Seguridad y Alta Disponibilidad

UNIDAD 6.
SEGURIDAD EN REDES CORPORATIVAS

Contenidos

1. Amenazas y ataques
    1.1. Amenazas externas e internas
2. Sistemas de detección de intrusos (IDS)
3. Riesgos potenciales en los servicios de red
4. Comunicaciones seguras
    4.1. VPN
5. Redes inalámbricas
    5.1. Clasificación de los ataques en redes Wi-Fi
    5.1. Sistemas de seguridad en redes Wi-Fi
    5.2. Recomendaciones de seguridad en redes Wi-Fi

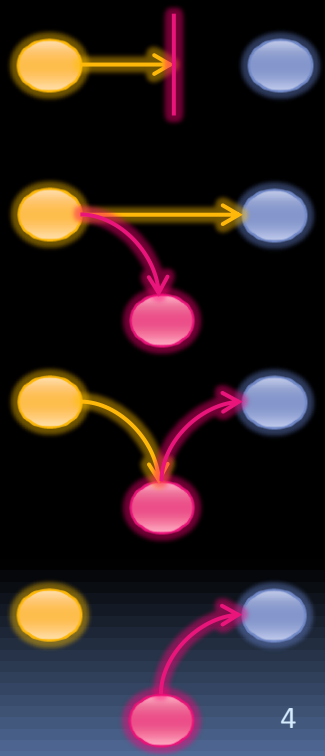
1

AMENAZAS Y ATAQUES

Amenazas y ataques

- Las redes de ordenadores cada vez son más esenciales para la vida diaria → Los ataques e intrusiones a través de las redes públicas y privadas son cada vez más frecuentes, y pueden causar interrupciones costosas de servicios críticos, pérdidas de trabajo, información y dinero.

- **Amenazas en comunicaciones**. División en 4 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 del acceso, consigue modificar el objeto, siendo posible incluso la **destrucción**.
  - **Fabricación**: modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el original y el "fabricado".



Amenazas y ataques

- Ejemplos reales de dichas amenazas.

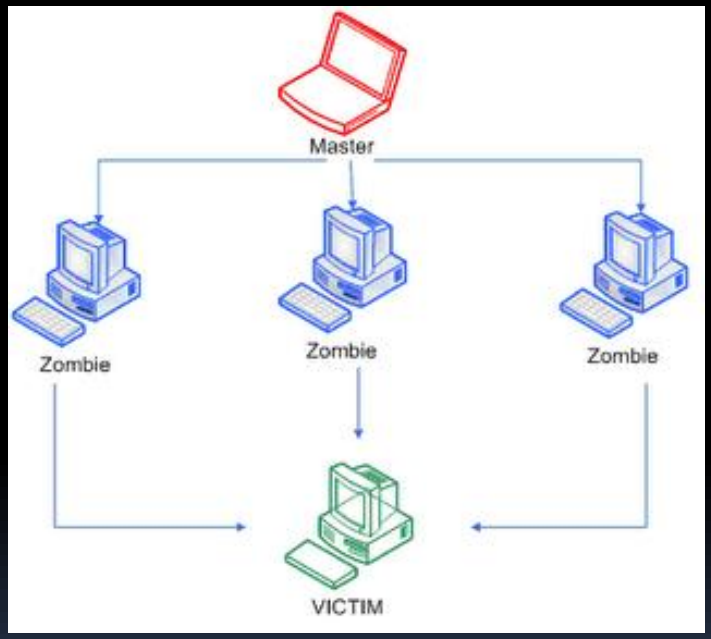
  Técnicas de ataques informáticos en redes:

  - **Ataque de denegación de servicio**
  - **Sniffing**
  - **Man in the middle**
  - **Spoofing**
  - **Pharming**

Amenazas y ataques

❖ Ataque de denegación de servicio

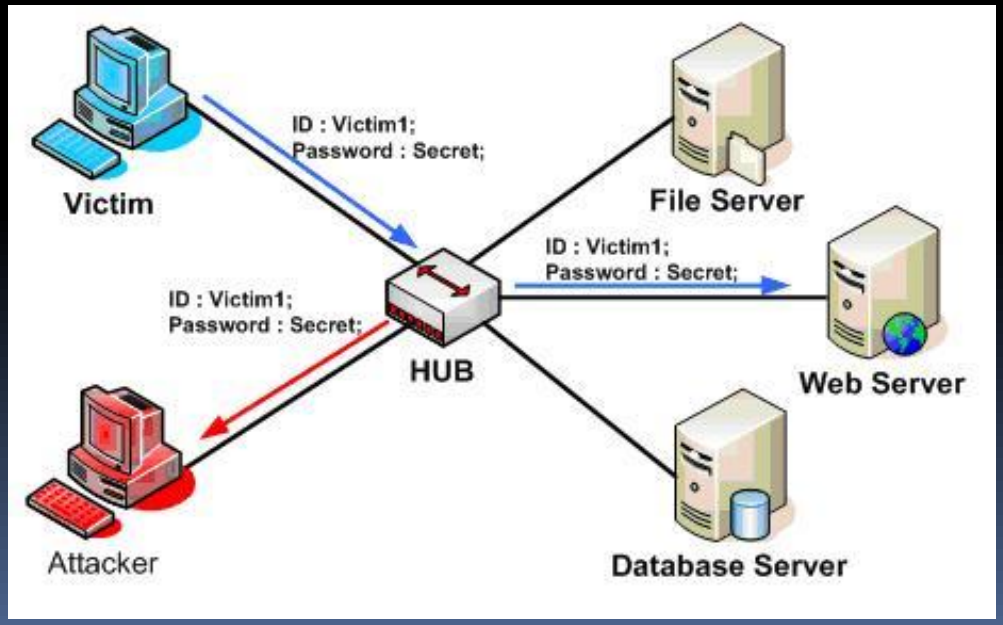
- ✓ También llamado ataque **DoS** *(Deny of Service)*
- ✓ Caso específico de **interrupción** de servicio.
- ✓ Causa que un recurso o servicio sea inaccesible, provocando la pérdida de conectividad de red por el consumo del ancho de banda o sobrecarga de los recursos.
- ✓ Ampliación: *ataque **distribuido** de deneg. de servicio* (**DDoS**), a través de una ***botnet***.



