



# Introducción a la Ciberseguridad

Clase 3: Fundamentos de Redes y Reconocimiento

Club de Programación - UNLP

# Objetivos de la Sesión



Hoy vamos a sumergirnos en los fundamentos esenciales que todo profesional de ciberseguridad debe dominar. Esta clase está diseñada para proporcionarte las bases sólidas que necesitas para entender cómo funcionan las redes modernas y cómo los atacantes pueden explotar sus vulnerabilidades.

01

## Direccionamiento y Servicios

Exploraremos los conceptos fundamentales de IP, MAC, puertos y DNS. Comprenderás cómo los dispositivos se identifican y comunican en las redes modernas.

02

## Protocolos de Transporte y Reconocimiento Activo

Aprenderemos sobre los protocolos que hacen posible la comunicación en red y cómo utilizar nmap para realizar reconocimiento de sistemas remotos.

03

## Análisis de Tráfico y Conceptos de Ataque

Descubriremos cómo analizar el tráfico de red con Wireshark y entenderemos los fundamentos teóricos detrás de los ataques más comunes.

# Direccionamiento Lógico: La Dirección IP

## El Identificador Universal en la Red

La **dirección IP** es mucho más que un simple número: es la piedra angular de toda comunicación moderna en Internet. Funciona como el "pasaporte digital" que permite a cualquier dispositivo ser localizado y alcanzado dentro de la vasta red global.

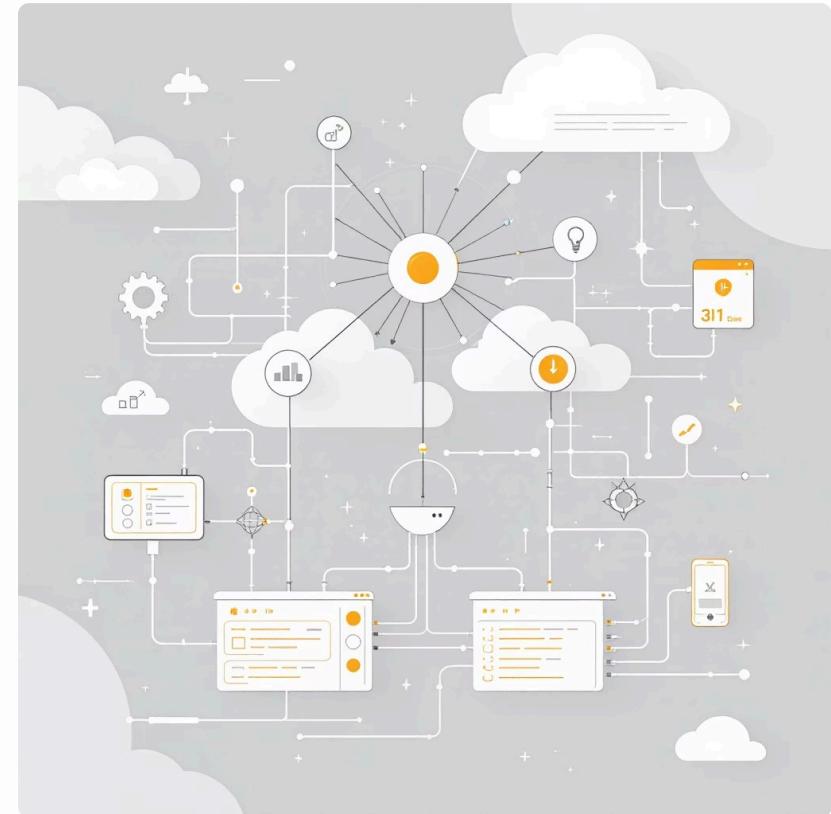
Cada dirección IP es única dentro de su contexto de red y opera bajo estrictos estándares internacionales. IPv4 utiliza 32 bits organizados en cuatro octetos (como 192.168.1.1), mientras que IPv6 emplea 128 bits para abordar las limitaciones de espacio de direcciones de su predecesor.

### ⓘ Comando Fundamental:

```
ip addr show
```

Este comando revela todas las interfaces de red activas en tu sistema, mostrando tanto direcciones IPv4 como IPv6 asignadas.

La comprensión profunda del direccionamiento IP es crucial para cualquier análisis de seguridad, ya que determina cómo los atacantes pueden alcanzar y comprometer sistemas remotos.



# Direccionamiento Físico: La Dirección MAC

## Identificador Hardware Único

La **dirección MAC** (Media Access Control) es un identificador de 48 bits grabado físicamente en cada tarjeta de red durante su fabricación. Este número hexadecimal es teóricamente único a nivel mundial.

## Capa de Enlace de Datos

Opera exclusivamente en la Capa 2 del modelo OSI, facilitando la comunicación directa entre dispositivos en la misma red local (LAN). No es enrutable a través de Internet.

## Implicaciones de Seguridad

Aunque las direcciones MAC pueden ser modificadas por software (MAC spoofing), siguen siendo fundamentales para la seguridad de red y el control de acceso en entornos corporativos.

En la práctica de ciberseguridad, las direcciones MAC son cruciales para entender la topología de red local y pueden revelar información valiosa sobre el fabricante del dispositivo. La dirección MAC aparece como `link/ether` en la salida del comando `ip addr show`, proporcionando insights sobre el hardware específico que estás analizando.

Es importante recordar que mientras las direcciones IP pueden cambiar dinámicamente, las direcciones MAC permanecen relativamente estáticas, lo que las convierte en un identificador más confiable para el seguimiento de dispositivos en redes locales.

