro (HTTPS), la herramienta SSLStrip intercepta esa petición, la remite al servidor web real, recibe la respuesta cifrada, pero devuelve al cliente la versión HTTP sin cifrar. La víctima puede no

notar la diferencia (especialmente en sitios sin HSTS) y enviar credenciales en texto. Si un intruso rompe la encriptación de capa de enlace (por ejemplo, tras un ataque KRACK), puede usar SSLStrip para forzar el uso de HTTP por parte del usuario, haciendo que ingrese datos confidenciales en sitios aparentemente seguros. Es importante destacar que hoy muchos sitios usan HSTS o redireccionan permanentemente a HTTPS, lo que dificulta el uso de SSLStrip en escenarios modernos; sin embargo, sigue siendo un vector relevante en redes abiertas o mal configuradas.

- **Ettercap** (*ARP spoofing*). **E**ttercap es una suite reconocida de *man-in-the-middle* que permite envenenar la caché ARP de los dispositivos en la red local. Al ejecutar un ataque de *ARP poisoning*, el atacante engaña tanto al cliente como al router, haciéndoles creer mutuamente que la dirección MAC del otro es suya. Así, el atacante recibe todo el tráfico entre ellos. Ettercap puede operar en modo texto o gráfico, y permite capturar conexiones en vivo (HTTP, POP3, etc.), filtrar contenidos al vuelo o inyectar respuestas (por ejemplo, reemplazar imágenes, HTML). Este tipo de ataque requiere que el dispositivo del atacante esté conectado a la misma red local (o que sea el punto de acceso), pero es muy efectivo para robar credenciales sin cifrar, cookies de sesión o incluso inyectar código JavaScript malicioso.
- **DNS *spoofing***. El atacante también puede redirigir el DNS de la víctima hacia servidores falsos para controlar qué sitio se visita. Por ejemplo, en combinación con un punto de acceso falso, se configura un servidor DNS malicioso (con dnsmasq u otras herramientas) que responde a las consultas con direcciones IP falsas. Así, si la víctima intenta acceder a «banco.com», el DNS envenenado la lleva a un servidor controlado por el atacante (clon del banco). Este método suele usarse junto a SSLStrip o falsos portales cautivos: el cliente ve lo que parece un sitio legítimo, pero está expuesto. Muchos kits de *pentesting* incluyen *plugins* de Ettercap o herramientas como Mitmproxy que facilitan la suplantación DNS dentro de la LAN.

En conjunto, estos ataques muestran que incluso con cifrado robusto en el enlace *wifi*, existe riesgo si el atacante se interpone entre el cliente y el punto de acceso. Por ello, es fundamental utilizar siempre HTTPS con HSTS, validar certificados y mantener a los clientes actualizados. Las herramientas para *man-in-the-middle* (por ejemplo, Ettercap, Mitmproxy, SSLStrip) son de código abierto y abundantes en distribuciones como Kali o Parrot, accesibles para entornos de aprendizaje.

Contramedidas y protección de redes wifi corporativas

La defensa contra los ataques descritos requiere un enfoque integral de seguridad inalámbrica. En entornos corporativos, es esencial migrar a estándares modernos y aplicar buenas prácticas:

