MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE SERVEI PÚBLIC D'OCUPACIÓ ESTATAL
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya
IRON HACK SPAIN

Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Identificación de servicios

Introducción
Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos
Resumen

Introducción

Introducción

Nos centramos en la importancia de la seguridad lógica y el acceso a los sistemas informáticos.

Se destaca cómo el uso de internet y las comunicaciones móviles ha difuminado los límites de los activos de una empresa.

También se mencionan los posibles puntos de ataque externo, como las interconexiones entre las diferentes redes.

Además, se introduce la idea de ampliar la perspectiva hacia la seguridad de redes para abordar las vulnerabilidades en los puntos de interconexión de equipos y redes.

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Introducción

Evolución de las arquitecturas de red

- Antes de internet, las redes necesitaban un medio de transmisión único, con rutas fijas y aplicaciones específicas.
- En 1973, el Departamento de Defensa de EE. UU. inició el desarrollo de redes que conectaran sistemas de transmisión diferentes, tolerantes a fallos y capaces de ejecutar diversas aplicaciones.
- En 1980, se estableció TCP/IP como conjunto de protocolos para interconectar redes, dando origen a internet.

Arquitectura TCP/IP y sus aplicaciones

La arquitectura TCP/IP, ampliamente utilizada, organiza las comunicaciones en capas, definiendo servicios y aplicaciones.

En los servidores interconectados por redes TCP/IP, se ejecutan diversas aplicaciones y servicios, como correo electrónico, transferencia de archivos y navegación web.

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Arquitectura TCP/IP

Las arquitecturas de red son estructuras complejas que abarcan una variedad de aspectos, desde la transmisión de datos hasta la gestión de la seguridad.

Estas arquitecturas se organizan en grupos según su función y finalidad. Uno de los modelos más conocidos es el modelo OSI de 7 capas, desarrollado por ISO (Organización Internacional de Normalización).

El modelo OSI divide las funciones de una red en siete capas, cada una con su propósito específico.

Estas capas son: física, de enlace, de red, de transporte, de sesión, de presentación y de aplicación.

Cada capa se encarga de aspectos particulares de la comunicación de red, lo que permite una separación clara de las funciones y facilita el diseño y la gestión de redes complejas.

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Arquitectura TCP/IP

La arquitectura TCP/IP es el conjunto de protocolos que define cómo se comunican los dispositivos en una red de Internet.

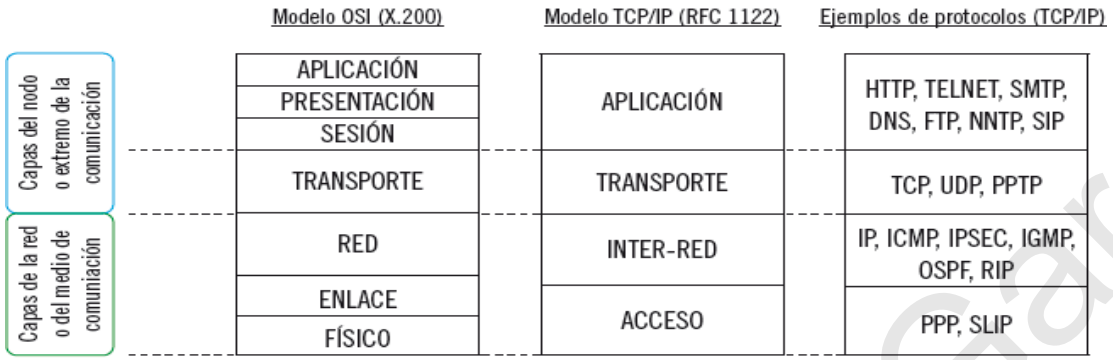
Está compuesta por una serie de protocolos normalizados que especifican cómo deben realizarse las diferentes operaciones de comunicación entre dispositivos para garantizar la interoperabilidad.

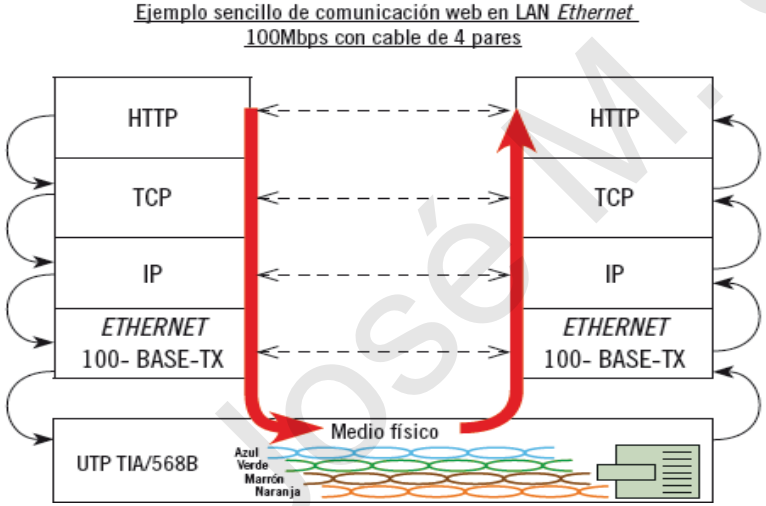
Algunos de los protocolos más importantes dentro de la arquitectura TCP/IP son el Protocolo de Internet (IP), que se encarga de enrutar los paquetes de datos a través de la red, y el Protocolo de Control de Transmisión (TCP), que se encarga de garantizar la entrega ordenada y confiable de los datos.