Amenazas y ataques

Sniffing

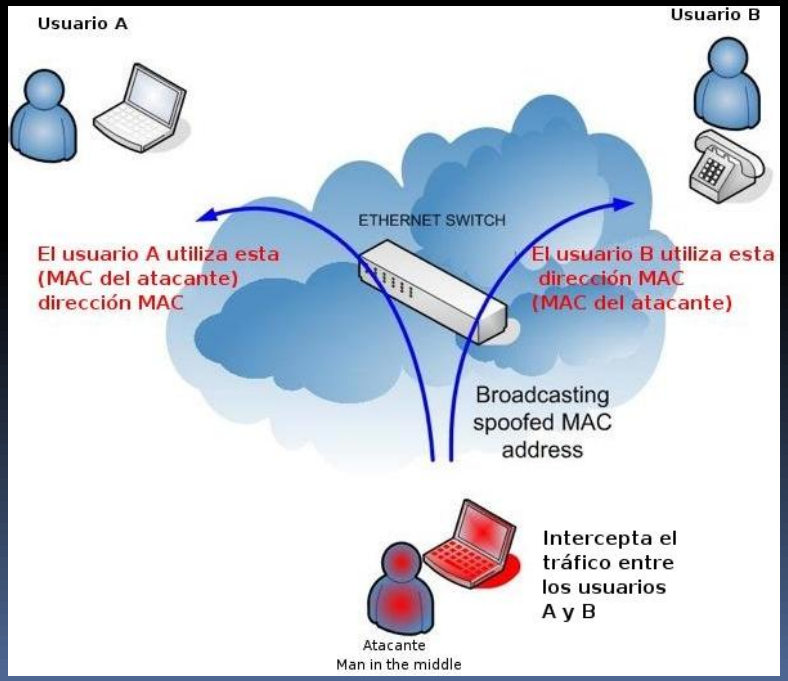
- Técnica de **interceptación**.
- Consiste en rastrear e interceptar, monitorizando el tráfico de una red, para hacerse con información confidencial.



Amenazas y ataques

Man in the middle *(MitM)*

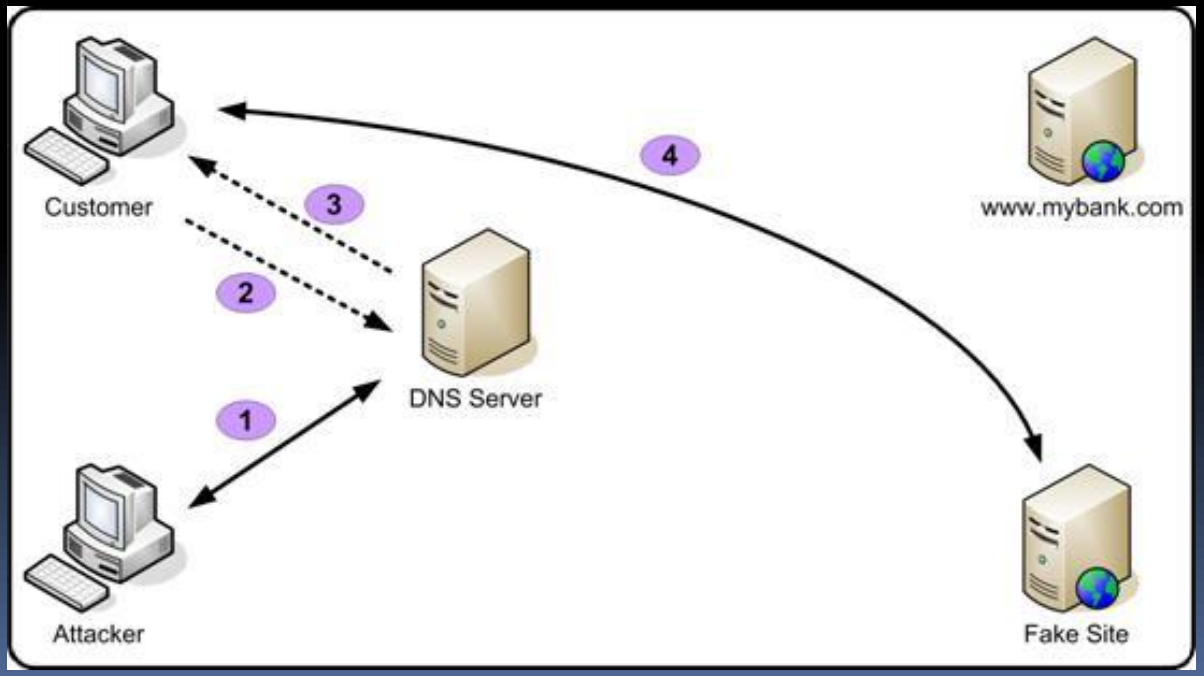
- Caso específico de **interceptación** y **modificación de identidad**.
- Un atacante supervisa una comunicación entre dos partes, falsificando las identidades de los extremos, y por tanto recibiendo el tráfico en los dos sentidos.



