Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

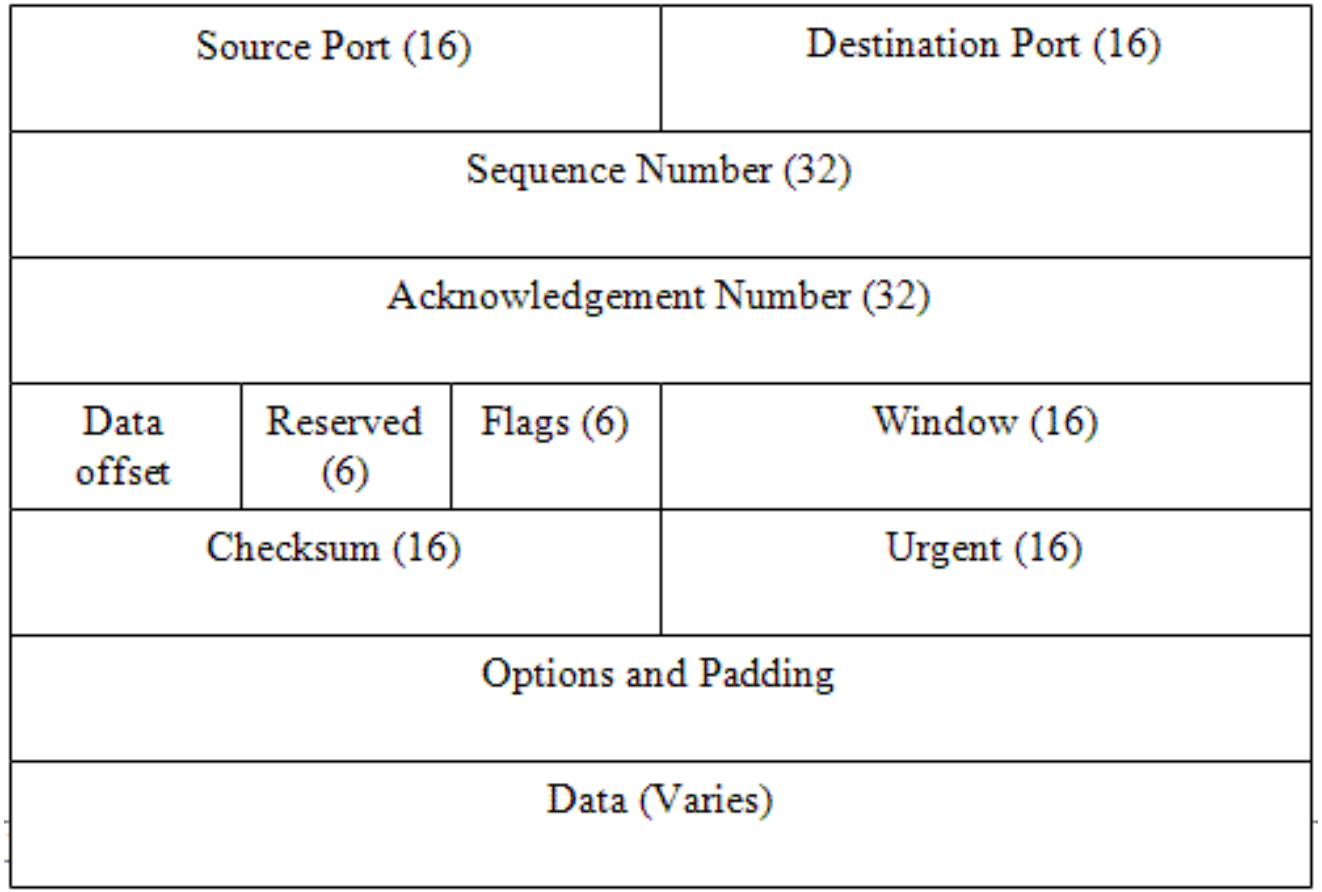
1. Port Scanning
   - Tipos de scanning
   - Herramientas
2. Packet Sniffing
   - Tipos de sniffing
   - Herramientas

Port Scanning

Port Scanning: es una técnica mediante la cual se realiza un barrido de los puertos TCP y/o UDP de un determinado host, en busca de puertos abiertos que permitan conectarse a algún servicio.