# ARP: El Puente entre Mundos Lógico y Físico

## Address Resolution Protocol

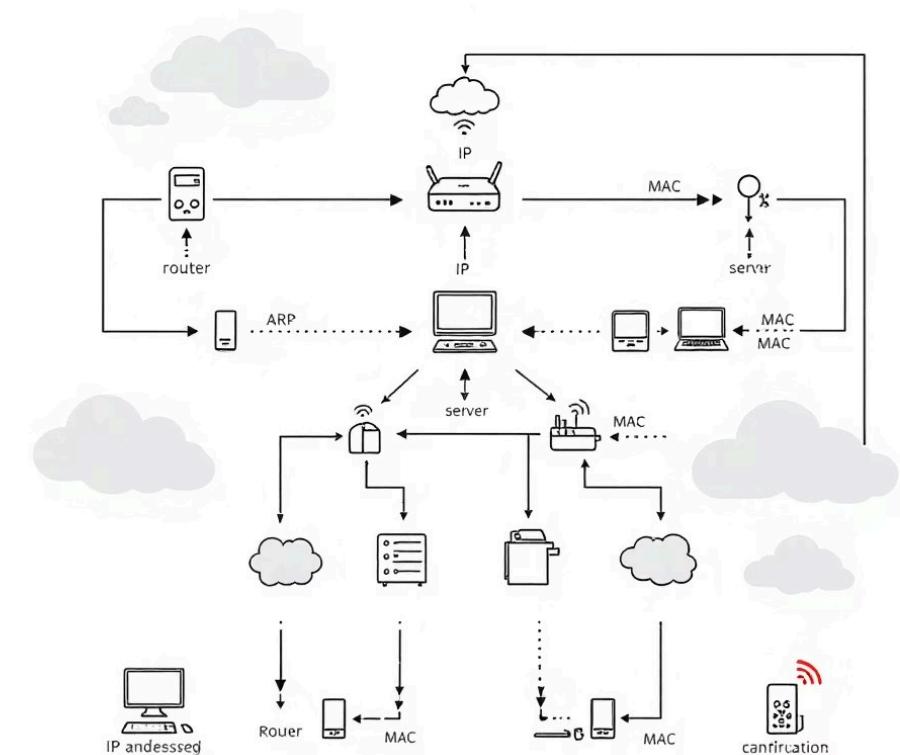
ARP es el protocolo que hace posible la magia de la comunicación en red local. Cuando tu computadora necesita enviar datos a otra máquina en la misma red, conoce la dirección IP de destino, pero necesita descubrir la dirección MAC correspondiente para poder enviar las tramas de datos.

Este proceso funciona mediante un intercambio de mensajes: primero se envía un **ARP Request** broadcast preguntando "¿quién tiene esta IP?", y el dispositivo propietario responde con un **ARP Reply** proporcionando su dirección MAC.

### Vulnerabilidad Crítica:

ARP no tiene mecanismos de autenticación, lo que lo hace vulnerable a ataques de envenenamiento (ARP poisoning) donde un atacante puede interceptar o redirigir el tráfico de red.

ARP notocol  
network communnnication (ARP)



La **tabla ARP** de tu sistema actúa como una memoria caché que almacena las correspondencias IP-MAC más recientes para acelerar futuras comunicaciones. Esta tabla es dinámica y se actualiza constantemente.

Comando: arp -a

Salida ejemplo:

```
? (192.168.1.1) at aa:bb:cc:dd:ee:ff [ether] on eth0
? (192.168.1.100) at 11:22:33:44:55:66 [ether] on eth0
```

Ejecutar arp -a revela la "caché ARP" actual: una lista completa de las direcciones IP y sus correspondientes direcciones MAC que tu máquina ha aprendido recientemente. Esta información es invaluable para el reconocimiento de red y la detección de dispositivos activos en tu segmento local.

# Puertos y Servicios: Los Puntos de Entrada

Si una dirección IP representa la dirección de un edificio en el vasto barrio de Internet, entonces los **puertos** son los números de los apartamentos individuales, cada uno albergando servicios específicos y únicos que pueden ser accesibles desde el exterior.



## Puertos Bien Conocidos (o-1023)

Reservados para servicios del sistema críticos. Ejemplos: HTTP (80), HTTPS (443), SSH (22), FTP (21), DNS (53). Requieren privilegios administrativos para ser utilizados.



## Puertos Registrados (1024-49151)

Asignados por IANA para aplicaciones específicas. Incluyen servicios como bases de datos, aplicaciones web personalizadas y herramientas de desarrollo.



## Puertos Dinámicos (49152-65535)

Utilizados para conexiones temporales y asignación dinámica. Típicamente empleados por aplicaciones cliente para establecer conexiones salientes.

El objetivo principal del **reconocimiento de red** en ciberseguridad es identificar qué puertos están abiertos y activos en un sistema objetivo. Cada puerto abierto representa una superficie de ataque potencial que podría ser explotada por un atacante malintencionado.

### Herramienta Fundamental:

```
ss -tulpn o netstat -tulpn
```

Estos comandos muestran todos los puertos que tu sistema tiene en estado de escucha (LISTEN), revelando qué servicios están activos y disponibles.

# DNS:



## Sistema de Nombres de Dominio

DNS es la infraestructura invisible que hace que Internet sea usable para los humanos. Sin este sistema, tendríamos que memorizar direcciones IP numéricas como 142.250.191.46 en lugar de recordar nombres amigables como www.google.com.

El sistema DNS funciona como una jerarquía distribuida de servidores que colaboran para resolver nombres de dominio. Cuando solicitas un sitio web, tu consulta viaja a través de varios niveles: desde tu resolver local, pasando por servidores raíz, servidores TLD (.com, .ar, .edu), hasta llegar al servidor autoritativo del dominio específico.



### 1 Cliente Local

Tu navegador solicita www.unlp.edu.ar



### 2 Resolver DNS

Servidor de tu ISP consulta la jerarquía DNS



### 3 Respuesta IP

Retorna 163.10.5.16 para establecer conexión



Desde una perspectiva de **ciberseguridad**, la enumeración de registros DNS constituye un paso fundamental en la fase de reconocimiento. Los atacantes pueden obtener información valiosa sobre la infraestructura de un objetivo analizando registros A, MX, NS, TXT y otros tipos de registros DNS que revelan servidores, subdominios y configuraciones de seguridad.

Además, DNS puede ser utilizado como vector de ataque a través de técnicas como DNS poisoning, DNS hijacking, y la exfiltración de datos mediante consultas DNS especialmente crafteadas que pueden evadir firewalls tradicionales.

# Herramientas de Consulta DNS



## dig - Domain Information Groper

La herramienta más potente y flexible para consultar servidores DNS. Proporciona control granular sobre las consultas y ofrece salidas detalladas ideales para análisis técnico profundo.



## nslookup - Name Server Lookup

Una alternativa más simple y directa, ideal para consultas rápidas y básicas. Aunque menos potente que dig, sigue siendo útil para verificaciones inmediatas.

El comando `dig www.unlp.edu.ar` es tu ventana hacia el mundo de la resolución DNS. Cuando ejecutas esta consulta, obtienes una respuesta estructurada que incluye múltiples secciones críticas:

```
;; ANSWER SECTION:  
www.unlp.edu.ar. 3600 IN A 163.10.5.16
```

La sección **ANSWER SECTION** es donde encontrarás la información más relevante: la dirección IP asociada al nombre de dominio consultado. El número "3600" representa el TTL (Time To Live) en segundos, indicando cuánto tiempo esta información permanecerá válida en la caché.

