Protocolos de red más comunes

En esta sección del curso, aprendiste sobre protocolos de red y cómo organizan la comunicación a través de una red. Esta lectura profundizará en los protocolos de red y repasará algunos de los protocolos básicos que has aprendido anteriormente. Además, se presentarán nuevos protocolos y se analizará cómo estos están involucrados en la seguridad de redes.

Descripción general de los protocolos de red

Un **protocolo de red** es un conjunto de reglas utilizadas por dos o más dispositivos de una red para describir el orden de entrega y la estructura de los datos. Los protocolos de red funcionan como instrucciones que vienen junto con la información en el paquete de datos. Estas instrucciones indican al dispositivo receptor qué hacer con los datos. Los protocolos son como un lenguaje común que permite que los dispositivos de todo el mundo se comuniquen entre sí y se entiendan .

Aunque los protocolos de red desempeñan una función esencial en la comunicación de red, las/los analistas de seguridad deben comprender las implicaciones de seguridad asociadas a ellos. Algunos protocolos tienen vulnerabilidades que pueden ser aprovechadas por agentes de amenaza. Por ejemplo, podría utilizar el protocolo del sistema de nombres de dominio (DNS), para desviar el tráfico desde un sitio web legítimo hacia un sitio web malicioso que contiene malware. Obtendrás más información sobre este tema en los materiales del curso que se presentará próximamente.

Las tres categorías de protocolos de red

Los protocolos de red se pueden dividir en tres categorías principales: protocolos de comunicación, de gestión y de seguridad. Existen decenas de protocolos de red diferentes, pero no es necesario que los memorices todos para desempeñar un puesto de analista de seguridad de nivel inicial. Sí es importante que conozcas aquellos que mencionamos en esta lectura.

Protocolos de comunicación

Los protocolos de comunicación rigen el intercambio de información en la transmisión de redes. Determinan cómo se transmiten los datos entre los dispositivos y el momento de la comunicación. También incluyen métodos para recuperar datos perdidos durante el trayecto. A continuación, se presentan algunos de ellos.

- El **protocolo de control de transmisión (TCP)** es un protocolo de comunicación de Internet que permite a dos dispositivos establecer una conexión y transmitir datos. El TCP utiliza un proceso de tres pasos. Primero, el dispositivo envía una solicitud de sincronización (SYN) a un servidor. Luego, el servidor responde con un paquete SYN/ACK para confirmar la recepción de la solicitud del dispositivo. Una vez que el servidor recibe el paquete ACK final desde el dispositivo, se establece una conexión TCP. En el modelo TCP/IP, el TCP se encuentra en la capa de transporte.

- El **protocolo de datagramas de usuario (UDP)** es un protocolo sin conexión que no establece un enlace entre dispositivos antes de la transmisión. Esto lo hace menos confiable que el TCP, pero también lo hace adecuado para transmisiones que requieren llegar rápidamente a su destino. Un ejemplo de uso de UDP se da en las transmisiones de juegos en línea. En el modelo TCP/IP, el UDP se encuentra en la capa de transporte.
- El **protocolo de transferencia de hipertexto (HTTP)** es un protocolo de capa de aplicación que proporciona un método de comunicación entre clientes y servidores de sitios web. El HTTP usa el puerto 80 y se considera inseguro. Aunque aún algunos sitios web lo utilizan, en muchos otros está siendo reemplazado por una versión segura, llamada HTTPS. En el modelo TCP/IP, el HTTP se encuentra en la capa de aplicación.
- El **sistema de nombres de dominio (DNS)** es un protocolo que traduce los nombres de dominio de Internet como direcciones IP. Cuando un equipo del cliente desea acceder a un dominio de sitio web utilizando su navegador de Internet, se envía una consulta a un servidor DNS dedicado. El servidor DNS luego busca la dirección IP que corresponde al dominio del sitio web. El DNS suele usar un protocolo de datagramas de usuario (UDP) en el puerto 53. Sin embargo, si la respuesta del DNS a una solicitud es grande, se pasará al protocolo TCP. En el modelo TCP/IP, el DNS se encuentra en la capa de aplicación.

Protocolos de gestión

La siguiente categoría es la de los protocolos de gestión. Estos se utilizan para monitorear y administrar la actividad en una red. Incluyen protocolos para notificar errores y optimizar el rendimiento en la red.

- El **protocolo simple de administración de red (SNMP)** es un protocolo de red utilizado para monitorear y gestionar los dispositivos en una red. El SNMP puede restablecer una contraseña en un dispositivo de red o cambiar su configuración básica. También puede enviar solicitudes a los dispositivos de red para obtener un informe sobre cuánto ancho de banda de la red está siendo utilizado. En el modelo TCP/IP, el SNMP se encuentra en la capa de aplicación.
- El **protocolo de mensajes de control de Internet (ICMP)** es un protocolo de Internet utilizado por los dispositivos para informarse mutuamente sobre errores de transmisión de datos en la red. El ICMP es utilizado por un dispositivo receptor para enviar un informe al dispositivo emisor sobre la transmisión de datos. Suele usarse como una forma rápida de solucionar problemas de conectividad y el tiempo de respuesta (o latencia) de la red mediante la emisión del comando “ping” en un sistema operativo Linux. En el modelo TCP/IP, el ICMP se encuentra en la capa de Internet.

Protocolos de seguridad

Los protocolos de seguridad garantizan que los datos se envíen y reciban de forma segura a través de una red. Estos utilizan algoritmos de cifrado para proteger los datos durante su transmisión. A continuación, se presentan algunos de los protocolos de seguridad más comunes.

- El **protocolo seguro de transferencia de hipertexto (HTTPS)** es un protocolo de red que proporciona un método de comunicación seguro entre clientes y servidores de sitios web. El

HTTPS es una versión segura del HTTP que utiliza cifrado de capa de conexión segura/seguridad en la capa de transporte (SSL/TLS) en todas las transmisiones para que los/as agentes de amenaza no puedan leer la información. El HTTPS utiliza el puerto 443. En el modelo TCP/IP, el HTTPS se encuentra en la capa de aplicación.

- El **protocolo seguro de transferencia de archivos (SFTP)** es un protocolo seguro utilizado para transferir archivos de un dispositivo a otro a través de una red. El SFTP utiliza el protocolo Secure Shell (SSH), en general, a través del puerto TCP 22. El SSH utiliza un estándar de cifrado avanzado (Advanced Encryption Standard, AES) y otros tipos de encriptación para asegurar que destinatarios no deseados no puedan interceptar las transmisiones. En el modelo TCP/IP, el SFTP se encuentra en la capa de aplicación. El SFTP suele utilizarse con almacenamiento en la nube. Cada vez que un/a usuario/a carga o descarga un archivo desde el almacenamiento en la nube, el documento se transfiere utilizando el protocolo SFTP.

Nota: Los protocolos de cifrado mencionados no ocultan la dirección IP de origen o el destino del tráfico de red. Esto significa que, si lo intercepta, un/a agente de amenaza aún puede obtener cierta información básica sobre el tráfico de red.

Conclusiones clave

En esta lectura, has aprendido acerca de protocolos de redes básicos que las/los analistas de ciberseguridad en nivel inicial deben conocer.. Comprender cómo funcionan los protocolos en una red es esencial. Con este conocimiento, las/los analistas de ciberseguridad pueden abordar de manera efectiva las vulnerabilidades en una red y potencialmente prevenir futuros ataques.