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.

1. 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).

2. 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 para implementar comunicación de red de área local inalámbrica (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 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. Luego el cliente se asocia al AP.
- **Modo con clave**: Utiliza una clave compartida (PSK) o frase de paso para autenticación y cifrado. El proceso de autenticación involucra cuatro pasos:
  i. El cliente envía una solicitud de autenticación abierta al AP.
  ii. El AP envía un texto de desafío aleatorio al cliente.
  iii. El cliente cifra el texto de desafío usando la clave compartida y lo envía de vuelta al AP.
  iv. El AP descifra la respuesta y la verifica. Si coincide, la autenticación es exitosa; de lo contrario, falla.
- **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:
  i. El cliente envía una solicitud de autenticación abierta y se asocia al AP.
  ii. El AP reenvía la solicitud al servidor RADIUS mientras bloquea todo el tráfico excepto el de autenticación.
  iii. El servidor RADIUS solicita las credenciales del usuario (por ejemplo, nombre de usuario y contraseña) a través del AP.
  iv. El servidor RADIUS verifica las credenciales usando su base de datos o un directorio externo (como LDAP o Active Directory).
  v. En base a la verificación, el servidor RADIUS envía un mensaje de aceptación o rechazo al AP.

vi. Si se concede el acceso, el AP 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).

---

3. Cortafuegos y proxies

Los cortafuegos y proxies son herramientas importantes en la seguridad de redes 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. Juntos, mejoran la seguridad bloqueando datos peligrosos y permitiendo un mejor control sobre la red.

Cortafuegos (Firewall)

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

Proxy

Un servidor proxy es una aplicación que pasa datos entre un cliente que solicita un recurso y el servidor que lo proporciona. El proxy en sí puede ser un sistema informático o un enrutador, y puede residir en el ordenador local del usuario o en cualquier punto entre el ordenador del usuario y los servidores de destino en Internet.

Los proxies actúan como intermediarios entre los clientes que solicitan un recurso y el servidor que lo proporciona. En lugar de conectarse directamente a un servidor, el cliente dirige la solicitud al servidor proxy, que evalúa la solicitud y realiza la transacción de red requerida. Esto sirve para simplificar o controlar la complejidad de la solicitud, o proporcionar beneficios adicionales como balanceo de carga, privacidad o seguridad.

Un servidor proxy que pasa solicitudes y respuestas sin modificar se llama generalmente "gateway" o, a veces, "proxy de túnel".

- **Proxy directo (Forward Proxy)**: Se usa para recuperar datos desde una amplia gama de fuentes.

- **Proxy inverso (Reverse Proxy)**: Normalmente se usa de forma interna como interfaz para controlar y proteger el acceso a un servidor en una red privada.

Cortafuegos vs Proxy

Característica	Cortafuegos	Proxy
Función principal	Controla el tráfico de red y bloquea conexiones no autorizadas	Intermedia las solicitudes entre clientes y servidores
Nivel de funcionamiento	Red o transporte	Aplicación
Protección contra ataques externos	Sí	Sí
Capa de filtrado	Paquetes, puertos, direcciones IP	Contenido, URLs, aplicaciones