Seminario de Solución de Problemas de Redes de Computadoras y Protocolos de Comunicación

Internet

WireShark

16 de abril de 2024

Romero Brambila Ignacio Aarón

Investigación y análisis de WireSharsk

Describir que es un analizador de protocolos

Un analizador de protocolos es una herramienta de software diseñada para capturar, analizar y diagnosticar el tráfico de red. Su función principal es interceptar y examinar los datos que fluyen a través de una red, desglosándolos en sus componentes individuales para su inspección y comprensión.

¿Qué es el Wireshark?

Wireshark es uno de los analizadores de protocolos más populares y potentes disponibles. Anteriormente conocido como Ethereal, Wireshark es una herramienta de código abierto que permite a los usuarios capturar y analizar el tráfico de red en tiempo real. Puede trabajar en una variedad de sistemas operativos, incluyendo Windows, macOS y Linux.

¿Qué puede analizar el Wireshark?

Wireshark es capaz de analizar una amplia gama de protocolos de red, desde los comunes como TCP, UDP, IP y HTTP, hasta protocolos más específicos de aplicaciones. Puede inspeccionar paquetes de datos a nivel de bit, decodificar estructuras de mensajes y filtrar el tráfico según una variedad de criterios.

Mencionar por lo menos tres aplicaciones más que son analizadores de redes de datos y dar una breve descripción de cada uno de ellos

Tcpdump:

Es una herramienta de línea de comandos para la captura y análisis de paquetes de red en sistemas Unix y derivados. Tcpdump proporciona una interfaz de usuario en la línea de comandos para examinar el tráfico de red en tiempo real, así como opciones avanzadas para filtrar y analizar paquetes.

Microsoft Network Monitor:

Desarrollado por Microsoft, es una herramienta de captura y análisis de paquetes para entornos Windows. Ofrece capacidades similares a las de Wireshark, permitiendo a los usuarios capturar y examinar el tráfico de red para diagnosticar problemas y monitorear la actividad de la red.

Ethereal:

Aunque ya no es la denominación oficial, Ethereal es el predecesor de Wireshark y todavía es utilizado en algunos entornos. Es una herramienta de análisis de protocolos de red de código abierto que ofrece una amplia gama de funcionalidades para capturar y analizar el tráfico de red en tiempo real.