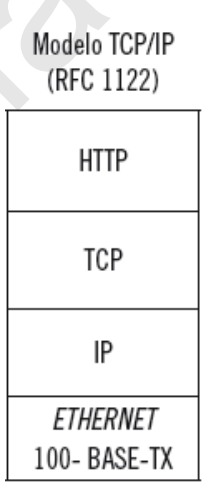
Estos protocolos, junto con otros como UDP (User Datagram Protocol) y ICMP (Internet Control Message Protocol), forman la base de la comunicación en Internet y otras redes basadas en TCP/IP.

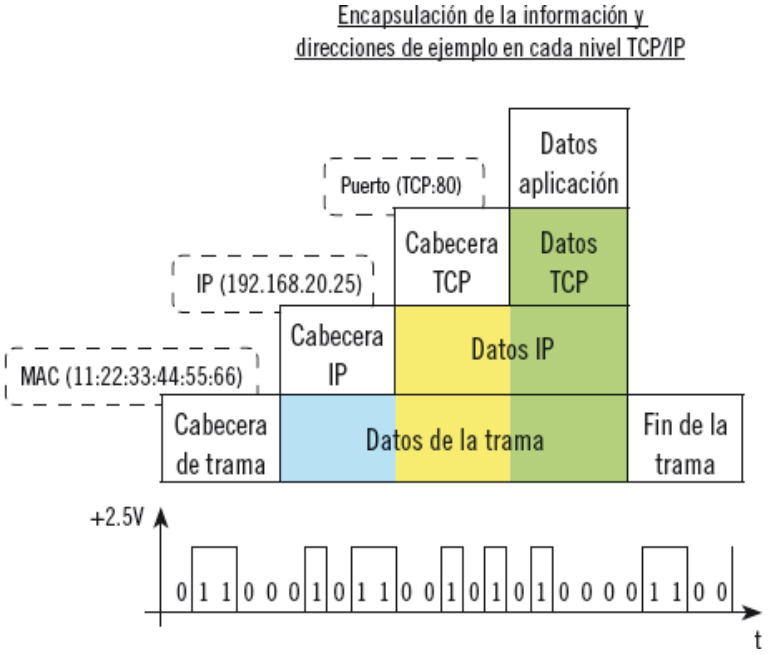
Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Modelo de comunicación OSI TCP/IP. Protocolos de ejemplo, representación gráfica del flujo de datos en una consulta web y encapsulación de la información









Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Arquitectura TCP/IP

Modelo TCP/IP y sus Capas

Modelo TCP/IP: Agrupa protocolos en cuatro capas para definir la comunicación en redes.

- Capa 1: Acceso al medio o de enlace. Establece la conexión del nodo a la red.
- Capa 2: Interredes. Permite el envío y recepción de paquetes entre nodos.
- Capa 3: Transporte. Facilita la comunicación y resuelve errores en la transmisión de datos.
- Capa 4: Aplicación. Proporciona protocolos para las aplicaciones del usuario, como HTTP para navegadores web.

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Protocolos, servicios y puertos más habituales

- Cada nodo de la red tiene una dirección MAC y una dirección IP.

  Dirección MAC: Un código único para el adaptador de red físico.

  Dirección IP: Una dirección numérica que identifica al dispositivo en la red.

- Los puertos diferencian las aplicaciones que usan una misma conexión de red.

  Para que diferentes aplicaciones o servicios en un dispositivo se comuniquen con otros dispositivos, se usan los puertos. Estos puertos funcionan como direcciones adicionales dentro de la red, permitiendo diferenciar entre las distintas aplicaciones que comparten la misma conexión a internet.

- Los puertos TCP y UDP tienen rangos de números específicos.

  Puertos del sistema (0-1023): reservados para servicios esenciales como HTTP (web), FTP (transferencia de archivos), SSH (administración remota) y DNS (nombres de dominio).
  Puertos de usuario (1024-49151): usados por aplicaciones como Telnet, SMB (compartir archivos), RDP (escritorio remoto) y BitTorrent.
  Puertos dinámicos (49152-65535): asignados temporalmente para conexiones

- La IANA define las asignaciones estándar de puertos.

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Protocolos, servicios y puertos más habituales

¿Qué es IANA?

La Autoridad de Números Asignados de Internet (IANA) es una organización sin fines de lucro que coordina:

- Direccionamiento IP: Asigna y administra las direcciones IP que identifican a los dispositivos en internet.
- Consultas DNS raíz: Mantiene la lista de servidores raíz del Sistema de Nombres de Dominio (DNS), que traducen los nombres de dominio a direcciones IP.
- Puertos de protocolos: Asigna los números de puerto que utilizan los diferentes protocolos de internet.

¿Por qué es importante IANA?

- IANA garantiza la unicidad e interoperabilidad de los recursos críticos de internet, como las direcciones IP y los nombres de dominio y es la fuente oficial de información sobre:
  - 13 categorías de servidores de nombres raíz:
  - Puertos TCP y UDP asignados a los servicios

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Protocolos, servicios y puertos más habituales

