**Obtén más información sobre las capturas de paquetes**

La labor de los analistas de seguridad implica monitorear y analizar los flujos de tráfico de red. Una forma de hacerlo es generando rastreos de paquetes y luego analizando el tráfico capturado, a fin de identificar actividades inusuales en una red.

Anteriormente, exploraste los fundamentos de las redes. A lo largo de esta sección, recurrirás a tus conocimientos básicos en redes para comprender mejor los flujos de tráfico de red. En esta lectura, aprenderás sobre los tres aspectos principales del análisis de redes: paquetes, analizadores de protocolos de red y rastreo de paquetes.

**Paquetes**

Anteriormente en el programa, aprendiste que un **paquete de datos** es una unidad básica de información que va de un dispositivo a otro dentro de una red. La detección de intrusiones en la red comienza a nivel de paquetes. Se debe a que estos constituyen la base del intercambio de información en una red. Cada vez que realizas una actividad en Internet, como visitar un sitio web, se envían y reciben paquetes entre tu computadora y el servidor del sitio web. Estos paquetes son los que ayudan a transmitir información a través de una red. Por ejemplo, al cargar una imagen en un sitio, los datos se dividen en varios paquetes, que luego se enrutan hacia el destino previsto y se vuelven a ensamblar al ser entregados.

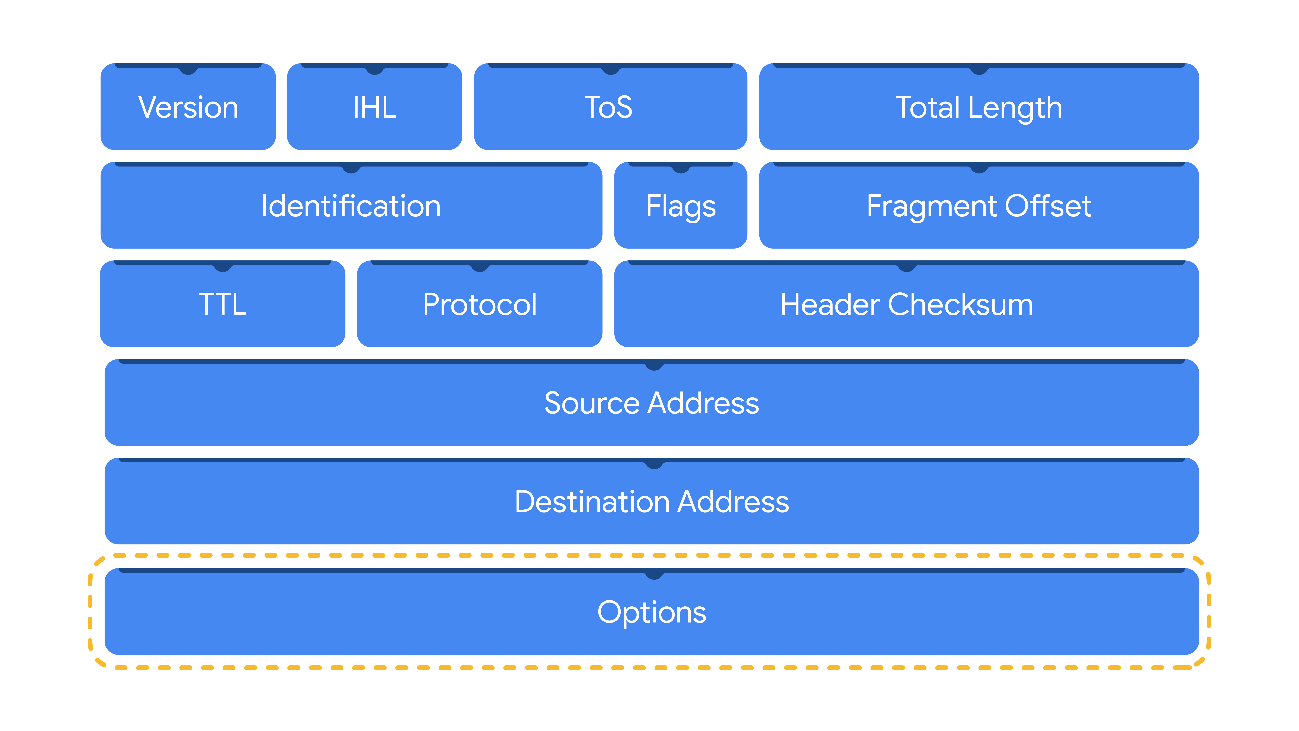
En ciberseguridad, los paquetes proporcionan información valiosa que añade contexto a los eventos durante las investigaciones. Comprender la transferencia de información a través de paquetes no solo te ayudará a desarrollar conocimiento sobre la actividad de la red, sino también a identificar anomalías y proteger mejor las redes contra los ataques.