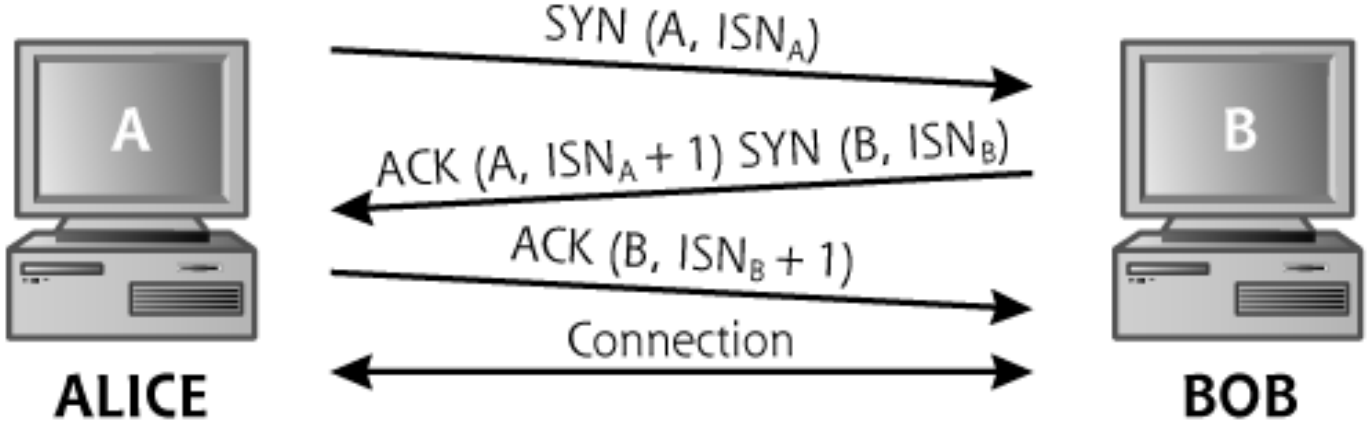
- Cada puerto con un servicio escuchando es una potencial puerta de entrada al equipo atacado.
- Los servicios "mayores" utilizan una serie de puertos conocidos (well-known ports).
  `http://www.iana.org/assignments/port-numbers`
- Mediante herramientas de port scanning se puede buscar una lista de puertos, un rango, o todos los posibles puertos TCP y UDP.

Port Scanning
Encabezado TCP



Tipos de scanning
TCP Connect

TCP Connect Scan: intenta completar la negociación de tres vías (3-way handshake) con cada puerto buscado en el equipo "target".



Tipos de scanning
TCP Connect

- **Puerto Abierto:** se completa correctamente la negociación.
- **Puerto Cerrado:** el target devuelve un RESET, ICMP Port Unreachable o nada.
- **Ventajas:** comportamiento estándar, no produce fallas en el target.
- **Desventajas:** fácil de detectar.

Tipos de scanning
TCP SYN

TCP SYN Scan: completa sólo los dos primeros pasos de la negociación: envía SYN y espera el SYN-ACK correspondiente.

- **Puerto Abierto:** se recibe SYN-ACK.
- **Puerto Cerrado:** el target devuelve un RESET, ICMP Port Unreachable o nada.
- **Ventajas:** es menos detectable y más rápido.
- **Desventajas:** algunos equipos viejos o desactualizados pueden fallar ante este tipo de scanning, produciéndose un DoS.

Tipos de scanning
TCP FIN Xmas Tree y Null

TCP FIN Scan: envía paquetes de finalización de la conexión (FIN) sin que la conexión exista.

- **Puerto Abierto:** no se recibe nada.
- **Puerto Cerrado:** el sistema target responde con un RESET (especificación TCP).

