Universidad del Istmo

Campus Tehuantepec

Carrera: Ingeniería en computación

Grupo: 704

Alumno:

Juan Emmanuel Becerril Nolasco

Materia: Redes II

Profesor: Carlos Mijangos Jimenéz

1er Parcial

Trabajo: “Investigación sobre Wireshark y Nmap”

Santo Domingo Tehuantepec, a 15 de octubre del 2025

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. 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.
- Cuenta con una herramienta de líneas de comandos para ejecutar funcionalidades llamada TShark, similar al terminal de linux. Entre los comandos más destacados, se puede mencionar rawshark, editcap, mergecap, text2pcap.

Entre sus ventajas más destacadas se puede mencionar que:

- Cuenta con una comunidad enorme, que ayuda cuando alguien necesita buscar algo muy específico en esos paquetes de red y disectores.
- Captura también todo tipo de paquetes al analizar la red.
- Muestra errores y problemas en niveles por debajo del protocolo HTTP.
- Permite guardar y restaurar los datos empaquetados capturados, en ficheros pcap.

Entre sus desventajas, se pueden destacar las siguientes:

- Al analizar la red no se pueden modificar datos de los paquetes, solo mediante ficheros de red, sus pcap.
- La interfaz que usa es poco intuitiva.

Entre los usos disponibles con los que cuenta 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; los protocolos de correo, como Post Office Protocol 3 y SMTP; y los protocolos de compartición de archivos, como Server Message Block y Common Internet File System. Más abajo en la pila, podemos 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.

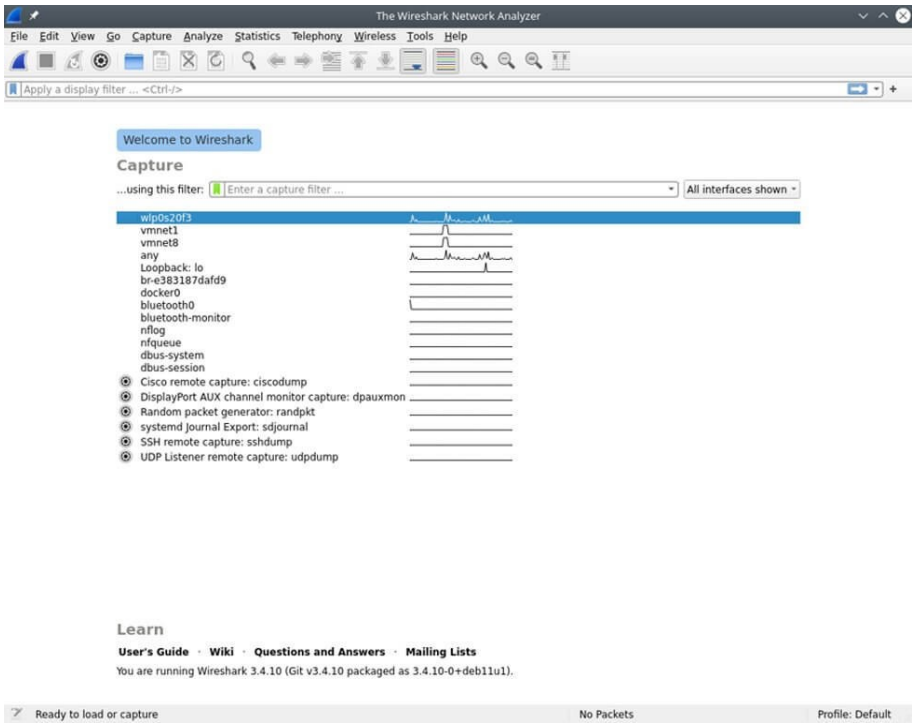

Imagen 1. Interfaz de Wireshark

Nmap

Nmap es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux 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.
- Interacción programable: el NSE (Nmap Scripting Engine) de Nmap permite a los usuarios crear análisis a medida y automatizar tareas complejas.
- 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.

Algunas características importantes de Nmap son las siguientes:

- 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.
- Encontrar información sobre el sistema operativo que se ejecuta en los dispositivos. Puede proporcionar información detallada, como las versiones del sistema operativo, lo que facilita la planificación de enfoques adicionales durante las pruebas de penetración.
- Durante la auditoría de seguridad y el escaneo de vulnerabilidades, es posible usar Nmap para atacar sistemas usando scripts existentes del motor de scripting de Nmap.
- Nmap tiene una interfaz gráfica de usuario llamada Zenmap, que ayuda a desarrollar mapeos visuales de una red para una mejor usabilidad y generación de informes.

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.

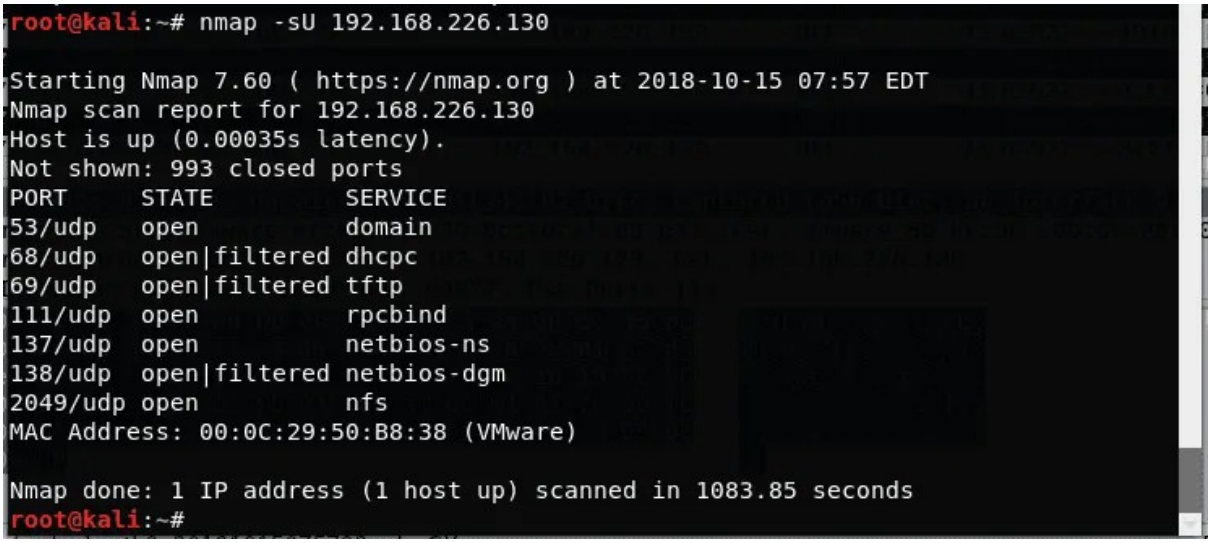

Imagen 2. Nmap realizando un escaneo de una dirección IP

Bibliografía

- https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/
- https://es.wikipedia.org/wiki/Nmap
- https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/
- https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/
- https://www.innovaciondigital360.com/iot/que-es-wireshark-y-casos-de-uso/