Para reconocimiento avanzado, puedes usar modificadores como:

- `dig MX unlp.edu.ar` - Para descubrir servidores de correo
- `dig NS unlp.edu.ar` - Para encontrar servidores de nombres autoritativos
- `dig TXT unlp.edu.ar` - Para obtener registros de texto que pueden contener información de configuración
- `dig ANY unlp.edu.ar` - Para solicitar todos los tipos de registros disponibles

Estas consultas DNS especializadas son fundamentales en las primeras fases del reconocimiento de objetivos, ya que pueden revelar infraestructura adicional, subdominios ocultos y configuraciones de seguridad que podrían ser explotadas posteriormente.

# IP Pública vs. IP Privada:

1

## IP Privada: Tu Identidad Local

Las direcciones IP privadas operan exclusivamente dentro de tu red local (LAN) y no son enruteables a través de Internet. Están definidas por el RFC 1918 en rangos específicos: 192.168.0.0/16, 10.0.0.0/8, y 172.16.0.0/12.

Tu router doméstico utiliza NAT (Network Address Translation) para traducir estas direcciones privadas a tu IP pública cuando los datos salen hacia Internet. Puedes ver tu IP privada ejecutando `ip addr` en sistemas Linux.

2

## IP Pública:

Tu dirección IP pública es única globalmente y asignada por tu ISP (Internet Service Provider). Es la identidad con la que apareces en Internet y la que utilizan los servicios web para enviarte respuestas.

Esta dirección puede ser estática (permanente) o dinámica (cambia periódicamente). Para descubrir tu IP pública actual, utiliza servicios externos como `curl ifconfig.me` o `dig +short myip.opendns.com @resolver1.opendns.com`.

3

La distinción entre IPs públicas y privadas es crucial para entender las **implicaciones de seguridad** en diferentes contextos. Los atacantes externos solo pueden acceder directamente a tu IP pública, mientras que los ataques a IPs privadas requieren que el atacante ya esté dentro de la red local o haya comprometido el perímetro de seguridad.

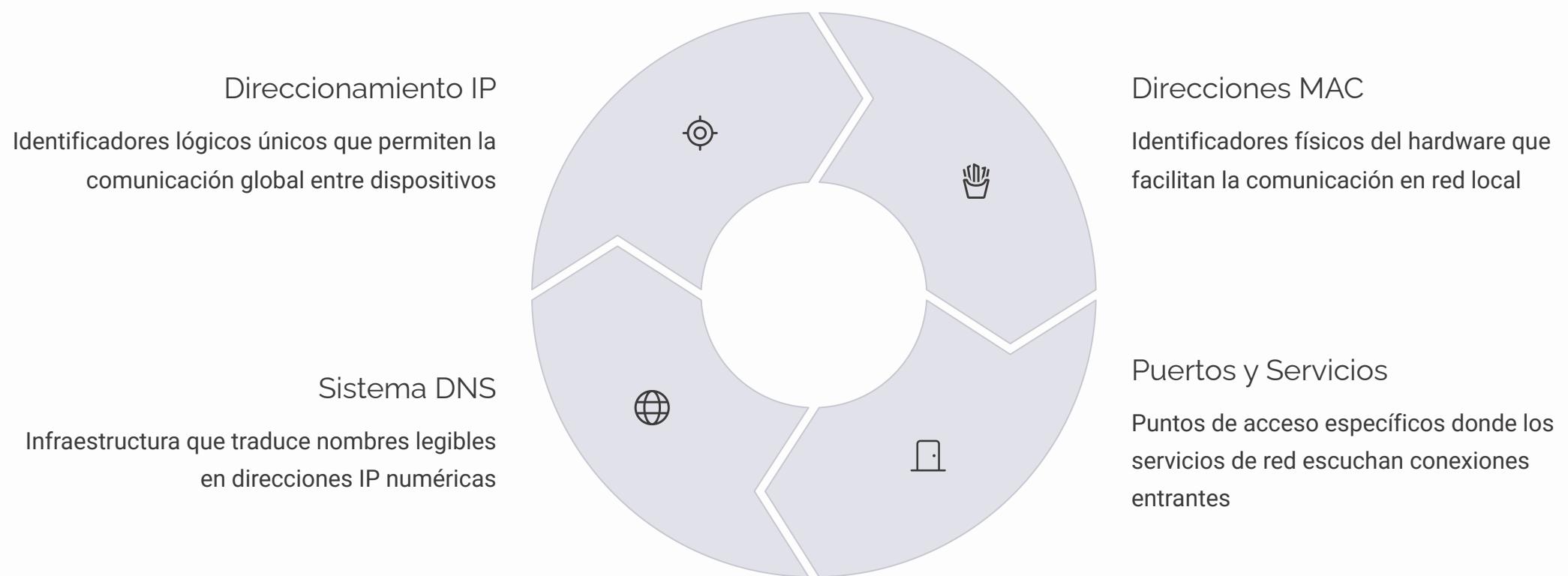
### Consideración de Seguridad:

Tu IP pública puede revelar tu ubicación geográfica aproximada y proveedor de Internet. En contextos de anonimato, considera el uso de VPNs o redes Tor para enmascarar tu verdadera IP pública.

Las herramientas de reconocimiento como nmap operan de manera diferente dependiendo de si estás escaneando IPs privadas (dentro de tu red local) o IPs públicas (a través de Internet), ya que las técnicas de detección y las respuestas del sistema varían significativamente entre estos dos entornos.

# Resumen:

Hemos recorrido los pilares fundamentales que sostienen toda la arquitectura de redes modernas. Estos conceptos no son simplemente teóricos: son las herramientas prácticas que utilizarás diariamente en tu carrera como especialista en ciberseguridad.



Las **herramientas de línea de comandos** que hemos explorado (`ip`, `arp`, `ss`, `dig`, `curl`) forman el arsenal básico de cualquier profesional de redes y seguridad. Dominar estas herramientas te permitirá diagnosticar problemas, realizar reconocimiento y entender el comportamiento de las redes en tiempo real.

En la próxima sesión, aplicaremos estos conocimientos fundamentales para adentrarnos en técnicas más avanzadas de reconocimiento activo y análisis de tráfico, donde verás cómo estos conceptos cobran vida en escenarios reales de evaluación de seguridad.

- ✓ **Próximo Paso:** Practica estos comandos en tu entorno local y observa cómo interactúan los diferentes componentes de red que hemos estudiado hoy.

