

Trabajo Práctico Integrador

Ciberseguridad – Escaneo de Puertos

Alumnos

Rolando Nebreda – Comisión 9

Valentín Rymaszewski – Comisión 3

Tecnicatura Universitaria en Programación - Universidad Tecnológica Nacional.

Arquitectura y Sistemas Operativos

Coordinador

Oscar Londero

Docentes Titulares

Profesor Martín Aristiarán

Profesor Ariel Enferrel

Docentes Tutores

David Roco – Comisión 9

Emmanuel Avellaneda – Comisión 3

6 de noviembre de 2025

Tabla de contenido

INTRODUCCIÓN	3
OBJETIVOS.....	3
DESARROLLO	4
Ciberseguridad - Escaneo de Puertos	4
Técnicas de Escaneo de Puertos	4
Prevención de Ataques de Escaneo de Puertos	5
Interpretación de los Resultados del Escaneo de Puertos	6
Nmap: El Mapeador de Redes Esencial	7
Zenmap: La Interfaz Gráfica de Nmap	8
Instalación y uso de Zenmap.....	9
Opciones de personalización del escaneo.....	10
CASO PRÁCTICO.....	13
Interpretación de los resultados. Deshabilitar una conexión activa vulnerable	13
CONCLUSIONES	15
REFERENCIAS	15

Trabajo Práctico Integrador

Introducción

El escaneo de puertos es una técnica fundamental en ciberseguridad que implica identificar puertos abiertos en un sistema de red para descubrir los servicios en ejecución. Esta práctica ayuda a determinar si estos puertos están abiertos, cerrados o filtrados por un firewall. Esta información permite a los administradores de sistemas tomar medidas proactivas para fortalecer las defensas de la red., ya que cada puerto puede representar una vulnerabilidad potencial si no se gestiona correctamente.

A un Técnico en Programación el conocimiento de métodos y herramientas de escaneo le permite entender cómo interactúan sus aplicaciones con los sistemas operativos y firewalls, asegurándose de que los servicios que desarrolla no expongan innecesariamente el sistema a riesgos. Además, un escaneo rápido puede confirmar si un servicio que acaba de programar está realmente "escuchando" en el puerto esperado.

Por último Nmap es una herramienta de código abierto fundamental en la administración de redes y ciberseguridad. Zenmap es la interfaz gráfica de usuario (GUI) oficial de Nmap. Esta aplicación está diseñada para hacer que el potente Nmap sea accesible tanto para principiantes como para usuarios avanzados, ofreciendo una herramienta visual y organizada para la auditoría y gestión de redes.

Objetivos

- Comprender qué es y la importancia del escaneo de puertos en ciberseguridad
- Reconocer los tipos de escaneo más comunes utilizados tanto por Administradores de Sistemas como por ciberdelincuentes.
- Reflexionar sobre la gestión proactiva de los puertos
- Promover el uso de Zenmap como herramienta.

Desarrollo

Ciberseguridad - Escaneo de Puertos

El escaneo de puertos es el proceso de enviar paquetes de red a puertos específicos de un sistema objetivo para determinar qué servicios están activos y escuchando.

Los puertos de una PC se escanean para verificar la seguridad de la red, ya que permite identificar si hay puertos abiertos que podrían ser vulnerabilidades explotables por atacantes.

Este proceso puede ser realizado tanto por administradores de sistemas para auditar su red como por ciberdelincuentes para encontrar debilidades

Técnicas de Escaneo de Puertos

Se utilizan varias técnicas, cada una con distintos niveles de precisión, velocidad y discreción:

Técnica	Descripción	Detección / Uso
Escaneo Ping (ICMP)	Envía solicitudes ICMP (similares a un "ping") a múltiples direcciones IP para identificar qué hosts están activos en una red. No escanea puertos, sino la disponibilidad del host.	Fácilmente bloqueado por firewalls. Usado para solución de problemas básicos.
Escaneo "Vanilla" (Conexión Completa TCP)	Intenta establecer una conexión TCP completa a los 65,536 puertos. Es el método más preciso porque completa el "apretón de manos" (handshake) SYN -> SYN-ACK -> ACK.	Muy fácil de detectar y registrar por los firewalls. Lento.
Escaneo SYN ("Semiabierto")	Envía un paquete SYN, pero no completa la conexión TCP, interrumpiendo la comunicación después de recibir el SYN-ACK inicial.	Rápido y menos propenso a ser registrado que el escaneo Vanilla, ya que la conexión nunca se establece por completo.
Escaneos	Métodos sigilosos que manipulan las	Buscan respuestas específicas

