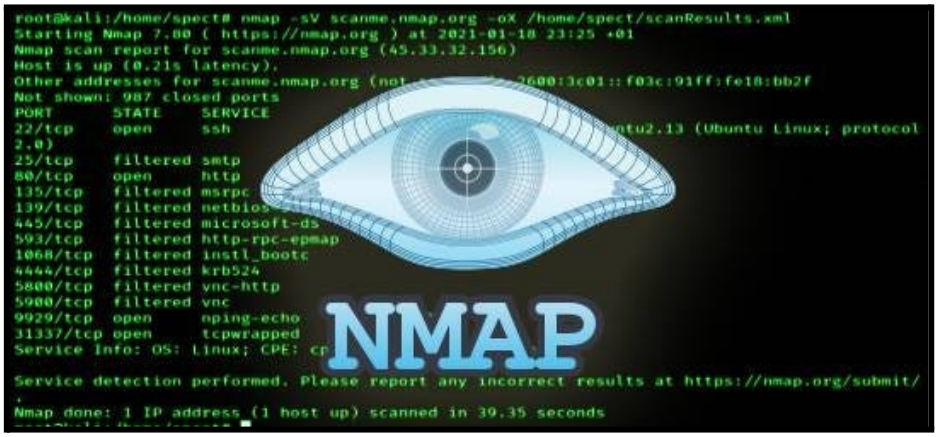
Nmap: Exploración y Auditoría de Redes
Introducción a Nmap



Nmap es una herramienta de red de código abierto que permite a los administradores de sistemas y a los profesionales de seguridad realizar escaneos de red detallados. Al enviar paquetes IP especialmente diseñados a los hosts de destino y analizar las respuestas, Nmap puede revelar una gran cantidad de información sobre un sistema o red, incluyendo:

- Hosts activos: Identifica qué dispositivos están en línea y responden a solicitudes.
- Servicios en ejecución: Detecta los servicios que se están ejecutando en cada host (HTTP, SSH, FTP, etc.).
- Sistemas operativos: Identifica el sistema operativo que ejecuta cada host.
- Vulnerabilidades: Con la ayuda de scripts, puede detectar posibles vulnerabilidades en los sistemas.

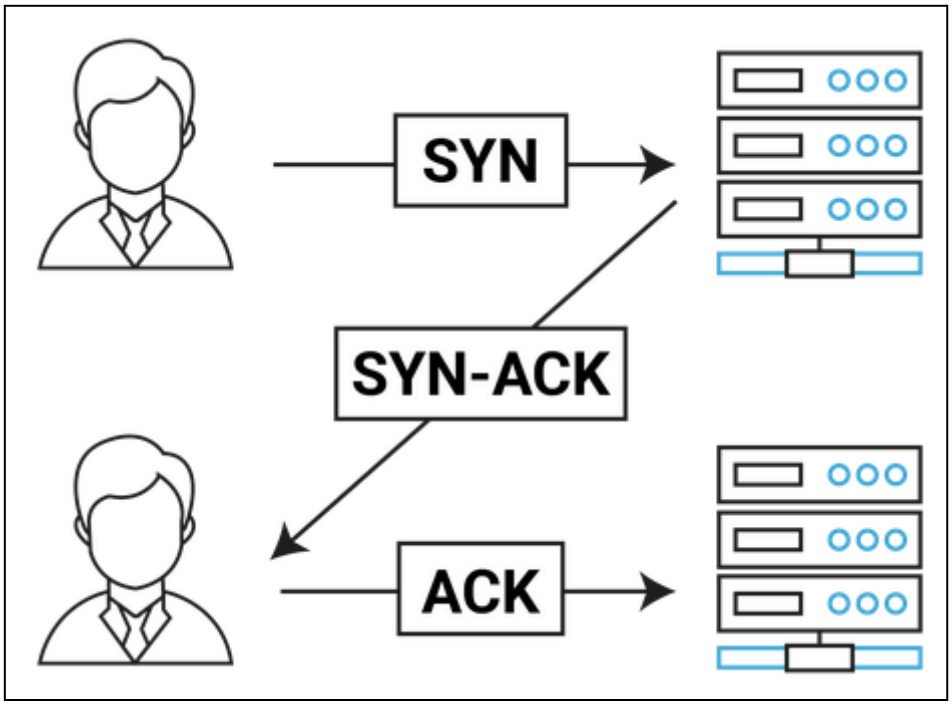
En Nmap, es fundamental entender cómo funcionan los procesos de conexión TCP y UDP, ya que cada protocolo tiene un comportamiento diferente al gestionar conexiones y puertos, lo cual influye en los resultados de los escaneos.