# Protocolos y Reconocimiento Activo con nmap



# ¿Cómo se Envían los Datos?

En el mundo de las redes, existen dos protocolos fundamentales que gobiernan cómo se transportan los datos: TCP y UDP. Cada uno tiene características únicas que los hacen ideales para diferentes tipos de aplicaciones.

## TCP - Transmission Control Protocol

**Orientado a la conexión** - Establece una conexión antes de transmitir datos

**Fiable y ordenado** - Garantiza que todos los datos lleguen sin errores y en el orden correcto

**Three-way handshake** - Proceso de establecimiento de conexión mediante intercambio SYN/ACK

- Navegación web (HTTP/HTTPS)
- Correo electrónico (SMTP, IMAP)
- Transferencia de archivos (FTP)
- Conexiones SSH

## UDP - User Datagram Protocol

**Sin conexión** - Envía datos directamente sin establecer conexión previa

**Rápido y eficiente** - Menor overhead, pero sin garantías de entrega

**"Dispara y olvida"** - No verifica si los datos llegaron correctamente

- Resolución DNS
- Streaming de video y audio
- Juegos online multijugador
- Servicios de tiempo (NTP)

La elección entre TCP y UDP depende de las necesidades específicas de cada aplicación: ¿necesitas garantía de entrega o prefieres velocidad?

# Estableciendo una Conexión Fiable

El proceso de three-way handshake es fundamental para entender cómo TCP establece conexiones seguras y fiables. Este mecanismo es también la base de muchas técnicas de escaneo que utilizaremos con nmap.

01

**SYN - Synchronize**

El cliente inicia la conexión enviando un paquete SYN al servidor. Este paquete incluye un número de secuencia inicial aleatorio que servirá para ordenar los datos posteriores.

**Estado del cliente:** SYN-SENT

02

**SYN/ACK - Synchronize/Acknowledge**

El servidor responde con un paquete SYN/ACK, confirmando que recibió la solicitud y proporcionando su propio número de secuencia inicial.

**Estado del servidor:** SYN-RECEIVED

03

**ACK - Acknowledge**

El cliente envía un ACK final confirmando que recibió la respuesta del servidor. En este punto, la conexión queda completamente establecida y pueden comenzar a intercambiarse datos.

**Estado de ambos:** ESTABLISHED

- Nota para pentesting:** Los escaneos de nmap explotan este mecanismo. Por ejemplo, un escaneo SYN envía paquetes SYN pero no completa el handshake, lo que lo hace más silencioso y rápido.

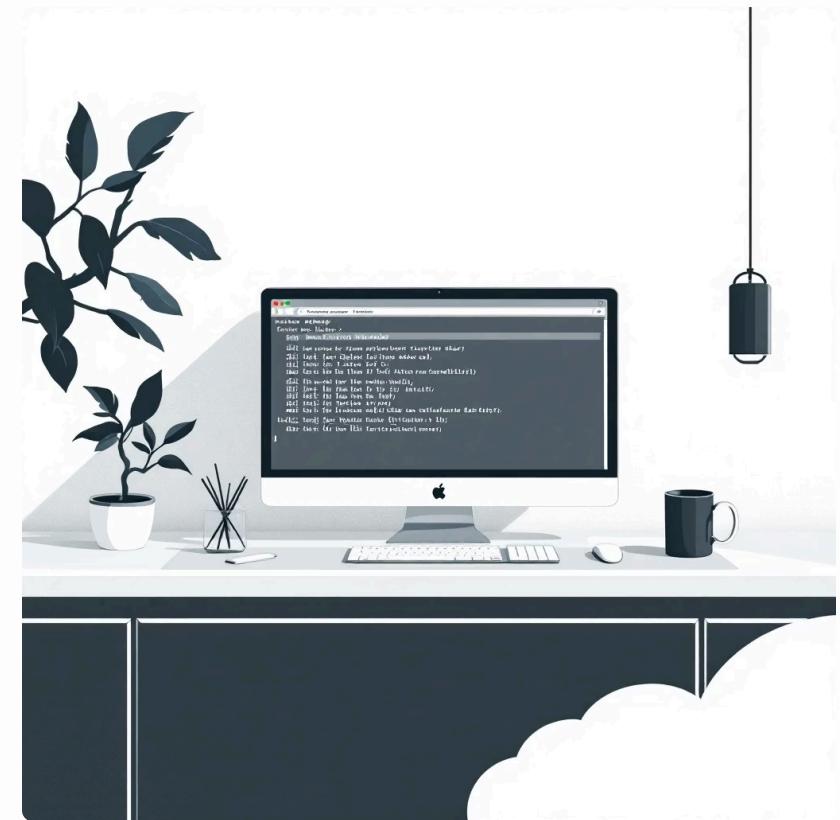
# Network Mapper:

nmap (Network Mapper) es indiscutiblemente la herramienta más importante en el arsenal de cualquier profesional de ciberseguridad. Desarrollada por Gordon Lyon (Fyodor) desde 1997, se ha convertido en el estándar de la industria para el descubrimiento de redes y la auditoría de seguridad.

Esta potente herramienta nos permite realizar una amplia gama de tareas de reconocimiento:

- **Descubrimiento de hosts activos** en rangos de red específicos
- **Identificación de puertos abiertos** en sistemas objetivo
- **Detección de servicios** y sus versiones exactas
- **Identificación del sistema operativo** del objetivo
- **Ejecución de scripts personalizados** para pruebas específicas

Toda la magia de nmap se ejecuta desde la **terminal**, lo que la convierte en una herramienta extremadamente poderosa y scriptable para automatizar tareas de reconocimiento.



"nmap es como tener rayos X para ver a través de las redes. Te muestra qué está vivo, qué puertas están abiertas, y qué secretos se esconden detrás de cada IP."

**Importante:** nmap debe usarse únicamente en redes propias o con autorización explícita. El uso no autorizado puede tener consecuencias legales graves.

# ¿Quién está vivo en la red?

Antes de comenzar cualquier escaneo de puertos, es fundamental realizar un reconocimiento inicial para identificar qué dispositivos están activos en la red. Esta fase de descubrimiento de hosts es crucial para optimizar nuestros esfuerzos posteriores.

1

Comando Principal

```
nmap -sn 192.168.1.0/24
```

El flag **-sn** indica a nmap que realice únicamente un "Ping Scan" sin escanear puertos. Esto hace que el proceso sea mucho más rápido y menos intrusivo.

2

¿Qué hace internamente?