- **WPA3 y WPA2-Enterprise (802.1X)**. Se recomienda usar WPA3 en todos los puntos de acceso si el hardware lo permite. WPA3 introduce mejoras importantes: autenticación *SAE* (reemplaza el intercambio *PSK*) y cifrado individualizado en redes abiertas (*OWE*), lo cual reduce drásticamente los ataques de diccionario y protege la privacidad incluso en *SSID* abiertos. Cuando no sea viable WPA3, debe emplearse WPA2-Enterprise con 802.1X/*EAP* y RADIUS, de modo que cada usuario se autentique con credenciales o certificados personales. Esto elimina el uso de contraseñas compartidas y dificulta que un atacante, incluso con un *evil twin*, descifre las comunicaciones *wifi*. Además, se recomienda integrar la infraestructura inalámbrica con gestión centralizada (Cisco ISE, Aruba ClearPass, Microsoft NPS, etc.) para reforzar las políticas de acceso y auditoría.
- **Protected Management Frames (802.11w)**. Como se describió anteriormente, habilitar PMF protege contra ataques de desautenticación y desasociación. En la configuración de red, se debe activar 802.11w en «Required» o «Capable» en los controladores de los puntos de acceso corporativos (obligatorio en WPA3). Así se asegura la integridad de las tramas de gestión críticas y se mitiga el riesgo de denegación de servicio a nivel *wifi*.
- **Seguridad física y segmentación**. Limitar el rango de transmisión del *wifi* (antenas direccionables, potencia mínima necesaria) reduce la posibilidad de ataques desde fuera del edificio. Segmentar la red inalámbrica mediante VLAN o *SSID* separados (por ejemplo, «corporativo», «invitados», «IoT») limita el impacto de una violación. Según buenas prácticas, si un ataque compromete un segmento, las VLAN impiden que el atacante acceda a toda la red. También es importante aplicar control físico (no permitir puntos de acceso no autorizados en las instalaciones) y usar filtrado de MAC para acceso inicial (aunque la dirección MAC puede falsificarse, añade una capa básica).
- **Sistemas de detección y monitoreo**. Implementar un IDS/WIDS (*Intrusion Detection System* para *wifi*) es fundamental. Estos sistemas escanean continuamente el espectro radioeléctrico en busca de puntos de acceso no registrados o comportamientos anómalos. Notifican automáticamente al equipo de seguridad ante *SSID* o *BSSID* desconocidos y pueden bloquear o aislar dichos dispositivos en tiempo real. Adicionalmente, soluciones de NAC (*Network Access Control*) y EMM/MDM en los dispositivos finales pueden detectar cuando un equipo intenta conectarse a un *SSID* no autorizado. El monitoreo constante y las actualizaciones frecuentes del firmware de los puntos de acceso garantizan que las contramedidas más recientes estén activas.

- **Políticas y capacitación**. A nivel organizacional, se deben dictar políticas estrictas: prohibir el uso de routers personales o *hotspots* inseguros en oficinas, exigir autenticación multifactor para acceder a recursos sensibles y capacitar a los usuarios sobre los riesgos del *wifi* público. Tal como indican las recomendaciones de seguridad, la concienciación evita que los empleados se conecten inadvertidamente a redes maliciosas.

En resumen, la seguridad *wifi* corporativa se basa en una combinación de estándares robustos (WPA3/WPA2-Enterprise), protección de tramas (802.11w), vigilancia activa (WIDS/WIPS) y buenas prácticas (segmentación, actualizaciones) para prevenir ataques como *rogue AP*, *deauth* y *man-in-the-middle*.

Ejemplo práctico

Supongamos un café con *wifi* gratuito llamado «Café_Público». Un atacante configura un punto de acceso con *SSID* «Café_Publico» (sin tilde) y una señal más intensa. Los clientes, al reconectarse, ven ambas redes («Café_Público» y «Café_Publico») y suelen elegir la señal más fuerte, que en este caso es la falsa. Una vez conectados, ingresan sus credenciales en un portal falso creado por el atacante, entregándoselas sin saberlo.

Herramientas de análisis

Para observar el tráfico y detectar comportamientos anómalos en redes inalámbricas, se pueden utilizar herramientas como **Wireshark**, **Kismet**, **Acrylic WiFi Home** o **Aircrack-ng**. Estas aplicaciones permiten analizar paquetes, identificar intentos de suplantación, evaluar la intensidad de señal y llevar a cabo pruebas de seguridad controladas en entornos de laboratorio.

2.4. Integración con RADIUS/LDAP

Para lograr una autenticación segura y centralizada en redes WPA3-Enterprise, es habitual integrar la infraestructura inalámbrica con servidores **RADIUS** y/o **LDAP**.

RADIUS (*Remote Authentication Dial-In User Service*) es un protocolo que permite centralizar los procesos de autenticación, autorización y auditoría (*AAA*) de accesos a la red. Su implementación es fundamental en entornos corporativos, ya que permite validar las

credenciales de los usuarios desde un servidor central, aplicar políticas de acceso y registrar la actividad.

LDAP (*Lightweight Directory Access Protocol*) provee una base de datos jerárquica de usuarios y dispositivos contra la cual puede autenticarse el cliente. Es común utilizarlo como repositorio de identidades, mientras que **RADIUS** actúa como intermediario entre el punto de acceso y el directorio.