Proceso TCP - *Three-Way Handshake*

El protocolo TCP utiliza un proceso de conexión estructurado llamado *Three-Way Handshake*, que asegura una comunicación confiable entre cliente y servidor. El procedimiento es así:

1. **SYN (Synchronize)**: El cliente inicia la conexión enviando un paquete SYN al servidor, solicitando el inicio de una comunicación.
2. **SYN-ACK (Synchronize-Acknowledge)**: El servidor recibe el SYN y responde con un paquete SYN-ACK, confirmando que está dispuesto a establecer la conexión.
3. **ACK (Acknowledge)**: El cliente responde con un paquete ACK, confirmando la recepción del SYN-ACK. A partir de aquí, la conexión se establece y se pueden intercambiar datos.

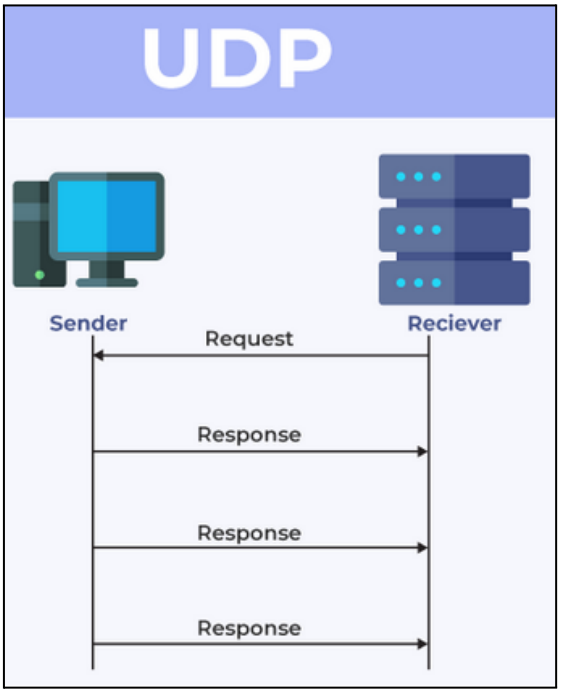
Este proceso es importante porque TCP garantiza que ambos extremos (cliente y servidor) acuerden establecer y mantener la comunicación antes de transferir datos. En Nmap, esto se utiliza para escanear puertos y determinar si están abiertos o cerrados. Por ejemplo, un puerto abierto responderá con un SYN-ACK, mientras que uno cerrado enviará un paquete RST (reset).



Proceso UDP

UDP es diferente de TCP porque no establece una conexión formal. No utiliza el *Three-Way Handshake* ni verifica que los paquetes lleguen a su destino, lo que lo convierte en un protocolo más rápido pero menos confiable. En UDP:

1. El cliente envía un paquete sin esperar confirmación de que fue recibido.
2. Si el puerto está abierto, es posible que no haya ninguna respuesta, ya que UDP no necesita confirmar la recepción.
3. Si el puerto está cerrado, el servidor normalmente envía un mensaje ICMP "Destination Unreachable".



Importancia de Conocer Ambos Procesos en Nmap

Conocer cómo funcionan TCP y UDP es vital porque determina cómo se comportan los puertos en los escaneos de Nmap:

- **TCP**: Los escaneos TCP, como el *SYN Scan*, aprovechan el *Three-Way Handshake* para detectar puertos abiertos, filtrados o cerrados. Esto permite obtener resultados más detallados y precisos sobre qué servicios están activos.
- **UDP**: Los escaneos UDP, en cambio, son más difíciles de interpretar, ya que la ausencia de respuesta puede significar que el puerto está abierto o simplemente que no se genera respuesta. Esto hace que los escaneos UDP sean más lentos y menos confiables.

Conocer la diferencia entre ambos tipos de puertos ayuda a adaptar los escaneos a los servicios que estés investigando, ya que algunos utilizan TCP (como HTTP y FTP) y otros UDP (como DNS o DHCP).

1. Escaneos Básicos de Puertos

Comenzamos con lo más esencial: los escaneos de puertos para identificar qué puertos están abiertos y qué servicios están corriendo.

- **TCP**: `nmap -p` — Escanea los puertos TCP especificados.
- **UDP**: `nmap -sU -p` — Escanea los puertos UDP especificados.
- `-p`: Escanea todos los puertos disponibles (65535).
- `--open`: Solo muestra los puertos abiertos en el objetivo, filtrando los cerrados o filtrados.

2. Escaneos Básicos de Dispositivos Activos y Servicios

Opciones que permiten identificar los dispositivos activos en la red y obtener información básica de los servicios que corren en ellos.

- `-sn`: Detecta dispositivos activos sin escanear puertos, útil para obtener un panorama rápido de los hosts en la red.
- `-sC`: Ejecuta scripts básicos que detectan vulnerabilidades comunes y servicios básicos en los puertos abiertos.
- `-sV`: Detecta las versiones de los servicios que están corriendo en los puertos abiertos.

3. Resolución de DNS y Modificaciones de Escaneo

Opciones que optimizan el escaneo al controlar la resolución de nombres de dominio y ajustar el comportamiento de Nmap.

- `-n`: No realiza resolución de DNS, acelerando el escaneo al evitar la consulta de nombres de host.
- `-Pn`: Deshabilita el descubrimiento de host mediante ping, útil cuando los pings están bloqueados o para evitar ser detectado por el objetivo.