Amenazas y ataques

Spoofing

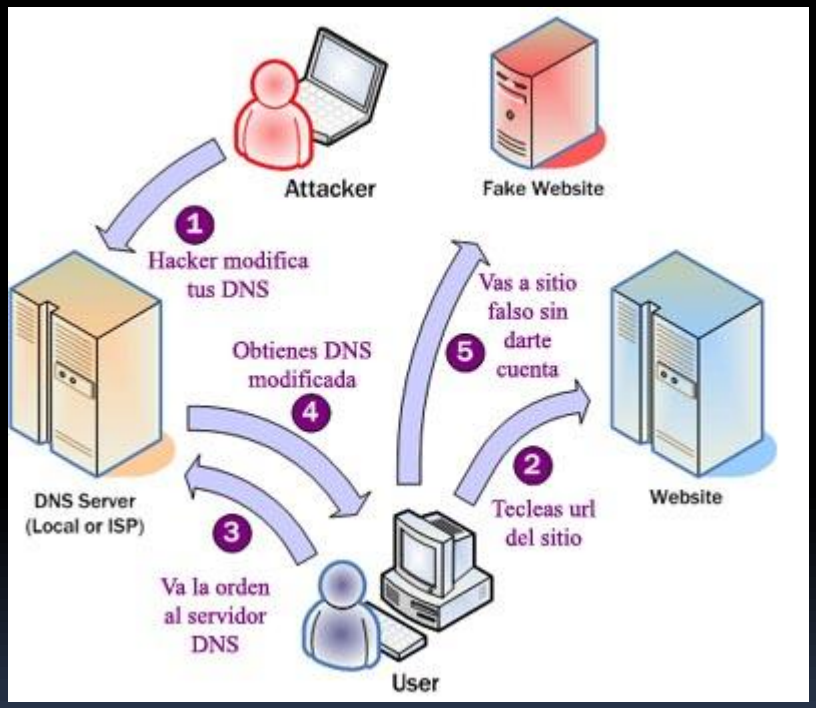
- Técnica de **fabricación**, suplantando la identidad o realizando una copia o falsificación.
- Ejemplo: falsificaciones de IP, MAC, web o mail.



Amenazas y ataques

Pharming

- Técnica de **modificación**.
- Explotación de una vulnerabilidad en el SW 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.



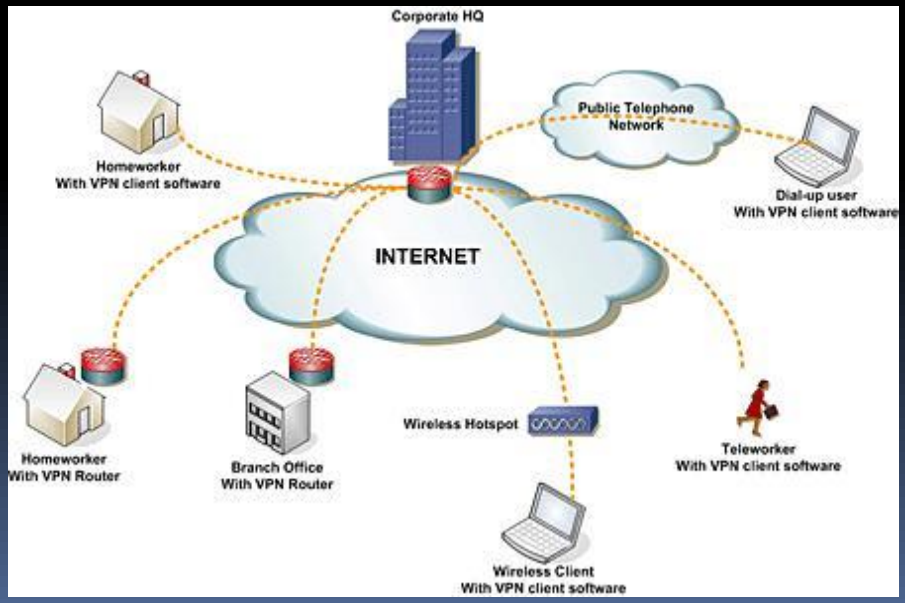
Práctica 1. Sniffing – MitM – ARP Spoofing - Pharming

- Para tomar precauciones y medidas de seguridad en una red → **Monitorizar el tráfico**
- Software de auditoría de seguridad en redes:
  - **Wireshark**
  - **NMAP**
  - ***Cain & Abel*** → Sniffing, Spoofing, MitM, Pharming
  - **Ettercap**
- **Recomendaciones**:
  - Uso de **tablas ARP estáticas** o entradas estáticas. Comando: `arp –s IP MAC` (Windows)
  - Monitorizar los intentos de modificación de tablas ARP.