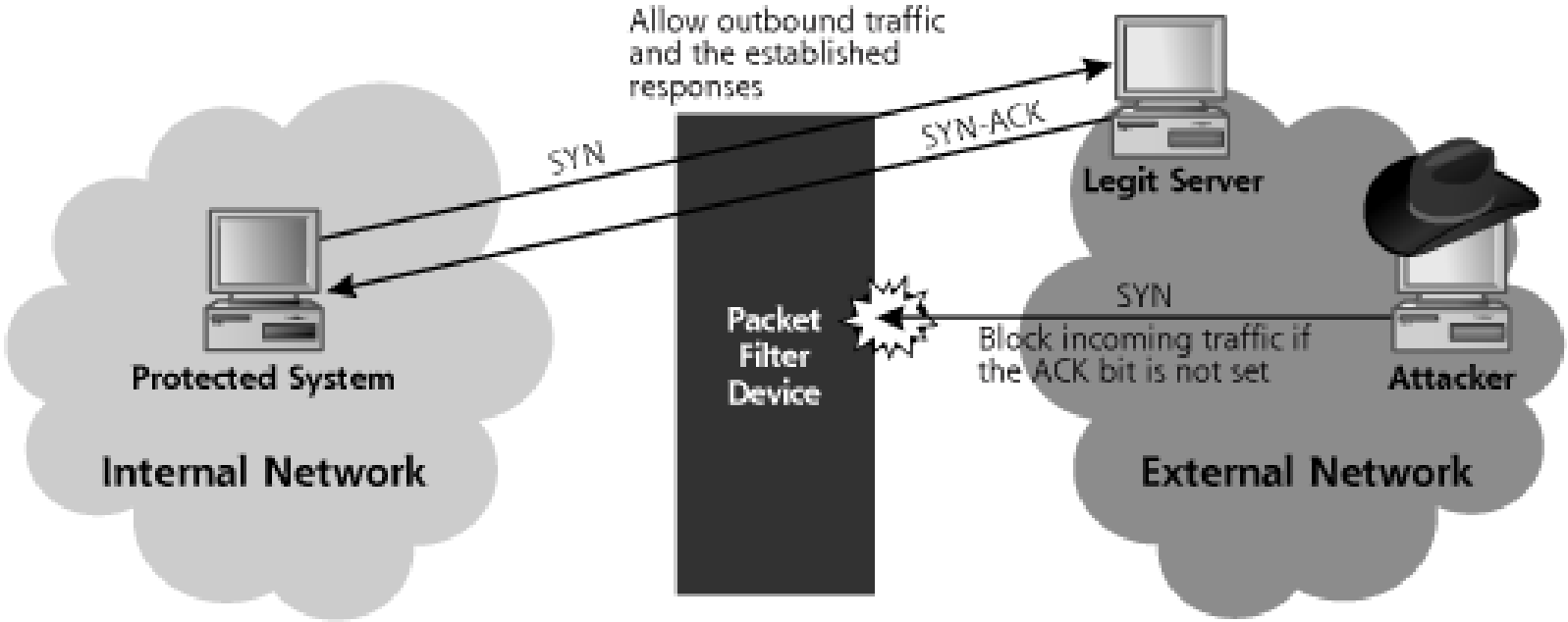
TCP Xmas Tree Scan: envía paquetes con todos los bits de control activados (URG, ACK, PSH, RST, SYN y FIN).

- **Ventajas:** puede pasar a través de algunos routers o firewalls que busquen que bits de control específicos estén activados.
- **Desventajas:** puede ser detectado por IDS modernos.

