TEMA 6. SEGURIDAD EN REDES CORPORATIVAS

¿Como proteger la red de nuestra empresa de intrusos?, ¿Que tipos de ataques hay y cómo detectarlos?.

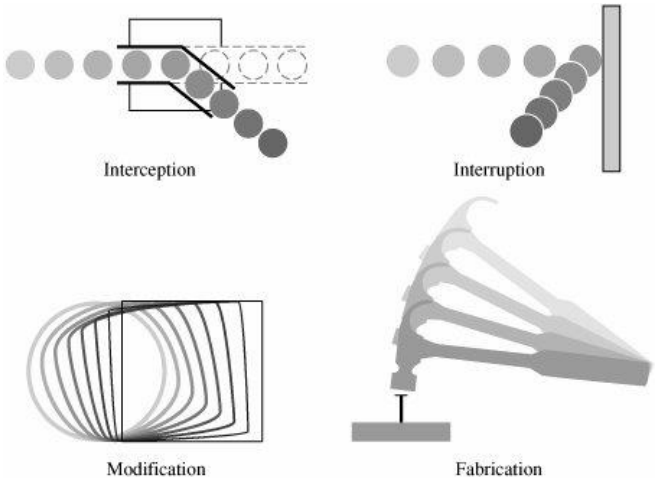
1. Amenazas y ataques

Sin importar si están conectadas por cable o de manera inalámbrica, las redes de ordenadores cada vez son más esenciales para las actividades diarias. Los ataques e intrusiones de personas no autorizadas a través de las redes públicas y privadas cada vez son más frecuentes, y pueden causar interrupciones costosas de servicios críticos y pérdidas de trabajo, información y dinero.

De forma genérica las amenazas en comunicaciones podemos dividirlas en **cuatro grandes grupos**:

- **Interrupción**: un objeto, servicio del sistema o datos en una comunicación se pierden, quedan inutilizables o no disponibles.
- **Interceptación**: un elemento no autorizado consigue un acceso a un determinado objeto.
- **Modificación**: además de conseguir el acceso consigue modificar el objeto, es posible incluso la destrucción una modificación que inutiliza al objeto afectado.
- **Fabricación**: modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "fabricado".

En la figura se muestran estos tipos de ataque de una forma gráfica:

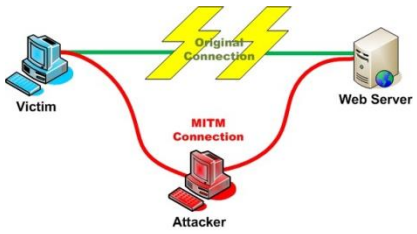


Como ejemplos prácticos de dichas amenazas, encontramos diversas técnicas de ataques informáticos en redes. Algunos son:

- **Ataque de denegación de servicio**: también llamado ataque DoS (Deny of Service), es un caso específico de interrupción de servicio. Causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red

por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Mediante **botnet** o **redes zombi** se pueden llegar a controlar cientos o miles de máquinas para realizar ataques distribuidos de saturación de servidores o DDoS.

- **Sniffing**, es una técnica de interceptación: consiste en rastrear monitorizando el tráfico de una red.
- **Man in the middle**: a veces abreviado MitM, es un caso específico de interceptación y modificación de identidad. Un atacante supervisa una comunicación entre dos partes, falsificando las identidades de los extremos, y por tanto recibiendo el tráfico en los dos sentidos.



- **Spoofing:** es una técnica de fabricación, suplantando la identidad o realizando una copia o falsificación, por ejemplo encontramos falsificaciones de IP, MAC, web o mail.
- **Pharming:** es una técnica de modificación. Mediante la explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, permite modificar las tablas DNS redirigiendo un nombre de dominio (domain name) conocido, a otra máquina (IP) distinta, falsificada y probablemente fraudulenta.

Amenazas internas y externas

Las amenazas de seguridad causadas por intrusos en redes corporativas o privadas de una organización, pueden originarse tanto de forma interna como externa.

- **Amenaza externa o de acceso remoto:** los atacantes son externos a la red privada o interna de una organización, y logran introducirse desde redes públicas. Los objetivos de ataques son servidores y routers accesibles desde el exterior, y que sirven de pasarela de acceso a la redes corporativa.
- **Amenaza interna o corporativa:** los atacantes acceden sin autorización o pertenecen a la red privada de la organización. De esta forma pueden comprometer la seguridad y sobre todo la información y servicios de la organización.

Con estos 2 frentes abiertos, veremos por un lado como defender la seguridad en la red corporativa de forma interna (tema 6), y por otro como disponer de medidas de protección perimetral (tema 7), en los equipos y servicios que están expuestos a redes públicas.