Los paquetes tienen tres componentes: el encabezado, la carga útil y el pie. A continuación, encontrarás una descripción de cada uno.

**Encabezado**

Los paquetes comienzan con el componente fundamental: elencabezado. Estos pueden tener varios encabezados según los protocolos utilizados, como un encabezado Ethernet, uno de IP o uno de TCP, entre otros. Los mismos proporcionan información que se utiliza para enrutar los paquetes a su destino. Esto incluye información sobre las direcciones IP de origen y destino, la longitud del paquete, el protocolo, los números de identificación y más.

He aquí un encabezado IPv4 con la información que proporciona:



**Carga útil**

Elcomponente de carga útil viene directamente después del encabezado y contiene los datos reales que se entregan. Si consideras el ejemplo de cargar una fotografía en un sitio web, la carga útil de este paquete sería la imagen en sí.

**Pie**

El pie, también conocido como el avance, se encuentra al final de un paquete. El protocolo Ethernet utiliza pies para brindar información de verificación de errores y determinar si los datos se dañaron. Además, puede que los paquetes de red Ethernet analizados no muestren información de pie debido a las configuraciones de red.

**Nota:** La mayoría de los protocolos, como el Protocolo de Internet (IP), *no* utilizan pies.

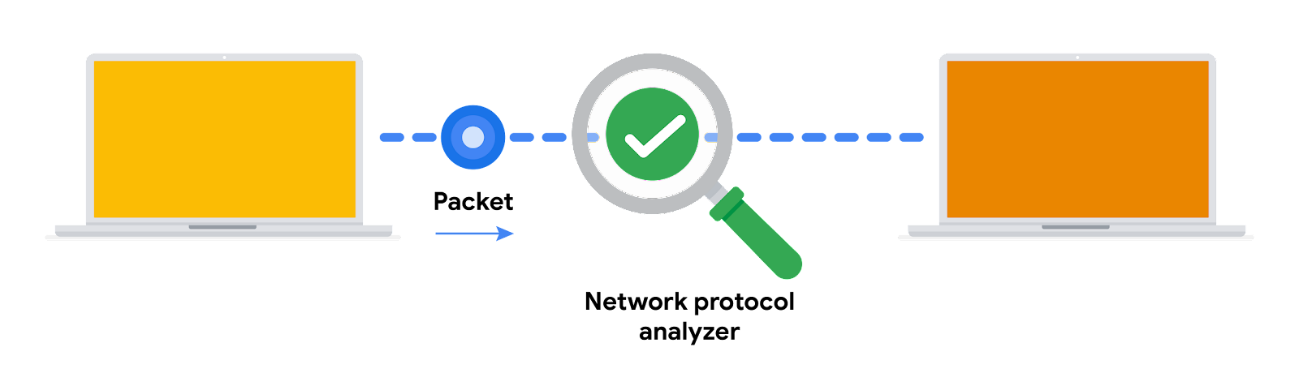
**Analizadores de protocolo de red**

**Los analizadores de protocolo de red,** **o rastreadores de paquetes,** son herramientas diseñadas para capturar y analizar el tráfico de datos dentro de una red. Algunos ejemplos son tcpdump, Wireshark y TShark.

Más allá de su uso en seguridad como una herramienta de investigación que monitorea redes e identifica actividades sospechosas, los analizadores de protocolo de red pueden utilizarse para recopilar estadísticas de redes, como el ancho de banda o la velocidad de conexión, y solucionar problemas de rendimiento, como las ralentizaciones.

No obstante, también se pueden utilizar con fines maliciosos. Por ejemplo, los agentes de amenaza pueden usar analizadores de protocolo de red para capturar paquetes que contienen datos confidenciales, como la información de inicio de sesión de la cuenta.

