AUDITORÍA DE RED CON WIRESHARK Y NMAP

REPORTE

INGENIERÍA EN COMPUTACIÓN

UNIVERSIDAD DEL ISTMO CAMPUS TEHUANTEPEC.

Autor del reporte:
Jeycson Gabriel López Hernández
0122040057

Curso:
Redes de computadoras II.

Docente:
Carlos Mijangos Jimenez.

Fecha de Entrega:
15 de Noviembre de 2025

Santo Domingo Tehuantepec, 15 de noviembre de 2025.

INDICE

INTRODUCCIÓN

La ciberseguridad es la práctica de proteger las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos (Kaspersky, s.f). Muchas veces los grandes corporativos tienden a contratar personal especializado para localizar vulnerabilidades en sus sistemas y entornos de trabajo de su empresa ya que un riesgo potencial puede causar pérdidas y grandes afectaciones a una compañía.

Las vulnerabilidades van desde las físicas como no contar con los sistemas adecuados de revisión del personal, hasta las digitales, cómo tener algún programa infectado sin que nadie sospeche. Una vulnerabilidad hace referencia a la posible intromisión en un sistema informático (Feito, 2007).

Una auditoría es un proceso que consiste en revisar y evaluar cómo se protegen los equipos, sistemas y datos (INCIBE, s.f.). Dentro de ellas pueden usarse diferentes medios para encontrar vulnerabilidades, por lo que regularmente se suelen dividir en dos equipos, el equipo rojo quienes simulan ataques a los sistemas de una compañía y el equipo azul quienes intentan bloquear estos ataques y recuperarse de las fallas provocadas.

Como parte de las herramientas populares en el mundo de la ciberseguridad encontramos a NMAP, una herramienta de código abierto para la exploración de redes y auditorías de seguridad (Nmap, s.f); y a Wireshark, un analizador de paquetes de red (Wireshark, s.f).

Para el desarrollo de la práctica se utilizará el sistema operativo linux Ubuntu 24.04.3 LTS, Nmap 7.94SVN, Wireshark 4.4.9, VirtualBox GUI 7.2.4 r170995 y XAMPP for linux 8.0.30.

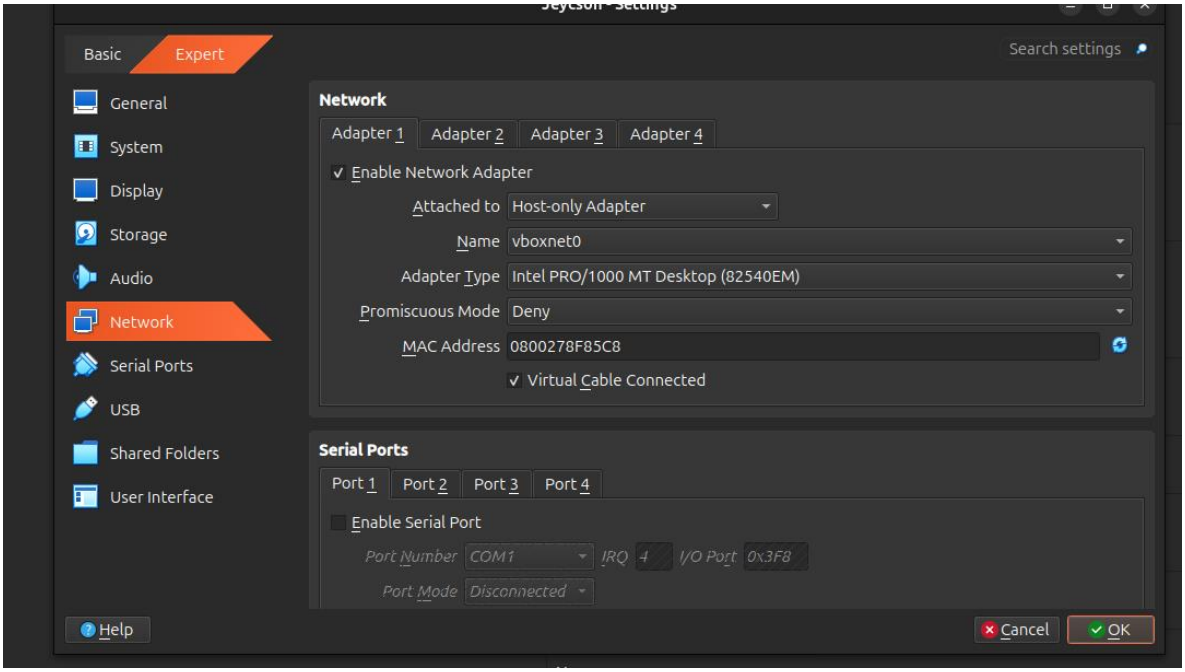
PRACTICA 1: AUDITORIA DE RED CON WIRESHARK Y NMAP