Servicios de sistema	Protocolo	Puerto
Transferencia de ficheros	FTP	21 (TCP)
Interprete de ordenes seguras	SSH	22 (TCP, UDP)
Terminal remoto	TELNET	23 (TCP)
Envío de correo	SMTP	25 (TCP)
Consultar de dominio o de IP	WHOIS	43 (TCP)
Servicio de nombres	DNS	53 (TCP, UDP)
Configuración de red dinámica	DHCP	67 (UDP)
Configuración de red dinámica	DHCP	68 (UDP)
Transferencia de ficheros	TFTP	69 (UDP)
Usuarios conectados a un servidor	FINGER	79 (TCP, UDP)
Navegación web	HTTP	80 (TCP)
Autenticación	KERBEROS	88 (TCP)
Lectura y descarga de correo electrónico	POP3	110 (TCP)
Transferencia de ficheros	SFTP	115 (TCP)
Noticias	NNTP	119 (TCP, UDP)
Sincronización de hora	NTP	123 (TCP, UDP)
Servicio de nombres Netbios	NBT	137 (TCP, UDP)
Servicio de datagrama Netbios	NBT	138 (TCP, UDP)
Servicio de sesión Netbios	NBT	139 (TCP, UDP)

Acceso a correo electrónico	IMAP	143 (TCP)
Transferencia de ficheros	BFTP	152 (TCP)
Gestión de red	SNMP	161 (TCP, UDP)
Chat	IRC	194 (TCP, UDP)
Acceso ligero a servicio de directorio	LDAP	389 (TCP, UDP)
Navegación web segura	HTTPS/SSL	443 (TCP)
Compartición de ficheros Windows		445 (TCP, UDP)
Envío de correos seguro	SMTP/SSL	465 (TCP)
Logs del sistema	SYSLOG	514 (UDP)
Información de enrutamiento	RIP	520 (UDP)
Terminal remoto seguro	TELNET/SSL	992 (TCP, UDP)
Acceso a correo electrónico seguro	IMAP4/SSL	993 (TCP, UDP)
Lectura y descarga de correo seguro	POP3/SSL	995 (TCP, UDP)

Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

Protocolos, servicios y puertos más habituales

Servicios de usuario	Protocolo	Puerto
Base de datos Microsoft SQL Server		1433-1434 (TCP, UDP)
Servicio de nombres WINS	WINS	1512 (TCP)
Base de datos Oracle		
Redes privadas virtuales VPN		1521 (TCP), 1701 (UDP), 1723
Servicio de escritorio remoto Windows	RDP	3389 (TCP, UDP)
Transferencia de archivos P2P Emule		4662 (TCP), 4672 (UDP)
Conexión remota Radmin		4899 (TCP)
AOL Messenger		5190 (TCP)
Base de datos PostgreSQL		5432 (TCP)
Conexión remota VNC	RDP	5400, 5500, 5600 (TCP)
Conexión remota PCAnywhere		5631 (TCP), 5632 (UDP)
Conexión remota VNC	RDP	5700, 5800, 5900 (TCP)
Intercambio de archivos Gnutella		6347-6350, 6355 (TCP)
Cliente de chat IRC		6667 (TCP)
Intercambio de archivos P2P BitTorrent		6881, 6969 (TCP)
MSN Messenger, archivos		6891-6900 (TCP)
MSN Messenger, voz		6901 (TCP)
Navegacion web alternativa	HTTP	8080 (TCP)
Administración remota Webmin	HTTP	10000 (TCP)
Acceso a MSN Game Zone		28800-29000 (TCP)
Administración BackOrifice (troyanos)		31337 (TCP)

Los puertos para el rango de usuario, que ascienden a unos cuarenta mil, son utilizados por una amplia gama de aplicaciones disponibles en el mercado.

A continuación, se enumeran algunos de los puertos empleados por herramientas comunes que permiten la conexión directa a la red para controlar un ordenador dentro de la LAN, así como por aplicaciones de usuario que podrían estar activas y consumir recursos significativos de conexión de red.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Reducción de vulnerabilidades

- Herramientas de análisis de puertos y servicios abiertos: Estas herramientas son esenciales para identificar los puertos de comunicación abiertos y los servicios asociados en un sistema, permitiendo así la detección de posibles vulnerabilidades y puntos de acceso para intrusos.
- Vulnerabilidades intrínsecas en aplicaciones, protocolos y servicios: Se resalta que las aplicaciones, protocolos y servicios suelen contener vulnerabilidades inherentes que podrían ser explotadas por intrusos para comprometer la seguridad de un sistema.
- Importancia de minimizar puertos de acceso a la red: Es crucial reducir al mínimo los puertos de acceso a la red para limitar las posibles vías de acceso de los intrusos, lo que se logra eliminando servicios innecesarios y restringiendo el acceso por defecto a todos los puertos.
- Eliminación de servicios no necesarios: Se recomienda eliminar todos los servicios que no sean esenciales para el funcionamiento del sistema, ya que cada servicio activo aumenta el riesgo de exposición a vulnerabilidades.
- Restricción del acceso por defecto a todos los puertos: Se destaca la importancia de configurar dispositivos de seguridad y servidores para que por defecto no permitan el acceso a ningún puerto, habilitando únicamente aquellos que sean necesarios.
- Habilitación selectiva de servicios y puertos de comunicación necesarios: Se sugiere habilitar solo los servicios y puertos de comunicación que sean indispensables, minimizando así el riesgo de exposición a vulnerabilidades.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

- Utilidades estándar en sistemas Windows y Linux: herramientas de red integradas en los sistemas operativos Windows y Linux, las cuales son fundamentales para evaluar la conexión de red y las posibilidades de conexión con otros equipos.
- Máxima utilidad para evaluar la conexión de red y posibilidades de conexión: Estas herramientas son de gran utilidad para conocer el estado de la conexión de red de un equipo y para evaluar las opciones de conexión con otros dispositivos en la red.
- Existen al menos seis utilidades básicas que son esenciales para llevar a cabo un análisis de seguridad de red efectivo, aunque se recomienda conocer y utilizar más herramientas según sea necesario.
- Punto de partida para cualquier análisis de red: Se resalta que estas utilidades son el punto de partida fundamental para cualquier análisis de seguridad de red, ya que permiten identificar posibles vulnerabilidades y puntos de acceso no autorizados que requieren atención y mitigación.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

PING

- Diagnóstico de conexión en red.
- Emplea el protocolo ICMP (Internet Control Message Protocol).
- Comprobación de conexión a diferentes niveles:
  - IP 127.0.0.1 o localhost: Instalación correcta de protocolos TCP/IP.
  - IP del nodo: Funcionamiento de la tarjeta de red.
  - IP de otro nodo de la LAN: Conexión dentro de la LAN.
  - IP del router: Conexión a internet.
  - IP de un servidor DNS del ISP: Confirmación de conexión a internet.

- Importancia en el diagnóstico de conexión y red.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

PING

- Existen herramientas que amplían sus funcionalidades:
  - "nping", "hping", "sing": Pruebas de red con configuración avanzada.
  - "nmap": Análisis de red, incluyendo comprobaciones ICMP.

- Medición del retraso en la respuesta (milisegundos).
- Importancia para un diagnóstico preciso de la conexión.
- Herramienta valiosa en entornos de redes y diagnóstico de conectividad.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

TRACEROUTE (TRACERT en Windows)

- Diagnóstico de la ruta de conexión en red.
- Emplea el campo TTL (Time To Live) de los paquetes IP.
- Funcionamiento: Cada equipo que procesa el paquete resta una unidad al TTL. Cuando alcanza 0, el equipo desecha el paquete e informa al remitente.
- Permite averiguar la ruta que sigue un paquete hasta su destino mediante el incremento progresivo del TTL.
- Presenta el tiempo de respuesta calculado para cada salto y la dirección IP del equipo de cada salto.

Ejemplo de Utilización

- Supongamos que queremos diagnosticar la ruta que sigue un paquete desde nuestro equipo hasta un servidor web remoto. Usamos el comando "traceroute" seguido de la dirección IP o nombre de dominio del servidor.
- El resultado nos mostrará cada salto (router o gateway) que el paquete realiza en su camino hacia el servidor.
- Podremos observar el tiempo de respuesta calculado para cada salto y la dirección IP correspondiente.
- Esto nos permite identificar posibles cuellos de botella o problemas en la ruta de conexión.
- Aplicación visual para Windows

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

NETSTAT

- Permite conocer las conexiones activas en un nodo.
- Disponible en Linux y Windows.
- Proporciona información sobre puertos TCP y UDP en uso, así como estadísticas de su uso.
- Existen aplicaciones con interfaz gráfico que utilizan Netstat.

Ejemplo de uso: En la línea de comandos, escribir "netstat" y obtener una lista de todas las conexiones activas.

netstat –ano Este comando mostrará una lista de todas las conexiones activas junto con los identificadores de proceso (PID) de los programas que están utilizando esas conexiones. A continuación, identificas el PID de un programa que no reconoces y sospechas que puede estar generando un problema. Luego, puedes usar el Administrador de tareas de Windows para encontrar el programa correspondiente al PID y, si es necesario, finalizar ese proceso para solucionar el problema de conexión a Internet.

Información proporcionada: Identificación de procesos, incluyendo el nombre de la aplicación asociada, estadísticas de uso como bytes transmitidos. Utilidad en el análisis de conexiones y diagnóstico de red.

Permite identificar procesos que están utilizando conexiones, lo que facilita la detección de posibles problemas o actividades sospechosas. Cheat Sheet netstat

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

NSLOOKUP

- Consulta de información de dominios o direcciones IP.
- Realiza consultas a servidores de nombres (DNS) para traducir nombres de dominio a direcciones IP y viceversa.
- En Linux, el comando equivalente es "dig".
- Permite realizar consultas sobre distintos tipos de registros DNS (A, ANY, SRV, MX, etc.).
- Facilita la evaluación de información disponible sobre servicios de un dominio.

Ejemplo de Uso

Supongamos que deseas obtener información sobre los servidores de correo electrónico asociados a un dominio específico.

En la línea de comandos, escribe: **nslookup -type=MX nombre_de_dominio_de_interes.**

El comando realizará una consulta al servidor de nombres DNS para obtener los registros MX (Mail Exchange) asociados al dominio. Esto te proporcionará una lista de los servidores de correo electrónico configurados para ese dominio, junto con su prioridad.

Útil para diagnosticar problemas de configuración de correo electrónico o para obtener información sobre la infraestructura de un dominio. Cheat Sheet nslookup

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

WHOIS

- Obtención de información de dominios o direcciones IP.
- Permite averiguar quién es el propietario de un nombre de dominio o una dirección IP.
- Dirige la consulta a un servidor whois, como whois.nic.es para los dominios ".es".
- Información detallada incluye domicilio, teléfono, correo electrónico y nombre del propietario, contacto técnico y contacto administrativo.

Ejemplo de Uso en Windows

La consulta puede realizarse de manera completa o en diferentes etapas.

La organización ICANN dirige consultas a través de un navegador web a INTERNIC en: **http://www.internic.net/whois.html**

Útil para obtener información sobre la propiedad de un dominio y para fines comerciales o de seguridad en internet.