En grandes organizaciones, un servidor **AAA** basado en **RADIUS** se integra con el protocolo 802.1X para gestionar el acceso a la red *wifi*. Esta solución permite abordar de forma eficaz los desafíos de seguridad vinculados con la confidencialidad, autenticación, integridad y control de acceso en redes inalámbricas.

RADIUS (remote authentication dial-in user service)

La tecnología inalámbrica *wifi* comenzó a consolidarse en 1999 con el estándar **IEEE 802.11b**, cuando los dispositivos eran compatibles únicamente con el cifrado **WEP**, basado en el algoritmo **RC4**. Sin embargo, este sistema resultó rápidamente vulnerable, ya que las claves podían ser descifradas con facilidad.

La necesidad de mejorar la seguridad dio lugar al desarrollo de **WPA**, que aunque más robusto que **WEP**, heredó varios de sus defectos. Posteriormente surgió **WPA2**, basado en el estándar **802.11i**, que incorporó mejoras importantes en los mecanismos de cifrado. En ambos casos, existen dos modos principales de operación:

- **WPA-PSK / WPA2-PSK** (*pre-shared key*). Utilizan una clave precompartida entre los usuarios.
- **WPA-Enterprise / WPA2-Enterprise**: utilizan autenticación dinámica mediante servidores externos, como **RADIUS.**

Respecto al cifrado, se puede optar entre estas opciones:

- **TKIP** (*temporal key integrity protocol*). Considerado inseguro, especialmente cuando se combina con *QoS*.

- **AES** (*advanced encryption standard*): un algoritmo mucho más seguro y recomendado.

Cuando se utiliza una clave precompartida (PSK), es posible que un atacante capture el tráfico durante el proceso de autenticación y obtenga el *handshake*. Esto permite intentar descifrar la clave mediante ataques de diccionario, una vulnerabilidad común en redes personales o mal configuradas. En cambio, al utilizar un servidor RADIUS, las claves se generan dinámicamente para cada sesión, lo que impide este tipo de ataques y mejora significativamente la seguridad de la red.

Servidor RADIUS en WPA-Enterprise / WPA2-Enterprise

En este tipo de configuración, se dispone de una máquina conectada por cable al punto de acceso, que reenvía las peticiones de autenticación al servidor RADIUS, normalmente a través de los puertos UDP 1812 (autenticación) y 1813 (contabilidad).

Los servidores RADIUS también se utilizan, por ejemplo, cuando un proveedor de servicios de Internet desea validar las credenciales de un abonado.

Sin embargo, un inconveniente frecuente en este tipo de configuraciones inalámbricas es la compatibilidad limitada con ciertos dispositivos multimedia, como consolas PlayStation 3, Xbox 360, servidores NAS, o equipos como BlackBerry. Estos dispositivos, al estar orientados a un uso doméstico, muchas veces no incluyen soporte para autenticación con certificados, ya sea por decisión del fabricante o por limitaciones técnicas. Esto no suele ser un problema en dispositivos actuales como los basados en Android o iOS, que sí soportan autenticación 802.1X.

Para estos casos existen alternativas:

- Conectar el dispositivo por cable a otro equipo que sí pueda autenticarse con un servidor **RADIUS** y compartir la conexión.

- Configurar un segundo *SSID* con **WPA-PSK**, de modo que coexistan redes separadas: una con autenticación personal para dispositivos sin soporte y otra con autenticación empresarial para los equipos compatibles.

La norma IEEE 802.1X emplea el protocolo *eap* (*extensible authentication protocol*), originalmente diseñado para conexiones *PPP* y luego adaptado para redes locales, bajo el nombre *eapol* (*eap over LAN*). En este esquema, el punto de acceso actúa como intermediario transparente, simplemente reenviando y encapsulando los paquetes hacia el servidor RADIUS.

Soluciones gratuitas recomendadas

Entre las soluciones gratuitas más utilizadas se encuentran **FreeRADIUS**, ampliamente adoptado en entornos empresariales por su soporte de métodos como *eap-tls* y *eap-ttls*, y su capacidad de integrarse con sistemas de autenticación existentes como **Active Directory** o **LDAP**. Complementariamente, **OpenLDAP** puede emplearse como backend para **FreeRADIUS**, proporcionando una base de datos estructurada de usuarios que facilita la gestión de identidades.