- Envía paquetes ICMP Echo Request (ping tradicional)
- Intenta conexiones TCP a los puertos 80 y 443
- Envía paquetes ARP si está en la misma red local
- Utiliza timestamp requests como método alternativo

3

Interpretando Resultados

nmap mostrará una lista de las IPs que respondieron, indicando que están "up" (activas). También proporcionará información sobre direcciones MAC si está en la red local.

**Ejemplo de salida:**

```
Nmap scan report for 192.168.1.1  
Host is up (0.0012s latency).
```

- Consejo práctico:** Si trabajas con rangos de red muy grandes, puedes usar el flag `--min-rate` para acelerar el escaneo, por ejemplo: `nmap -sn --min-rate 1000 192.168.1.0/24`

# Estados de los Puertos

Interpretar correctamente la salida de nmap es fundamental para tomar decisiones informadas durante una evaluación de seguridad. nmap clasifica los puertos en diferentes estados según la respuesta (o falta de respuesta) del sistema objetivo.

## OPEN (Abierto)

**Significado:** El puerto está abierto y hay un servicio activamente escuchando y aceptando conexiones.

**Respuesta TCP:** SYN/ACK al paquete SYN inicial

**Acción recomendada:** ¡Este es nuestro objetivo principal! Investiga qué servicio se está ejecutando y su versión.

**Implicaciones de seguridad:** Representa una superficie de ataque potencial que debe ser evaluada.

## CLOSED (Cerrado)

**Significado:** El puerto es accesible (no bloqueado por firewall), pero no hay ningún servicio escuchando en él.

**Respuesta TCP:** RST/ACK (Reset) al paquete SYN

**Acción recomendada:** Generalmente no es interesante desde el punto de vista de la seguridad, pero confirma que el host está activo.

**Información útil:** Puede indicar que un servicio fue deshabilitado recientemente.



## FILTERED (Filtrado)

**Significado:** nmap no puede determinar el estado del puerto porque un filtro (firewall, router, etc.) está bloqueando los paquetes.

**Respuesta TCP:** Sin respuesta o mensaje ICMP de error

**Acción recomendada:** Prueba diferentes técnicas de escaneo o considera métodos de evasión de firewall.

**Nota importante:** Podría ocultar servicios que realmente están ejecutándose.



**⚠️ Estados menos comunes:** También existen los estados "open|filtered" (nmap no puede distinguir entre abierto y filtrado) y "closed|filtered" (típico en escaneos UDP). Estos requieren técnicas de escaneo más específicas para clarificar.

# ¿Qué software se está ejecutando?

Identificar la versión exacta del software que se ejecuta en los puertos abiertos es **CRUCIAL** para cualquier evaluación de seguridad. Las versiones antiguas frecuentemente contienen vulnerabilidades conocidas que pueden ser explotadas por atacantes.

## Detección de Servicios y Versiones

```
nmap -sV <IP_objetivo>
```

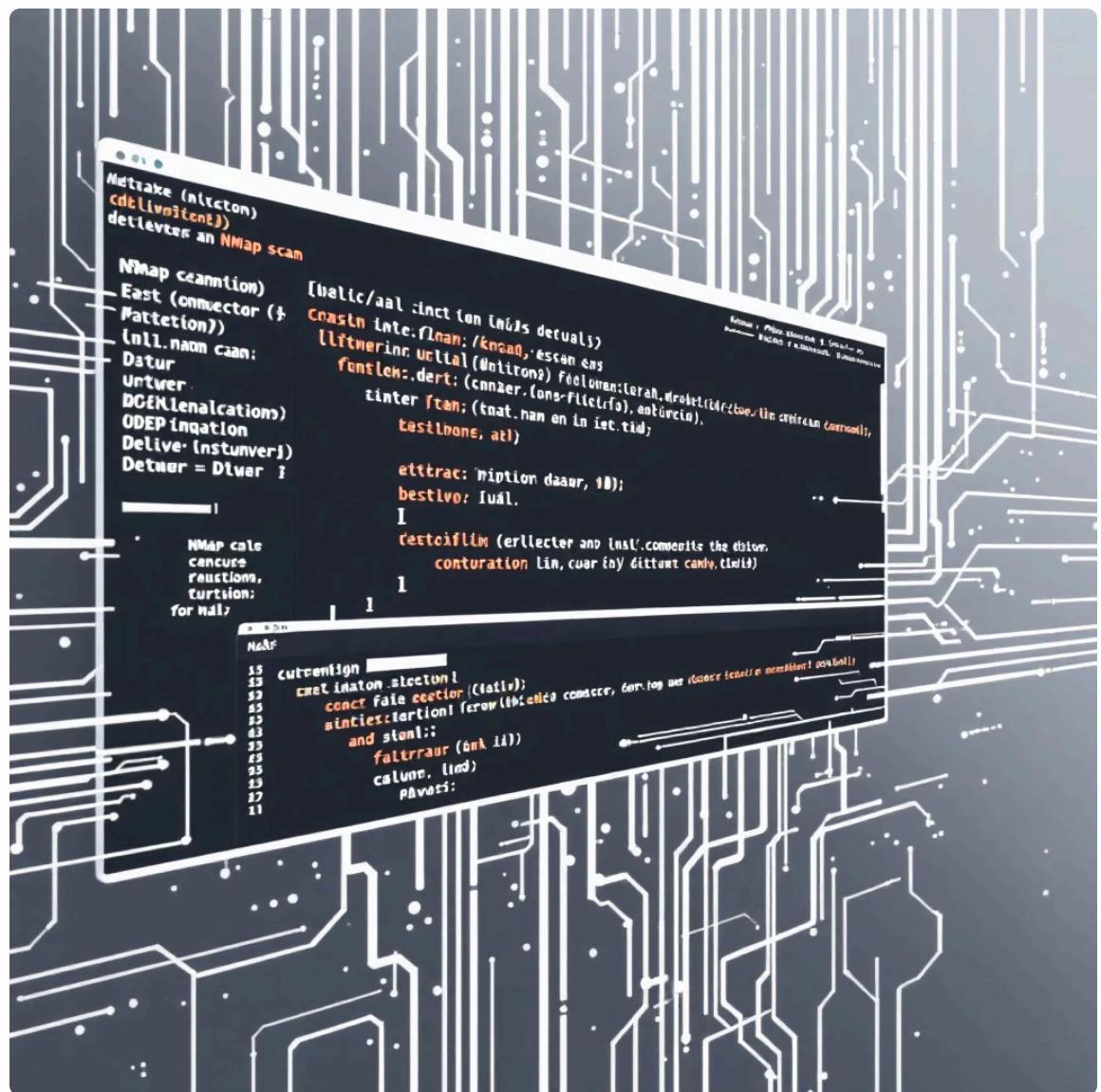
El flag **-sV** activa la detección de versiones, haciendo que nmap:

- Se conecte a puertos abiertos
- Envíe probes específicos para cada servicio
- Analice las respuestas para identificar el software
- Compare las huellas digitales con su base de datos

Intensidad del escaneo:

Puedes controlar la intensidad con **--version-intensity** (0-9):

- **0:** Solo probes ligeros
- **5:** Intensidad por defecto
- **9:** Todos los probes disponibles



Ejemplo de salida detallada:

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.4
80/tcp	open	http	Apache 2.4.41
443/tcp	open	https	Apache 2.4.41
3306/tcp	open	mysql	MySQL 5.7.32

Información adicional obtenida:

- **Nombre del servicio**
- **Versión específica**
- **Sistema operativo** (cuando es posible)
- **Información del hostname**
- **Detalles de configuración**

**⚠️ ¡Importante!** El escaneo **-sV** es más lento y "ruidoso" que un escaneo básico. Genera más tráfico de red y es más fácil de detectar por sistemas de monitoreo. Úsalo conscientemente en entornos de producción.

**Consejo profesional:** Combina **-sV** con **-sC** para ejecutar scripts de detección: `nmap -sV -sC target_ip`

# Obteniendo Más Información

Cuando necesitamos realizar un reconocimiento exhaustivo de un objetivo, nmap ofrece el modo "agresivo" que combina múltiples técnicas de escaneo en una sola ejecución. Este modo es ideal para evaluaciones de seguridad completas.



## Detección de Sistema Operativo

nmap analiza las características únicas de las respuestas TCP/IP de cada sistema operativo. Examina campos como el TTL, window size, y opciones TCP para crear una "huella digital" del OS.

**Precisión típica:** 85-95% en sistemas comunes



## Nmap Scripting Engine (NSE)

Ejecuta scripts en Lua que pueden detectar vulnerabilidades específicas, obtener información adicional de servicios, e incluso realizar algunos ataques básicos.

**Scripts incluidos por defecto:** Más de 600 scripts disponibles



## Traceroute

Muestra la ruta que toman los paquetes desde tu máquina hasta el objetivo, revelando routers intermedios y posibles puntos de filtrado.

**Información valiosa:** Topología de red y posibles cuellos de botella

## Comando del Modo Agresivo

```
nmap -A <IP_objetivo>
```

El flag **-A** equivale a usar **-sV -sC -O --traceroute** simultáneamente.

### Ventajas del modo -A:

- Información completa en una sola ejecución
- Ideal para evaluaciones de seguridad completas
- Detecta configuraciones inseguras automáticamente
- Proporciona contexto detallado del objetivo

### Consideraciones importantes:

- Genera mucho tráfico de red
- Fácilmente detectable por IDS/IPS
- Puede tomar considerable tiempo
- Algunos scripts pueden ser intrusivos

# Práctica y Síntesis del Reconocimiento con nmap

Hemos recorrido un camino completo desde los fundamentos de los protocolos de transporte hasta el dominio de nmap como herramienta de reconocimiento. Es momento de consolidar todo este conocimiento con una práctica estructurada y un resumen de los conceptos clave.

01

## Preparación del Entorno

Identifica un objetivo legítimo para practicar. Puedes usar:

- Una máquina virtual como Metasploitable
- Tu propia red doméstica
- Laboratorios online como TryHackMe o HackTheBox

**¡NUNCA escanees sistemas sin autorización!**

02

## Reconocimiento Básico

```
nmap <IP_objetivo>
```

Ejecuta un escaneo básico para identificar puertos abiertos. Analiza qué servicios están disponibles y toma notas sobre los hallazgos.

03

## Detección Avanzada

```
nmap -sV <IP_objetivo>
```

Ejecuta la detección de versiones. Compara los resultados con el escaneo anterior. ¿Qué información nueva obtuviste? ¿Hay versiones desactualizadas?

04

## Análisis Completo

```
nmap -A <IP_objetivo>
```

Realiza un escaneo agresivo completo. Documenta toda la información obtenida: OS, scripts ejecutados, rutas de red, y servicios detallados.

## Resumen de Conceptos Clave

### Protocolos de Transporte

- **TCP:** Orientado a conexión, fiable (HTTP, SSH, FTP)
- **UDP:** Sin conexión, rápido (DNS, streaming)
- **Three-way handshake:** SYN → SYN/ACK → ACK

### Comandos nmap Esenciales

- `nmap -sn` - Descubrimiento de hosts
- `nmap -sV` - Detección de versiones
- `nmap -A` - Escaneo agresivo completo
- `nmap -T4` - Control de velocidad

### Estados de Puertos

- **Open:** Servicio activo escuchando
- **Closed:** Puerto accesible, sin servicio
- **Filtered:** Bloqueado por firewall

# Análisis de Tráfico y Conceptos de Ataque

Explorando las técnicas pasivas de reconocimiento y los fundamentos de los ataques de red. Desde el análisis de paquetes hasta las metodologías de explotación, descubriremos cómo los atacantes aprovechan las vulnerabilidades de la comunicación en red.



# ¿Qué pasa si no podemos escanear?

## Las Limitaciones del Reconocimiento Activo

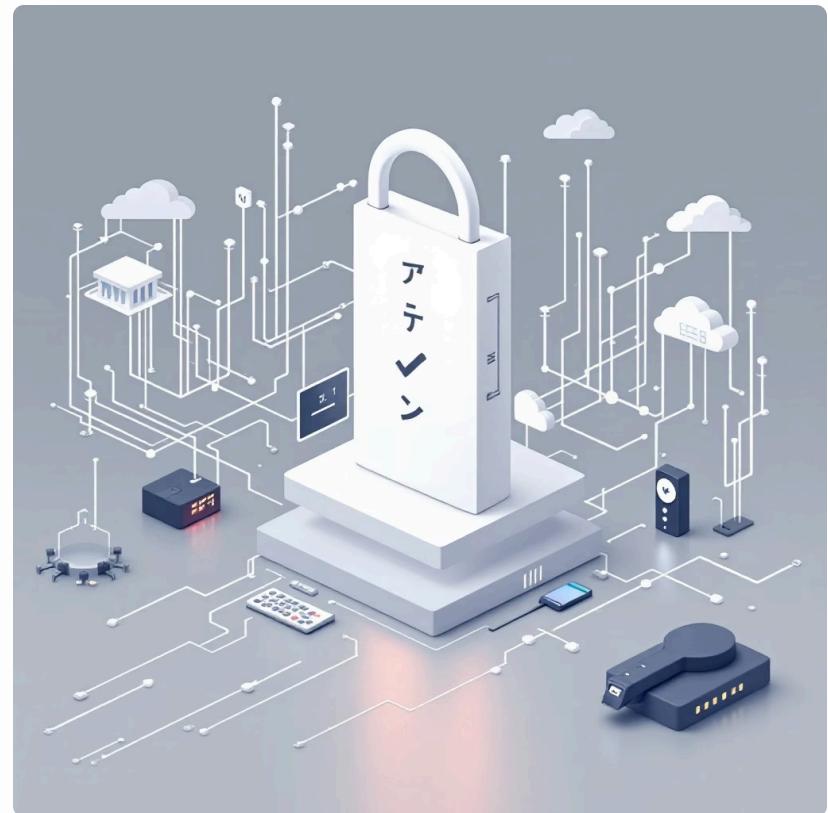
El reconocimiento activo con herramientas como **nmap** es extremadamente efectivo, pero presenta un problema fundamental: es "**ruidoso**" desde la perspectiva de la detección.

