Protocolos de red adicionales

En lecturas y videos anteriores, aprendiste cómo los protocolos de red organizan el envío y la recepción de datos a través de una red. También viste que los protocolos de red pueden dividirse en tres categorías: protocolos de comunicación, de gestión y de seguridad.

En esta lectura, te presentaremos algunos conceptos y protocolos adicionales que surgirán con frecuencia en tu trabajo como analista de seguridad. Algunos protocolos tienen números de puerto asignados por la Internet Assigned Numbers Authority (IANA, por sus siglas en inglés). Estos números de puerto se incluyen en la descripción de cada protocolo, si están asignados.

Traducción de direcciones de red

Los dispositivos en tu red doméstica u oficina local tienen cada uno una dirección IP privada que utilizan para comunicarse entre sí. Para que los dispositivos con direcciones IP privadas puedan comunicarse con Internet pública, necesitan tener una dirección IP pública. De lo contrario, las respuestas no se enrutarán correctamente. En lugar de tener una dirección IP pública dedicada para cada uno de los dispositivos en la red local, el enrutador puede reemplazar la dirección IP de origen privado con su dirección IP pública y realizar la operación inversa para las respuestas. Este proceso se conoce como traducción de direcciones de red (NAT) y generalmente requiere que el enrutador o cortafuegos (firewall) se configuren específicamente para tal fin. La NAT es parte de la capa 2 (capa de Internet) y la capa 3 (capa de transporte) del modelo TCP/IP.

Direcciones IP privadas

- Las asignan los administradores de red
- Son únicas solo dentro de la red privada
- No tienen costo de uso
- Rangos de direcciones:
    - 10.0.0.0-10.255.255.255
    - 172.16.0.0-172.31.255.255
    - 192.168.0.0-192.168.255.255

Direcciones IP públicas

- Las asignan el IANA y el ISP
- Las direcciones son únicas en Internet a nivel mundial
- Alquilar una dirección IP pública tiene costo
- Rangos de direcciones:
    - 1.0.0.0-9.255.255.255
    - 11.0.0.0-126.255.255.255
    - 128.0.0.0-172.15.255.255
    - 172.32.0.0-192.167.255.255
    - 192.169.0.0-233.255.255.255

Protocolo de configuración dinámica de host

El protocolo de configuración dinámica de host (DHCP) pertenece a la familia de los protocolos de gestión de redes. El DHCP es un protocolo de capa de aplicación utilizado en una red para configurar dispositivos. Asigna una dirección IP única y proporciona las direcciones del servidor DNS adecuado y la puerta de enlace predeterminada para cada dispositivo. Los servidores DHCP operan en el puerto UDP 67, mientras que los clientes DHCP operan en el puerto UDP 68.

Protocolo de resolución de direcciones

Para este momento, ya debes saber bastante acerca de las direcciones IP y las de control de acceso al medio (MAC). Has aprendido que cada dispositivo tiene una dirección IP que lo identifica en la red y una dirección MAC que es única para esa interfaz de red. La dirección IP de un dispositivo puede cambiar con el tiempo, pero su dirección MAC permanece. El protocolo de resolución de direcciones (ARP) es un protocolo de la capa de Internet en el modelo TCP/IP que se utiliza para traducir las direcciones IP que se encuentran en los paquetes de datos, en la dirección MAC del dispositivo de hardware.

Cada dispositivo en la red ejecuta el ARP y realiza un seguimiento de las direcciones IP y MAC coincidentes en un caché ARP. El ARP no tiene un número de puerto específico.

Telnet

Telnet es un protocolo de capa de aplicación que permite que un dispositivo se comunique con otro equipo o servidor. Telnet envía toda la información en texto claro. Si bien utiliza indicadores de línea de comando para controlar otro dispositivo similar al protocolo Secure Shell (SSH), no es tan seguro como el SSH. Telnet se puede usar para conectarse a dispositivos locales o remotos y utiliza el puerto TCP 23.

Protocolo Secure Shell (SSH)

El protocolo Secure Shell (SSH) se utiliza para crear una conexión segura con un sistema remoto. Este protocolo de capa de aplicación proporciona una alternativa para la autenticación segura y la comunicación cifrada. El SSH opera sobre el puerto TCP 22 y es un reemplazo para protocolos menos seguros, como Telnet.

