Universidad del Istmo

Campus Tehuantepec

Carrera: Ingeniería en computación

Grupo: 704

Alumno:

Juan Emmanuel Becerril Nolasco

Materia: Redes II

Profesor: Carlos Mijangos Jimenéz

2do Parcial

Trabajo: “Práctica 1. Utilización de las herramientas NMap y Wireshark”

Santo Domingo Tehuantepec, a 14 de noviembre del 2025

Índice

1. Introducción

2. Documentación de herramientas

3. Desarrollo de la práctica

4. Evidencias

5. Conclusiones

Introducción

Dentro de la seguridad en redes, la auditoría de redes tiene como objetivo evaluar la seguridad y eficiencia de una red informática mediante la identificación de vulnerabilidades. El proceso incluye un análisis de vulnerabilidades, el parchado de brechas de seguridad y la creación de un plan de contingencia. Las auditorías pueden considerar diferentes aspectos como el tipo de red (cableada o inalámbrica), ámbito (interno o externo) y enfoque (técnico o de cumplimiento). Los objetivos que se buscan al cumplir una auditoría de red son los siguientes:

- **Identificar vulnerabilidades**
    - La auditoría de redes busca identificar debilidades en la infraestructura de red que podrían ser aprovechadas por atacantes tanto internos como externos.
- **Evaluar controles de seguridad**
    - Se examinan los controles implementados para proteger la red y los datos almacenados que circulan por ella.
- **Cumplimiento normativo**
    - La auditoría de redes ayuda a organizaciones a garantizar el cumplimiento de estándares y reglamentos importantes como GDPR, HIPAA o PCI DSS.
- **Mejora continua**
    - La auditoría de redes proporciona una visión general de la infraestructura de red y sus áreas de mejora.

En resumen, la auditoría de redes es esencial para proteger los activos digitales de una organización y garantizar la continuidad del negocio. Al evaluar la seguridad de la red e identificar áreas de mejora, se puede fortalecer la resiliencia de la infraestructura de TI y minimizar el riesgo de amenazas internas y externas.

Entre las herramientas que son utilizadas por los expertos para realizar las auditorías de red se encuentran las herramientas open-source NMap y Wireshark, que permiten realizar un escaneo de puertos en direcciones IP y leer el tráfico de una red, de manera que son indispensables para realizar una buena auditoría de red.

Documentación de herramientas

Wireshark

Es un analizador de protocolos de red, llamado analizador de paquetes, diseñado para proporcionar visibilidad del tráfico que se produce en una red o entre máquinas. Permite mirar desde el interior de la red y examinar los detalles del tráfico inalámbrico y por cable a varios niveles: desde la información a nivel de conexión hasta los bits que hacen un determinado paquete y los datos que contiene. A su vez, Wireshark también permite visualizar la información en varios niveles de la pila, de modo que el operador puede aislar, identificar y depurar las conexiones de red desde los niveles más bajos hasta la capa de aplicación. Las características de Wireshark son las siguientes:

Permite seguir el rastro a los paquetes TCP stream, por lo que se puede ver todo lo relacionado con dicho paquete, el antes y el después, pudiendo aplicar filtros personalizados a estos mismos sin perder el flujo.

- Se puede **decodificar los paquetes** y exportar en formatos específicos y guardar dichos objetos.
- Permite **ver estadísticas de los paquetes capturados** incluyendo un resumen, jerarquía de protocolos, conversaciones, puntos finales y gráfica de flujos entre otros.
- **Análisis fácil e informativo** mediante resolución de nombres por MAC, por red, etc. y reensamblaje de paquetes.

Entre los usos más importantes de Wireshark se pueden destacar los siguientes:

- **Ver los datos que atraviesan varias redes**, incluidas las redes cableadas, como Ethernet, las redes inalámbricas, las redes Bluetooth o las interfaces de red virtuales, como Docker o un hipervisor.
- **Navegar y ver las distintas capas de la pila**, incluidos los protocolos a nivel de aplicación, como HTTP/HTTPS; protocolos de correo, como POP3 y SMTP; y protocolos de compartición de archivos, como Server Message Block y Common Internet File System. Más abajo en la pila, se puede ver TCP/IP y el Protocolo de Datagramas de Usuario. Aún más abajo en la pila, se pueden ver artefactos como las tramas Ethernet.
- **Registrar y capturar el tráfico de la red** para su posterior análisis.