Cuando ejecutamos escaneos de puertos o fingerprinting de servicios, estamos enviando múltiples paquetes hacia el objetivo, lo que puede activar sistemas de seguridad como:

- **IDS (Intrusion Detection Systems)**: Detectan patrones de escaneo sospechosos
- **Firewalls**: Pueden bloquear nuestra IP después de detectar actividad anómala
- **Rate limiting**: Los servicios pueden implementar límites de velocidad
- **Logs de seguridad**: Nuestras actividades quedan registradas para análisis forense

## La Solución: Reconocimiento Pasivo

El análisis pasivo nos permite **observar sin ser observados**. En lugar de enviar paquetes propios, simplemente escuchamos y analizamos el tráfico existente en la red, manteniéndonos invisibles ante los sistemas de detección.



**⚠ Importante:** En entornos de producción, siempre solicita autorización antes de realizar cualquier tipo de reconocimiento, incluso pasivo.

# Wireshark:



## ¿Qué es Wireshark?

Wireshark es el analizador de protocolos de red más utilizado en el mundo. Nos permite capturar el tráfico que pasa por nuestra interfaz de red y examinar cada paquete individualmente, desde la capa física hasta la aplicación.



## Interfaz Gráfica Potente

Aunque es una herramienta con interfaz gráfica intuitiva, la iniciaremos desde la terminal para mantener consistencia con nuestro flujo de trabajo. Su GUI nos permite análisis detallado con filtros avanzados y visualizaciones.

Wireshark decodifica automáticamente cientos de protocolos, desde HTTP y DNS hasta protocolos industriales especializados. Su capacidad de **disección profunda de paquetes** nos permite entender exactamente qué información está viajando por la red, convirtiéndolo en una herramienta esencial tanto para administradores de red como para profesionales de ciberseguridad.

La herramienta nos proporciona una vista en tres paneles: lista de paquetes, detalles del protocolo y datos en hexadecimal/ASCII, permitiendo un análisis completo desde múltiples perspectivas.

# Preparando la Captura desde la Terminal

## Identificando la Interfaz de Red

Antes de iniciar cualquier captura con Wireshark, es fundamental identificar correctamente la interfaz de red sobre la cual queremos monitorear el tráfico. Linux proporciona varias formas de obtener esta información.

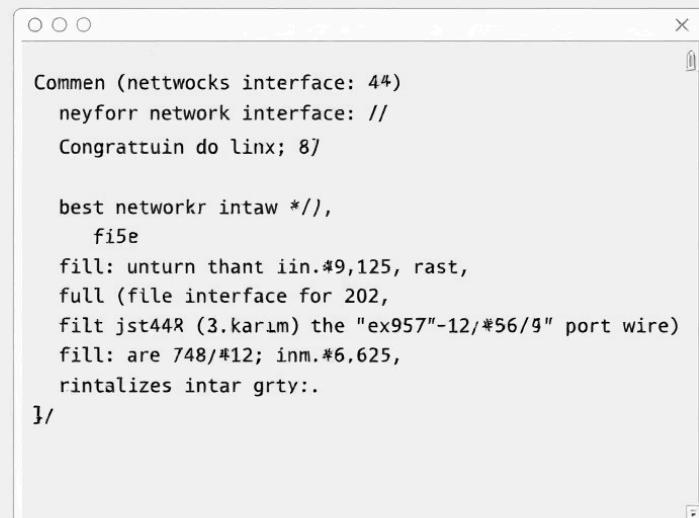
## Comando Esencial

```
ip addr show
```

Este comando nos mostrará todas las interfaces de red disponibles en el sistema, junto con su estado y configuración. Buscaremos:

- **eth0**: Interfaz Ethernet cableada
- **wlan0**: Interfaz Wi-Fi inalámbrica
- **lo**: Interfaz de loopback (tráfico interno)

Identifica la interfaz que esté **UP** y tenga una dirección IP asignada. Este será el nombre que seleccionaremos en Wireshark para iniciar la captura.



```
Commen (nettworks interface: 44)
neyforr network interface: //
Congrattein do linx; 8)

best networkr intaw */,
fi5e
fill: unturn than iin.#9,125, rast,
full (fille interface for 202,
filt jst448 (3.karum) the "ex957"-12/*56/9" port wire)
fill: are 748/#12; inm.#6,625,
rintalizes intar grty:.

1/
```

## Alternativas Útiles

También puedes usar:

- **ifconfig** (si está instalado)
- **ip link show** (solo interfaces)
- **nmcli dev status** (NetworkManager)

# DEMO EN VIVO con Wireshark

## Viendo el Tráfico HTTP en Texto Plano



### Iniciar Captura

Abre Wireshark desde la terminal y selecciona la interfaz de red identificada anteriormente (eth0, wlan0, etc.). La captura comenzará inmediatamente mostrando todos los paquetes en tiempo real.

### Generar Tráfico HTTP

En tu navegador, visita una página **HTTP** (no HTTPS). Un excelente ejemplo es <http://neverssl.com>, diseñado específicamente para pruebas de conectividad sin cifrado.

### Detener y Filtrar

Detén la captura y aplica el filtro `http` en la barra de filtros. Esto mostrará únicamente el tráfico HTTP, eliminando el ruido de otros protocolos.

### Resultado Impactante

Podrás ver las peticiones GET completas y las respuestas del servidor, incluyendo todo el HTML, cookies, y headers en **texto completamente legible**. Esta demostración visual ilustra dramáticamente el riesgo del tráfico no cifrado.