Protocolo de oficina postal

El protocolo de oficina postal (POP, por Post Office Protocol) es un protocolo de capa de aplicación (capa 4 en el modelo TCP/IP) que se utiliza para gestionar y recuperar correos electrónicos de un servidor de correo. Muchas organizaciones tienen un servidor de correo dedicado que maneja el correo entrante y saliente para los/as usuarios/as en la red. Los dispositivos de usuario envían solicitudes al servidor y descargan mensajes de correo electrónico de forma local. Si alguna vez has actualizado tu aplicación de correo electrónico y has visto nuevos correos electrónicos aparecer en tu bandeja de

entrada, estás experimentando el POP y el protocolo de acceso a mensajes de Internet (IMAP). La autenticación de texto no encriptada utiliza el puerto TCP/UDP 110, mientras que los correos electrónicos cifrados utilizan capa de conexión segura/seguridad en la capa de transporte (SSL/TLS) sobre el puerto TCP/UDP 995. Al usar el POP, el correo debe terminar de descargarse en un dispositivo local antes de poder leerse. Además, no permite que un/a usuario/a sincronice los correos electrónicos.

Protocolo de acceso a mensajes de Internet (IMAP)

El protocolo de acceso a mensajes de Internet (IMAP) se utiliza para correos electrónicos entrantes. Descarga sus encabezados, pero no el contenido, que permanece en el servidor, posibilitando a los/as usuarios/as acceder a su correo electrónico desde diferentes dispositivos. El IMAP utiliza el puerto TCP 143 para correos electrónicos no encriptados y el puerto TCP 993 con el protocolo TLS. El uso del IMAP permite a las personas leer parcialmente los correos electrónicos antes de que se terminen de descargar y sincronizarlos. Sin embargo, el IMAP es más lento que el POP3.

Protocolo para transferencia simple de correo (SMTP)

El protocolo para transferencia simple de correo (SMTP) se utiliza para transmitir y enrutar correos electrónicos desde el remitente hasta la dirección del/de la destinatario/a. El SMTP funciona con el software Message Transfer Agent (MTA), que consulta los servidores de sistema de nombres de dominio (DNS) para obtener las direcciones IP correspondientes a las direcciones de correo electrónico, asegurando que estos lleguen al destino previsto. El SMTP usa el puerto TCP/UDP 25 para correos electrónicos no cifrados y el puerto TCP/UDP 587 utiliza TLS para los cifrados. Con cierta frecuencia, el puerto TCP 25 se usa para el spam de alto volumen. El SMTP ayuda a filtrar el spam regulando la cantidad de correos electrónicos que una fuente puede enviar al mismo tiempo.

Protocolos y números de puerto

Recuerda que los números de puerto son utilizados por los dispositivos de red para determinar qué se debe hacer con la información contenida en cada paquete de datos una vez que lleguen a su destino. Los cortafuegos (firewalls) pueden filtrar el tráfico no deseado, basándose en los números de puerto. Por ejemplo, una empresa puede configurar un cortafuegos para permitir solo el acceso al puerto TCP 995 (POP3) a través de direcciones IP que pertenecen a la organización.

Como analista de seguridad, necesitarás conocer muchos de los protocolos y los números de puerto mencionados en este curso. Es posible que te pregunten por estos durante una entrevista laboral para evaluar tus conocimientos técnicos, así que es una buena idea memorizarlos. También aprenderás sobre nuevos protocolos mientras te desempeñas en una posición de seguridad.

Conclusiones clave

Como analista de ciberseguridad, te encontrarás con varios protocolos comunes en tu trabajo diario. Los protocolos abordados en esta lectura son los siguientes: NAT, DHCP, ARP, Telnet, SSH, POP3,

IMAP y SMTP. Es igualmente importante comprender dónde se ubica cada protocolo en el modelo TCP/IP y qué puertos ocupa.

Protocolo	Puerto
DHCP	Puerto UDP 67 (servidores) Puerto UDP 68 (clientes)
ARP	Ninguno
Telnet	Puerto TCP 23
SSH	Puerto TCP 22
POP3	Puerto TCP/UDP 110 (sin cifrar) Puerto TCP/UDP 995 (cifrado, SSL/TSL)
IMAP	Puerto TCP 143 (sin cifrar) Puerto TCP 993 (cifrado, SSL/TSL)
SMTP	Puerto TCP/UDP 25 (admite cifrado TSL) Puerto TCP/UDP 587 (cifrado, TSL)