Aquí hay un diagrama de red que ilustra la transmisión de los paquetes de un emisor al receptor. Un analizador de protocolos de red se coloca en el medio de las comunicaciones para capturar los paquetes de datos que viajan a través del cable.



**Cómo funcionan los analizadores de protocolo de red**

Estos analizadores utilizan capacidades de software y hardware para capturar el tráfico de red y mostrarlo para que los analistas de seguridad lo examinen y analicen. A continuación, te contamos cómo lo hacen:

1. Primero, los paquetes deben recopilarse de la red a través de la **tarjeta de interfaz de red (NIC)**, que es el hardware que conecta las computadoras a una red, como un router. Las NIC reciben y transmiten tráfico de red, pero por defecto solo consideran el tráfico de red que está dirigido a ellas. Para capturar todo el tráfico que se envía a través de la red, una NIC debe ser cambiada a un modo que tenga acceso a todos los paquetes de datos de red visibles. En las interfaces inalámbricas, esto se conoce con frecuencia como modo de monitoreo, y en otros sistemas se puede llamar modo promiscuo. Este modo permite que la NIC acceda a todos los paquetes de datos de red visibles, pero no ayudará a los analistas a acceder a todos los paquetes a través de una red. Un analizador de protocolos de red debe posicionarse en un segmento de red apropiado para acceder a todo el tráfico entre diferentes hosts.
2. El analizador de protocolos de red recopila el tráfico de red en formato binario sin procesar. El formato binario consta de ceros y unos, y las personas no pueden interpretarlo con facilidad. El analizador de protocolos de red toma el formato binario y lo convierte para que se muestre en un modo legible para las personas, de modo que los analistas puedan leer y comprender la información con facilidad.

**Cómo capturar paquetes**

El **rastreo de paquetes** es la práctica de capturar e inspeccionar paquetes de datos a través de una red. Un archivo **pcap (captura de paquetes )** es un archivo que contiene paquetes de datos interceptados desde una interfaz o red. Estas capturas se pueden ver y analizar adicionalmente mediante analizadores de protocolo de red. Por ejemplo, puedes filtrar las capturas de paquetes para mostrar solo la información más relevante para tu investigación, como los paquetes enviados desde una dirección IP específica.

**Nota**: En muchos lugares, se considera ilegal utilizar analizadores de protocolo de red para interceptar y examinar las comunicaciones de red privada sin permiso.

Los archivos pcap pueden venir en diversos formatos según la biblioteca de captura de paquetes que se utilice. Cada uno tiene diferentes usos y las herramientas de red pueden utilizar o admitir formatos de archivo de captura de paquetes específicos de forma predeterminada. Te recomendamos familiarizarte con las siguientes bibliotecas y formatos:

1. **Libpcap** es una biblioteca de captura de paquetes diseñada para que la utilicen sistemas similares a Unix, como Linux y MacOS®. Las herramientas como tcpdump utilizan Libpcap como formato predeterminado de archivo de captura de paquetes.
2. **WinPcap** es una biblioteca de captura de paquetes de código abierto diseñada para dispositivos que ejecutan sistemas operativos Windows. Se considera un formato de archivo más antiguo y no se usa principalmente.
3. **Npcap** es una bibliotecadiseñada por la herramienta de escaneo de puertos Nmap que se utiliza comúnmente en los sistemas operativos Windows.
4. **PCAPng** es un formato de archivo moderno que puede capturar paquetes y almacenar datos en simultáneo. Su capacidad para hacer ambas cosas explica el “ng”, que significa “próxima generación”.

**Consejo profesional:** Analizar tu red doméstica puede ser una buena manera de poner en práctica el uso de estas herramientas.

**Conclusiones clave**

Los analizadores de protocolo de red son herramientas de investigación útiles que te brindan información sobre la actividad en una red. Como analista, utilizarás herramientas de análisis de protocolo de red para ver y examinar archivos de captura de paquetes, comprender mejor las comunicaciones de red y defenderte de las intrusiones.

**Recursos para obtener más información**

Este artículo de Infosec describe los riesgos de la [elaboración de paquetes](https://resources.infosecinstitute.com/topic/packet-crafting-a-serious-crime/), una técnica utilizada para probar la estructura de una red.