Universidad Autónoma de Baja California

Facultad de Ciencias de la Ingeniería y Tecnología

Gestión y Seguridad de Redes (564)

Meta 3.3

Isai Almeraz

Sofia Perez Almaraz

Paola Gomez

08 de Septiembre del 2025

Herramientas de análisis de vulnerabilidades en sistemas operativos de red

El análisis de vulnerabilidades es un componente clave de cualquier estrategia eficiente de ciberseguridad. Involucra procesos automatizados para detectar vulnerabilidades en el software, los sistemas y la red, para permitir a las organizaciones corregir las brechas de seguridad antes que los ciberatacantes se lucren de ellas. En sí, el análisis de vulnerabilidades de red es esencial para la gestión de la seguridad y es necesario para el cumplimiento normativo en muchos sectores.

El análisis de vulnerabilidades de red utiliza herramientas de software especializadas para analizar una infraestructura o un sistema de red e identificar posibles vulnerabilidades. Estas herramientas envían sondas o paquetes a la red, simulan las acciones del atacante y analizan las respuestas para identificar posibles vulnerabilidades.

En el mercado actual, existen muchas herramientas de análisis de vulnerabilidades de red. Estas son algunas de las más comunes:

1. **Nmap:** Aunque es conocido como una herramienta de detección de redes, también incluye potentes funciones de análisis de vulnerabilidades. Cuenta con un motor de scripts permite a los usuarios personalizar los análisis, lo que lo convierte en una solución adaptable para identificar inseguridades en redes, aplicaciones y servicios.
2. **Nessus:** Es uno de los escáneres de vulnerabilidades más fiables en el mercado. Se destaca por su detección de inseguridades, configuraciones erróneas y problemas de cumplimiento normativo en una amplia gama de sistemas y aplicaciones.
3. **OpenVAS:** Es otro escáner popular de vulnerabilidades de red de código abierto que permite a los profesionales de la seguridad analizar redes en busca de inseguridades.

Metodología

Para el desarrollo de esta práctica se adoptó un enfoque experimental orientado al análisis de vulnerabilidades en sistemas operativos de red. La metodología se estructuró en las siguientes fases:

Selección de la herramienta de análisis

Se identificaron diversas herramientas de escaneo de vulnerabilidades de red (Nmap, Nessus, OpenVAS). Con base en la accesibilidad, facilidad de uso y compatibilidad con el entorno disponible, se eligió Nmap como herramienta principal de análisis.

Definición del entorno de pruebas

Se utilizó el sistema operativo Kali Linux, dada su integración nativa de herramientas de seguridad y análisis. El entorno se configuró para realizar pruebas controladas sobre la propia red y dispositivos disponibles, considerando las restricciones de seguridad establecidas por la institución.

Diseño de la estrategia de análisis

Se planificó la ejecución de distintos tipos de escaneo (verificación de instalación, escaneo básico y exploración de puertos comunes) con el fin de observar las capacidades de Nmap en la detección de servicios activos y potenciales vulnerabilidades.

Registro y análisis de resultados

Los resultados obtenidos en cada fase del escaneo fueron documentados y contrastados con la teoría revisada. Posteriormente, se evaluaron los hallazgos en función de su relevancia para la seguridad en redes y la gestión de vulnerabilidades.

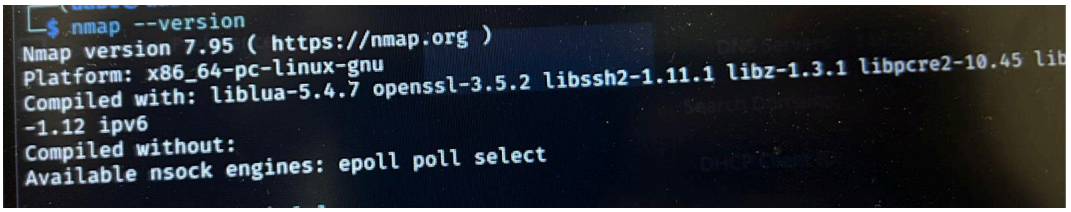
Esta metodología permitió estructurar el trabajo de manera ordenada, garantizando que la práctica no se limitará a la ejecución de comandos, sino que incluyera un análisis crítico de los resultados y su importancia dentro del campo de la ciberseguridad.

Proceso y Resultados

En esta práctica decidimos utilizar la herramienta de análisis de vulnerabilidades de red: **Nmap**, en Kali Linux.

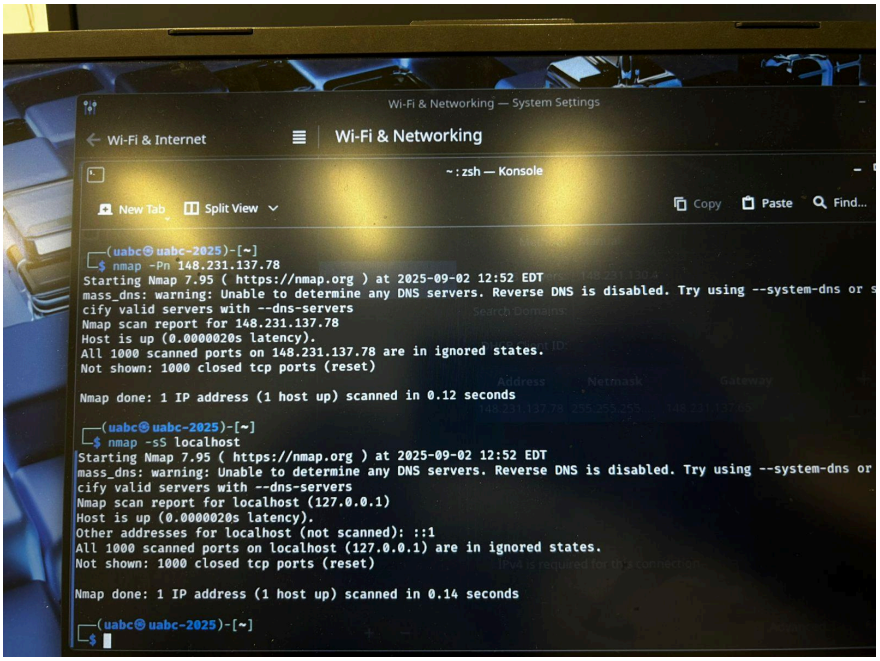
Paso 1. Verificar si Kali Linux tiene instalado nmap con el siguiente comando.

```
nmap --version
```



Paso 2. Probar Nmap con un escaneo básico.

```
# Escanear a tu propia máquina (loopback)
nmap 127.0.0.1
# Escanear puertos comunes
nmap -sS localhost
```



Conclusiones

En conclusión, se vieron algunas herramientas de vulnerabilidades que se usan diariamente en el área de seguridad en redes, las cuales son relativamente fáciles de usar e instalar. En nuestro caso utilizamos **Nmap,** el cual nos ayudó a buscar puertos abiertos en nuestra red y ver sus vulnerabilidades, a pesar de tener algunas restricciones por el firewall de UABC, pudimos ver en acción el proceso de escaneo y detección de puertos vulnerables.

Referencias

Balbix. (2019, November 27). What to know about Vulnerability Scanners and Scanning Tools. Balbix. https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/

Jacky. (2023, October 18). Sapphire. Wordpress-331244-3913986.Cloudwaysapps.com. https://www.sapphire.net/blogs-press-releases/network-vulnerability-scanning/