Un **analizador de protocolo de red**, a veces llamado sniffer de paquetes (rastreador de paquetes) o analizador de paquetes, es una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red. Suele usarse como herramienta de investigación para monitorear redes e identificar actividades sospechosas. Existe una gran variedad de analizadores de protocolos de red. Algunos de los más comunes son:

* Analizador de tráfico NetFlow de SolarWinds
* ManageEngine OpManager
* Azure Network Watcher
* Wireshark
* tcpdump

Esta lectura se centrará exclusivamente en tcpdump, aunque puedes aplicar lo que aprendas aquí a muchos de los otros analizadores de protocolos de red que utilizarás como analista de ciberseguridad, para defender el sistema de cualquier intrusión. En una próxima actividad, revisarás un registro de tráfico de datos tcpdump e identificarás un ataque DoS para practicar estas habilidades.

**tcpdump**

**tcpdump** es un analizador de protocolos de red de línea de comandos. Es popular, ligero (o sea, utiliza poca memoria y tiene un bajo uso de CPU) y usa la biblioteca de código abierto libpcap. tcpdump se basa en texto, lo que significa que todos los comandos se ejecutan en el terminal. También se puede instalar en otros sistemas operativos basados en Unix, como macOS®. Está preinstalado en muchas distribuciones de Linux.

tcpdump proporciona un breve análisis de paquetes, convierte información clave sobre el tráfico de red en formatos fácilmente legibles para las personas e imprime información sobre cada paquete directamente en el terminal. tcpdump también muestra la dirección IP de origen, las direcciones IP de destino y los números de puerto que se utilizan en las comunicaciones.

**Interpretación de la salida**

tcpdump imprime la salida del comando como los paquetes detectados en la línea de comandos y, opcionalmente, en un archivo de registro, después de ejecutar un comando. La salida de una captura de paquetes contiene mucha información importante sobre el tráfico de red.

Parte de la información que se recibe de una captura de paquetes es:

* **Marca de tiempo**: la salida comienza con la marca de tiempo, en el formato de horas, minutos, segundos y fracciones de segundo.
* **IP de origen**: el origen del paquete es proporcionado por su dirección IP de origen.
* **Puerto de origen**: el número de puerto de donde se originó el paquete.
* **IP de destino**: la dirección IP de destino es el lugar al que se transmite el paquete.
* **Puerto de destino**: el número de puerto del lugar al que se transmite el paquete.

**Nota:** De forma predeterminada, tcpdump intentará convertir direcciones de host a nombres de host. También reemplazará los números de puerto con los servicios comúnmente asociados que usan estos puertos.

**Usos comunes**

tcpdump y otros analizadores de protocolos de red se utilizan habitualmente para capturar y visualizar comunicaciones de red y para recopilar estadísticas sobre la red, por ejemplo, para solucionar problemas de rendimiento. También se pueden usar para:

* Establecer una línea de base para los patrones de tráfico de red y las métricas de utilización de la red.
* Detectar e identificar tráfico malicioso.
* Crear alertas personalizadas para enviar las notificaciones adecuadas cuando surgen problemas de red o amenazas a la seguridad.
* Localizar mensajería instantánea (IM), tráfico o puntos de acceso inalámbricos no autorizados.

Sin embargo, las/los atacantes también pueden utilizar maliciosamente los analizadores de protocolos de red para obtener información sobre una red específica. Por ejemplo, podrían capturar paquetes de datos que contengan información sensible, como nombres de usuario y contraseñas de cuentas. Como analista de ciberseguridad, es importante comprender la finalidad y los usos de los analizadores de protocolos de red.

**Conclusiones clave**

Los analizadores de protocolos de red, como tcpdump, son herramientas que se usan con frecuencia para monitorear patrones de tráfico de red e investigar actividades sospechosas. tcpdump es un analizador de protocolos de red de línea de comandos, compatible con Linux/Unix y macOS®. Al ejecutar un comando tcpdump, la herramienta mostrará información sobre el enrutamiento de paquetes, como la marca de tiempo, la dirección IP de origen y el número de puerto, así como la dirección IP de destino y su número de puerto. Por desgracia, las/los atacantes también pueden usar los analizadores de protocolos de red para capturar paquetes de datos que contienen información confidencial, como nombres de usuario y contraseñas de cuentas.