XMAS y FIN	banderas TCP. Un escaneo XMAS enciende varias banderas ("parpadea como un árbol de Navidad") y un escaneo FIN envía solo la bandera FIN.	del sistema que puedan revelar el estado del puerto o la presencia de un firewall, a menudo evadiendo la detección simple.
Escaneo de Rebote FTP	Utiliza un servidor FTP intermediario y vulnerable para rebotar el escaneo.	Permite al atacante ocultar su dirección IP real.
Escaneo de Barrido (Sweep)	Envía tráfico a un puerto específico a través de un rango de direcciones IP.	Ayuda a identificar qué sistemas están activos en la red, sin dar detalles sobre los puertos abiertos.

Prevención de Ataques de Escaneo de Puertos

Los ciberdelincuentes utilizan el escaneo de puertos como técnica preliminar para identificar vulnerabilidades en las redes, evaluar la seguridad de la infraestructura y detectar servidores susceptibles de ser explotados. Para mitigar este riesgo, las organizaciones deben implementar una estrategia de defensa proactiva y en capas.

Las medidas preventivas clave incluyen:

1. Implementación de un Firewall Robusto

Un firewall (cortafuegos) es la primera línea de defensa. Es fundamental para controlar el tráfico de red, limitar la visibilidad de los puertos y denegar el acceso no autorizado. Los firewalls modernos pueden configurarse para:

- **Detectar y bloquear escaneos:** Identificar patrones de escaneo anómalos en curso y mitigar la actividad antes de que se complete.
- **Restringir el acceso:** Controlar qué puertos son accesibles desde el exterior de la red y desde dónde.

2. Gestión Proactiva de Puertos

La mejor defensa es reducir la superficie de ataque. Las empresas deben:

- **Realizar Auditorías regularmente:** Utilizar herramientas de escaneo de puertos (como Nmap o Netcat) y verificadores de puertos para identificar qué puertos están abiertos.
- **Cerrar puertos innecesarios:** Asegurarse de que solo estén abiertos los puertos absolutamente necesarios para las operaciones comerciales, minimizando posibles puntos débiles.

3. Uso de Envoltorios TCP (TCP Wrappers)

Los envoltorios TCP son una capa de seguridad a nivel de host que permite a los administradores de sistemas definir reglas de control de acceso. Permiten o deniegan el acceso a servicios basándose en la dirección IP o el nombre de dominio del cliente que intenta conectarse.

4. Inteligencia de Amenazas y Software de Seguridad

Mantenerse a la vanguardia requiere:

- **Inteligencia de Amenazas (Threat Intelligence):** Estar al día con el panorama de amenazas en evolución para anticipar nuevas técnicas de ataque.
- **Software de Seguridad Sólido:** Implementar soluciones que monitoreen continuamente la actividad de la red y emitan alertas de seguridad ante comportamientos sospechosos o intentos de escaneo.

Interpretación de los Resultados del Escaneo de Puertos

Los resultados revelan información crítica sobre la red o el servidor objetivo, clasificándose generalmente en tres estados fundamentales:

Estado del Puerto	Descripción	Implicaciones de Seguridad
1. Abierto (Aceptado / Listening)	El host objetivo recibe la solicitud y un servicio activo está escuchando en ese puerto. Responde con un paquete de confirmación (ej. SYN-ACK en TCP).	Riesgo Alto: El objetivo principal de los atacantes. Representa un punto de entrada potencial que el personal de seguridad debe monitorear y proteger cuidadosamente.

2. Cerrado (No escucha / Not Listening)	El host objetivo recibe la solicitud, pero no hay ningún servicio activo esperando conexiones en ese puerto. El sistema responde con un paquete de "puerto inalcanzable" o "restablecer" (RST).	Riesgo Moderado: Aunque no hay servicio activo, confirma que el host está activo en la dirección IP. El personal de seguridad debe considerar bloquear estos puertos con un firewall (filtrarlos).
3. Filtrado (Descartado / Bloqueado)	El host objetivo no responde a la solicitud. Un firewall, un router o un sistema de prevención de intrusiones (IPS) ha interceptado y descartado el paquete.	Riesgo Bajo: El atacante no obtiene información útil, ya que los paquetes no llegan al servicio objetivo. Este es el estado ideal de seguridad para los puertos no esenciales.

