COMANDOS Y EJERCICIOS PRÁCTICOS

Nmap y Análisis de Redes

Fecha: 15 de febrero de 2026 **Estado:** Documento de Referencia

1. Introducción

El presente documento constituye una guía práctica de comandos y ejercicios para el análisis de redes utilizando Nmap y Wireshark. Se presentan los puertos más comunes, sus estados, y los comandos esenciales para realizar auditorías de red efectivas.

2. Puertos Comunes y Estados al Escanear

La siguiente tabla muestra los puertos TCP más frecuentemente analizados durante un escaneo de red, junto con sus servicios asociados y la interpretación de sus estados.

Puerto	Estado	Servicio	Significado del Estado
21/tcp	open	ftp	El servicio FTP está activo y aceptando conexiones
22/tcp	open	ssh	Acceso remoto habilitado (Secure Shell)
22/tcp	filtered	ssh	Firewall o filtro de red bloquea el puerto
23/tcp	closed	telnet	No hay servicio activo escuchando
25/tcp	open	smtp	Servidor de correo electrónico (Simple Mail Transfer Protocol)
53/tcp	open	domain	Servicio DNS (Domain Name System)
80/tcp	open	http	Servidor web HTTP estándar
143/tcp	open	imap	Servidor de correo IMAP (Internet Message Access Protocol)
443/tcp	open	https	Servidor web seguro con SSL/TLS

3. Estados Comunes en Nmap

Nmap clasifica los puertos en distintos estados según la respuesta obtenida durante el escaneo. A continuación se describen los estados más relevantes:

Estado	Descripción
open	El puerto está abierto y hay un servicio escuchando activamente. Acepta conexiones TCP, datagramas UDP o asociaciones SCTP.
closed	El puerto es accesible (recibe y responde paquetes de prueba de Nmap), pero no hay ninguna aplicación escuchando en él.
filtered	Nmap no puede determinar si el puerto está abierto debido a un filtrado de paquetes (firewall, reglas de router, IDS/IPS, etc.).
open—filtered	Estado ambiguo típico en escaneos UDP. Nmap no puede determinar si el puerto está abierto o filtrado.
closed—filtered	Nmap no puede determinar si el puerto está cerrado o filtrado. Solo aparece en escaneos IP ID idle.
unfiltered	El puerto es accesible, pero Nmap no puede determinar si está abierto o cerrado. Solo aparece en escaneos ACK.

4. ¿Cuándo un Puerto Aparece como `filtered`?

Un puerto se muestra con estado **filtered** cuando Nmap envía paquetes de prueba pero no recibe respuesta, o recibe un mensaje de error ICMP indicando que el paquete fue descartado. Las causas principales son:

- **Firewall activo:** Reglas de firewall configuradas para descartar o rechazar paquetes a puertos específicos.
- **IDS/IPS:** Sistemas de detección o prevención de intrusiones que bloquean escaneos sospechosos.
- **Reglas de red:** ACLs (Access Control Lists) en routers o switches que restringen el tráfico.
- **Paquetes descartados:** Configuraciones de red que simplemente descartan paquetes sin responder.

Ejemplo de escaneo con puerto filtrado

```
nmap -p 22 10.10.10.1
```

Salida esperada:

```
PORT   STATE    SERVICE
22/tcp filtered ssh
```

5. Comandos Básicos de Nmap

Escaneo simple de host

Escanea los 1000 puertos más comunes de un host específico:

```
nmap 192.168.1.1
```

Escaneo de rango de puertos específicos

```
nmap -p 1-100 192.168.1.1
nmap -p 22,80,443 192.168.1.1
```

Escaneo de todos los puertos

```
nmap -p- 192.168.1.1
```

Detección de servicios y versiones

```
nmap -sV 192.168.1.1
```

Detección de sistema operativo

```
nmap -O 192.168.1.1
```

Escaneo agresivo (OS, versión, scripts, traceroute)

```
nmap -A 192.168.1.1
```

Escaneo sin ping (útil si ICMP está bloqueado)

```
nmap -Pn 192.168.1.1
```

Escaneo UDP

```
sudo nmap -sU 192.168.1.1
```

Guardar resultados en diferentes formatos

```
nmap -oN salida.txt 192.168.1.1      # Formato normal
nmap -oX salida.xml 192.168.1.1      # Formato XML
nmap -oG salida.grep 192.168.1.1     # Formato grepable
nmap -oA salida 192.168.1.1          # Todos los formatos
```

6. Ejercicios Prácticos

Ejercicio 1: Identificación de servicios web

Objetivo: Identificar todos los servidores web en tu red local.

```
# Escanear la subred 192.168.1.0/24 en busca del puerto 80
nmap -p 80 192.168.1.0/24
```

Preguntas:

- ¿Cuántos hosts tienen el puerto 80 abierto?
- ¿Qué versión del servidor web están ejecutando?