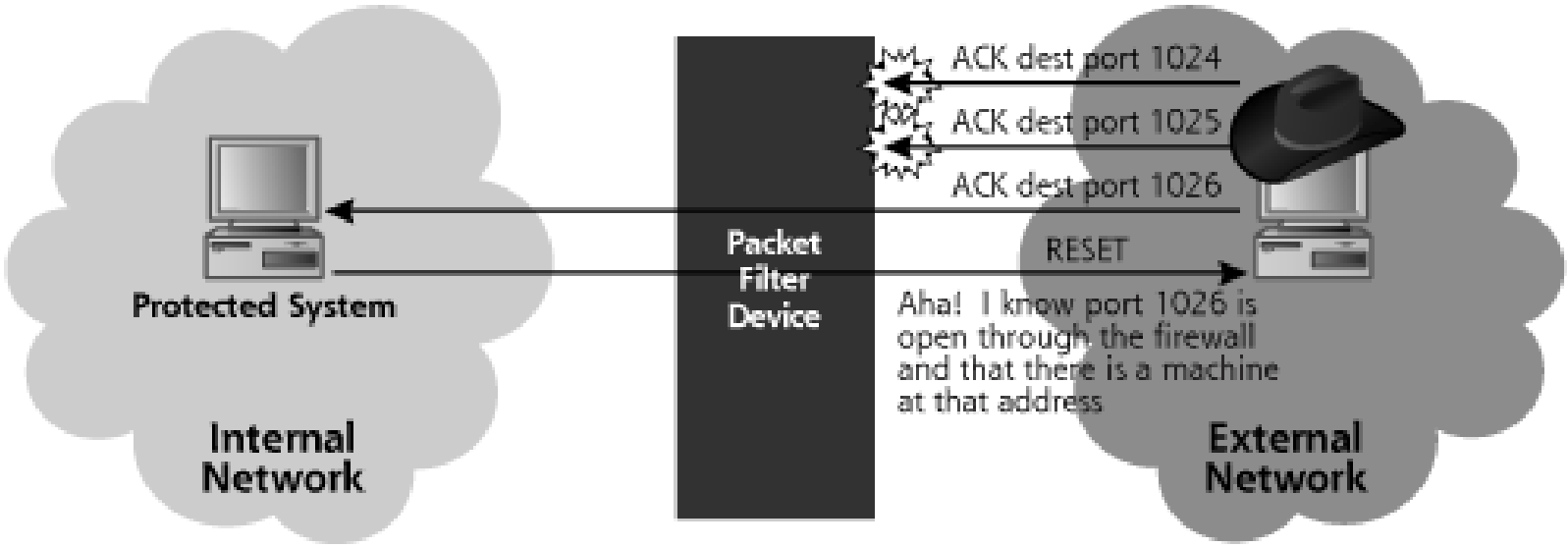
TCP Null Scan: envía paquetes con todos los bits de control desactivados.

Tipos de scanning
TCP ACK

TCP ACK Scan: se envían paquetes con el bit ACK activado para que los firewalls crean que son paquetes de respuesta.



