Universidad del Istmo

Campus Tehuantepec

Redes de Computadoras II

ING. Carlos Mijangos Jiménez

Monitoreo y escaneo de vulnerabilidades con las herramientas nmap y wireshark

---

Christian Hernández Mares

Ingeniería en Computación

7mo Semestre - 2do Parcial

Grupo 704

17 de noviembre de 2025

Índice general

1 Introducción

1.1 Requisitos

- Oracle VirtualBox instalado en el anfitrión.
- Dos máquinas virtuales con sistemas operativos instalados.
- Wireshark instalado en una máquina virtual (victima).
- Nmap instalado en una máquina virtual (atacante).
- Configuración de red interna entre las máquinas virtuales.

1.2 Descripción de conceptos

Máquina virtual: Software que simula un sistema computacional completo, permitiendo ejecutar sistemas operativos de manera aislada dentro de otro equipo físico (Susnjara, s. f.).

Dirección IP: Identificador numérico único asignado a cada dispositivo en una red, necesario para el enrutamiento y comunicación entre dispositivos (Fortinet, 2025).

Protocolo ARP: Protocolo de red que permite asociar una dirección IP con una dirección MAC en una red local (IBM, 2021).

Protocolo ICMP: Protocolo de control utilizado para enviar mensajes de error y operativos, fundamental para diagnosticar conectividad (Amazon Web Services, 2024).

TCP: Protocolo de transporte orientado a conexión que garantiza la entrega confiable de datos (mdn, s. f.).

UDP: Protocolo de transporte sin conexión, más rápido pero no garantiza la entrega de paquetes (Cloudflare, s. f.).

Puerto de red: Punto lógico de comunicación numerado entre 1-65535, asociado a servicios específicos en un sistema (Jesús, 2024).

Three-Way Handshake: Proceso que consta tres pasos, necesario para establecer una conexión TCP (Microsoft, s. f.).

- SYN - Cliente envía solicitud de conexión
- SYN-ACK - Servidor confirma y responde
- ACK - Cliente finaliza el establecimiento

IDS: Sistema de Detección de Intrusiones que monitoriza la red para identificar actividades sospechosas o maliciosas (IONOS, 2024).

1.3 Documentación de herramientas

1.3.1 Oracle Virtual Box

Para la práctica se utilizó Oracle VirtualBox, una plataforma de virtualización de escritorio que permite ejecutar distintos sistemas operativos dentro de un mismo equipo físico. Esta herramienta proporciona un entorno flexible y completamente aislado, ideal para realizar pruebas, configuraciones o simulaciones sin comprometer la estabilidad ni la seguridad del sistema anfitrión. Gracias a su capacidad para crear entornos virtuales independientes, VirtualBox facilita el aprendizaje y la experimentación con diferentes sistemas operativos y aplicaciones, permitiendo a los usuarios probar escenarios complejos de manera segura y controlada (Oracle, s. f.).

VirtualBox funciona creando máquinas virtuales que ejecutan sistemas operativos dentro del anfitrión, asignando recursos como memoria, almacenamiento y redes virtuales para cada instancia. Esto permite experimentar con software o configuraciones críticas que, en un equipo físico, podrían implicar riesgos como pérdida de datos, conflictos de compatibilidad o necesidad de particionar discos (Fernández, 2020).

1.3.2 Wireshark

Wireshark es un analizador de protocolos de red de código abierto que permite capturar y examinar el tráfico que circula por una red de manera detallada e interactiva. Su capacidad para inspeccionar cientos de protocolos diferentes lo convierte en una herramienta altamente valiosa para el análisis, monitoreo y solución de problemas en redes de cualquier tamaño (Wireshark, s. f.).

En el ámbito de la ciberseguridad y el análisis de redes, Wireshark se considera fundamental, ya que facilita la identificación de problemas de conectividad, anomalías en el tráfico o posibles intentos de ataque. Permite a los usuarios visualizar los paquetes de datos a diferentes niveles de la pila de protocolos, registrando información clave como direcciones IP, puertos, tiempos de transmisión y contenido de los paquetes. Su compatibilidad multiplataforma y capacidad de ejecutarse en entornos portátiles o distribuciones orientadas a seguridad aseguran un análisis controlado y confiable, útil tanto para prácticas educativas como para auditorías y pruebas de seguridad (Cilleruelo, 2024).

1.3.3 Nmap

Nmap es una de las herramientas de escaneo más reconocidas y ampliamente utilizadas tanto en pruebas de penetración como en administración y monitoreo de redes. Su funcionalidad principal consiste en mapear de manera rápida y precisa la infraestructura de una red, permitiendo identificar hosts activos, descubrir puertos y servicios abiertos, detectar aplicaciones instaladas e incluso inferir el sistema operativo que ejecutan los dispositivos mediante técnicas de fingerprinting. Esta versatilidad hace de Nmap una herramienta esencial para quienes buscan evaluar la seguridad y el estado de sus redes (Shivanandhan, 2023).

2 Desarrollo de la practica

2.1 Creación de las maquinas virtuales

Se configuraron dos máquinas virtuales en VirtualBox utilizando una red interna (RedTest), generando un entorno aislado para realizar pruebas de seguridad sin afectar la red del anfitrión.

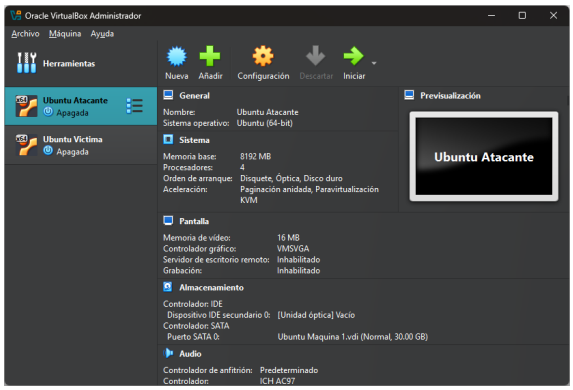

Figura 1: Maquinas a usar

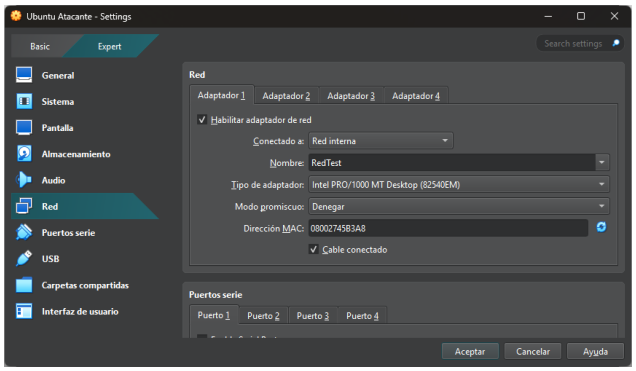

Figura 2: Configuración de la red

2.2 Asignación de direcciones IP y verificación de conectividad

Se asignaron direcciones IP a cada máquina virtual y se realizaron pruebas de conectividad mediante el comando ping para confirmar que todas las máquinas se encontraban correctamente interconectadas dentro de la misma red interna. Las redes fueron `10.0.0.10` para la victima y `10.0.0.11` para el atacante