    Herramientas software: *SNORT*, *Aarpwatch* (Linux) o *DecaffeinatID* (Win), *Wireshark*.
  - En caso de **DNS Spoofing**: precaución con los fake websites, comprobar el uso de HTTPS, certificado digital, veracidad de la URL…

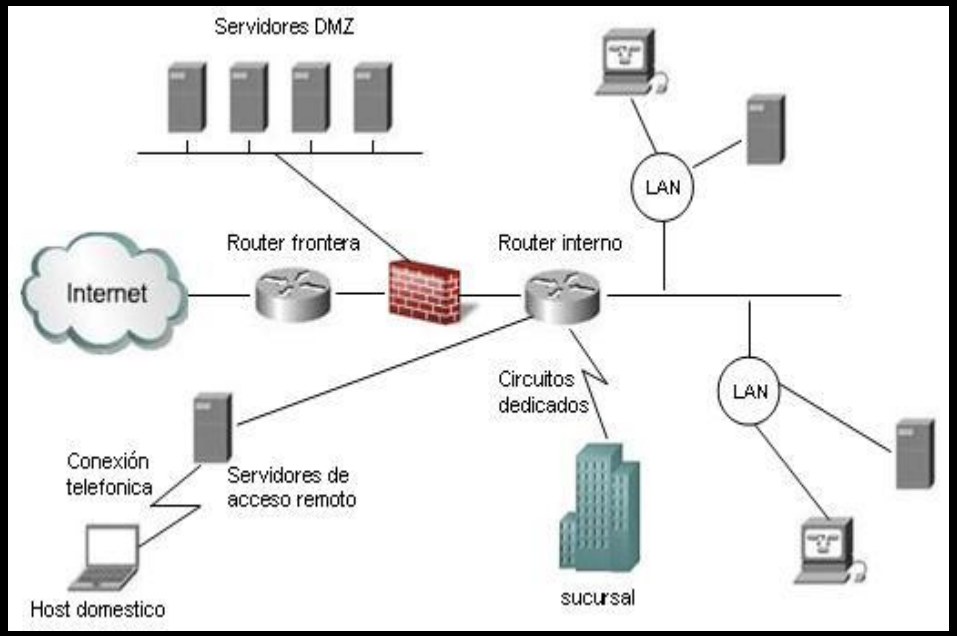
Amenazas externas e internas

- Las amenazas de seguridad causadas por **intrusos** en **redes corporativas** pueden ser:
  - **Amenaza externa** (o de acceso remoto)
    - Los atacantes son externos a la red privada y logran introducirse desde redes públicas.
    - Objetivos de ataques: **servidores** y **routers** accesibles desde el exterior, y que sirven de pasarela de acceso a la red corporativa.
  - **Amenaza interna** (o corporativa)
    - Los atacantes acceden sin autorización o pertenecen a la red privada de la organización.
    - Comprometen la seguridad, y sobre todo, la información y servicios de la organización.



Amenazas externas e internas

- Propuestas para la protección ante posibles amenazas internas:
  - ✓ Realizar un **buen diseño de subredes** dentro de la red corporativa. Para ello:
    - Subnetting
    - Redes locales virtuales o VLAN
    - Creación de zonas desmilitarizadas o DMZ
  - ✓ 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**, en especial, contraseñas por defecto de la administración de servicios.
  - ✓ **Máximo nivel de seguridad** en redes inalámbricas.

2

SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Sistemas de Detección de Intrusos (IDS)

- **¿Qué es un IDS *(Intrusion Detection System)*?**
  - Herramienta software de seguridad usada para detectar accesos no autorizados a un computador o a una red.
- **¿Cómo funciona?**
  - Suelen disponer de una base de datos de **"firmas" de ataques conocidos**.
  - **Analizan el tráfico de red**, comparando con firmas de ataques conocidos o comportamientos sospechosos (escaneo de puertos, paquetes mal formados…)
  - No están diseñados para **detener un ataque**. Normalmente se integran con un **firewall** (encargado de bloquear los paquetes si detecta que son peligrosos).
  - Aportan capacidad de prevención y de alerta anticipada.

Sistemas de Detección de Intrusos (IDS)

- **Tipos de IDS**
  - **HIDS** *(Host IDS)*: protegen un único servidor, PC o host.
  - **NIDS** *(Net IDS)*: protegen un sistema basado en red. Capturan y analizan paquetes de red, es decir, son *sniffers* del tráfico de red.