Nmap: El Mapeador de Redes Esencial

Nmap (Network Mapper) es una herramienta de código abierto fundamental en la administración de redes y ciberseguridad. Su propósito principal es escanear redes para descubrir dispositivos, servicios y sistemas operativos activos, lo que permite a los profesionales evaluar la seguridad y el estado de la infraestructura de red.

Funciones Principales:

Nmap ofrece un conjunto de funciones para el descubrimiento y auditoría de redes:

- **Descubrimiento de Hosts:** Identifica qué dispositivos están operativos y activos en una red.
- **Escaneo de Puertos:** Detecta puertos TCP y UDP abiertos para ver qué servicios están escuchando.
- **Detección de Servicios y Versiones:** Determina exactamente qué aplicaciones y versiones se ejecutan detrás de los puertos abiertos.
- **Identificación del Sistema Operativo:** Averigua el sistema operativo (incluyendo la versión) que corre en un dispositivo remoto.

- **Análisis de Vulnerabilidades:** Mediante el uso de scripts (Nmap Scripting Engine), puede identificar vulnerabilidades potenciales o servicios obsoletos.
- **Adaptabilidad:** Ajusta su comportamiento para adaptarse a diferentes condiciones de red, como la latencia o la congestión.

Casos de Uso Comunes:

Nmap es una herramienta versátil utilizada por diversos profesionales:

- **Administradores de Redes:** Para inventariar, mapear y monitorear la infraestructura de la red.
- **Profesionales de Ciberseguridad:** Para realizar auditorías de seguridad, análisis de vulnerabilidades y mantener la higiene de la red.
- **Hacker Éticos:** Para realizar pruebas de penetración y evaluar la resiliencia de los sistemas ante ataques.
- **Comprensión de la Infraestructura:** Para obtener una visión completa de todos los componentes que conforman una red.

Zenmap: La Interfaz Gráfica de Nmap

Zenmap es la interfaz gráfica de usuario (GUI) oficial de **Nmap**. Esta aplicación gratuita, de código abierto y multiplataforma (compatible con Linux, Windows, macOS, BSD, entre otros) está diseñada para hacer que el potente Nmap sea accesible tanto para principiantes como para usuarios avanzados, ofreciendo una herramienta visual y organizada para la auditoría y gestión de redes.

Características Principales:

- **Facilidad de Uso:** Simplifica la ejecución de escaneos complejos.
- **Gestión de Perfiles:** Permite guardar escaneos frecuentes como perfiles para su ejecución repetida.

- **Creador Interactivo de Comandos:** Facilita la creación de líneas de comandos de Nmap de forma interactiva.
- **Visualización y Comparación de Resultados:** Guarda los resultados de los escaneos para su visualización posterior y permite compararlos para identificar diferencias.
- **Base de Datos de Escaneos:** Almacena los resultados recientes en una base de datos con capacidad de búsqueda.

Instalación y uso de Zenmap

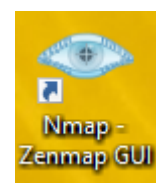
Para descargar e instalar Zenmap, visita la página oficial de Nmap (nmap.org) y descarga el instalador para tu sistema operativo (Windows, Linux, macOS). Para Windows, ejecuta el archivo descargado y sigue las instrucciones del instalador.



1. Abrir Zenmap:

Hacer clic en el icono de Zenmap en el escritorio o menú de inicio.

O desde la terminal (CMD / PowerShell) y escribir “zenmap” y presionar Enter.



2. Definir el objetivo:

En la sección superior, donde dice "Objetivo", ingresa la dirección IP o el rango de IPs que deseas escanear.

Ejemplo: `192.168.1.1-100` para escanear un rango de IPs.

3. Seleccionar el perfil de escaneo:

A la derecha del campo "Objetivo" se encuentra un menú desplegable.

Seleccionar un perfil de escaneo (como "Escaneo rápido", "Escaneo intenso", "Escaneo de ping", etc.) según lo que necesite.

4. Iniciar el escaneo:

Hacer clic en el botón "Escanear" para iniciar el análisis.

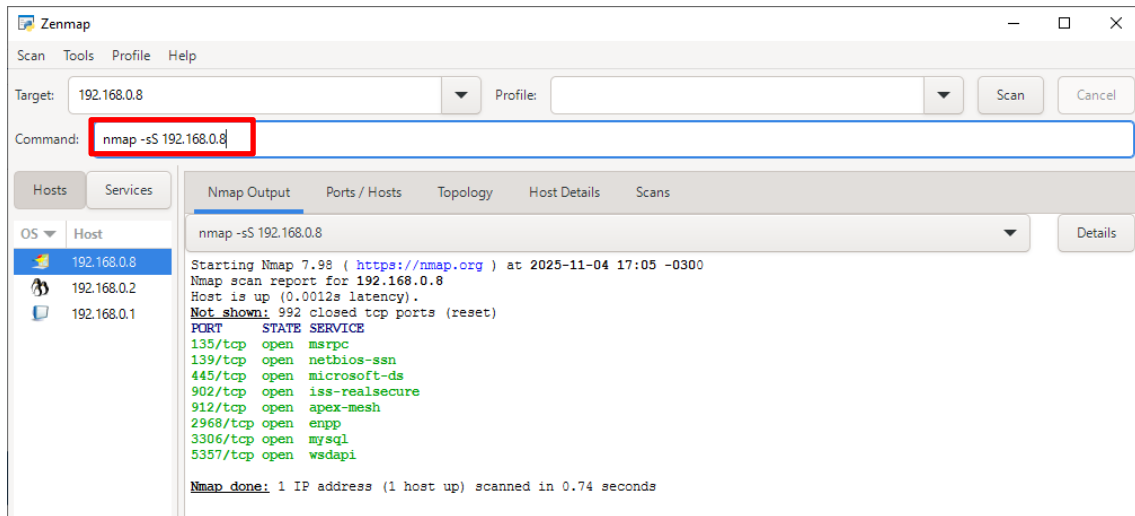
5. Interpretar los resultados:

En la ventana principal verás los resultados del escaneo.

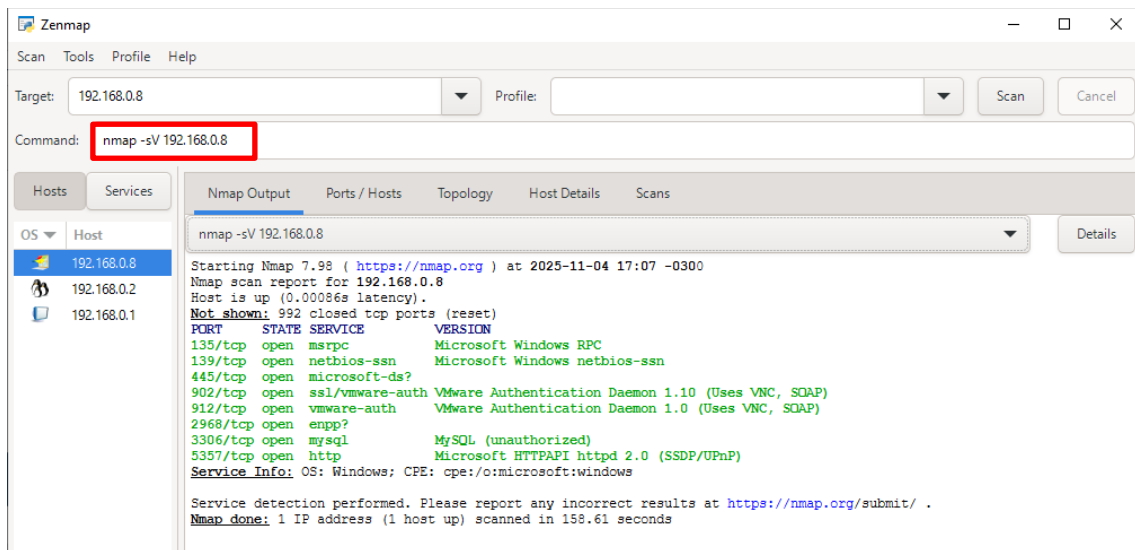
Opciones de personalización del escaneo

Zenmap puede mostrar información como el sistema operativo de los dispositivos, los puertos abiertos y los servicios activos. También posee varias opciones personalizables para la identificación de servicios. Por ejemplo:

-sS: Realiza un escaneo SYN (half-open), el modo por defecto para escanear puertos TCP de manera rápida y relativamente furtiva.