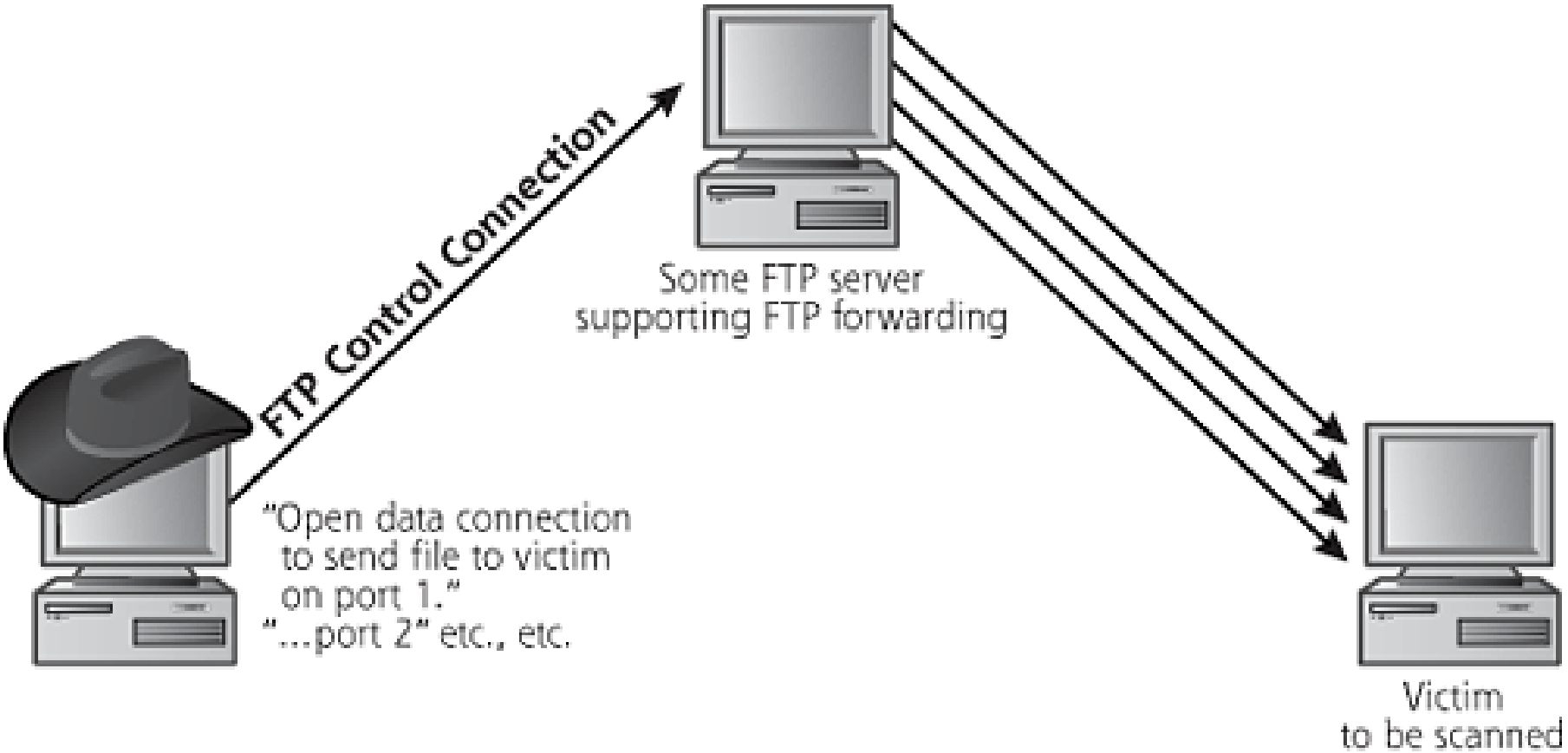
Tipos de scanning
TCP ACK



Tipos de scanning

Otros

FTP Bounce Scan: el atacante utiliza una vieja funcionalidad habilitada en algunos servicios de FTP para ocultarse.



Tipos de scanning
Otros

UDP Scan: se envía un paquete UDP a cada puerto.

- **Puerto Abierto:** se recibe otro paquete UDP.
- **Puerto Cerrado:** el sistema target responde con un ICMP Port Unreachable.

Version Scan: luego de identificar los puertos abiertos, intenta determinar qué servicio y versión en particular está escuchando en ellos.

Ping Sweep: se envían paquetes ICMP Echo Request a una lista o rango de direcciones IP para determinar cuáles tienen hosts activos.

OS Fingerprinting: se envía una serie de paquetes a varios puertos en el target para, en base a la respuesta recibida, determinar el Sistema Operativo remoto.

Nmap

- Herramienta más popular para scanning.
- Open Source y disponible libremente.
- Corre en los Sistemas Operativos más utilizados (Unix, Linux, Windows)

Nmap

Tipo Scan	Opción línea comandos
TCP Connect	-sT
TCP SYN	-sS
TCP FIN	-sF
TCP Xmas Tree	-sX
Null	-sN
TCP ACK	-sA
FTP Bounce	-b
UDP	-sU
Version	-sV
Ping Sweep	-sP
OS Fingerprint	-O