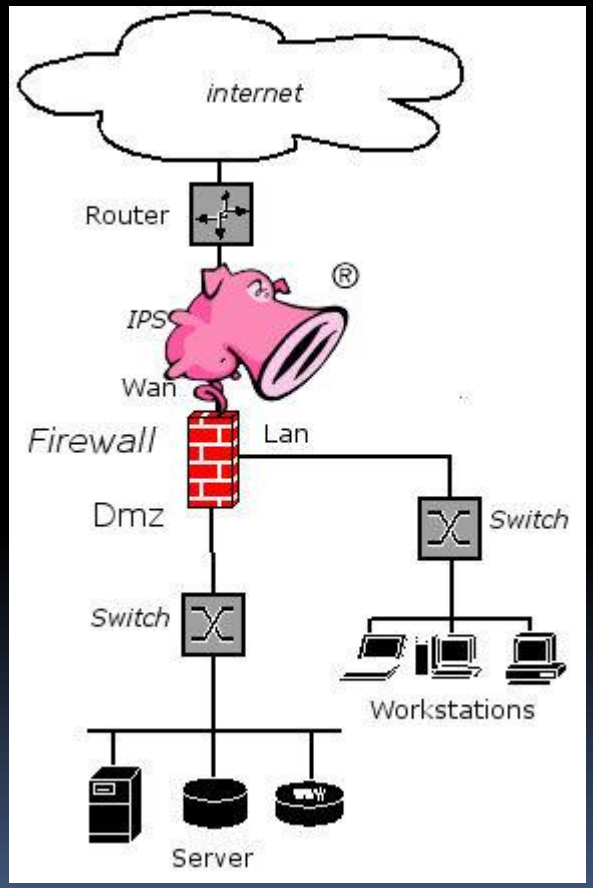
- **La arquitectura de un IDS, a grandes rasgos, está forma por:**
  - La fuente de recogida de datos (un log, dispositivo de red, o el propio sistema en el caso de los *HIDS*).
  - Reglas y filtros sobre los datos y patrones para detectar anomalías de seguridad.
  - Dispositivo generador de informes y alarmas (algunos pueden enviar alertas vía mail o SMS).

- **Ubicación recomendada del IDS**
  - Uno delante y otro detrás del cortafuegos perimetral de nuestra red.

Práctica 2. IDS - SNORT

SNORT

- Sistema de detección de intrusiones basado en red (***NIDS***)
- Puede funcionar como ***sniffer*** (viendo en consola en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), **registro de paquetes** (permite guardar en un archivo los logs para su posterior análisis offline) o como un ***NIDS*** normal.
- Está disponible bajo licencia GPL, gratuito y funciona bajo Windows y GNU/Linux.
- Descarga e información: www.snort.org



3

RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

Riesgos potenciales en los servicios de red

TCP/IP

- **TCP/IP** es la arquitectura de protocolos que usan los ordenadores para comunicarse en 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.
- Servicios de red más habituales (**puertos bien conocidos**):

Puerto	Servicio
20 y 21	FTP
22	SSH comunicación cifrada
23	Telnet no cifrado
25	SMTP
110	POP3
53	DNS
80	HTTP
443	HTTPS cifrado

Riesgos potenciales en los servicios de red

Análisis y control de puertos

- Los sistemas y sus aplicaciones de red ofrecen y reciben servicios a través de dichos puertos de comunicaciones ➡ análisis exhaustivo a nivel de puertos para proteger nuestras conexiones.

- El análisis y control de los puertos se pueden realizar:
  - En una **máquina local**, observando qué conexiones y puertos se encuentran abiertos y qué aplicaciones controlan.
    - Comando **netstat**, permite ver el estado de nuestras conexiones en tiempo real.
    - Cortafuegos (**firewall**) personales, como medida de protección frente ataques externos.
  - En la **administración de la red**, para ver qué puertos y en qué estado se encuentran los de un conjunto de equipos.
    - Aplicación **nmap**, permite escaneo de puertos, aplicaciones y SSOO en un rango de direcciones.
    - **Cortafuegos** y **proxys perimetrales**, ofrecen protección mediante filtrado de puertos y conexiones hacia y desde el exterior de una red privada.