-sV: Realiza la detección de versiones, identificando qué servicios y versiones están corriendo en los puertos abiertos.

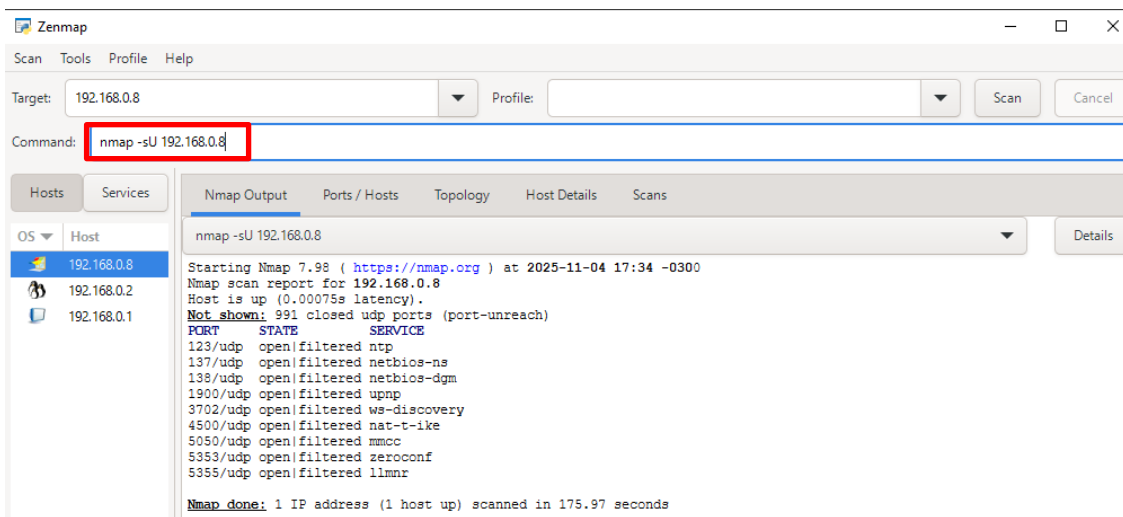


-sT: Realiza un escaneo de conexión TCP completa (TCP Connect Scan), útil cuando el SYN scan no es posible.

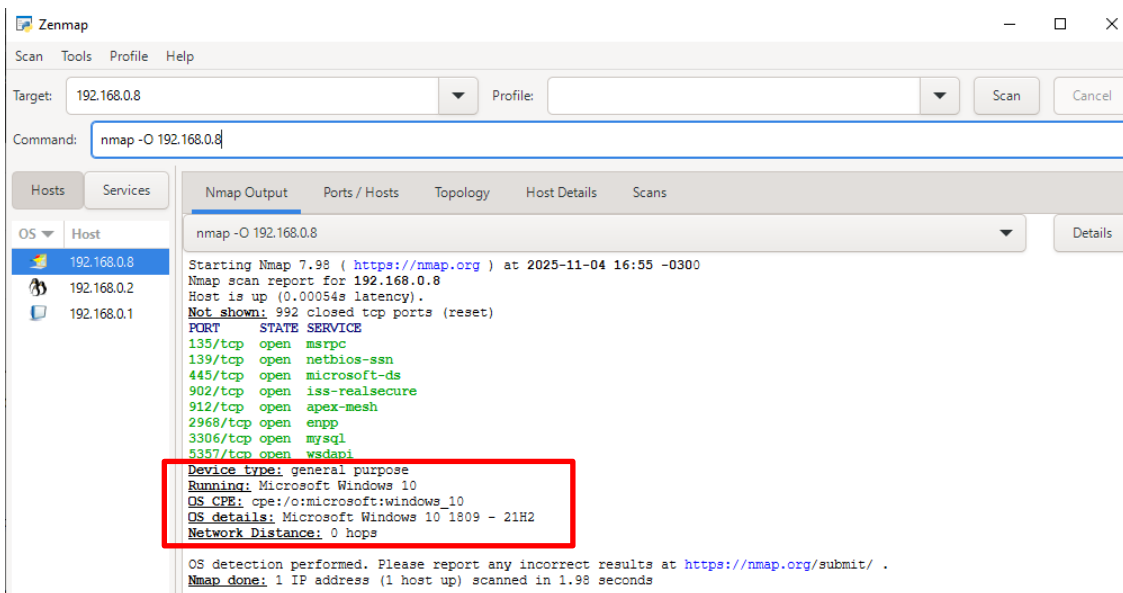
-T: Define el nivel de agresividad del escaneo, de -T0 (muy lento y furtivo) a -T5 (rápido y agresivo). La opción predeterminada es -T3.

-A: Escaneo agresivo que combina detección de OS, detección de versiones, ejecución de scripts NSE y traceroute. Este comando recopila mucha información, pero puede ser más ruidoso.

-sU: Realiza un escaneo de puertos UDP, útil para identificar servicios basados en UDP como DNS, DHCP y SNMP.



-O: Detección del sistema operativo. Nmap envía paquetes específicos y analiza las respuestas para identificar la plataforma del host.

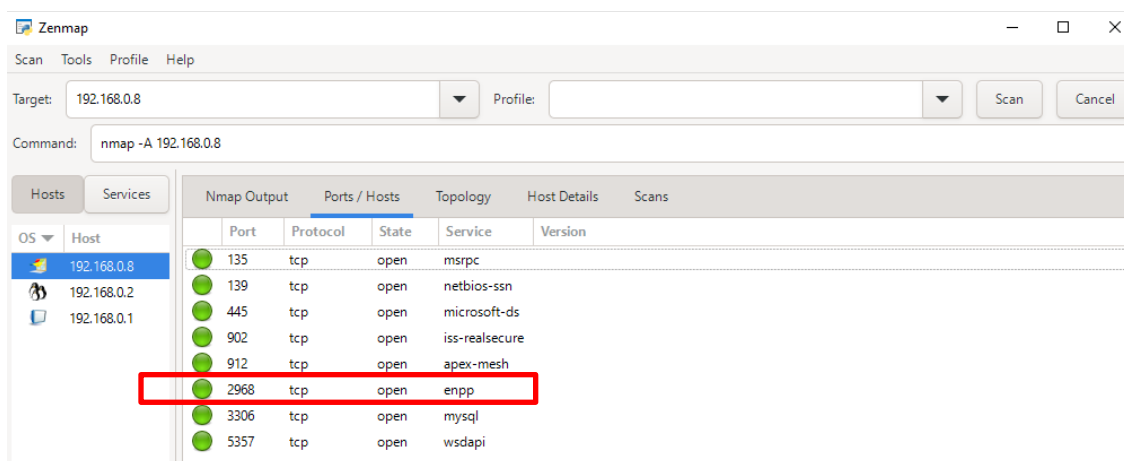


Caso práctico

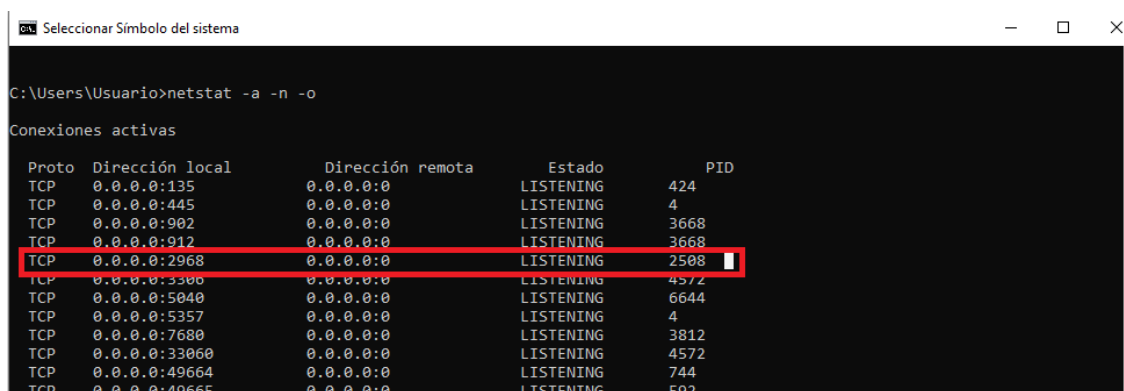
Interpretación de los resultados. Deshabilitar una conexión activa vulnerable

Ante conexiones vulnerables detectadas en el escaneo, se puede deshabilitar la conexión activa.

En este ejemplo se muestra como realizarlo por comandos en consola. Se observa aquí que en el puerto 2968 existe un servicio dudoso no reconocido:



Accediendo en CMD, se utiliza el comando **netstat -a -n -o** para listar los PID de los procesos activos en los puertos. En este caso **PID 2508**



Luego se utiliza el comando taskkill junto al PID obtenido: **taskkill /PID 2508 /F**

```
Simbolo del sistema
UDP [fe80::4e38:e761:81a5:9407%12]:1900 *:* 3204
UDP [fe80::4e38:e761:81a5:9407%12]:64484 *:* 3204
UDP [fe80::4f27:8d62:3a32:3dcd%8]:1900 *:* 3204
UDP [fe80::4f27:8d62:3a32:3dcd%8]:64485 *:* 3204

C:\Users\Usuario>taskkill /PID 2508 /F
Correcto: se terminó el proceso con PID 2508.

C:\Users\Usuario>
```

Aparecerá un mensaje de haber terminado el proceso con éxito.

Se lista nuevamente el estado de los puertos en CMD y se observa que el proceso en el puerto 2968 ya no aparece.

```
Simbolo del sistema

C:\Users\Usuario>netstat -a -n -o

Conexiones activas

Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 424
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:902 0.0.0.0:0 LISTENING 3668
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING 3668
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING 4572
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 6644
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 3812
TCP 0.0.0.0:33060 0.0.0.0:0 LISTENING 4572
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 744
```

De igual manera, se ejecuta nuevamente el escaneo con Zenmap, y se verá que el puerto 2968 ya no aparece asociado a ningún servicio.

```
Zenmap
Scan Tools Profile Help

Target: 192.168.0.8 192.168.0.8 Profile:
Command: nmap -sS 192.168.0.8 192.168.0.8

Hosts Services
OS Host
192.168.0.8
192.168.0.2
192.168.0.1

Nmap Output
nmap -sS 192.168.0.8 192.168.0.8
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-04 18:06 -0300
Nmap scan report for 192.168.0.8
Host is up (0.00069s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iis-realsecure
912/tcp   open  apex-mesh
3306/tcp  open  mysql
3307/tcp  open  wsuapi

Nmap scan report for 192.168.0.8
Host is up (0.00037s latency).
Not shown: 993 closed tcp ports (reset)
```

Conclusiones

Este trabajo ha puesto de relieve la importancia del escaneo de puertos como una medida preventiva contra accesos no deseados y ciberataques dirigidos a una red o sus equipos.

Se ha destacado la herramienta Nmap y, en particular, su interfaz gráfica Zenmap. Estas aplicaciones facilitan la realización de escaneos de puertos y la detección de vulnerabilidades, siendo accesibles para usuarios de diversos niveles de experiencia.

Finalmente, es importante entender que Zenmap y Nmap son solo una parte del conjunto de herramientas a disposición del administrador de sistemas. Estas soluciones de auditoría complementan otras prácticas esenciales para mantener la "salud" de los sistemas informáticos, incluyendo la prevención, la implementación de buenas prácticas y el uso de firewalls robustos para fortalecer la seguridad general de la infraestructura de red

Referencias

Tecnicatura Universitaria en Programación. Arquitectura y Sistemas Operativos.

Unidad 8 – Seguridad NMAP (Apunte de la materia)

Páginas web:

Zenmap: interfaz gráfica oficial para NMAP

<https://nmap.org/zenmap/>

Fortinet - ¿Qué es un escaneo de puertos? ¿Cómo prevenir los ataques de escaneo de puertos?

<https://www.fortinet.com/lat/resources/cyberglossary/what-is-port-scan>

Paloalto networks - ¿Qué es un escaneo de puertos?

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan>