U4. Seguridad en redes

Descargar estos apuntes

Índice

> **Introducción**
>
> La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y monitorear el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y de los recursos accesibles a través de ella. Se refiere a cualquier actividad diseñada para proteger la usabilidad e integridad de la red y sus datos. Incluye tecnologías tanto hardware como software.

Protocolos seguros

Los protocolos TCP y UDP sobre IP no utilizan mecanismos de cifrado o autenticación para la transmisión de datos. Por tanto, **los protocolos a nivel de aplicación** que dependen de TCP/IP o UDP/IP, como HTTP, FTP, SMTP, POP, DNS, DHCP, TELNET, etc., **no garantizan ni la confidencialidad ni la integridad**. Esto puede llevar, por ejemplo, al envío de contraseñas en texto claro si el protocolo a nivel de aplicación proporciona algún mecanismo de autenticación (como por ejemplo en un formulario web).

Para mejorar la seguridad de las comunicaciones, se han establecido varias extensiones del pila de protocolos TCP/IP estándar :

IPsec (Internet Protocol Security)

Es una **capa adicional sobre la capa IP**, que proporciona comunicaciones seguras a los protocolos de transporte (TCP y UDP). Por tanto, los protocolos a nivel de aplicación pueden operar de manera segura sin aplicar ningún cambio. Se utiliza en redes privadas o redes privadas virtuales.

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Es una **capa adicional sobre TCP**, que proporciona comunicaciones seguras a los protocolos de aplicación.

SSH (Secure Shell)

Es un **protocolo de capa de aplicación** que permite la operación remota de ordenadores y la transferencia de datos mediante comunicación segura. También define una función llamada "port forwarding" que permite el uso de una conexión SSH segura para mensajes correspondientes a otros protocolos a nivel de aplicación. De este modo es posible, por ejemplo, acceder de forma segura a un servidor FTP estándar (inseguro).

IPSec, SSL/TLS o SSH no solo protegen las comunicaciones en redes inalámbricas o a través de Internet, sino que también **se aplican a redes cableadas para evitar la monitorización del tráfico y la captura de datos por parte de terceros**. De este modo, incluso en una LAN, es recomendable cifrar el tráfico entre dispositivos para garantizar la confidencialidad de la información.

> ⚠ **Importante**
>
> Además de implementar protocolos seguros para proteger las comunicaciones, **es fundamental inventariar** y controlar **los servicios de red** que están **activos** en una infraestructura. Cada servicio que se ejecuta sobre TCP/IP representa una posible vulnerabilidad si no se supervisa adecuadamente. Por ello, mantener un registro actualizado de los servicios disponibles, así como aplicar políticas de seguridad específicas (como desactivar los innecesarios o restringir el acceso a ciertos puertos y protocolos), permite reducir las posibilidades de ataque y garantizar que las comunicaciones seguras como SSH, SSL/TLS o IPsec se utilicen de forma efectiva.

Redes de área local inalámbricas (WLAN)

Las redes de área local inalámbricas (**WLAN**) son redes dentro de un área localizada donde los dispositivos se comunican utilizando **señales de radiofrecuencia en lugar de cables físicos**. En las WLAN, múltiples dispositivos comparten una parte del espectro de radiofrecuencia para transmitir datos, lo que permite la conectividad inalámbrica.

Las WLAN ofrecen la **ventaja de la movilidad**, permitiendo a los usuarios conectarse desde cualquier lugar dentro del área de cobertura sin estar atados a una ubicación específica. **Sin embargo**, las WLAN **transmiten datos** por el aire, lo que las hace **susceptibles a ser interceptadas** por cualquier dispositivo dentro del rango. Debido a esta vulnerabilidad, es **esencial** implementar métodos robustos de **cifrado y autenticación**.