Ejemplo de flujo

Un ejemplo típico de flujo en una red WPA3-Enterprise comienza cuando el cliente *wifi* inicia el proceso de conexión. El controlador de red reenvía las credenciales al servidor **RADIUS**, que a su vez consulta a un directorio como **LDAP** o **Active Directory** para verificar si el usuario está autorizado. Si la autenticación es exitosa, se concede el acceso, normalmente asignando una VLAN dinámica según el perfil del usuario, y se registra el evento para fines de auditoría.

Actividades prácticas complementarias

A continuación, se proponen algunas actividades para reforzar los conceptos trabajados sobre seguridad en redes inalámbricas.

- **Diseño de red *wifi* segura**: crear un plan de segmentación para una empresa ficticia de 50 empleados, definiendo SSID, VLAN y políticas de acceso diferenciadas para personal interno, visitantes y dispositivos *IoT*.

- **Simulación de autenticación con FreeRADIUS (entorno virtual)**: instalar un servidor **FreeRADIUS** en una máquina virtual con **Linux** y configurarlo para autenticar a dos usuarios distintos mediante *eap-ttls*. Verificar los registros de acceso generados.

- **Mitigación de ataques en redes inalámbricas**: utilizar herramientas como **Kismet** o **Wireshark** para detectar puntos de acceso sospechosos en un entorno de pruebas, y aplicar PMF en un punto de acceso compatible como medida de protección.

Caso práctico

Contexto

En una oficina pequeña de tipo pyme con red *wifi* propia, varios empleados reportan desconexiones intermitentes y pérdida de datos confidenciales. Se sospecha de un ataque localizado.

Desarrollo

Después de inspeccionar la red, se observa que un intruso ha estacionado un vehículo cerca del edificio con un dispositivo portátil de hacking. El atacante llevó a cabo los siguientes ataques combinados: primero, usando «aireplay-ng», envió tramas de desautenticación al punto de acceso legítimo, provocando que varios empleados se desconectaran. Al caer sus conexiones, algunos dispositivos automáticos intentaron reconectarse y acabaron uniéndose a un *evil twin* que el atacante había configurado con el mismo SSID corporativo y señal más fuerte. En ese punto de acceso falso, se ejecutaba un servidor DNS malicioso: cuando las

víctimas intentaban abrir aplicaciones bancarias o corporativas, eran redirigidas a páginas falsas para capturar sus credenciales (*DNS spoofing* + *captive portal*). Además, mediante «sslstrip», las conexiones *https* se transformaban en *http*, exponiendo los datos. En conjunto, el atacante logró obtener *tokens* de acceso y correos electrónicos sin cifrar.

Resolución propuesta

Para contrarrestar el ataque detectado, los analistas siguen una serie de pasos basados en buenas prácticas de ciberseguridad:

- **Identificar puntos de acceso falsos.** Al activar un sistema **WIDS** local, se detecta rápidamente el punto de acceso malicioso al observar que proviene de un fabricante no reconocido y tiene la misma dirección **MAC** que un AP legítimo, aunque clonada. Esta comprobación permite aislar y marcar el dispositivo no autorizado.

- **Aplicar PMF (802.11w).** Se configura el router corporativo para exigir **PMF** en modo «Required». De esta forma, los ataques de desautenticación dejan de surtir efecto, ya que las tramas falsificadas carecen de la firma de integridad válida que exige el estándar.

- **Rotar credenciales y habilitar 802.1x.** Se anulan todas las contraseñas **PSK** de la red y se migra a **WPA2-Enterprise** con **RADIUS/EAP-TLS**. Este esquema obliga a que solo los dispositivos con credenciales y certificados válidos puedan autenticarse, lo que impide que un *evil twin* simple acepte nuevas conexiones de clientes.

- **Monitorear actividad DNS y HTTPS.** Se instalan reglas de **IDS** para detectar respuestas DNS que redirijan a dominios no

oficiales o no autorizados. Los administradores verifican además que todo el tráfico sensible esté cifrado mediante **HTTPS**; para servicios internos, se bloquea cualquier intento de comunicación en texto plano (*http*) en puertos de aplicación segura.