Ejercicio 2: Análisis de servicios SSH

Objetivo: Encontrar sistemas con SSH habilitado y determinar su versión.

```
# Escaneo con deteccion de version
nmap -p 22 -sV 192.168.1.0/24
```

Análisis:

- Identificar versiones de SSH obsoletas que puedan tener vulnerabilidades conocidas.
- Verificar si existen sistemas con SSH en puertos no estándar.

Ejercicio 3: Detección de firewall

Objetivo: Determinar si un host tiene un firewall activo.

```
# Escaneo SYN (sigiloso)
sudo nmap -sS 192.168.1.1

# Escaneo ACK (detecta reglas de firewall)
sudo nmap -sA 192.168.1.1
```

Interpretación:

- Puertos `filtered`: Indica presencia de firewall.
- Comparar resultados de `-sS` y `-sA` para identificar reglas de filtrado.

Ejercicio 4: Escaneo completo de red

Objetivo: Realizar un análisis exhaustivo de la red para inventariar todos los activos.

```
# Escaneo agresivo con detecci n de OS y scripts
sudo nmap -A -T4 192.168.1.0/24 -oA inventario_red
```

Documentación:

- Revisar el archivo `inventario_red.xml` para análisis posterior.
- Crear un mapa de red con los hosts descubiertos y sus servicios.

7. Integración con Wireshark

Para complementar el análisis de Nmap, se recomienda capturar el tráfico de red durante los escaneos utilizando Wireshark:

```
# En terminal 1: Iniciar captura con tcpdump
sudo tcpdump -i eth0 -w captura_nmap.pcap

# En terminal 2: Ejecutar el escaneo Nmap
nmap -sS -p 1-1000 192.168.1.1

# Detener tcpdump con Ctrl+C
# Abrir captura_nmap.pcap en Wireshark para analisis
```

8. Materiales Complementarios de Práctica

Para profundizar en los conocimientos adquiridos en este taller, se han seleccionado ejercicios prácticos de plataformas especializadas en ciberseguridad. Estos ejercicios serán explorados de manera preliminar en esta sesión, y su solución completa será desarrollada en el próximo taller.

Ejercicio 1: SSH - PicoCTF

Plataforma: PicoCTF
Temática: Conexión y autenticación SSH
Descripción: Serie de retos enfocados en el protocolo SSH, conexiones remotas y conceptos básicos de autenticación segura.
Enlace de acceso:

`https://play.picoctf.org/practice?difficulty=1&page=1&search=ssh`

Objetivo del ejercicio:

- Familiarizarse con la sintaxis del comando `ssh`
- Comprender los métodos de autenticación
- Identificar puertos SSH no estándar
- Practicar conexiones seguras a sistemas remotos

Ejercicio 2: SSH + Nmap - Hack The Box (Máquina Meow)

Plataforma: Hack The Box
Temática: Enumeración de red y explotación básica
Descripción: Máquina virtual diseñada que integra el uso de Nmap para enumeración de servicios y SSH para acceso al sistema objetivo.
Enlace de acceso:

`https://app.hackthebox.com/machines/Meow`

Habilidades a desarrollar:

- Escaneo de red con Nmap para identificación de servicios
- Análisis de puertos abiertos y servicios expuestos
- Enumeración de información del sistema objetivo
- Aplicación de técnicas básicas de pentesting
- Conexión SSH con credenciales predeterminadas

Nota importante: Es necesario crear una cuenta gratuita en cada plataforma para acceder a los ejercicios. Se recomienda completar el registro previo al próximo taller.

Consideraciones Éticas y Legales:

- Solo realizar escaneos en redes donde se tenga autorización explícita.
- Los escaneos no autorizados pueden ser considerados actividades ilegales.
- Utilizar estas herramientas únicamente con fines educativos o de auditoría autorizada.
- Las plataformas mencionadas proveen entornos legales y controlados para práctica.

9. Referencias

1. **Nmap Project.** (2024). *Nmap Reference Guide - Documentación Oficial en Español*. Recuperado de `https://nmap.org/man/es/index.html`
2. **Hack The Box.** (2024). *Hack The Box - Penetration Testing Labs*. Plataforma de práctica de ciberseguridad. Recuperado de `https://www.hackthebox.com`
3. **PicoCTF.** (2024). *picoCTF - CMU Cybersecurity Competition*. Carnegie Mellon University. Plataforma educativa de Capture The Flag. Recuperado de `https://picoctf.org`
4. **Lyon, G. F.** (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.

Los comandos y técnicas presentados en este documento han sido adaptados de la documentación oficial de Nmap y materiales educativos de las plataformas mencionadas.

Saludos, Equipo CSH