Nmap

Nmap es la abreviatura de Network Mapper. Es una herramienta de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas. Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

El conjunto de funciones de Nmap, por lo tanto, va más allá de la exploración básica de redes e incluye:

- **Descubrimiento del host**: Nmap identifica los hosts activos en una red, sentando las bases para una exploración más profunda.
- **Exploración de puertos**: Nmap descubre puertos y servicios abiertos, lo que permite a los administradores conocer la superficie de ataque de una red.
- **Detección de versiones**: Nmap puede identificar versiones de servicios y ayudar a localizar posibles vulnerabilidades asociadas a versiones específicas.
- **Huella digital del sistema operativo**: las capacidades de detección de SO de Nmap permiten a los administradores identificar los sistemas operativos que se ejecutan en los hosts descubiertos, lo que ayuda con el inventario de la red y las evaluaciones de seguridad.
- **Ayuda a mapear rápidamente una red sin comandos ni configuraciones sofisticados**. También admite comandos simples (por ejemplo, para verificar si un host está activo) y secuencias de comandos complejas a través del motor de secuencias de comandos Nmap.
- **Capacidad para reconocer rápidamente todos los dispositivos**, incluidos servidores, enrutadores, conmutadores, dispositivos móviles, etc. en redes únicas o múltiples.
- **Ayuda a identificar los servicios que se ejecutan en un sistema**, incluidos los servidores web, los servidores DNS y otras aplicaciones comunes. Nmap también puede detectar versiones de aplicaciones con una precisión razonable para ayudar a detectar vulnerabilidades existentes.

Gracias a estas características, Nmap ha llegado a ser una de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Desarrollo

Los pasos que se realizaron durante la práctica fueron los siguientes:

1. Utilizando un segundo equipo de computo propio, se obtuvo su dirección IP dentro de la red de internet de mi hogar mediante el comando *ipconfig* en la consola de Windows, con el objetivo de realizar un escaneo de puertos NMap para escanear puertos abiertos dentro de este dispositivo.

2. Dentro de la herramienta NMap, se realizo el comando nmap -p 1-65535 -T4 -A -v 192.168.100.33 (el comando se obtuvo al ejecutar la opción de escaneo *Intense scan, all TCP ports*) para escanear todos los puertos abiertas de la dirección IP 192.168.100.33, que fue de la computadora secundaria, revisando desde el puerto 1 hasta el puerto 65535, buscando posibles puertos abiertos que tuviera la computadora, y se encontraron algunos puertos abiertos mediante este escaneo, como 135, 139, etc.

3. De igual manera, también se probó otra opción de escaneo (con comando nmap -sS -sU -T4 -A -v 192.168.100.33, obtenido al ejecutar la opción de escaneo *Intense scan plus UDP*) para escanear puertos abiertas de la dirección IP 192.168.100.33, buscando posibles puertos abiertos que tuviera la computadora y escaneando el UDP tras este primer escaneo.

> Entre los puertos obtenidos en el paso 2 y 3, se encontraron 2 puertos abiertos notables por ser susceptibles de sufrir ataques.
>
> El primero fue el puerto 445 (SMB - Server Message Block), utilizado para compartir archivos, impresoras y comunicarse entre máquinas de una red local en Windows. Este puerto es notorio debido a que está profundamente integrado dentro del sistema operativo, por lo que un fallo de seguridad aquí puede ser catastrófico. Un ejemplo de fallo fue usado en la vulnerabilidad EternalBlue, que permitía la ejecución remota de código (RCE) dentro de la computadora y fue utilizada por el ransomware WannaCry, que se esparcía en equipos dentro de una misma red usando esta vulnerabilidad en equipos con el puerto abierto.
>
> A su vez, el otro puerto abierto notorio encontrado fue el 3306, utilizado por el sistema de gestión de bases de datos MySQL. Aunque el riesgo de este puerto no es la ejecución de código, como en el caso anterior, si puede sufrir ataques de acceso no autorizado a datos en servidores SQL, como por ejemplo mediante fuerza bruta, lo que podría provocar el filtrado de información sensible en dispositivos que cuenten con servidores a los que se pueda acceder a través de internet.

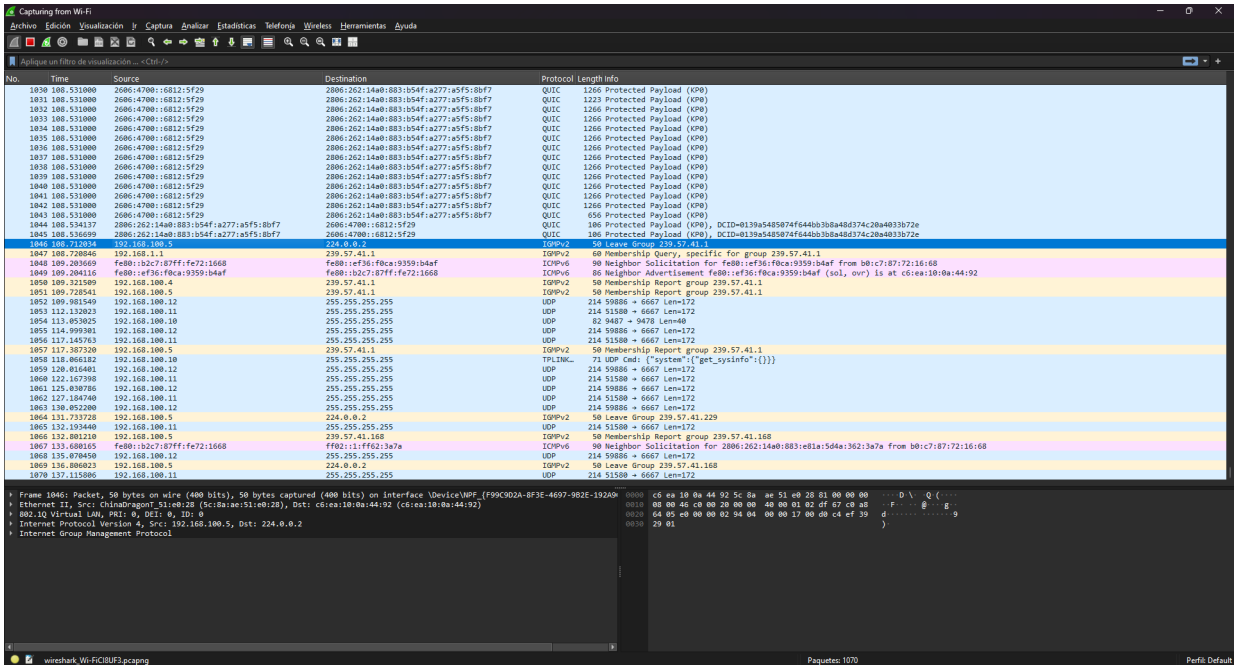
4. Después de realizar el escaneo mediante NMap, se procedió a utilizar la herramienta de lectura de paquetes de redes Wireshark, con el objetivo de visualizar de manera precisa todos los paquetes de información viajando dentro del internet en mi hogar. Al leer el tráfico que ocurría en el controlador Wifi en mi equipo (es decir, el dispositivo de red que Windows utiliza para conectarse a mi red local) es posible analizar todos los paquetes que son enviados en la red Wifi. Al visualizar los datos de estos paquetes, se pueden observar en qué protocolos fueron enviados (por ejemplo, TCP, UDP, IPMPv6, ARP, QUIC, etc.), de qué direcciones fueron enviadas y hacia qué dirección se dirigían (en mi caso, la mayoría de IPs se mostraban como IPv6, aunque también hubieron muchas en IPv4, tanto de broadcast (por ejemplo, 255.255.255.255) como de la propia red (por ejemplo, 192.168.100.10) y el tipo de mensajes que se emitían (por ejemplo, *Membership Report group 224.0.0.251*).

5. Posteriormente, se analizó el tráfico exclusivamente de la dirección IP 192.168.100.33, que, como se destaco anteriormente, es la dirección de mi equipo de cómputo secundario. Si bien no se puede ver toda la información que envía el dispositivo al modem de internet, si se podía visualizar información enviada por broadcast, como los pings que se pueden realizar en la consola de Windows, o las identificaciones que emitía mi computadora a la dirección 192.168.100.255 (*Host Announcement JUAN, Workstation, Server, NT Workstation, Potential Browser*).

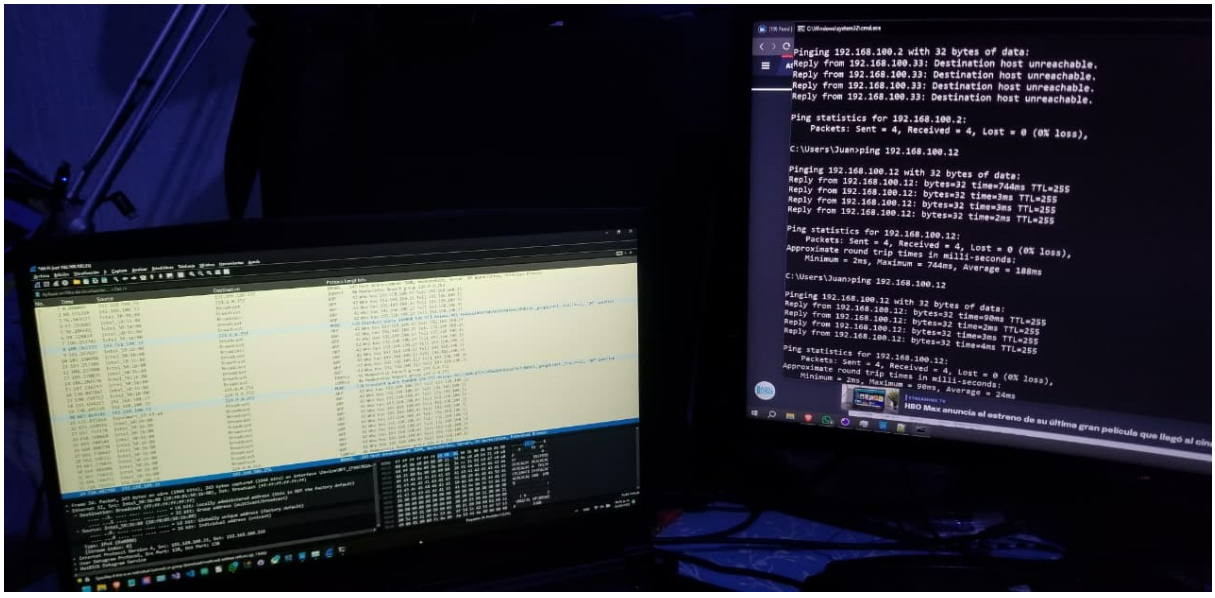
6. Finalmente, tras haber utilizado ambas herramientas para analizar la dirección IP de mi computadora, se puede destacar su utilidad en operaciones de auditoría reales, sirviendo como software indispensable para asegurar que las redes de internet en un entorno donde es importante garantizar los 3 principios de la triada de la ciberseguridad (confidencialidad, disponibilidad e integridad) y los dispositivos que se conecten dentro de la red. Si bien estas herramientas son utilizadas por expertos en ciberseguridad para prevenir ataques o descubrir vulnerabilidades, es factibles destacar que los atacantes también pueden utilizar estos programas para vulnerar servicios y ejecutar ataques más fácilmente, por lo que es necesario reforzar bien las redes y los dispositivos que las utilizan para prevenir intrusiones indeseadas que puedan provocar grandes problemas dentro de sus entornos de uso.

Evidencias

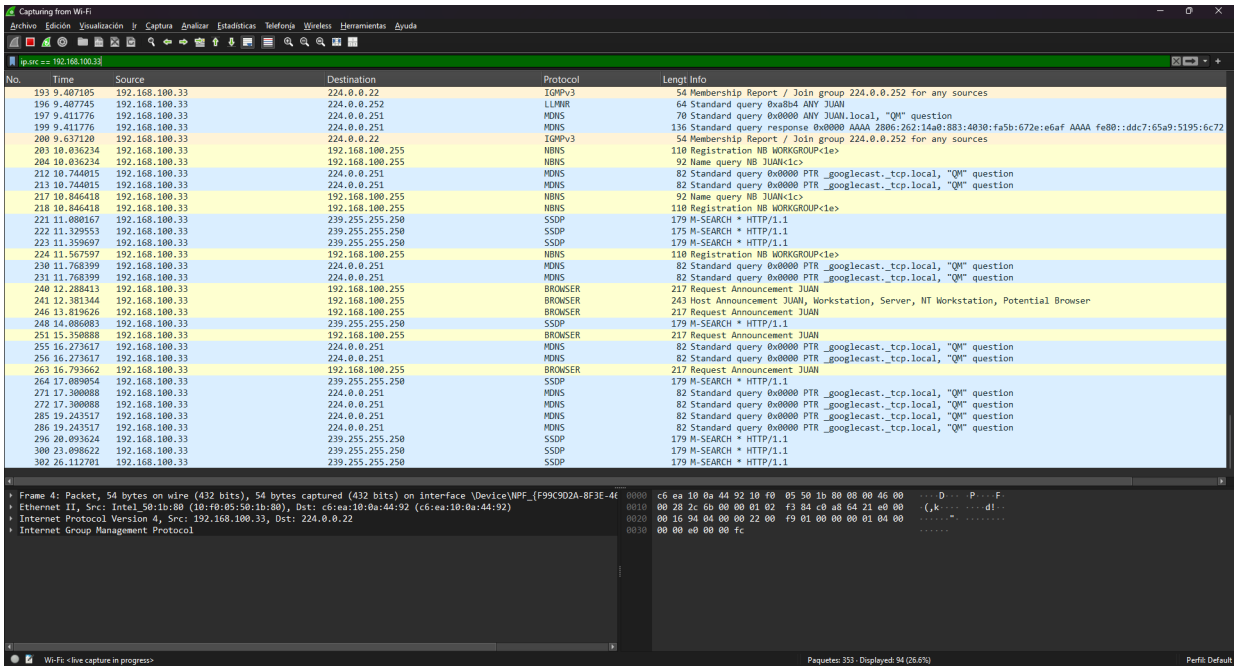
A continuación se muestran las capturas de pantalla e imágenes de las evidencias de la práctica:



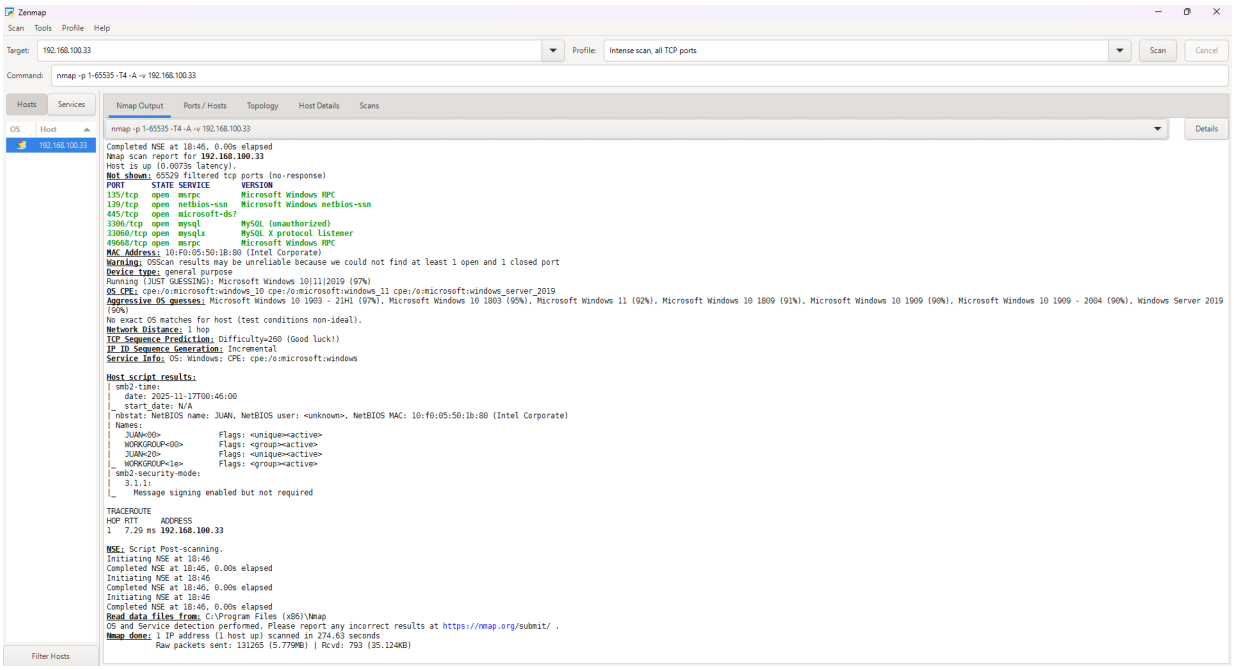
Wireshark: Escaneo general.



Wireshark: escaneo del tráfico generado por mi equipo secundario, con una ventana CMD para generar pings a través de la red, que son recolectados por Wireshark.



Wireshark: captura de pantalla del escaneo del tráfico generado por mi equipo secundario.



NMap: Escaneo de puertos a la dirección IP de mi equipo secundario.

Conclusiones

Wireshark es muy importante para la ciberseguridad, empleado tanto para la defensa como para la auditoría técnica de entornos complejos. Uno de los casos más habituales es el análisis forense de incidentes, ya que tras una intrusión, permite revisar el tráfico capturado para entender qué ocurrió, cómo se movió el atacante y qué datos se vieron comprometidos.

A su vez, también es clave en la detección de tráfico malicioso, permitiendo identificar actividad problemática como la comunicación con dominios sospechosos o realización de conexiones inusuales en puertos no estándar. Gracias a sus filtros, es posible aislar sesiones sospechosas y reconstruirlas, incluso si no se cuenta con un sistema IDS activo.

En auditorías de red, se usa para validar que todo el tráfico sensible (como inicios de sesión, transferencias de archivos o comunicaciones con sistemas críticos) esté cifrado. Si Wireshark detecta credenciales en texto plano o sesiones sin TLS, se puede afirmar que la red no es segura. Otro uso habitual es la comprobación de configuraciones en sistemas firewall o segmentación de red. Si se detecta tráfico cruzando barreras que deberían estar aisladas, Wireshark lo expone de inmediato.

Por su parte, Nmap (Network Mapper) es una herramienta fundamental en la fase de reconocimiento y auditoría de seguridad, ayudando a descubrir hosts activos y crear un registro de estos, permitiendo a los administradores y auditores entender qué dispositivos están conectados y qué servicios están ofreciendo.

Su función más importante es la detección de puertos abiertos y la identificación precisa de los servicios y versiones que se ejecutan en ellos. Esto es esencial para cuantificar la superficie de ataque de un sistema. Gracias a su motor de scripts (NSE), Nmap puede detectar configuraciones inseguras, como bases de datos que aceptan conexiones externas (puerto 3306) o servicios de compartición de archivos expuestos (puerto 445), e incluso identificar vulnerabilidades conocidas en versiones de software obsoletas.

En las auditorías de red, Nmap es indispensable para validar la eficacia de las reglas del firewall y la correcta segmentación de la red. Un analista puede simular un ataque desde diferentes segmentos de la red para comprobar si es posible alcanzar sistemas críticos. Si un escaneo de Nmap revela un puerto abierto que debería estar bloqueado, se demuestra de forma concluyente un fallo en la política de seguridad, exponiendo un riesgo tangible antes de que un atacante pueda explotarlo. De allí que ambas herramientas sean indispensables para una auditoría de redes completa y exitosa.