- **Segmentación de red.** Los sistemas y servicios de mayor criticidad se colocan en una **VLAN** aislada, de modo que, incluso si se logra establecer una conexión *rogue*, la intrusión queda contenida en un segmento restringido de la red y no puede propagarse fácilmente.

En conclusión, en este caso integrador se combinaron ataques de desautenticación (*deauth*), puntos de acceso no autorizados (*rogue AP*, como *evil twin*) y ataques tipo *man-in-the-middle* (*DNS spoofing* y SSLStrip). Su mitigación requirió habilitar **PMF**, fortalecer la autenticación inalámbrica, aplicar cifrado de extremo a extremo y desplegar sistemas de detección como **WIDS**. El ejercicio demuestra la importancia de implementar contramedidas en capas: herramientas preventivas (802.11w, WPA3 y 802.1x), junto con prácticas de monitoreo y respuesta coordinada, reducen significativamente el riesgo.

Preguntas de repaso

A continuación, se presentan una serie de preguntas orientadas a repasar, consolidar e internalizar los conceptos abordados. Cada una incluye una pauta orientadora que permite al estudiante desarrollar su propia respuesta a partir de los contenidos trabajados.

Esta dinámica tiene como finalidad favorecer la apropiación de los aprendizajes teórico-prácticos desarrollados a lo largo del módulo, promoviendo la reflexión, el análisis y la autoevaluación. La propuesta no requiere entrega obligatoria ni calificación, y se plantea como una estrategia formativa destinada a que el alumnado pueda afianzar y poner a prueba su nivel de comprensión.

- ¿Qué ventaja ofrece WPA3 sobre WPA2 respecto al *handshake* inicial?
  Pista: SAE (*simultaneous authentication of equals*) evita ataques de diccionario *offline*.

- ¿Qué herramienta se usa para ofrecer autenticación centralizada vía RADIUS?
  Pista: FreeRADIUS.

- ¿Cuál es la función de PMF en WPA3?
  Pista: proteger los marcos de administración y evitar ataques de desautenticación.

- ¿Qué es un suplicante en 802.1X?
  Pista: el cliente que solicita autenticación a través del protocolo EAP.

- ¿Cómo ayuda la segmentación por SSID y VLAN en una red inalámbrica?
  Pista: permite aplicar políticas diferenciadas de seguridad y control de acceso.

CONTINUAR

Referencias

Cano, H. y Salgado, D. (2016). *Estudio de esquemas de seguridad en redes inalámbricas: aplicación de buenas prácticas en pymes y usuarios finales.* http://bibliotecadigital.usbcali.edu.co/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf

Referencias bibliográficas de consulta

Avast. (2023). *¿Qué es un ataque de gemelo malvado y cómo actúa?* https://www.avast.com/es-es/c-evil-twin-attack

Bitdefender. (s. f.). *Evil twin attacks.* https://www.bitdefender.com/en-us/business/infozone/what-is-evil-twin-attack

Cloudflare. (s. f.). *¿Qué es un ataque KRACK? | Cómo protegerse contra los ataques KRACK.* https://www.cloudflare.com/es-es/learning/security/what-is-a-krack-attack/

Ettercap Project. (s. f.). *Ettercap.* https://www.ettercap-project.org/

InfoProtección. (s. f.). *Seguridad en redes inalámbricas empresariales: WPA3, autenticación 802.1X y amenazas avanzadas.* https://www.infoproteccion.com/ciberseguridad/seguridad-redes-inalambricas-empresariales/

LabEx. (s. f.). *Comprender los marcos de gestión protegidos como defensa.* https://labex.io/es/tutorials/kali-understand-protected-management-frames-as-a-defense-594484

Minery Report. (s. f.). *Ataque de desautenticación*. https://mineryreport.com/ciberseguridad/glosario/tipos-de-amenazas/termino/ataque-desautenticacion/

Splashtop (Foxpass). (2025). *Combating the evil twin attack with RADIUS*. https://www.splashtop.com/foxpass/blog/evil-twin-attack-lesson

CONTINUAR