Packet Sniffing

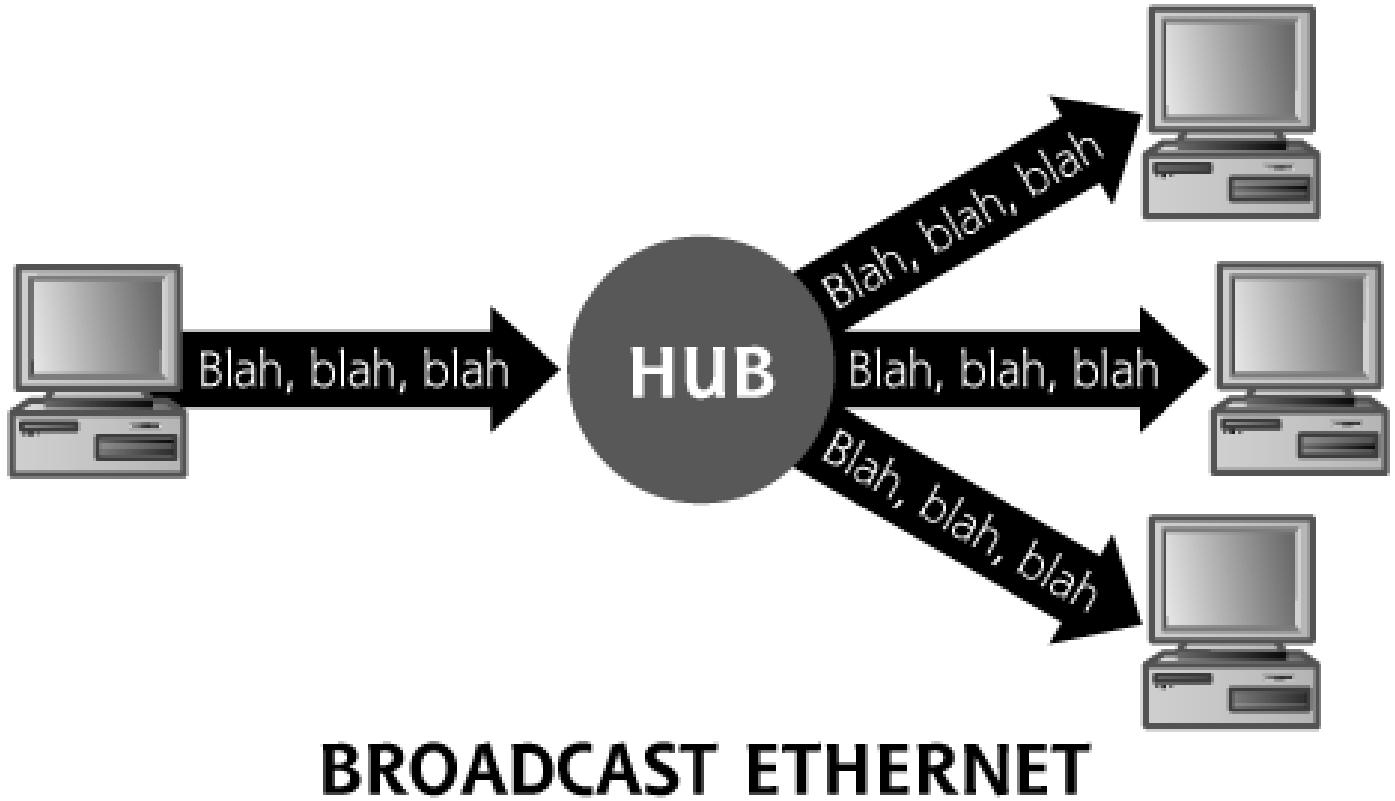
Packet Sniffer: también conocido como "packet analyzer", "protocol analyzer" o "network analyzer". Es un software o hardware que puede interceptar y registrar el tráfico que pasa a través de una red digital, o parte de ella.

USOS

- Analizar problemas de red.
- Detectar intentos de intrusiones en la red.
- Obtener información para atacar una red.
- Monitorear el uso de red.
- Espiar usuarios u obtener información sensible.
- Hacer ingeniería reversa de protocolos propietarios.