El objetivo de esta práctica es aprender y comprender como usar NMAP y Wireshark para hacer auditoria en redes, en este caso llevándolo a un entorno seguro y limitado entre una máquina virtual y una máquina anfitriona.

En el caso de la práctica realizada, ambas máquinas sirven el sistema operativo Ubuntu, aunque en WireShark y el NMAP están instalados en la máquina anfitriona, mientras que en la máquina virtual tenemos instalada la aplicación de XAMPP, para servir diferentes aplicaciones.

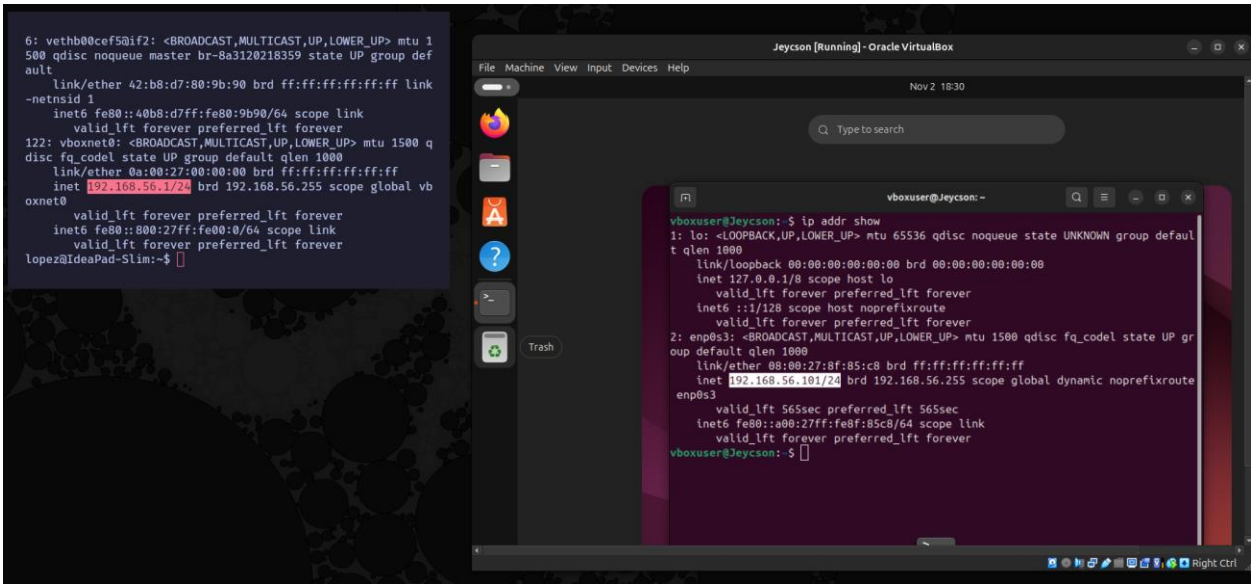
Como primer paso después de instalar las herramientas necesarias, es configurar nuestra máquina virtual para crear una red privada entre las dos máquinas simulando un entorno real donde la empresa tiene una red para cierto departamento.