Mecanismos de autenticación y cifrado en WLAN

WEP (Wired Equivalent Privacy)

Fue uno de los primeros protocolos de cifrado utilizados para asegurar las WLAN. Opera cifrando los datos transmitidos entre dispositivos usando una clave compartida. Se considera **inseguro** y ya **no se recomienda**.

WPA (Wi-Fi Protected Access)

Reemplazó a WEP. Utiliza un algoritmo de **cifrado** conocido como **TKIP** (Temporal Key Integrity Protocol) para proporcionar mejor protección de datos. También incorpora un método de **autenticación** llamado **WPA-PSK** (Pre-Shared Key) o WPA Personal, que requiere que los usuarios ingresen una contraseña para acceder a la red. Es **susceptible a ataques de fuerza bruta** contra contraseñas débiles.

WPA2 (Wi-Fi Protected Access 2)

Es el **estándar actual** de seguridad. Utiliza el algoritmo de **cifrado AES** (Advanced Encryption Standard), mucho más fuerte y seguro que TKIP. WPA2 también introduce un método robusto de **autenticación** llamado **IEEE 802.1X/EAP** (Extensible Authentication Protocol).

- **WPA3 (Wi-Fi Protected Access 3)**: Introduce nuevas características, incluidos protocolos de **cifrado** más fuertes como **SAE** (Simultaneous Authentication of Equals).

Wi-Fi (Wireless Fidelity)

IEEE 802.11 es un conjunto de estándares que implementan la comunicación en una WLAN. Comúnmente conocido como Wi-Fi, IEEE 802.11 define los métodos para establecer conexiones, transmitir datos y gestionar el tráfico de red, asegurando interoperabilidad y compatibilidad entre dispositivos.

Estándares Wi-Fi comunes hoy en día

- **IEEE 802.11n**: tasas de datos de hasta 600 Mbps.
- **IEEE 802.11ac**: tasas de datos de hasta varios gigabits por segundo.
- **IEEE 802.11ax (Wi-Fi 6)**: tasas de datos de hasta varios gigabits por segundo.

Métodos de autenticación Wi-Fi

Modo abierto

Cualquier dispositivo dentro del radio de alcance **puede conectarse** a la red sin requerir contraseña o autenticación. El cliente inalámbrico envía una solicitud de autenticación al punto de acceso (AP), que acepta sin hacer preguntas. No se necesita clave compartida ni credenciales. Tras la autenticación, el cliente se asocia con el punto de acceso.

Modo con clave

Utiliza una **clave compartida** (PSK - pre-shared key) o contraseña para la autenticación y el cifrado. El proceso de autenticación consiste en cuatro pasos:

1. El cliente envía una solicitud de autenticación al punto de acceso.
2. El punto de acceso envía un texto llamado desafío al cliente.
3. El cliente cifra desafío usando la clave compartida y lo envía de vuelta al punto de acceso.
4. El punto de acceso descifra la respuesta y la verifica. Si la verificación es correcta, la autenticación es exitosa; de lo contrario, devuelve un error.

RADIUS (Remote Authentication Dial-In User Service)

La autenticación de usuarios se centraliza a través de un servidor RADIUS, que almacena las credenciales de los usuarios y maneja las solicitudes de autenticación desde los puntos de acceso Wi-Fi. El proceso de autenticación IEEE 802.1X EAP incluye seis pasos:

1. El cliente envía una solicitud de autenticación y se asocia al punto de acceso.
2. El punto de acceso reenvía la solicitud al servidor RADIUS mientras bloquea todo el tráfico excepto el de autenticación.
3. El servidor RADIUS solicita las credenciales del usuario (por ejemplo, nombre de usuario y contraseña) a través del punto de acceso.
4. El servidor RADIUS verifica las credenciales usando su base de datos o un directorio externo (como LDAP o Active Directory).
5. En base a la verificación, el servidor RADIUS envía un mensaje de aceptación o rechazo al punto de acceso.
6. Si se concede el acceso, el punto de acceso permite que el cliente se conecte y acceda a la red.