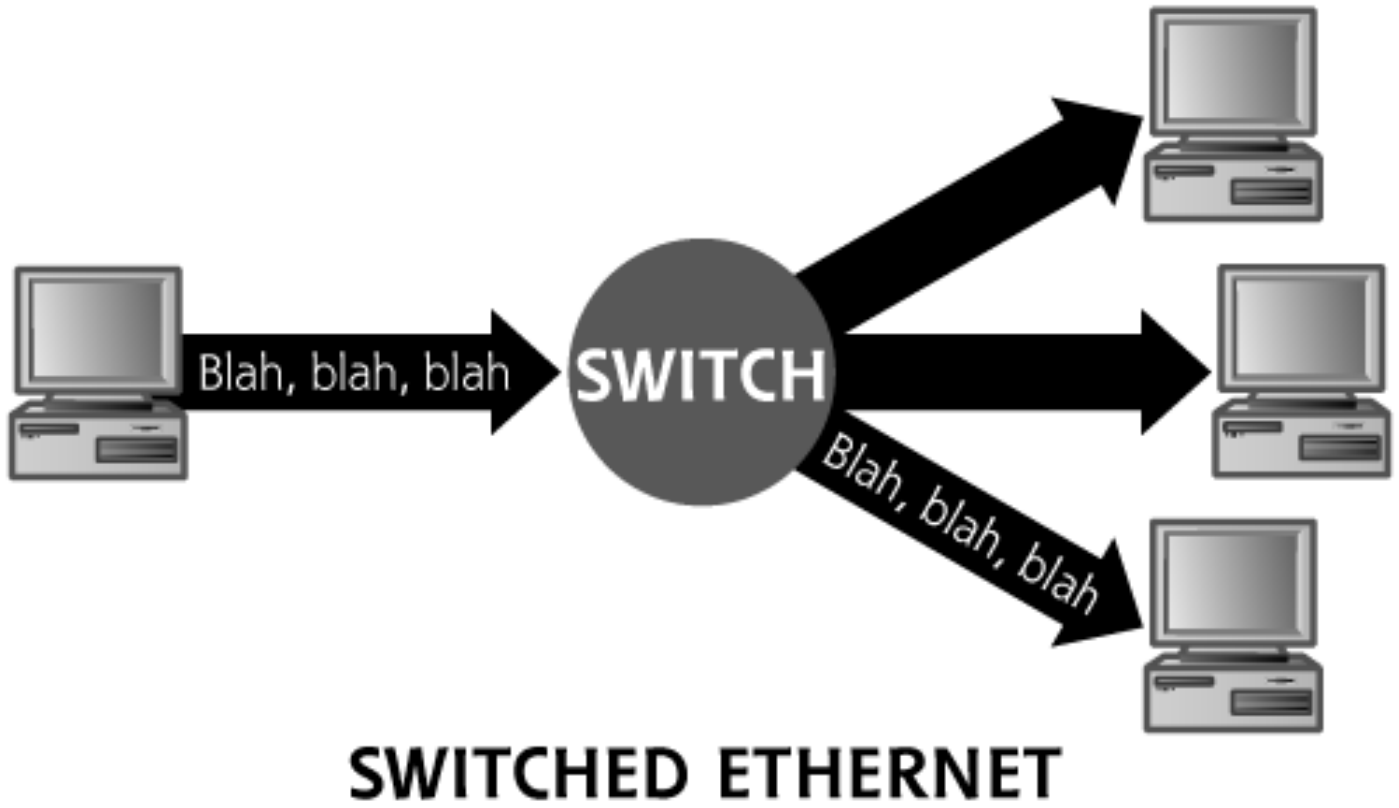
Tipos de sniffing

- **Pasivo:** consiste en escuchar y capturar el tráfico que pasa por la red. Para ver el tráfico de toda la red, se requiere un dispositivo del tipo hub. No es detectable.