Para ello después de crear nuestra máquina virtual entramos a la configuración en el apartado de Red:



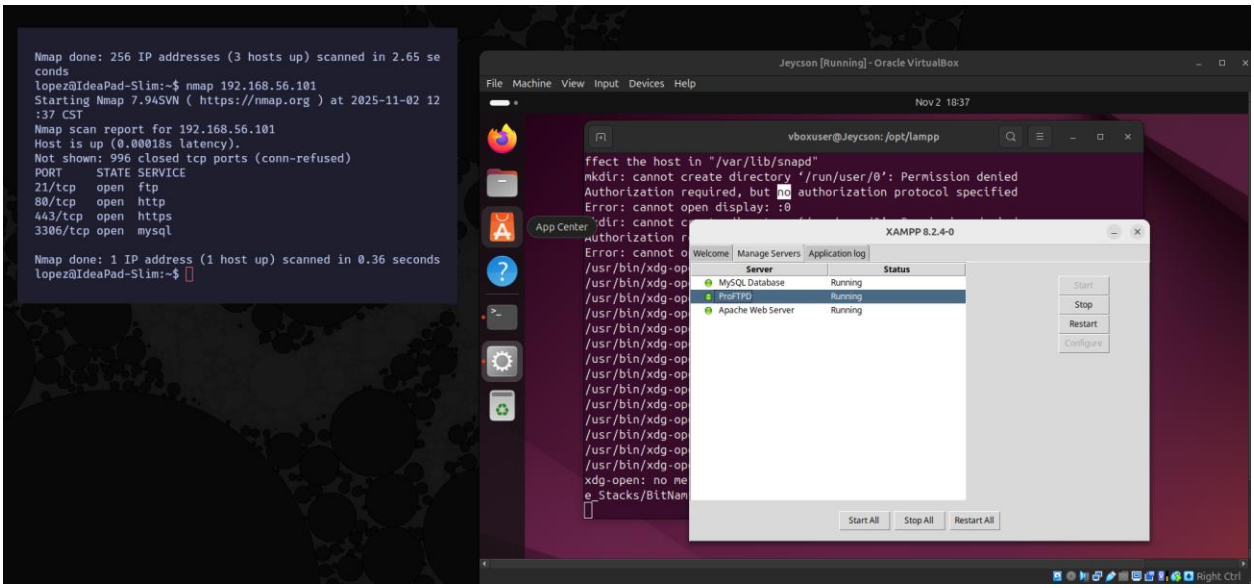
Ahí tendremos que elegir la opción de Host-only Adapter para crear una red privada entre la máquina anfitriona y la máquina virtual.

La siguiente imagen muestra las dos IP´s de nuestras máquinas, a la izquierda la IP de la máquina anfitriona y a la derecha la IP de la máquina virtual.