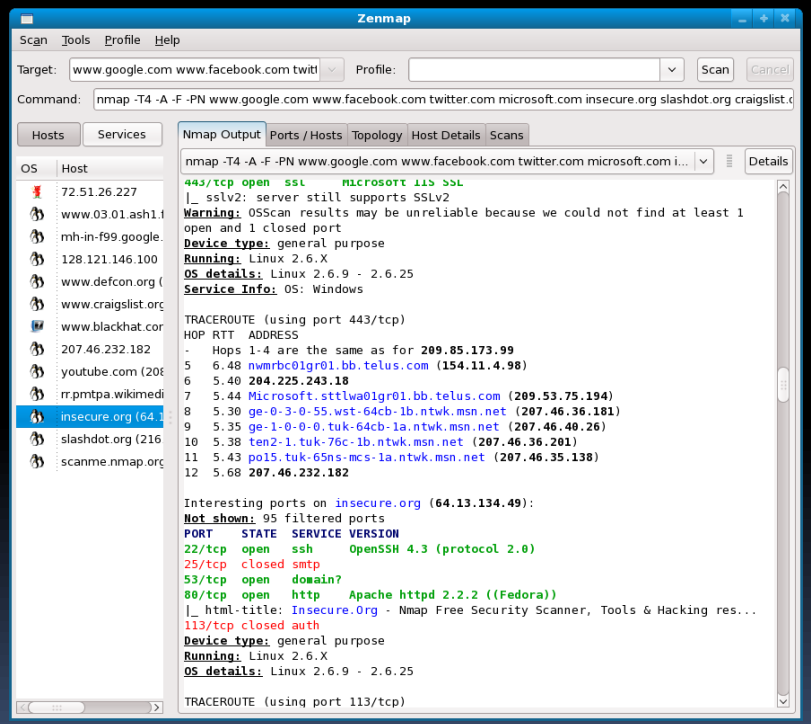
Práctica 3. Análisis de Puertos

netstat

- Comando para analizar el estado de nuestras conexiones y puertos.
- Windows: `netstat -anob`
- Linux: `netstat -atup`

nmap

- Análisis de puertos y aplicaciones de red, en 192.168.1.0/24
- Aplicación gráfica **ZENMAP**



Recomendaciones

- ✓ Controlar el estado de conexiones
- ✓ Evitar protocolos inseguros como Telnet
- ✓ Evitar configuraciones y contraseñas por defecto.

4
COMUNICACIONES SEGURAS

Comunicaciones seguras

Comunicaciones sin cifrado

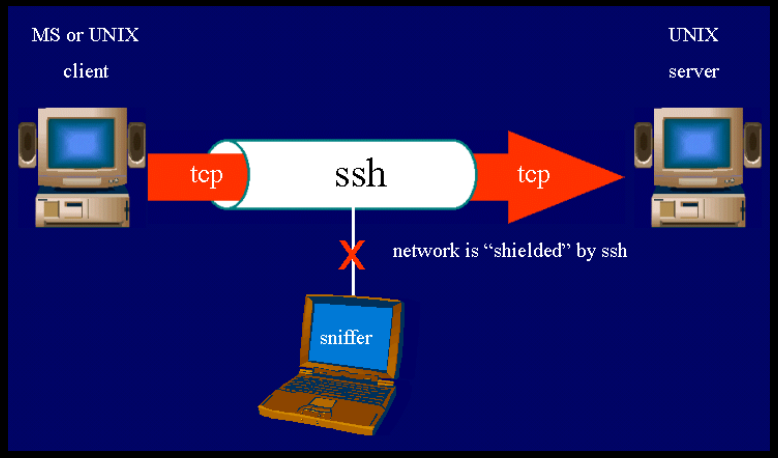
- Protocolos **HTTP**, **FTP** o **SMTP/POP**.
- *"Cain & Abel"* tiene la capacidad de recuperar tráfico y contraseñas de dichos protocolos.

Comunicaciones cifradas

- **SSH** (*Secure Shell*, Intérprete de órdenes segura): permite acceder a máquinas remotas y ejecutar comandos a través de una red. Puerto 22.
- **SSL** (*Secure Sockets Layer*, Protocolo de Capa de Conexión Segura) y **TLS** (*Transport Layer Security*, Seguridad de la Capa de Transporte), su sucesor. Entre otros, se emplea a través de puertos específicos con: **HTTPS**, **FTPS**, **SMTP**, **POP3**, etc.
- **IPSEC** (*Internet Protocol Security*): 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. Se utiliza para crear VPNs.

Práctica 4. SSH

- Instalación de un **servidor SSH** al que accederemos desde un intérprete de comandos desde *GNU/Linux* y desde *Windows*.



1. Instalación del **servidor SSH** en GNU/Linux
   - Buscamos todos los paquetes que tengan relación con *ssh*:

     ```
     $ aptitude search ssh
     ```
   - En la lista de paquetes encontrados estará "openssh-server". Lo instalamos:

     ```
     $ sudo aptitude install openssh-server
     ```
   - Para arrancar | parar | reiniciar: `$ sudo service ssh start | stop | restart`

Práctica 4. SSH

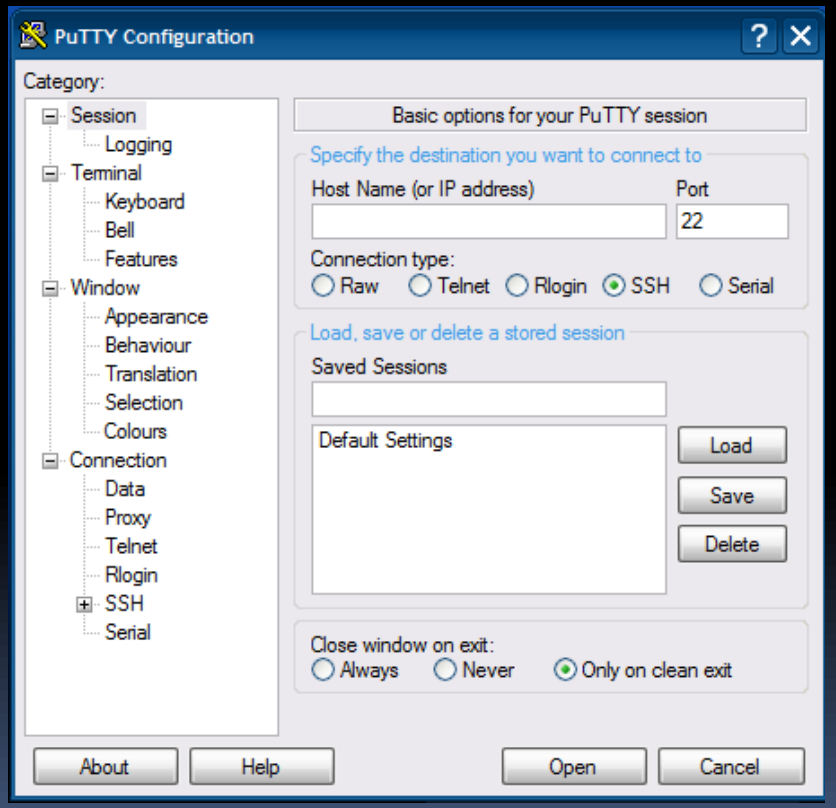
2. Conexión al servidor *ssh* desde una **máquina cliente *GNU/Linux***
   - Conexión con nuestro nombre de usuario:

     ```
     $ ssh direcIPserver
     ```

   - Conexión como usuario remoto:

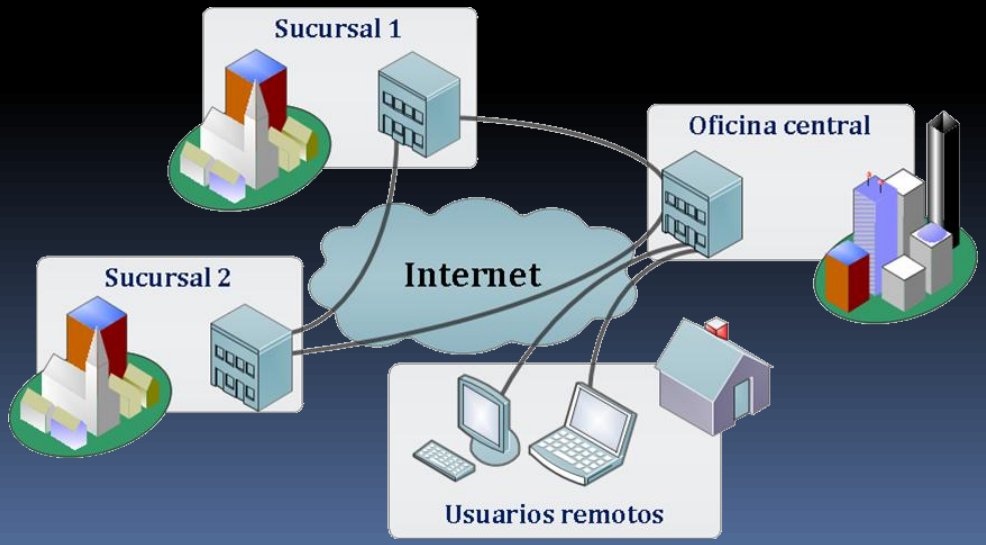
     ```
     $ ssh usuario@direcIPserver
     ```

3. Conexión al servidor *ssh* desde una **máquina cliente *Windows***
   - Conexión mediante ***PuTTY***



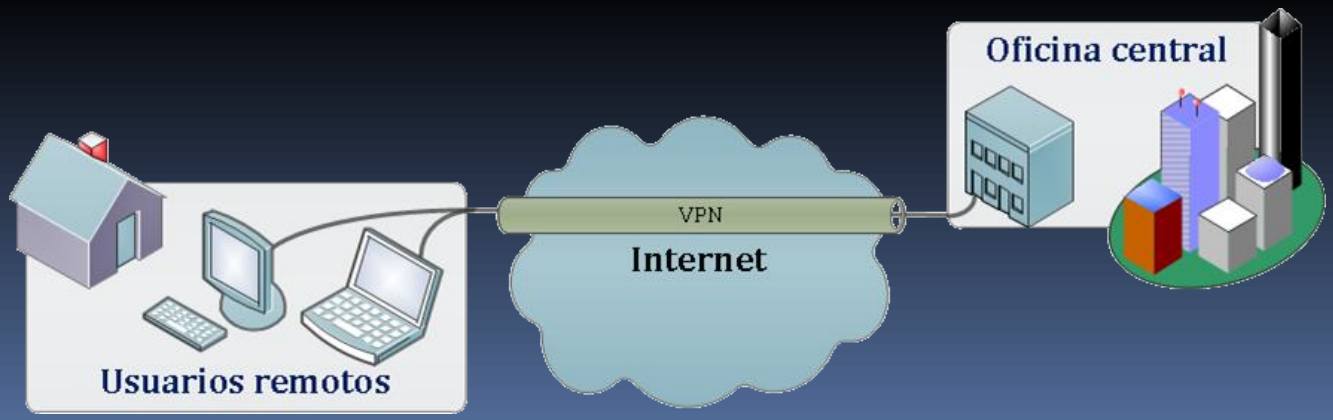
Redes Privadas Virtuales (VPN)

- **VPN** *(Virtual Private 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:
    - Conectar dos o más sucursales de una empresa a través de Internet.
    - Conexión desde casa al centro de trabajo (*teletrabajo*).
    - Acceso desde un sitio remoto (hotel, biblioteca…) de un usuario al PC de casa.



Redes Privadas Virtuales (VPN)

- Para hacerlo posible de manera segura, las **VPN** garantizan:
  - **Autenticación y autorización**: mediante la gestión de usuarios y permisos.
  - **Integridad**: los datos enviados no han sido alterados, con el uso de funciones hash (*MD5* o *SHA*).
  - **Confidencialidad**: la información que viaja a través de la red pública es cifrada con DES, 3DES, AES… y sólo puede ser interpretada por los destinatarios de la misma.
  - **No repudio**: los datos se transmiten firmados.



Redes Privadas Virtuales (VPN)

- Existen **tres arquitecturas de conexión VPN**:
  - **VPN de acceso remoto**: usuarios o proveedores se conectan con la empresa desde sitios remotos (oficinas públicas, domicilios, hoteles…) utilizando Internet como vínculo de acceso. Es el más usado.
  - **VPN punto a punto**: conecta oficinas remotas con la 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***. *Tunneling*.
  - **VPN over LAN**: 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, pudiendo añadir cifrado y autenticación adicional mediante VPN.
- Protocolo estándar que utiliza VPN: **IPSEC**
- Ejemplo de conexiones remotas: ***LogmeIn Hamachi.*** Crea red privada entre host remotos.

5
REDES INALÁMBRICAS

Introducción a la seguridad en redes Wi-Fi

- Redes inalámbricas o redes Wi-Fi, basadas en los **estándares IEEE 802.11**
- Envío de información a través de **señales de radiofrecuencia** por el aire.
  - Alcance teórico: 100 m.
  - Alcance real: varios kilómetros (depende de la existencia de obstáculos, potencia de transmisión, sensibilidad de recepción, utilización de antenas, etc…)
- **Ventajas** frente al cable:
  - Conectividad en cualquier momento y lugar (mayor disponibilidad y acceso a redes).
  - Instalación simple y económica.
  - Fácilmente escalable (permite que las redes se amplíen fácilmente)
- **Riesgos y limitaciones:**
  - Rangos de radiofrecuencia saturados , interferencias entre señales.
  - **Poca seguridad** (un equipo con tarjeta de red inalámbrica puede interceptar una comunicación de su entorno)

Clasificación de los ataques en redes Wi-Fi

- Ataques de negación de servicio *(DoS)*
  - Difícilmente evitable al afectar al funcionamiento de la tecnología.
  - Afecta a la disponibilidad.
- Interceptación de las comunicaciones
  - Acceso a los datos si no están cifrados. Indetectable.
  - Afecta a la confidencialidad.
- Inyección de tráfico en la red Wi-Fi
  - Acceso a los datos si no están cifrados. Indetectable.
  - Afecta a la integridad.
- Acceso a la red Wi-Fi
  - Conexión no autorizada a la red Wi-Fi. Acceso completo.
  - Afecta a la integridad.

Sistemas de seguridad en redes Wi-Fi

- **WEP** *(Wired Equivalent Privacy)*
  - Mecanismo de autentificación y cifrado antiguo e inseguro.
  - Requiere contraseña ⟹ falsa sensación de seguridad.
  - Un atacante puede obtener la contraseña en menos de un minuto.
  - Se desaconseja su utilización.

- **WPA** *(Wireless Protected Access)*
  - Mecanismo de autentificación y cifrado temporal, empleado durante la migración de WEP a WPA2 en redes Wi-Fi.
  - Inicialmente basado en TKIP (*Temporary Key Integrity Protocol*).
  - Se desaconseja su utilización

Sistemas de seguridad en redes Wi-Fi

- **WPA2** *(Wireless Protected Access 2)* ***Personal*** *o PSK*
  - Mecanismo de autentificación y cifrado:
    - Cifrado: AES *(Advanced Encryption Standard)*
    - Autentificación: PSK (*Pre-Shared Key*)
  - Contraseña compartida entre el punto de acceso y los clientes Wi-Fi. La contraseña debe ser suficientemente larga (más de 20 caracteres y difícilmente adivinable)
  - Opción recomendada para redes Wi-Fi personales o de pequeñas empresas

- **WPA2** *(Wireless Protected Access 2)* ***Enterprise***
  - Mecanismo de autentificación y cifrado:
    - Cifrado: AES *(Advanced Encryption Standard)*
    - Autentificación: 802.1X/EAP
  - Contraseñas aleatorias (servidor RADIUS). Múltiples tipos de protocolos EAP.
  - Opción recomendada para redes Wi-Fi empresariales o corporativas.

Recomendaciones de seguridad en redes Wi-Fi

- **Redes Wi-Fi**
  - Reducir el alcance de la señal.
  - No configurar la red Wi-Fi como oculta.
  - Utilizar WPA2-AES Personal (PSK) o Enterprise (802.1x-EAP).

- **Clientes Wi-Fi**
  - Actualización del sistema operativo y controlador Wi-Fi.
  - Deshabilitar el interfaz Wi-Fi cuando no se está utilizando.
  - Evitar conectarse a redes Wi-Fi inseguras, como por ejemplo redes públicas abiertas o basadas en WEP.
  - Mantener actualizada la lista de redes preferidas (PNL)