Medidas de protección

Además de emplear métodos de cifrado para asegurar una red inalámbrica, se pueden tomar medidas adicionales para mejorar la seguridad en casa:

- Desactivar la difusión del SSID.
- Habilitar el filtrado de direcciones MAC.
- Desactivar el servicio DHCP.
- Desactivar WPS (Wi-Fi Protected Setup).

Cortafuegos

Un **cortafuegos** es un dispositivo de seguridad de red que monitoriza el tráfico entrante y saliente y filtra paquetes basándose en reglas. Puede ser hardware, software, software como servicio (SaaS), nube pública o nube privada (virtual).

Los cortafuegos son herramientas importantes en la seguridad de redes ya que ayudan a proteger los sistemas del acceso no autorizado y del tráfico perjudicial. **Controlan y filtran el flujo de datos entre una red y fuentes externas, mejoran la seguridad bloqueando datos peligrosos y permiten un mejor control sobre la red**.

Ingeniería social y fraudes informáticos

Uno de los mayores riesgos para la seguridad en redes no reside únicamente en las vulnerabilidades técnicas, sino en la manipulación de los usuarios mediante técnicas de **ingeniería social**. Este tipo de amenazas aprovecha la confianza, la desinformación o el descuido de las personas para obtener acceso no autorizado a sistemas, redes o información sensible, afectando directamente la confidencialidad e integridad de los datos.

Aunque la implementación de **protocolos seguros** como SSH, TLS o IPsec, y el uso de **mecanismos de autenticación robustos** en redes inalámbricas, ofrecen una capa importante de protección técnica, estos sistemas pueden verse comprometidos si un atacante logra engañar a un usuario para que revele sus credenciales o desactive medidas de seguridad. De igual forma, **un cortafuegos correctamente configurado** puede ser ineficaz si el acceso es facilitado involuntariamente por el propio usuario.

Entre las técnicas de ingeniería social más comunes se encuentran:

- **Phishing**: mensajes o sitios web falsos que simulan ser entidades legítimas para engañar al usuario y obtener información confidencial.
- **Vishing**: variante del phishing a través de llamadas telefónicas.
- **Smishing**: engaños por medio de mensajes SMS con enlaces maliciosos.
- **Pretexting**: el atacante se hace pasar por una figura de autoridad o una situación creíble para solicitar datos personales.
- **Baiting**: se ofrece un recurso tentador (como una memoria USB aparentemente abandonada) que contiene malware.

Estas prácticas demuestran que, más allá de las herramientas tecnológicas, la **concienciación de los usuarios y la formación en ciberseguridad** son elementos esenciales en cualquier estrategia de protección de redes. Solo mediante la combinación de tecnología, buenas prácticas y vigilancia activa se puede reducir efectivamente la probabilidad de un de ataque.

Publicidad y correo no deseado en redes

Además de las amenazas técnicas y humanas, las redes informáticas también están expuestas a un alto volumen de **tráfico no deseado** generado por **publicidad invasiva, spam y correos electrónicos maliciosos**. Este tipo de tráfico, aunque no siempre implique un ataque directo, puede afectar el rendimiento de la red, saturar los recursos del sistema y **facilitar la entrada de otras amenazas** como el malware. La **minimización del tráfico no deseado** es una medida clave para optimizar la seguridad y eficiencia de la red.

Desde el punto de vista del usuario, es importante adoptar prácticas como:

- No hacer clic en enlaces sospechosos o anuncios emergentes.
- No compartir direcciones de correo en sitios públicos.
- Utilizar navegadores y extensiones que bloqueen scripts de publicidad (adblockers).
- Configurar adecuadamente los filtros de spam en los clientes de correo.

Este tipo de medidas, junto con el uso de **protocolos seguros de comunicación** y una **configuración adecuada de los servicios de red**, ayudan a mantener el entorno más limpio, eficiente y protegido.