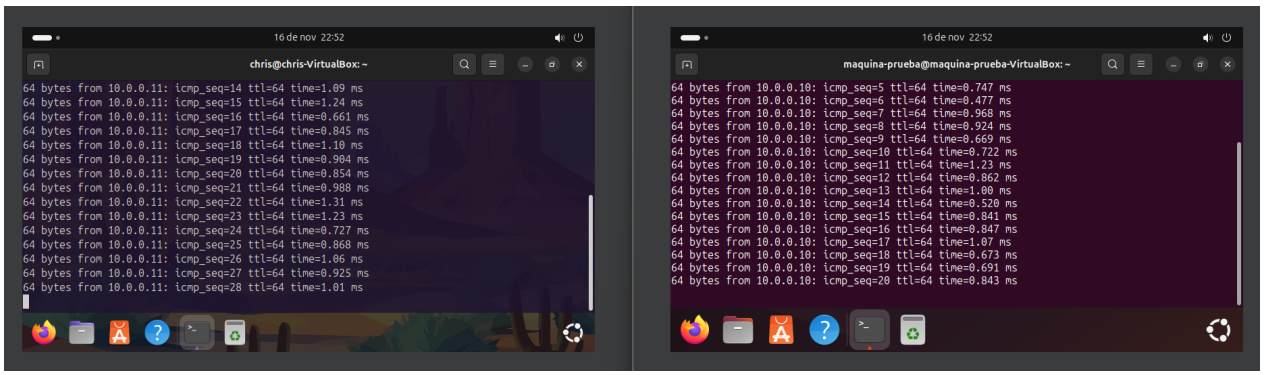

Figura 3: Ping para probar que efectivamenten están conectadas

2.3 Prueba de funcionamiento de Wireshark

Se verificó el correcto funcionamiento de Wireshark realizando una captura de tráfico en la interfaz *enp0s3* . Durante la prueba, se ejecutó un ping desde otra máquina dentro de la misma red

interna, y Wireshark logró identificar y mostrar los paquetes ICMP correspondientes. Esto confirmó que la herramienta estaba capturando el tráfico en tiempo real y sobre la interfaz adecuada.

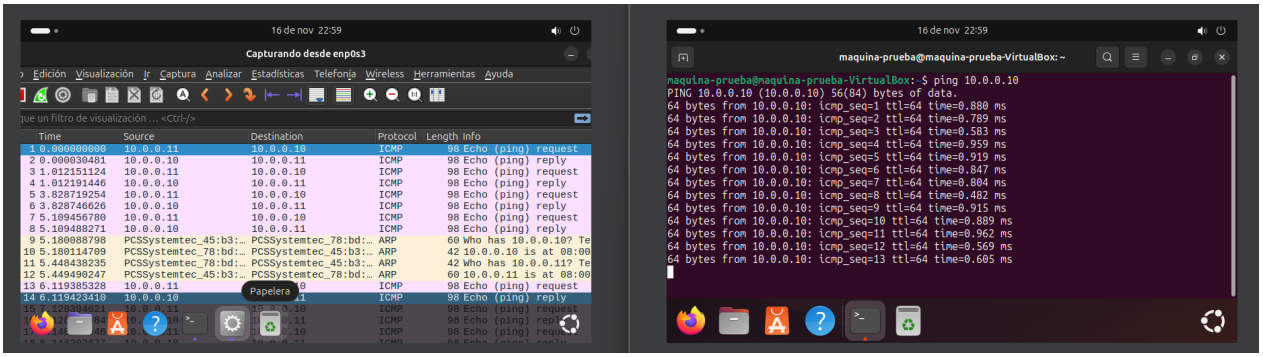

Figura 4: Prueba de Wireshark realizando una captura de tráfico

2.4 Escaneo de Descubrimiento de Host (Ping Scan)

Comando: `nmap -sn 10.0.0.10`

Este escaneo solo verifica si el host está activo. En redes LAN utiliza ARP en lugar de ICMP. En Wireshark se observan solicitudes ARP del atacante y respuestas ARP de la víctima. Es sigiloso a nivel de puertos, pero visible en la capa de enlace.