Para protegernos de las posibles amenazas internas algunas propuestas son:

- Realizar un buen **diseño** de **direccionamiento**, **parcelación** y **servicios** de subredes dentro de nuestra red corporativa. Para ello se emplean técnicas como, **subnetting**, **redes locales virtuales** o **VLAN** y creación de **zonas desmilitarizadas** o **DMZ**, aislando y evitando que los usuarios puedan acceder directamente en red local con los sistemas críticos.
- Políticas de **administración** de **direccionamiento estático** para servidores y routers.
- **Monitorización del tráfico de red** y de las asignaciones de direccionamiento dinámico y de sus tablas **ARP**.
- **Modificación** de configuraciones de seguridad y, en especial **contraseñas por defecto** de la administración de servicios.
- En redes inalámbricas emplear **máximo nivel de seguridad**.

2. Sistemas de detección de intrusos (IDS)

Un sistema de detección de intrusos o IDS es una herramienta de seguridad que intenta **detectar o monitorizar los eventos ocurridos en un determinado sistema informático** en busca de intentos de comprometer la seguridad de dicho sistema.

Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host, aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, pero aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y **detectan las primeras fases de cualquier ataque** como pueden ser el análisis de nuestra red, barrido de puertos, etc.

Los tipos de IDS que encontramos son:

- **HIDS** (Host IDS): protegen un único servidor, PC o host, Monitorizan gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como ficheros, logs, recursos, etc., para su posterior análisis en busca de posibles incidencias.
- **NIDS** (Net IDS): protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Actúan mediante la utilización de un **dispositivo de red configurado en modo promiscuo** (analizan en tiempo real todos los paquetes que circulan por un segmento de red aunque estos nos vayan dirigidos a ese determinado dispositivo).

La arquitectura de un IDS, a grandes rasgos, está formada por:

- La **fuente de recogida de datos.** Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.
- **Reglas y filtros sobre los datos y patrones** para detectar anomalías de seguridad en el sistema.
- Dispositivo **generador de informes y alarmas**. En algunos casos con la sofisticación suficiente como para enviar alertas vía mail, o SMS.

Con respecto a la ubicación del IDS se recomienda disponer **uno delante y otro detrás del cortafuegos perimetral** de nuestra red, para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

3. Riesgos potenciales en los servicios de red

TCP/IP es la arquitectura de protocolos que usan los ordenadores para comunicarse en Internet y, actualmente, casi en cualquier otra red. Emplean puertos de comunicaciones o numeración lógica que se asigna para identificar cada una de las conexiones de red, tanto en el origen como en el destino. No tiene ninguna significación física.

Los servicios de red más habituales tienen asignados los llamados puertos bien conocidos, por ejemplo el 80 para HTTP o web, el 21 para transferencia de ficheros FTP, el 23 para TELNET, etc.

Rango	Puertos	Servicios sobre puertos bien conocidos
0-1023	Servicios bien conocidos	20 y 21: FTP
1024-49151	Registrados	22: SSH comunicación cifrada
49152-65535	Dinámicos y/o privados	23: Telnet no cifrado 24: SMTP y 110: POP3 53: DNS 80: HTTP y 443 HTTPS cifrado 137,138,139: NetBIOS compartir archivos e impresora y 445: SMB

Los distintos sistemas y sus aplicaciones de red, ofrecen y reciben servicios a través de dichos puertos de comunicaciones. Solo a través de un conocimiento y análisis exhaustivo de los puertos y las aplicaciones y equipos que los soportan podemos asegurar nuestras redes. El análisis y control de los puertos se pueden realizar desde distintos frentes:

- **En una máquina local** observando qué conexiones y puertos se encuentran abiertos y qué aplicaciones los controlan.
  - El comando **netstat** permite ver el estado en tiempo real de nuestras conexiones.
  - Los **cortafuegos** o **firewall** personales son una medida de protección frente a ataques externos.
- En la **administración de red** para ver qué puertos y en qué estado se encuentran los de un conjunto de equipos.
  - La aplicación **nmap** permite un escaneo de puertos, aplicaciones y sistemas operativos, en un rango de direcciones.
  - Los **cortafuegos y proxys perimetrales** ofrecen protección mediante un filtrado de puertos y conexiones hacia y desde el exterior de una red privada.

Tras realizar un análisis exhaustivo a nivel de puertos, debemos proteger nuestras conexiones, haciéndolas seguras, por ejemplo cuando enviemos información confidencial.