Este ejercicio práctico demuestra por qué HTTP es considerado inseguro en entornos modernos. Cualquier persona con acceso a la red puede interceptar y leer toda la comunicación, incluyendo formularios, credenciales, y datos sensibles.

# La Importancia del Cifrado: HTTPS

## HTTP: La Vulnerabilidad Expuesta

**HTTP (HyperText Transfer Protocol)** transmite toda la información en texto plano, sin ningún tipo de protección criptográfica. Esto significa que:

- Las credenciales de usuario son visibles
- Los datos del formulario pueden ser interceptados
- Las cookies de sesión quedan expuestas
- Todo el contenido es susceptible al "sniffing"

Esta vulnerabilidad fundamental convierte HTTP en un protocolo **totalmente inadecuado** para cualquier comunicación que contenga información sensible.

## HTTPS: La Protección Criptográfica

**HTTPS (HTTP Secure)** utiliza TLS/SSL para crear un túnel cifrado entre cliente y servidor. Cuando captures tráfico HTTPS en Wireshark, solo verás:

- Datos completamente ilegibles (cifrados)
- Handshakes criptográficos
- Certificados digitales
- Metadata de conexión (pero no contenido)

El cifrado TLS moderno (v1.2 y v1.3) proporciona confidencialidad, integridad y autenticación, haciendo prácticamente imposible la interceptación de datos.

### ✓ Lección Crítica de Seguridad

Siempre verifica el **candado verde** en tu navegador antes de introducir información sensible. Es tu primera línea de defensa contra la interceptación de datos.

# Conceptos de Ataques de Red

## Explotando el Conocimiento Adquirido

### Sniffing (Espionaje)

**Definición:** Captura y análisis pasivo del tráfico de red, exactamente lo que practicamos con Wireshark.

**Impacto:** Permite interceptar credenciales, datos sensibles, y patrones de comunicación sin que la víctima lo detecte.

**Defensa:** Cifrado end-to-end, VPNs, y segmentación de red.

### Spoofing (Suplantación)

**Definición:** Falsificación de direcciones IP, MAC, o identidades para hacerse pasar por otro sistema legítimo.

**Variantes:** ARP spoofing, IP spoofing, DNS spoofing, email spoofing.

**Defensa:** Autenticación robusta, monitoreo de ARP, y validación de origen.

### Denial of Service (DoS)

**Definición:** Inundación de un servicio con tráfico malicioso para volverlo inaccesible para usuarios legítimos.

**Evolución:** DDoS (distribuido), amplificación DNS, y ataques de capa 7.

**Defensa:** Rate limiting, CDNs, y sistemas anti-DDoS.

Estos ataques representan las técnicas fundamentales que los atacantes utilizan para comprometer redes. Comprender sus mecanismos nos permite implementar defensas más efectivas y detectar actividad maliciosa en nuestros sistemas.

# El Flujo Completo de un Ataque

## De la Información a la Explotación



### 1. Reconocimiento

Utilizamos herramientas como **dig** para recopilar información DNS, e **nmap** para descubrir servicios activos, puertos abiertos y versiones específicas de software ejecutándose en el objetivo.

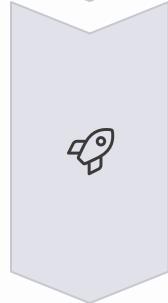
**Ejemplo:** Descubrimos Apache 2.4.29 ejecutándose en el puerto 80.



### 2. Análisis de Vulnerabilidades

Investigamos si las versiones de software identificadas tienen vulnerabilidades conocidas registradas en bases de datos como **CVE** (**Common Vulnerabilities and Exposures**).

**Ejemplo:** Apache 2.4.29 tiene CVE-2021-41773 (Path Traversal).



### 3. Explotación

Utilizamos frameworks como **Metasploit** o desarrollamos exploits personalizados para aprovechar las vulnerabilidades identificadas y obtener acceso no autorizado al sistema.

**Próximos cursos:** Técnicas avanzadas de explotación y post-explotación.

Esta metodología sistemática es la base del **pentesting ético** y la evaluación de seguridad. Cada fase construye sobre la anterior, creando un enfoque estructurado para identificar y explotar vulnerabilidades de manera controlada y documentada.

# Resumen de la Clase

## Lo que Aprendimos Hoy

### Estructura de Redes

Analizamos la arquitectura completa de las comunicaciones de red, desde el direccionamiento físico (MAC) hasta los protocolos de transporte (TCP/UDP), comprendiendo cómo interactúan las diferentes capas.

### Fundamentos de Seguridad

Establecimos los conceptos básicos de ataques de red (sniffing, spoofing, DoS) y las defensas correspondientes, creando una base sólida para el análisis de riesgos de red.



Esta clase nos ha proporcionado las herramientas fundamentales para entender y analizar las comunicaciones de red desde una perspectiva de ciberseguridad. El conocimiento adquirido nos permite tanto atacar como defender sistemas de red de manera informada y ética.

### Reconocimiento con Nmap

Dominamos el uso profesional de nmap para realizar reconocimiento activo, incluyendo escaneos de puertos, detección de servicios, fingerprinting de sistemas operativos y evasión básica de firewalls.

### Análisis con Wireshark

Visualizamos el tráfico de red en tiempo real, comprendiendo la diferencia crítica entre comunicaciones cifradas y no cifradas, y las implicaciones de seguridad de cada protocolo.

# ¿Preguntas?

## Espacio Abierto para Dudas

Este es el momento perfecto para resolver cualquier duda que haya surgido durante nuestra exploración de los conceptos de red y ciberseguridad. Algunas áreas comunes donde suelen aparecer preguntas:

- **Configuración de Nmap:** Parámetros avanzados, interpretación de resultados, técnicas de evasión
- **Uso de Wireshark:** Filtros específicos, análisis de protocolos complejos, exportación de datos
- **Conceptos de red:** Diferencias entre protocolos, funcionamiento de NAT, subnetting
- **Ética en ciberseguridad:** Límites legales, mejores prácticas, responsible disclosure
- **Próximos pasos:** Recursos adicionales, laboratorios prácticos, certificaciones

## Conectando con la Clase 4

En nuestra próxima y última sesión, integraremos todo lo aprendido: desde el dominio del **sistema operativo** hasta las **comunicaciones de red**, construyendo una metodología completa de pentesting y principios fundamentales de ciberseguridad.



### ② Recursos Adicionales

¿Quieres profundizar más?

- Laboratorios de Wireshark online
- Challenges de Nmap en HackTheBox
- Documentación oficial de protocolos