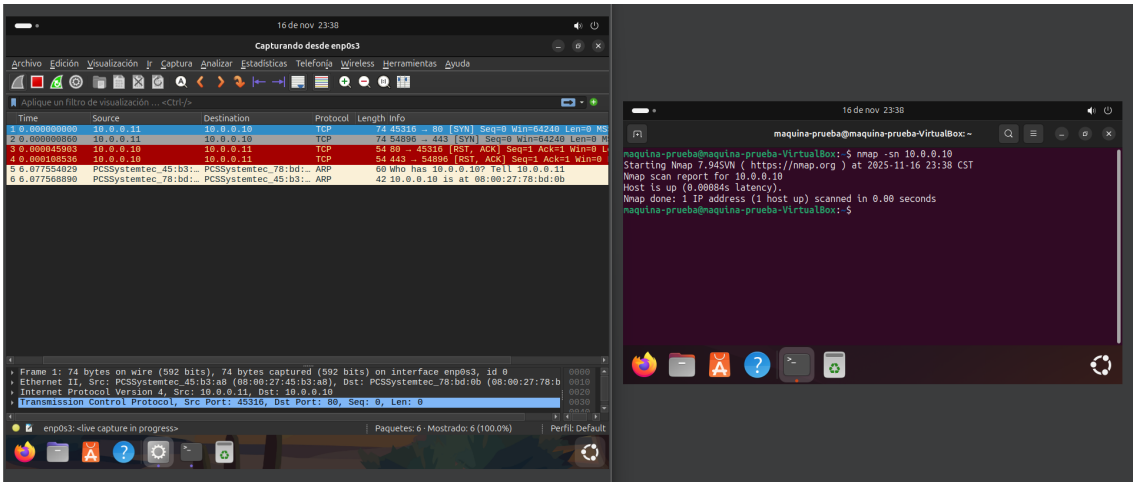

Figura 5: Captura ARP en Wireshark durante ping scan

2.5 Escaneo TCP Connect (Por Defecto)

Comando: `nmap 10.0.0.10`

Realiza el handshake completo (SYN, SYN/ACK, ACK) para cada puerto. En Wireshark se aprecia gran cantidad de tráfico y múltiples respuestas `RST`, `ACK`. Es exacto, pero muy detectable por IDS por la cantidad de conexiones completas.

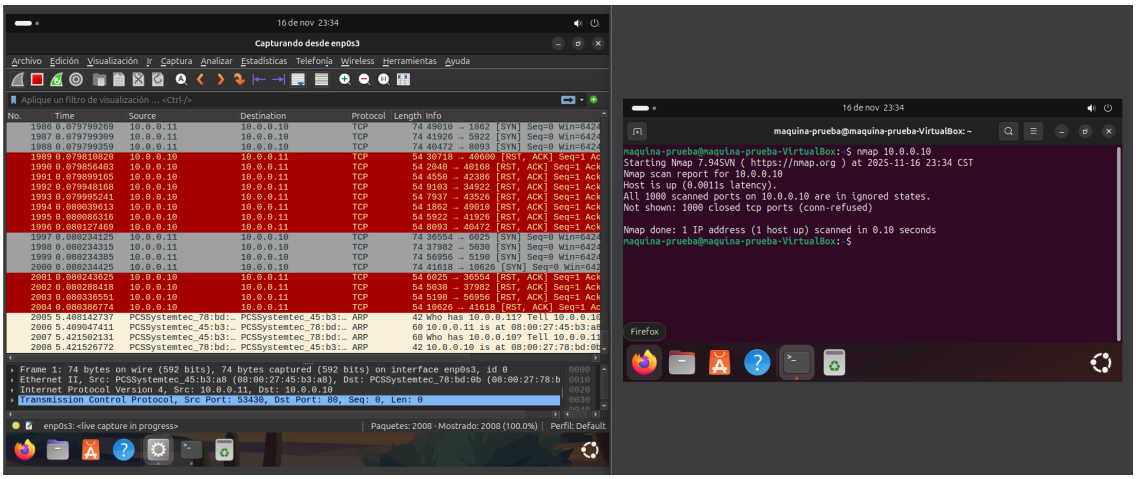

Figura 6: Tráfico TCP Connect en Wireshark

2.6 Escaneo TCP Connect Explícito

Comando: `sudo nmap -sT 10.0.0.10`

Versión explícita del escaneo anterior usando la llamada `connect()`. Wireshark muestra muchas respuestas `RST, ACK`. Genera registros en la máquina víctima, por lo que no es sigiloso.

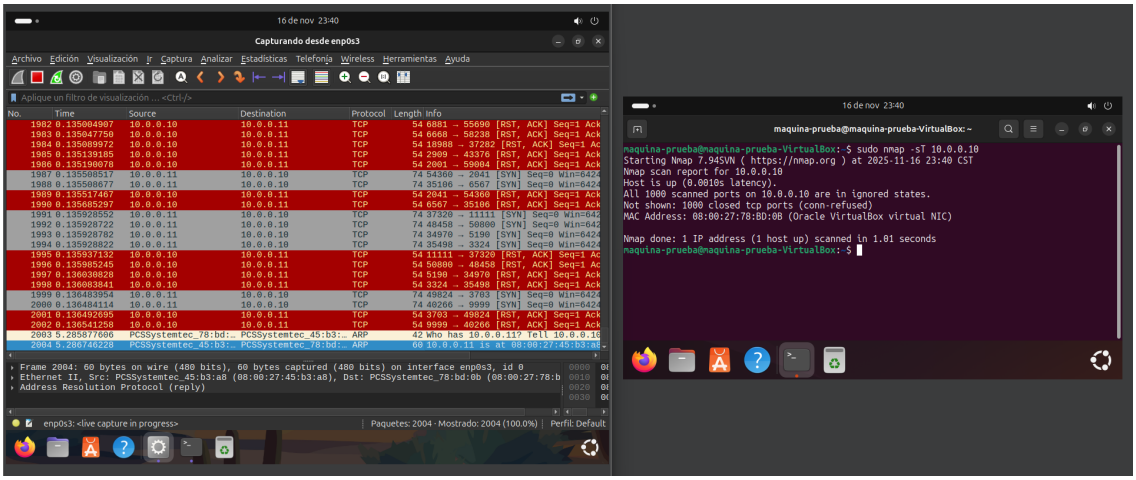

Figura 7: Tráfico de escaneo TCP explícito

2.7 Escaneo TCP SYN (Stealth)

Comando: `sudo nmap -sS 10.0.0.10`

Escaneo medio abierto: envía `SYN`, recibe `SYN/ACK`, pero responde `RST` para evitar completar la conexión. El patrón en Wireshark es: SYN → SYN/ACK → RST. Es más discreto que `-sT` y suele evitar registros de servicios.

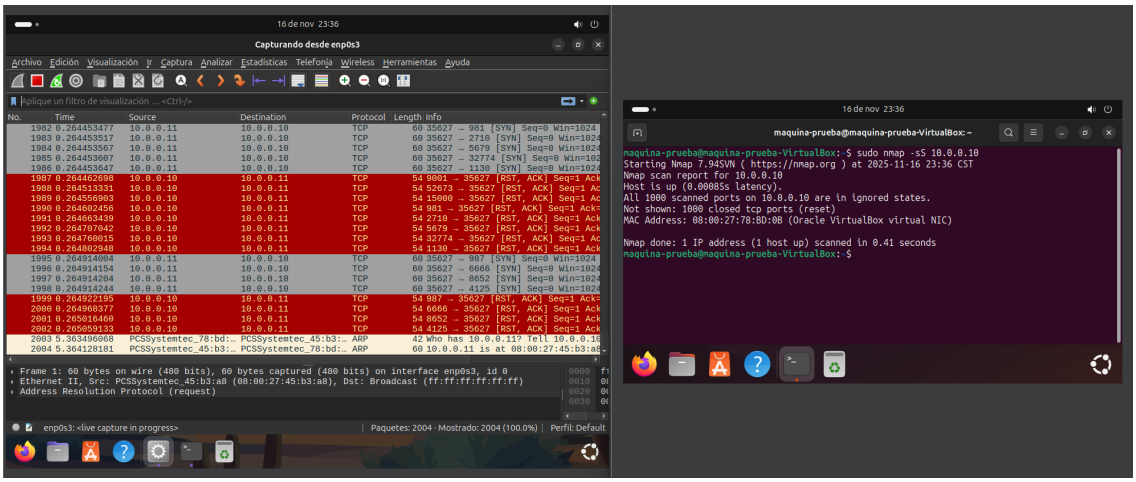

Figura 8: Secuencia SYN-SYN/ACK-RST en escaneo sigiloso

2.8 Escaneo a Puertos Específicos

Comando: `sudo nmap -sS -p 200,1000,9999 10.0.0.10`

Escanea únicamente puertos definidos. La captura muestra exactamente tres intentos `SYN` y sus respuestas, sin ruido adicional. Reduce la detección basada en volumen.

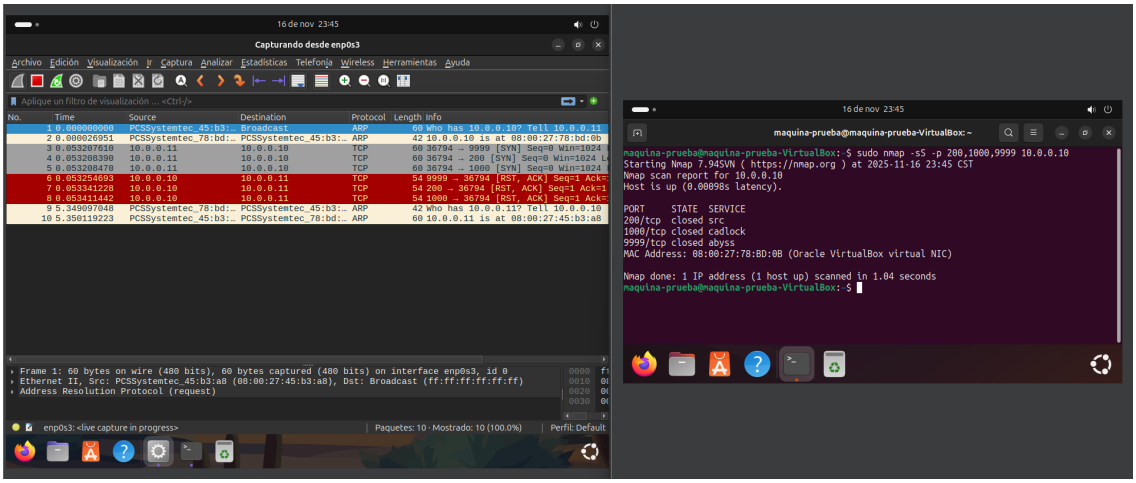

Figura 9: Escaneo limitado a puertos específicos

2.9 Escaneo UDP

Comando: `sudo nmap -sU 10.0.0.10`

Envía paquetes UDP vacíos. En Wireshark predominan mensajes ICMP Type 3 Code 3 (*Port Unreachable*). Es lento y ruidoso, por lo que se detecta fácilmente.

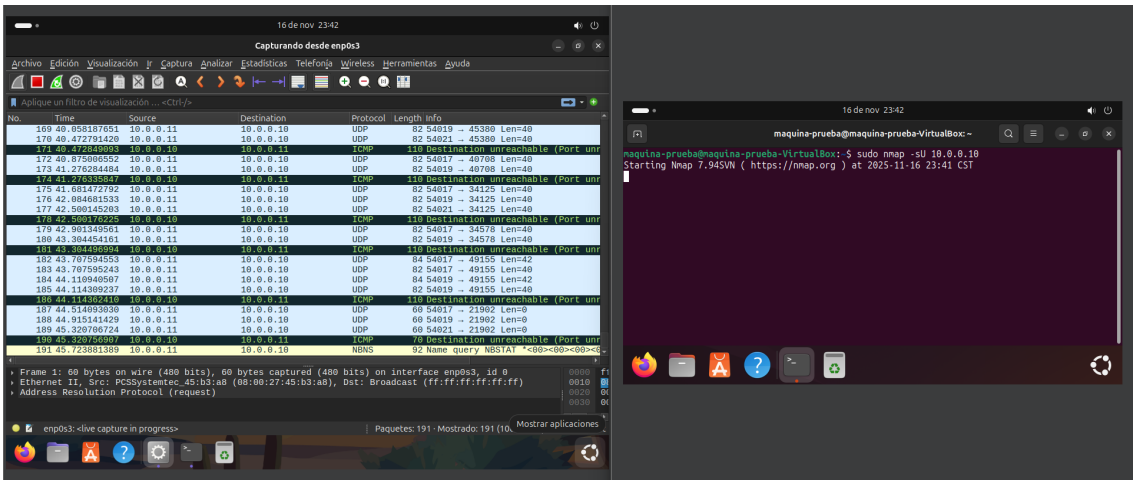

Figura 10: Mensajes ICMP en escaneo UDP

3 Conclusiones

3.1 Resultados

Los resultados obtenidos en la práctica demostraron la utilidad y complementariedad de las herramientas Nmap y Wireshark dentro de un entorno controlado. La creación del sandbox mediante máquinas virtuales en VirtualBox permitió realizar escaneos y capturas de tráfico sin comprometer la red del anfitrión. Durante las pruebas, Wireshark permitió visualizar en tiempo real el tráfico generado por los distintos tipos de escaneo, identificando con claridad paquetes ARP, ICMP, TCP y UDP. De forma paralela, Nmap proporcionó información relevante sobre el estado de los puertos, la disponibilidad de los hosts y la forma en que los servicios responden ante diferentes técnicas de reconocimiento, lo que permitió observar diferencias notables en niveles de ruido, velocidad y grado de detección entre métodos como `-sn`, `-sT`, `-sS` o `-sU`.

Los resultados mostraron también que ninguna técnica de escaneo es completamente indetectable. Incluso los métodos considerados sigilosos, como el escaneo SYN, dejan evidencias claras en el tráfico de red cuando se monitorea con herramientas como Wireshark, esto evidencia que aunque Nmap puede evadir ciertos registros en aplicaciones o servicios, siempre existirán rastros.

3.2 Recomendaciones

Es recomendable utilizar herramientas de monitoreo como Wireshark para supervisar la red y detectar posibles actividades anómalas o intrusiones. Asimismo, es aconsejable mantener activas medidas de seguridad como firewalls, antivirus y filtros de red para proteger los equipos y la información, incluso durante prácticas de auditoría en entornos seguros. Realizar escaneos de manera planificada, enfocándose en puertos o rangos específicos, ayuda a reducir el riesgo de afectar el funcionamiento de la red y facilita la identificación de comportamientos inusuales.

Referencias Bibliográficas

Amazon Web Services (2024). *¿Qué es ICMP?* URL: https://aws.amazon.com/es/what-is/icmp.

Cilleruelo, Carlos (2024). *¿Qué es Wireshark?* URL: https://keepcoding.io/blog/que-es-wireshark.

Cloudflare (s. f.). *¿Qué es el User Datagram Protocol (UDP/IP)?* URL: https://www.cloudflare.com/es-es/learning/ddos/glossary/user-datagram-protocol-udp.

Fernández, Yúbal (2020). *VirtualBox: qué es y cómo usarlo para crear una máquina virtual con Windows u otro sistema operativo*. URL: https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-otro-sistema-operativo.

Fortinet (2025). *Definición y explicación de la dirección IP*. URL: https://www.fortinet.com/lat/resources/cyberglossary/what-is-ip-address.

IBM (2021). *Address Resolution Protocol (Protocolo de resolución de direcciones)*. URL: https://www.ibm.com/docs/es/aix/7.1.0?topic=protocols-address-resolution-protocol.

IONOS (2024). *¿Qué es un intrusion detection system (IDS)?* URL: https://www.ionos.mx/digitalguide/servidores/seguridad/intrusion-detection-system-ids.

Jesús (2024). *Qué es un Puerto de Red: Conceptos Básicos y Aplicaciones*. URL: https://ghost2.dongee.com/tutoriales/que-es-un-puerto-de-red.

mdn (s. f.). *TCP*. URL: https://developer.mozilla.org/es/docs/Glossary/TCP.

Microsoft (s. f.). *Explicación del protocolo de enlace triple a través de TCP/IP*. URL: https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/three-way-handshake-via-tcpip.

Oracle (s. f.). *Oracle VirtualBox*. URL: https://www.oracle.com/latam/virtualization/virtualbox.

Shivanandhan, Manish (2023). *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos*. URL: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos.

Susnjara, Stephanie (s. f.). *¿Qué es una máquina virtual (VM)?* URL: https://www.ibm.com/mx-es/think/topics/virtual-machines.

Wireshark (s. f.). *The world's leading network protocol analyzer*. URL: https://www.wireshark.org.