4. Comunicaciones seguras

La mayoría de las comunicaciones que empleamos en la red como HTTP, FTP o SMTP/POP, **no emplean cifrado en las comunicaciones**. Aunque existen protocolos que emplean comunicaciones cifradas como SSH a través del puerto 22, SSH, soportando incluso el envío seguro de archivos mediante SFTP

Otras alternativas para establecer comunicaciones seguras entre 2 sistemas cifrando las comunicaciones a distintos niveles son:

- **SSL y TLS**: Secare Sockets Layer -Protocolo de Capa de Conexión Segura- (SSL) y Transport Layer Security -Seguridad de la Capa de Transporte- (TLS), su sucesor. Se ejecutan en una capa entre los protocolos de aplicación y sobre el protocolo de transporte TCP. Entre otros se emplea a través de puertos específicos con: HTTPS , FTPS, SMTP, POP3, etc.
- **IPSEC** o Internet Protocol security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. Actúan en la capa 3 lo que hace que sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo **TCP** y **UDP**. Una ventaja importante frente a otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec **no hay que hacer ningún cambio**.

VPN

Una red privada virtual o **VPN** (Virtual Prívate Network), es una tecnología de red que permite una extensión de una red local de forma segura sobre una red pública, como Internet.

Algunas aplicaciones de dicha tecnología son la posibilidad de conectar utilizando la infraestructura de Internet, dos o más sucursales de una empresa, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de trabajo, etc. Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar l a autenticación, integridad y confidencialidad de toda la comunicación:

- **Autenticación y autorización:** se controlan los usuarios y/o equipos y qué nivel de acceso debe tener.
- **Integridad:** los datos enviados no han sido alterados, se utilizan funciones resumen o hash, como MD5 y SHA.
- **Confidencialidad:** que la información que viaja a través de la red pública solo puede ser interpretada por los destinatarios de la misma. Para ello se hace uso de algoritmos de cifrado como DES, 3DES y AES.
- No **repudio**: los mensajes tienen que ir firmados.

Básicamente existen tres arquitecturas de conexión VPN:

- **VPN de acceso remoto:** el modelo más usado, usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas públicas compartidas, domicilios, hoteles, etc.) utilizando Internet como vínculo de acceso.
- **VPN punto a punto:** conecta ubicaciones remotas como oficinas, con una sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Mediante la técnica de tunneling se encapsulará un protocolo de red sobre otro creando un túnel dentro de una red.
- **VPN over LAN:** es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Emplea la misma red de área local (LAN) de la empresa, aislando zonas y

servicios de la red interna, a los que se les puede añadir cifrado y autenticación adicional mediante VPN. Permite también mejorar las prestaciones de seguridad de las redes inalámbricas, haciendo uso de túneles cifrados IPSEC o SSL que agregan credenciales de seguridad del propio túnel VPN.

El protocolo estándar que utiliza VPN es IPSEC, pero también trabaja con PPTP, L2TP, SSL/TLS, SSH, etc. Dos de las tecnologías más utilizadas para crear VPN's, en realidad son diferentes protocolos o conjuntos de protocolos, PPTP y L2TP:

- **PPTP o Point to Point Tunneling Protocol:** es un protocolo desarrollado por Microsoft y disponible en todas las plataformas Windows. Es sencillo y fácil de implementar pero ofrece menor seguridad que L2TP.
- **L2TP o Layer Two Tunneling Protocol:** Se trata de un estándar abierto y disponible en la mayoría de plataformas Windows, Linux, Mac, etc. Se implementa sobre IPSec y proporciona altos niveles de seguridad. Se pueden usar certificados de seguridad de clave pública para cifrar los datos y garantizar la identidad de los usuarios de la VPN.

5. Redes inalámbricas

En los últimos años ha irrumpido con fuerza, en el sector de las redes locales, las comunicaciones inalámbricas, también denominadas wireless. La tecnología inalámbrica ofrece muchas ventajas en comparación con las tradicionales redes conectadas por cable.

- Una de las principales ventajas es la capacidad de brindar **conectividad en cualquier momento y lugar**, es decir mayor disponibilidad y acceso a redes.
- La instalación de la tecnología inalámbrica es **simple y económica**. El coste de dispositivos inalámbricos domésticos y comerciales continúa disminuyendo.
- La tecnología inalámbrica permite que las redes se amplíen fácilmente, sin limitaciones de conexiones de cableado, por lo que es **fácilmente escalable**.

A pesar de la flexibilidad y los beneficios de la tecnología inalámbrica, existen algunos riesgos y limitaciones:

- Utilizan rangos del espectro de radiofrecuencia (RF) sin costes de licencia por su transmisión y uso. Estos rangos al ser de uso público **están saturados** y las señales de distintos dispositivos suelen interferir entre sí.
- El área problemática de la tecnología inalámbrica es la **seguridad**. Permite a cualquier equipo con tarjeta de red inalámbrica interceptar cualquier comunicación de su entorno.

Para tratar estas cuestiones de seguridad se han desarrollado técnicas para ayudar a proteger las transmisiones inalámbricas, por ejemplo la encriptación y la autenticación. A pesar de las siguientes técnicas que se presentan a continuación, y de los problemas propios asociados a las comunicaciones cableadas (fibra, cable de pares, coaxial) como las interferencias y deterioros o daños físicos del material, éstas siguen siendo los medios de acceso físico más seguros que existen en la actualidad.

Sistemas de seguridad en WLAN

Los sistemas de cifrado empleados para autenticación como encriptación en redes inalámbricas son:

- **Sistema abierto u Open System**: es decir sin autenticación en el control de acceso a la red, normalmente realizado por el punto de acceso, ni cifrado en las comunicaciones.
- **WEP o Wired Equiualent Privacy o Privacidad Equivalente a Cableado:** sistema estándar diseñado en la norma básica de redes inalámbricas 802.11. Emplea para la encriptación de los mensajes claves de 13 (104 bits) o 5 (40 bits) caracteres, también denominadas WEP 128 o WEP 64 respectivamente. Existen también dispositivos que permiten configuraciones de 152 y 256 bits. En cuanto a la autenticación existen 2 métodos:
    - **Sistema abierto u Open system**, el cliente no se tiene que identificar en el Punto de Acceso durante la autenticación. Después de la autenticación y la asociación a la red, el cliente tendrá que tener la clave WEP correcta.
    - **Claves precompartida, Pre-Shared Keys o PSK**. En la autenticación mediante clave precompartida, se envía la misma clave de cifrado WEP para la autenticación, verificando y controlando el acceso de este modo el punto de acceso.

  Es aconsejable usar la autenticación de sistema abierto para la autenticación WEP, ya que es posible averiguar la clave WEP interceptando los paquetes de la fase de autenticación.
- **WPA** o Wi-Fi Protected Access o Acceso Protegido Wi-Fi: creado para corregir las deficiencias del sistema previo WEP. Se han realizado 2 publicaciones del estándar WPA como solución intermedia, y el definitivo WPA2 bajo el estándar 802.lli. Se proponen 2 soluciones según el ámbito de aplicación:
    - **WPA Empresarial o WPA-Enterprise** (grandes empresas): la autenticación es mediante el uso de un servidor RADIUS, donde se almacenan las credenciales y contraseñas de los usuarios de la red.
    - **WPA Personal** (pequeñas empresas y hogar): la autenticación se realiza mediante clave precompartida, de un modo similar al WEP.

Una de las mejoras de WPA sobre WEP, es la implementación del protocolo de integridad de clave temporal (**TKIP** - Temporal Key Integrity Protocol), que **cambia claves dinámicamente** a medida que el sistema es utilizado.

Aportando un mayor nivel de seguridad en el cifrado, es posible emplear el algoritmo de cifrado simétrico **AES**, más robusto y complejo que TKIP, aunque su implementación requiere de hardware más potente por lo que no se encuentra disponible en todos los dispositivos.

Aunque WPA es indiscutiblemente el sistema más seguro, uno de los grandes problemas que se plantea es la **compatibilidad y disponibilidad** de las distintas versiones y algoritmos de cifrado del mismo.

Recomendaciones de seguridad en WLAN

Dado que el acceso a redes inalámbricas plantea un punto muy débil de seguridad en redes corporativas algunas recomendaciones para mejorar la seguridad son:

- **Asegurar la administración del punto de acceso (AP)**, por ser un punto de control de las comunicaciones de todos los usuarios, y por tanto crítico en la red, cambiando la contraseña por defecto. Actualizar el firmware disponible del dispositivo para mejorar sus prestaciones, sobre todo de seguridad.
- **Aumentar la seguridad de los datos transmitidos:** usando encriptación WEP o WPA/WPA2 o servidor Radius, y cambiando las claves regularmente.
- **Cambia el SSID por defecto y desactiva el broadcasting SSID**. Los posibles intrusos tendrán que introducir manualmente el SSID y conocerlo previamente. Aunque la administración de los clientes se complica ya que deberán conocer el nombre exacto del SSID.
- Realizar una administración y monitorización minuciosa:
    - **Desactivar el servidor DHCP**, y asignar manualmente en los equipos las direcciones IP.
    - **Cambiar las direcciones IP** del punto de acceso y el rango de la red por defecto.
    - Activar el **filtrado de conexiones permitidas** mediante direcciones MAC.
    - Establecer un **número máximo de dispositivos** que pueden conectarse.
    - **Analizar periódicamente los usuarios conectados** verificando si son autorizados o no.
    - **Desconexión** del AP cuando no se use.
    - **Actualizar el firmware del dispositivo**, para evitar vulnerabilidades o añadir nuevas funciones de seguridad.

0. Índice