4. Escaneos SYN y TCP

Estos son métodos más avanzados para escanear puertos TCP. El escaneo SYN es rápido y sigiloso, mientras que el escaneo TCP es más completo, pero también más detectable.

- `-sS`: Realiza un *SYN Scan*, un escaneo rápido que no completa el *Three-Way Handshake*, ideal para descubrir puertos abiertos de manera eficiente.
- `-sT`: Realiza un escaneo TCP completo, estableciendo la conexión completa con el objetivo (menos sigiloso que el *SYN Scan*).

5. Control de Velocidad y Tiempo de Escaneo

Opciones que permiten ajustar la rapidez del escaneo, lo cual es crucial en redes grandes o entornos sensibles.

- `-t5`: Configura Nmap para el modo más rápido, pero genera más tráfico y es más intrusivo.
- `--min-rate`: Especifica el número mínimo de paquetes que Nmap enviará por segundo.
- `--min-rate 5000`: Asegura que Nmap no envíe menos de 5000 paquetes por segundo, acelerando el escaneo.
- `--min-rtt-timeout`: Define el tiempo mínimo que Nmap espera por las respuestas, optimizando la eficiencia.
- `--max-rtt-timeout`: Define el tiempo máximo antes de que Nmap considere que un paquete está perdido.

6. Escaneos Silenciosos y Sigilosos

Estas opciones permiten realizar escaneos discretos, reduciendo la probabilidad de ser detectado por firewalls o sistemas de detección de intrusos (IDS).

- `-Pn`: Desactiva el ping de descubrimiento de host, útil para evitar ser bloqueado por firewalls o IDS.
- `--min-rtt-timeout 50ms --max-rtt-timeout 300ms`: Ajusta los tiempos de respuesta para minimizar la posibilidad de ser detectado.
- `--scan-delay 100ms`: Introduce un pequeño retraso entre el envío de paquetes para evitar saturar la red o activar sistemas de alerta.
- `-f`: Fragmenta los paquetes enviados, lo que puede evadir ciertos firewalls o IDS que no pueden reconstruir los fragmentos.

Ejemplo de escaneo sigiloso:

- `nmap -Pn -n -sS -p- --open -sC 10.10.11.130 -vvv`

7. Opciones de Evasión y Avanzadas para Seguridad

Estas opciones están diseñadas para evitar detección y minimizar la interferencia en las redes objetivo, ideales para situaciones donde necesitas evitar medidas de seguridad.

- `-f`: Fragmenta los paquetes enviados para evitar la detección por IDS o firewalls.
- `--scan-delay 100ms`: Añade un retraso entre el envío de paquetes para evitar activar alarmas de seguridad.

Diferencia clave:

- **SYN Scan (-sS)**: No completa el *Three-Way Handshake*, por lo que es más rápido y menos detectable que el escaneo TCP completo.
- **TCP Scan (-sT)**: Completa el *Three-Way Handshake*, lo que lo hace más detectable, pero también más detallado en la información que recopila.

Escaneos Avanzados y Personalizados

1. Escaneo de rangos de IP: nmap -sS 192.168.1.1-254
2. Escaneo de una red completa: nmap -sS 192.168.1.0/24
3. Escaneo de puertos específicos: nmap -sS -p 22,80,443 192.168.1.100
4. Detección de sistemas operativos: nmap -O -sV 192.168.1.100
5. Escaneo de vulnerabilidades: nmap -sV -sC -p- 192.168.1.100
6. Escaneo UDP: nmap -sU -p 53,123 192.168.1.100
7. Escaneo silencioso: nmap -Pn -n -sS -p- -oG output.txt 192.168.1.100

OPCIONES CLAVES:

-sS: Escaneo TCP SYN (más rápido y menos intrusivo).
-sT: Escaneo TCP Connect (más lento pero más confiable).
-sU: Escaneo UDP.
-sV: Determina la versión del servicio.
-sC: Realiza una serie de scripts para detectar vulnerabilidades comunes.
-O: Detección del sistema operativo.
-p: Especifica los puertos a escanear.
-oG: Guarda los resultados en formato grepeable.
-oN: Guarda los resultados en formato normal.
-oX: Guarda los resultados en formato XML.
-n: No realiza resolución de DNS.
-Pn: No realiza ping.
--min-rate: Establece la velocidad mínima de escaneo.
--max-retries: Establece el número máximo de reintentos.

Detecta un WAF antes de hacer Directory Fuzzing

El directory fuzzing puede ser bloqueado por un WAF (Web Application Firewall). Para evitar esto, verifica si hay un WAF activo con estas herramientas:

wafw00f:

bash

Copiar código

wafw00f http://ejemplo.com

Nmap:

bash

Copiar código

nmap -Pn -p80,443 -T4 --script http-waf-* ejemplo.com

Así podrás ajustar tus pruebas y evitar bloqueos antes de hacer fuzzing.