Software para Windows: WhoisThisDomain

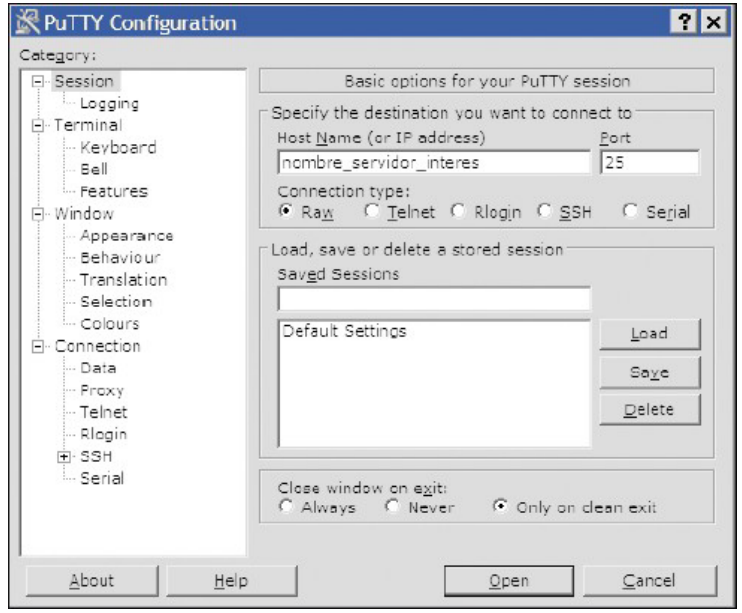
Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas Básicas de Trabajo en Red

TELNET

- Establecimiento de conexiones remotas en modo carácter o modo terminal.
- Permite gestionar un equipo remoto mediante comandos.
- Ejemplo de uso: **telnet nombre_servidor_correo 25** para verificar si un servidor de correo electrónico está funcionando en su puerto estándar.
- Alternativa segura: La aplicación SSH, recomendada por su cifrado de conexiones y seguridad en la transmisión de datos.

- Cheat Sheet ssh
- Descarga Putty



Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

Herramientas básicas:

- Ping: Confirma la conectividad ICMP.
- Traceroute: Muestra la ruta a un destino.
- Netstat: Revisa las conexiones locales.
- Nslookup y whois: Obtienen información pública sobre un destino.
- Telnet y ssh: Establecen conexiones a puertos específicos.
- Necesidad de herramientas específicas para análisis de puertos remotos.

PortQueryUI: Herramienta específica para Windows que intenta establecer una conexión a un puerto.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

Herramientas básicas:

- Ping: Confirma la conectividad ICMP.
- Traceroute: Muestra la ruta a un destino.
- Netstat: Revisa las conexiones locales.
- Nslookup y whois: Obtienen información pública sobre un destino.
- Telnet y ssh: Establecen conexiones a puertos específicos.
- Necesidad de herramientas específicas para análisis de puertos remotos.

PortQueryUI: Herramienta específica para Windows que intenta establecer una conexión a un puerto.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

NMAP

Características:

- Escaneo de puertos y redes
- Detección de sistemas operativos y servicios
- Scripting para automatización
- Análisis de vulnerabilidades
- Multiplataforma (Windows, Linux, macOS, etc.)

Nmap es una herramienta poderosa y versátil para el análisis de redes. Es ideal para administradores de redes, pentesters y entusiastas de la seguridad.

Zenmap es una interfaz gráfica de usuario (GUI) para Nmap, una herramienta de código abierto para la exploración de redes y auditoría de seguridad. Es una herramienta gratuita y multiplataforma disponible para Windows, Linux y macOS.

Cheat Sheet nmap

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

Advanced IP Scanner

Características:

- Escaneo rápido de redes
- Detección de dispositivos y servicios
- Visualización de información de red
- Exportación de datos a diferentes formatos
- Interfaz gráfica intuitiva

Advanced IP Scanner es una herramienta fácil de usar para el escaneo de redes. Es ideal para usuarios principiantes o para obtener una vista rápida de una red.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

Angry IP Scanner

Características:

- Escaneo rápido de puertos y redes
- Detección de sistemas operativos y servicios
- Filtrado y clasificación de resultados
- Exportación de datos a diferentes formatos
- Portable (no requiere instalación)

Angry IP Scanner es una herramienta portable y rápida para el escaneo de redes. Es ideal para usuarios que necesitan una herramienta ligera y eficiente.

Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

Herramientas de análisis de puertos

Fing

Características:

- Escaneo de redes
- Detección de dispositivos y servicios
- Mapeo de red
- Análisis de seguridad
- Disponible en Android e iOS

Fing es una herramienta multiplataforma que permite escanear redes desde un dispositivo móvil. Es ideal para usuarios que necesitan una herramienta para administrar redes desde cualquier lugar.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de un instante de tiempo

Netstat:

- Muestra las conexiones existentes en un momento dado.
- Se puede ejecutar con un intervalo para obtener un registro de puertos abiertos.
- Ventajas: rápido, ocupa poco espacio.
- Desventaja: no captura conexiones entre ejecuciones, o sea que solo muestra las conexiones que están activas en el momento exacto en que se ejecuta la herramienta. En otras palabras, no tiene la capacidad de registrar o mostrar las conexiones que se establecieron y cerraron entre el momento en que se ejecutó la herramienta por última vez y la ejecución actual.

Herramientas gráficas:

TCPView (Sysinternals): muestra conexiones, permite ordenarlas y grabar el resultado.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de registro continuo

Microsoft Port Reporter:

- Funciona como un servicio de Windows.
- Registra la actividad en un archivo de texto.
- Ventaja: captura todas las conexiones, incluso las breves.
- Desventaja: requiere espacio de almacenamiento y puede afectar el rendimiento.

Herramientas gráficas:

TCPLogview (Nirsoft): registra la actividad de red de forma sencilla.

Port Reporter (Microsoft)

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

¿Qué son?

- Aplicaciones que capturan y analizan el tráfico de red.
- Permiten ver detalles de las conexiones y el contenido de los paquetes.

Requisitos:

- Acceso directo al adaptador de red.
- Librerías o controladores adicionales.

Limitaciones:

- Instalación de software puede ser compleja o no deseada.
- No capturan tráfico en diferentes dominios de colisión (switch). No puede ver el tráfico que se envía a otros dispositivos en la misma red a menos que esos dispositivos estén conectados al mismo switch que el sniffer.

Soluciones:

- Modo mirroring: Reenviar tráfico del puerto del servidor al puerto del sniffer (si el switch lo permite).
- Switcher de gama superior: Usar un switch con función de mirroring.
- Hub: Conectar el servidor y el sniffer al mismo hub.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Beneficios:

- Visibilidad completa del tráfico de red.
- Análisis de protocolos, aplicaciones y contenido.
- Detección de problemas de seguridad y rendimiento.

Ejemplo: Analizar el tráfico de un servidor en producción sin afectar el entorno.

Para analizar el tráfico de un servidor en producción, una alternativa sería usar un sniffer con dos adaptadores de red, configurado como un puente o bridge, de manera que en un adaptador se conectaría el servidor, y en el otro se conectaría el switch. Incluso se pueden emplear técnicas más agresivas, como simular una suplantación de dirección de nivel de enlace (MAC), emulando un ataque del tipo man in the middle.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

TCPdump

Tcpdump es una herramienta gratuita de línea de comandos que te permite capturar y analizar el tráfico de red en tiempo real en sistemas operativos Unix, como Linux, macOS y Solaris.

Funciones principales:

- Capturar paquetes: Tcpdump te permite capturar paquetes de red que se envían o reciben en tu ordenador o en un servidor remoto. Puedes filtrar los paquetes por protocolo, dirección IP, puerto o cualquier otra información que te interese.
- Analizar paquetes: Tcpdump te permite ver el contenido de los paquetes que capturas. Puedes ver la información de la capa de red, como la dirección IP y el puerto, así como la información de la capa de transporte, como el tipo de protocolo y los datos del protocolo.
- Resolver nombres: Tcpdump puede resolver las direcciones IP a nombres de dominio y los puertos a nombres de servicios. Esto facilita la identificación de los dispositivos y aplicaciones que están generando el tráfico.
- Guardar capturas: Tcpdump te permite guardar las capturas de tráfico en un archivo para analizarlas posteriormente. Puedes guardar las capturas en diferentes formatos, como ASCII, pcap y libpcap.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

TCPdump

Uso de tcpdump:

Tcpdump se ejecuta desde la línea de comandos. Para iniciar una captura, debes especificar la interfaz de red que deseas capturar y los filtros que deseas aplicar.

- Por ejemplo, para capturar todo el tráfico que se envía o recibe en la interfaz eth0, puedes usar el siguiente comando:

  tcpdump -i eth0

- Para filtrar el tráfico por protocolo, puedes usar la opción -p. Por ejemplo, para capturar solo el tráfico TCP, puedes usar el siguiente comando:

  tcpdump -i eth0 -p tcp

- Para obtener más información sobre tcpdump, puedes consultar la página de manual:

  man tcpdump

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

TCPdump

Ejemplos de uso:

- Solucionar problemas de red: se puede usar para solucionar problemas de red, como errores de conexión, lentitud o mal funcionamiento. Puedes capturar el tráfico de red y analizarlo para identificar la causa del problema.
- Analizar el rendimiento: se puede usar para analizar el rendimiento de la red. Puedes capturar el tráfico de red y medir el ancho de banda y la latencia de las conexiones.
- Seguridad: se puede usar para detectar tráfico sospechoso o detectar intentos de intrusión. Puedes capturar el tráfico de red y buscar patrones que indiquen actividad maliciosa.
- Cheat Sheet TCPdump

Alternativas a tcpdump:

- Wireshark: una herramienta gratuita y de código abierto popular para capturar y analizar paquetes de red.
- Microsoft Message Analyzer (MMA): la herramienta sucesora de Network Monitor, aunque se suspendió en 2019.
- Ngrep: una herramienta similar a tcpdump, pero con una interfaz gráfica de usuario.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

TCPflow

¿Qué es tcpflow?

Tcpflow es una herramienta gratuita de código abierto similar a tcpdump, pero diseñada específicamente para capturar y analizar el tráfico de red TCP (Transmission Control Protocol). Mientras que tcpdump captura todo tipo de tráfico de red, tcpflow se centra únicamente en las conexiones TCP, lo que ofrece varias ventajas para casos de uso específicos.

Características principales:

- Objetivo: Captura y analiza datos transmitidos como parte de las conexiones TCP (flujos).
- Salida: Almacena los datos capturados en archivos separados para cada flujo TCP individual, lo que facilita el análisis de conexiones específicas.
- Funcionalidad: Ofrece control sobre nombres de archivo, agrupación de conexiones por protocolo, dirección IP o número de conexión, y se integra con programas proporcionados por el usuario para el procesamiento posterior de los datos capturados.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

TCPflow

¿Por qué usar TCPflow?

- Análisis específico de TCP: Ideal para situaciones en las que solo necesitas analizar la comunicación TCP y no necesitas el overhead de capturar todo el tráfico de la red.
- Organización eficiente de archivos: Los archivos separados por flujo simplifican el análisis y la identificación de conexiones específicas.
- Personalización: Ofrece opciones para la organización flexible de datos y la integración con herramientas externas para un procesamiento posterior.
- Análisis forense de redes: Valioso para investigar la actividad de la red, identificar conexiones sospechosas y analizar el rendimiento de la red.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Ngrep

Es una herramienta gratuita y de código abierto similar a tcpdump, pero diseñada específicamente para buscar patrones dentro del contenido de los paquetes de red. Mientras que tcpdump captura y muestra todos los paquetes, ngrep te permite filtrar esos paquetes en función de patrones de texto o expresiones regulares que se encuentren en el payload (datos) de los mismos.

Características principales:

- Filtrado basado en expresiones regulares: Permite buscar texto o patrones específicos dentro del contenido de los paquetes, no solo en las cabeceras.
- Soporte para múltiples protocolos: Funciona con diferentes protocolos de red, como TCP, UDP, HTTP, ARP, DNS, etc.
- Decodificación automática: Decodifica automáticamente parte del payload para una fácil lectura, dependiendo del protocolo utilizado.
- Salida personalizada: Permite personalizar la salida para mostrar solo la información que te interesa de cada paquete.
- Modos de captura: Puede capturar paquetes en vivo o leerlos de un archivo de captura previamente creado.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Ngrep

¿Para qué se utiliza ngrep?

- Solucionar problemas de red: Puedes usar ngrep para identificar rápidamente paquetes que contienen mensajes de error, patrones sospechosos o indicadores de problemas de rendimiento.
- Analizar el tráfico de aplicaciones: Puedes usar ngrep para ver el contenido de las comunicaciones entre aplicaciones específicas, como mensajes HTTP o consultas DNS.
- Seguridad de la red: Puedes usar ngrep para detectar intentos de intrusión, malware o actividad sospechosa en la red.
- Análisis forense: Puedes usar ngrep para examinar capturas de tráfico a posteriori para buscar evidencia de actividad maliciosa o encontrar información específica.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Ngrep

Ventajas de ngrep:

- Rapidez y eficiencia: Filtra los paquetes directamente en función del contenido, ahorrando tiempo y recursos.
- Flexibilidad: Soporta múltiples protocolos, expresiones regulares y diferentes formatos de salida.
- Gratuito y de código abierto: Disponible para todos con acceso a software gratuito.

Limitaciones de ngrep:

- Requiere acceso root: Necesita permisos elevados para capturar tráfico de red en la mayoría de los sistemas.
- Complejidad: Las expresiones regulares pueden ser difíciles de aprender y usar para usuarios principiantes.
- Potencialmente intrusivo: Capturar y visualizar el tráfico de otros usuarios puede tener implicaciones de privacidad.

Página web oficial y Manual de ngrep

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Wireshark

Wireshark es un analizador de protocolos de red gratuito y de código abierto. Es una herramienta popular entre profesionales de redes, administradores de seguridad y desarrolladores para capturar, analizar y comprender el tráfico de red.

Características principales:

- Captura de tráfico en vivo: Captura paquetes de red de diferentes interfaces de red.
- Análisis profundo: Decodifica protocolos de alto nivel como HTTP, DNS, TCP, UDP, etc., mostrando información detallada sobre cada paquete.
- Filtros: Permite filtrar el tráfico capturado para centrarse en paquetes específicos basados en varios criterios (dirección IP, protocolo, puerto, etc.).
- Búsqueda: Puedes buscar texto específico dentro de los paquetes capturados.
- Exportación: Exporta capturas de tráfico a varios formatos para análisis fuera de línea.
- Interfaz gráfica: Ofrece una interfaz gráfica de usuario intuitiva y fácil de usar.
- Plataformas múltiples: Funciona en Windows, macOS, Linux y otros sistemas operativos.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Wireshark

¿Para qué se utiliza Wireshark?

- Solucionar problemas de red: Identificar la fuente de problemas de conexión, lentitud o mal funcionamiento de la red.
- Analizar el rendimiento: Medir el ancho de banda, la latencia y otros indicadores de rendimiento de la red.
- Seguridad de la red: Detectar tráfico sospechoso, intentos de intrusión y otros problemas de seguridad.
- Análisis forense: Examinar capturas de tráfico para investigar actividades maliciosas o encontrar información específica.
- Desarrollo de redes y protocolos: Comprender el funcionamiento de los protocolos de red y desarrollar nuevas aplicaciones de red.

Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

Herramientas de captura de tráfico

Wireshark

Ventajas de Wireshark:

- Gratuito y de código abierto: Disponible para todos sin costo alguno.
- Completo y potente: Ofrece una amplia gama de funciones para análisis profundo.
- Interfaz gráfica user-friendly: Fácil de usar incluso para usuarios no expertos.
- Gran comunidad: Amplia comunidad de usuarios que proporciona soporte y recursos.

Limitaciones de Wireshark:

- Puede ser complejo para principiantes: La cantidad de información disponible puede ser abrumadora al inicio.
- Requiere permisos elevados: Necesita acceso root para capturar tráfico en algunas plataformas.
- Gran consumo de recursos: Puede consumir recursos del sistema durante la captura y análisis de tráfico.

Sitio web oficial, documentación y tutoriales

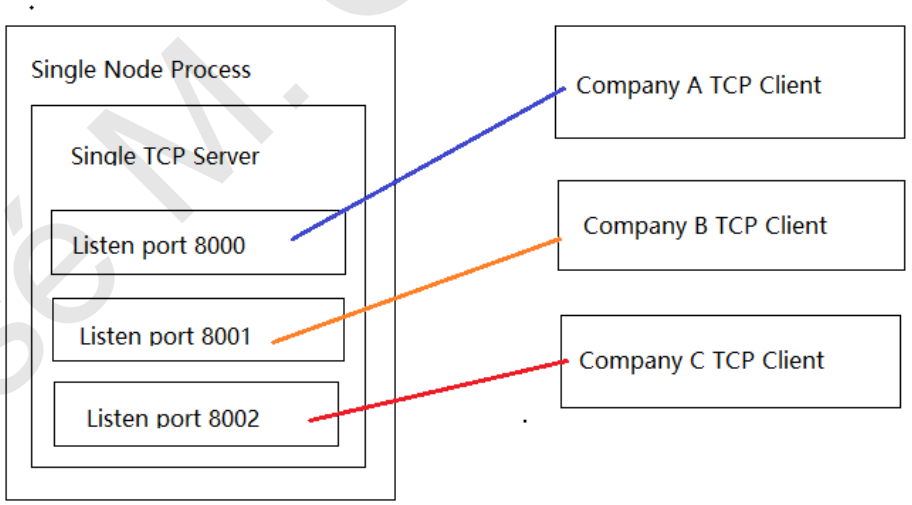
Resumen

Puertos en Redes: Organización y Seguridad

Los servidores con la misma dirección IP usan diferentes puertos para organizar sus servicios.

Los puertos se dividen en:

- Puertos del sistema o bien conocidos (1.024): HTTP (80), HTTPS (443), SSH (22), correo electrónico (25, 110), etc.
- Puertos registrados o de usuario (49.000): Asignados a aplicaciones específicas por la IANA.
- Puertos dinámicos o privados (15.000): Usados temporalmente por aplicaciones para conexiones específicas.



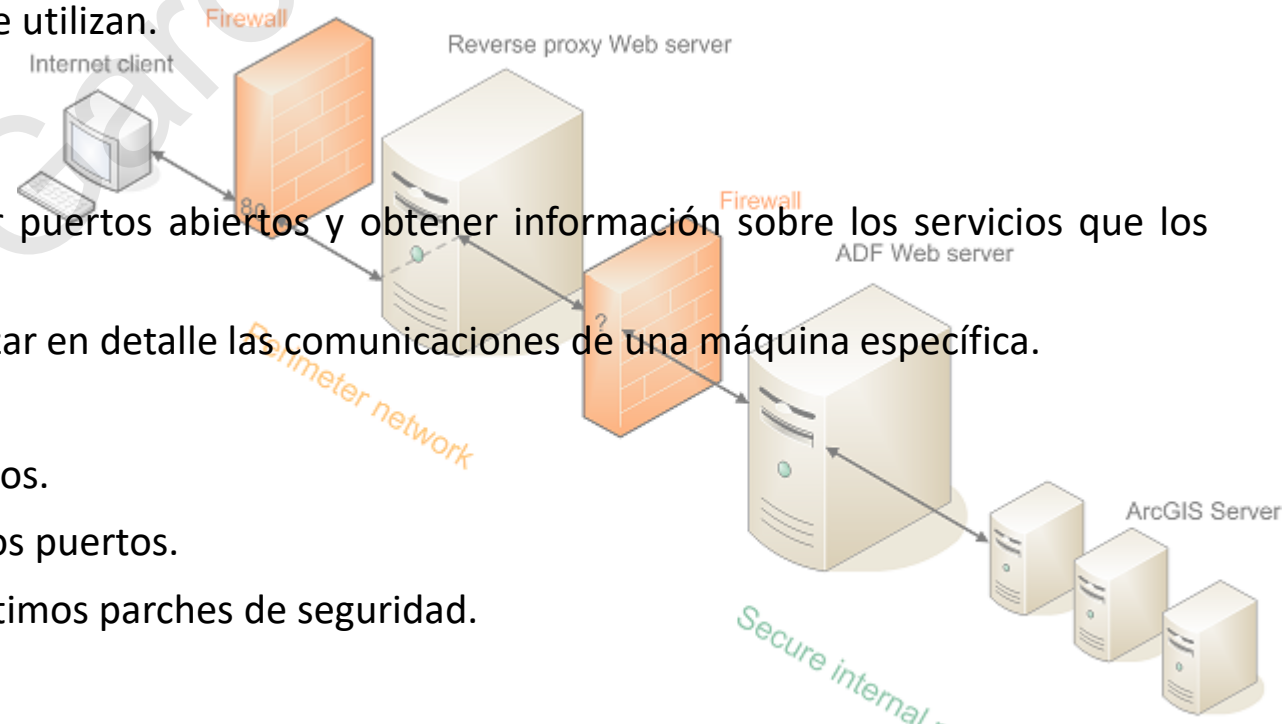
Resumen

Seguridad de los Puertos: Riesgos y Recomendaciones

Los puertos abiertos pueden ser vulnerabilidades para ataques.

Es importante:

- Identificar qué puertos están abiertos en las direcciones IP de la empresa.
- Restringir el acceso a los puertos que no se utilizan.
- Fortalecer la seguridad de los puertos que se utilizan.



Herramientas:

- Nmap: Analizador de redes para identificar puertos abiertos y obtener información sobre los servicios que los utilizan.
- Wireshark: Capturador de tráfico para analizar en detalle las comunicaciones de una máquina específica.

Recomendaciones:

- Mantener solo los puertos necesarios abiertos.
- Utilizar firewalls para controlar el acceso a los puertos.
- Mantener el software actualizado con los últimos parches de seguridad.