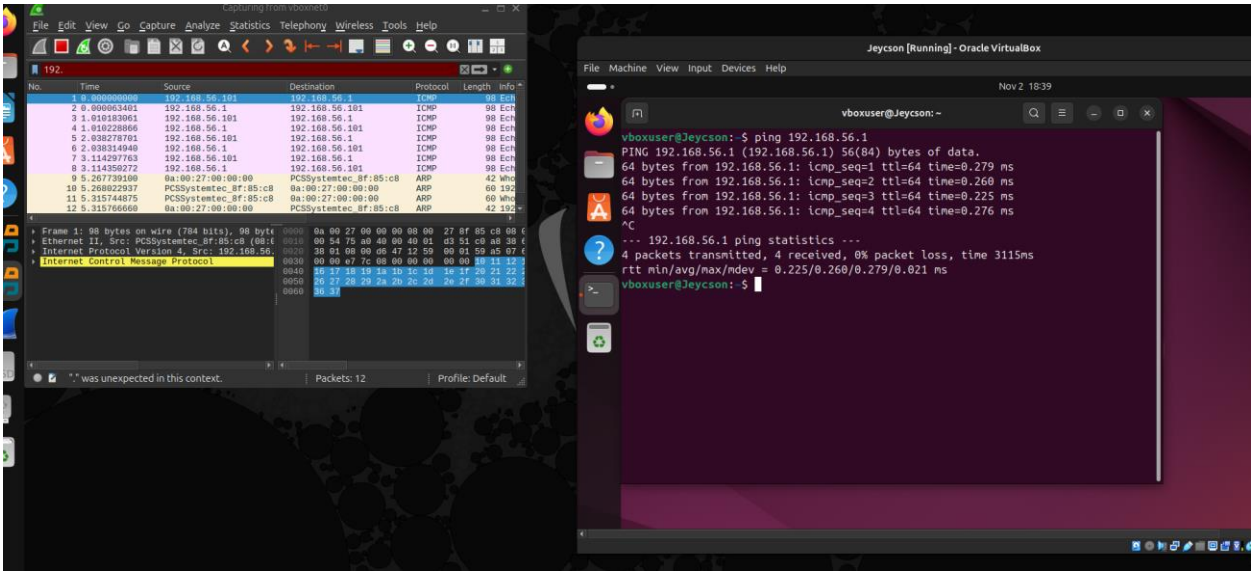


El siguiente paso es encender en nuestra máquina virtual los servicios de apache como son MySQL, ProFTPD y Apache Web Server.

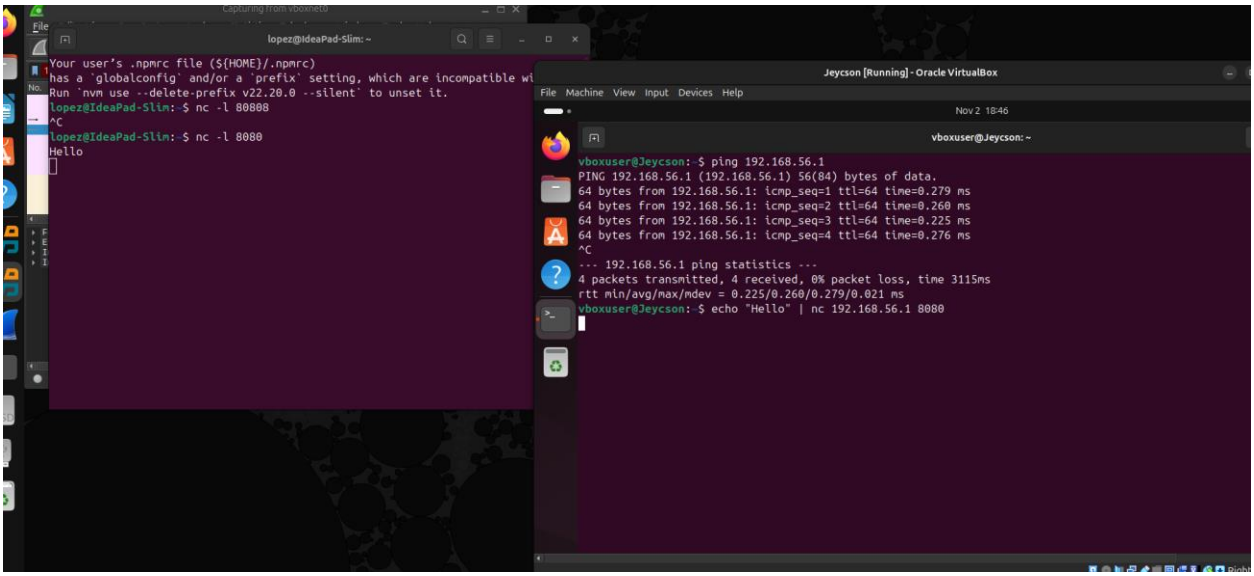
Con ayuda de NMAP vamos a analizar que puertos estan abiertos en la maquina victima en este caso, nos muestra los servicios que nosotros hemos activado con XAMPP.



Wireshark es una herramienta más completa que captura y analiza el tráfico de red, para esta práctica, la máquina virtual lanza un ping a la máquina anfitriona enviando 4 paquetes, y en nuestra máquina anfitriona vemos reflejado precisamente ese flujo de datos en la aplicación del Wireshark. Dentro de cada solicitud podemos ver el contenido de los paquetes y cómo están organizados.