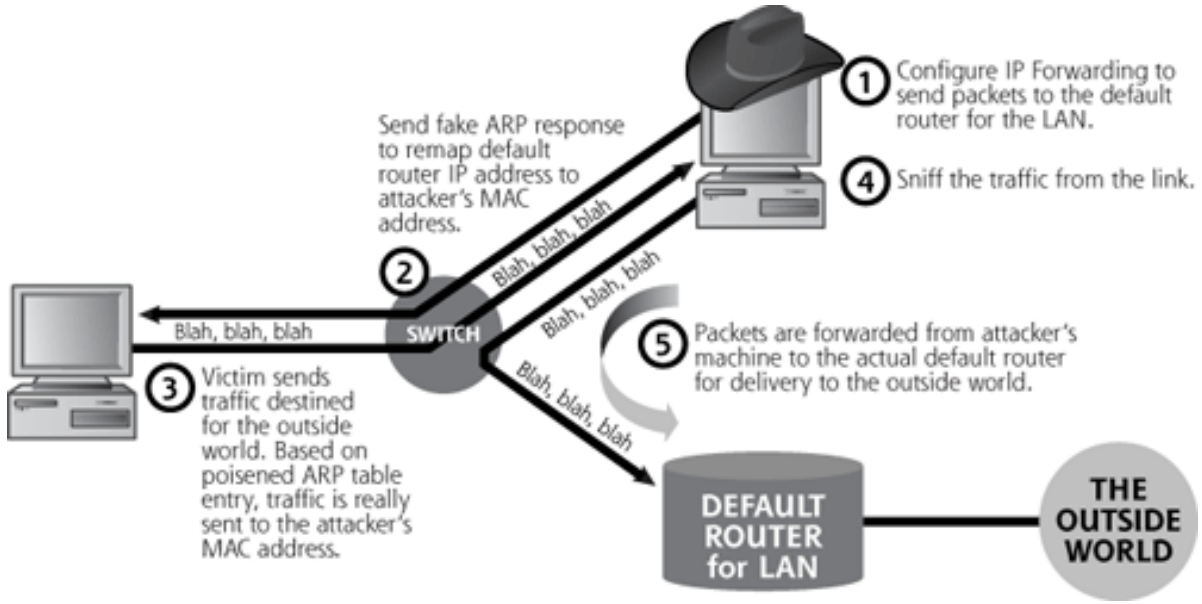
Tipos de sniffing

- **Activo:** se lanza un ataque de ARP Spoofing para capturar tráfico en redes con dispositivos como un switch. Es detectable.



ARP Spoofing

ARP Spoofing: también conocido como ARP Poisoning, es una técnica utilizada para atacar a una red Ethernet y que permite al atacante capturar tráfico en una red con switchs. Para ello se envían mensajes ARP falsos, confundiendo así a los hosts y dispositivos de la red.



Prevención: definir una entrada estática en la tabla ARP del equipo con la IP y MAC del gateway por defecto.

TCPDump

tcpdump: herramienta de línea de comandos para analizar el tráfico que circula por la red.

Filtros

- **type:** indica a qué se refiere el nombre o número pasado como parámetro. Tipos posibles son `host`, `net`, `port` y `portrange`. Ejemplo: 'host foo', 'net 128.3', 'port 20', 'portrange 6000-6008'
- **dir:** especifica la dirección desde/hacia el nombre o número indicado. Direcciones posibles son `src`, `dst`, `src or dst`, `src and dst`, etc. Ejemplo: 'src foo', 'dst net 128.3', 'src or dst port ftp'
- **proto:** restringe la búsqueda a un protocolo en particular. Protocolos válidos son: `ether`, `fddi`, `tr`, `wlan`, `ip`, `ip6`, `arp`, `rarp`, `tcp`, `udp`, etc. Ejemplo: 'ether src foo', 'arp net 128.3', 'tcp port 21', 'udp portrange 7000-7009'

TCPDump

- **Ejemplo 1:** capturar el tráfico de la interfaz eth0 y enviarlo a un archivo

```
tcpdump -w archivo.cap -ni eth0
```

- **Ejemplo 2:** capturar el tráfico ICMP de la interfaz wlan0, a excepción del dirigido a la IP 192.168.10.200

```
tcpdump -ni wlan0 icmp and not host 192.168.10.200
```

- **Ejemplo 3:** capturar en un archivo el tráfico HTTP o HTTPS de la interfaz wlan0

```
tcpdump -w captura.cap -ni wlan0 port 80 or port 443
```

Wireshark

Wireshark: es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, y como herramienta didáctica para educación. Se caracteriza por tener múltiples herramientas de análisis de tráfico y una completa interfaz gráfica.

Wireshark
Filtros

- Filtros de captura: filtra paquetes durante la captura. Ejemplos:
  - src net 192.168.1.0/24
  - host 10.20.30.1 and not port 80 and not port 22
- Filtros de pantalla: muestra u oculta en la pantalla paquetes de la captura analizada. Ejemplos:
  - tcp.port eq 25
  - ip.addr == 10.43.54.65
  - http.host matches "acme\.(org|com|net)"

Más información

- **wireshark.org.** Sample captures. `https://wiki.wireshark.org/SampleCaptures`
- **freesoft.org.** *Connected: An Internet Encyclopedia*. `http://freesoft.org/CIE/Course/Section4/8.htm`
- **GRAVES, Kimberly.** *CEH Official Ethical Hacker Review Guide.* Capítulo 6
- **SANDERS, Chris.** *Practical Packet Analysis.*
- **SKOUDIS - LISTON.** *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Capítulos 6 y 8.