Finalmente se adjunta la evidencia de la conectividad entre ambas máquinas enviando un mensaje a través de nuestra red privada.



CONCLUSIONES

La práctica de auditoría de redes realizada en un entorno virtualizado, utilizando Ubuntu, VirtualBox, NMAP y Wireshark, permitió alcanzar los objetivos planteados, que consistían en comprender y aplicar herramientas fundamentales de ciberseguridad. Los resultados obtenidos y las recomendaciones clave se resumen a continuación:

Resultados Obtenidos

- Configuración de Entorno Controlado: Se logró configurar exitosamente una red privada y aislada mediante el adaptador Host-only Adapter de VirtualBox, simulando un entorno de red real y seguro para la práctica. Esta configuración facilitó la interacción controlada entre la máquina anfitriona y la máquina virtual.
- Identificación de Servicios y Vulnerabilidades Potenciales: Mediante la herramienta NMAP, se llevó a cabo una exploración de puertos a la máquina virtual, identificando los servicios activos (Apache Web Server, MySQL, ProFTPD) habilitados por XAMPP. Este resultado demostró la eficacia de NMAP para mapear la superficie de ataque de un sistema, replicando el primer paso en una auditoría de seguridad.
- Análisis Profundo de Tráfico: Wireshark permitió la captura y el análisis detallado del flujo de datos, verificando la conectividad de la red privada con el envío de paquetes *ping* y visualizando la estructura interna de las solicitudes. Este resultado resalta la importancia de Wireshark como herramienta para el monitoreo de red y la detección de actividad anómala.
- Verificación de Conectividad: La comunicación y conectividad entre la máquina virtual y la máquina anfitriona fue confirmada exitosamente, asegurando la funcionalidad del entorno de prueba.

Recomendaciones

- Fortalecimiento de la Seguridad en Servicios: Los puertos abiertos para servicios como Apache o MySQL son puntos críticos. Se recomienda implementar reglas de *firewall* estrictas para restringir el acceso a estos puertos únicamente a las direcciones IP necesarias.
- Monitoreo Continuo de Red: Para un entorno real, se aconseja establecer una práctica de monitoreo de red constante utilizando herramientas como Wireshark o similares. Esto permite detectar patrones de tráfico sospechosos, intentos de conexión no autorizados o la transferencia de datos inusual, facilitando una respuesta temprana a incidentes de seguridad.

- Actualización y Parcheo de Sistemas: Mantener el sistema operativo, los servicios de red (como XAMPP) y las herramientas de auditoría (NMAP y Wireshark) siempre actualizados es fundamental. Las actualizaciones de software a menudo incluyen parches para vulnerabilidades de seguridad conocidas, reduciendo el riesgo de explotación.
- Aplicación Práctica en Roles de Ciberseguridad: Los conocimientos adquiridos con NMAP (perspectiva de ataque o *Red Team*) y Wireshark (perspectiva de defensa o *Blue Team*) deben ser la base para continuar el estudio y la práctica en el campo de las auditorías de seguridad y la respuesta a incidentes.

REFERENCIAS.

Feito, L. (2007). Vulnerabilidad. *Anales del Sistema Sanitario de Navarra*, *30*(Supl. 3). https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272007000600002

INCIBE. (s.f.). Auditoría de ciberseguridad: qué es, para qué sirve y cómo formarte en este campo. Recuperado el 15 de noviembre de 2025, de https://www.incibe.es/ed2026/talento-hacker/blog/auditoria-de-ciberseguridad-que-es-para-que-sirve-y-como-formarte-en-este-campo

Kaspersky. (s.f.). ¿Qué es la ciberseguridad? Definición y conceptos básicos. Recuperado el 15 de noviembre de 2025, de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Nmap. (s.f.). Nmap documentation. Recuperado el 15 de noviembre de 2025, de https://nmap.org/docs.html

Wireshark. (s.f.). Chapter 1. Introduction. Recuperado el 15 de noviembre de 2025, de https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs