El Modelo OSI

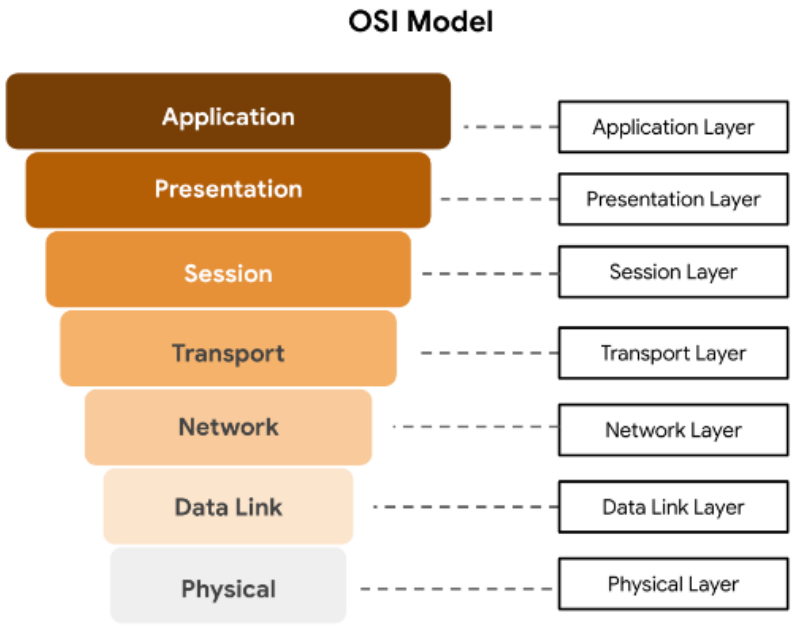
Toda la comunicación en una red se organiza mediante protocolos de red. El Protocolo de Control de Transmisión (TCP) establece conexiones entre dos dispositivos, y el Protocolo de Internet (IP) se utiliza para el enrutamiento y direccionamiento de paquetes de datos a medida que viajan entre los dispositivos de una red. Estos protocolos se utilizan en capas específicas de Internet en el Modelo TCP/IP. El Modelo TCP/IP de 4 capas es una forma condensada del Modelo OSI (Interconexión de sistemas abiertos), que consta de 7 capas. El modelo OSI proporcionará una comprensión más profunda de los procesos que tienen lugar en cada capa.

El Modelo TCP/IP frente al modelo OSI

El **Modelo TCP/IP** es un framework utilizado para visualizar cómo se organizan y transmiten los datos a través de una red. Este Modelo ayuda a los ingenieros de redes y a los analistas de seguridad a conceptualizar los procesos en la red y a comunicar dónde se producen las interrupciones o las amenazas a la seguridad.

El Modelo TCP/IP tiene cuatro capas: la capa de accesibilidad a la red, la capa de Internet, la capa de transporte y la capa de aplicación. Al analizar los incidentes de red, los profesionales de la seguridad pueden determinar en qué capa o capas se produjo un ataque en función de los procesos que intervinieron en el incidente.

El **modelo OSI** es un concepto estandarizado que describe las siete capas que utilizan los ordenadores para comunicarse y enviar datos a través de la red. Los profesionales de las redes y la seguridad suelen utilizar este Modelo para comunicarse entre sí sobre las posibles fuentes de problemas o amenazas a la seguridad cuando se producen.



Algunas organizaciones se basan en gran medida en el Modelo TCP/IP, mientras que otras prefieren utilizar el Modelo OSI. Como analista de Seguridad, es importante estar familiarizado con ambos Modelos. Tanto el modelo TCP/IP como el OSI son útiles para comprender cómo funcionan las redes.

Capa 7: Capa de aplicación

La capa de aplicación incluye procesos que implican directamente al usuario cotidiano. Esta capa incluye todos los protocolos de redes que las aplicaciones de software utilizan para conectar a un usuario a Internet. Esta característica es el rasgo identificativo de la capa de aplicación: la conexión del usuario a Internet a través de aplicaciones y solicitudes.

Un ejemplo de un tipo de comunicación que se produce en la capa de aplicación es el uso de un navegador de Internet. El navegador de Internet utiliza HTTP o HTTPS para enviar y recibir información del servidor del sitio web. La aplicación de correo electrónico utiliza el Protocolo simple de transmisión de correo (SMTP) para enviar y recibir información por correo electrónico. Además, los navegadores web utilizan el protocolo del sistema de nombres de dominio (DNS) para traducir los nombres de dominio de los sitios web en direcciones IP que identifican el servidor web que aloja la información del sitio web.

Capa 6: Capa de presentación

Las funciones de la capa de presentación implican la traducción y encriptación de datos para la red. Esta capa añade y sustituye Datos por formatos que puedan ser entendidos por las aplicaciones (capa 7) tanto en los sistemas emisores como en los receptores. Los formatos en el extremo del usuario pueden ser diferentes de los del sistema receptor. Los procesos en la capa de presentación requieren el uso de un formato estandarizado.

Algunas funciones de formateo que tienen lugar en la capa 6 incluyen la encriptación, la compresión y la confirmación de que el conjunto de códigos de caracteres puede ser interpretado en el sistema receptor. Un ejemplo de encriptación que tiene lugar en esta capa es SSL, que encripta los datos entre los servidores web y los navegadores como parte de los sitios web con HTTPS.

Capa 5: Capa de sesión

Una Sesión describe el momento en que se establece una conexión entre dos dispositivos. Una sesión abierta permite que los dispositivos se comuniquen entre sí. Los protocolos de la capa de sesión mantienen la sesión abierta mientras se transfieren los datos y la terminan una vez finalizada la transmisión.

La capa de sesión también es responsable de actividades como la autenticación, la reconexión y el establecimiento de puntos de control durante una transferencia de datos.

Si se interrumpe una sesión, los puntos de control garantizan que la transmisión se retome en el último punto de control de la sesión cuando se reanude la conexión. Las Sesiones incluyen una solicitud y una respuesta entre aplicaciones. Las funciones de la capa de sesión responden a las solicitudes de servicio de los procesos de la capa de presentación (capa 6) y envían solicitudes de servicios a la capa de transporte (capa 4).

Capa 4: Capa de transporte

La capa de transporte es responsable de la entrega de Datos entre dispositivos. Esta capa también se encarga de la Velocidad de transferencia de datos, del Flujo de la transferencia y de dividir los datos en segmentos más pequeños para facilitar su transporte. Segmentación es el proceso de dividir una gran transmisión de Datos en trozos más pequeños que puedan ser procesados por el sistema receptor. Estos segmentos tienen que volver a ensamblarse en su destino para que puedan ser procesados en la capa de sesión (capa 5). La velocidad y el ritmo de la transmisión también tienen que coincidir con la velocidad de conexión del sistema de destino. TCP y UDP son protocolos de capa de transporte.

Capa 3: Capa de red

La capa de red supervisa la recepción de las tramas desde la capa de enlace de datos (capa 2) y las entrega al destino previsto. El destino previsto puede encontrarse basándose en la dirección que reside en la trama de los paquetes de datos. Los paquetes de datos permiten la comunicación entre dos redes. Estos paquetes incluyen direcciones IP que indican a los routers dónde enviarlos. Se encaminan desde la red emisora hasta la red receptora.

Capa 2: Capa de vínculo de datos

La capa de enlace de datos organiza el envío y la recepción de paquetes de datos dentro de una misma red. En la capa de vínculo de datos se encuentran los conmutadores de la red local y las tarjetas de interfaz de red de los dispositivos locales.

En la capa de enlace de datos se utilizan protocolos como el protocolo de control de red (NCP), el control de enlace de datos de alto nivel (HDLC) y el protocolo de control de enlace de datos síncrono (SDLC).

Capa 1: Capa física

Como su nombre indica, la capa física corresponde al hardware físico que interviene en la transmisión de la red. Los concentradores, los módems y los cables y el cableado que los conectan se consideran parte de la capa física. Para viajar a través de un cable ethernet o coaxial, un paquete de datos necesita ser traducido a un flujo de 0s y 1s. El flujo de 0s y 1s

se envía a través del cableado físico y los cables, se recibe y, a continuación, pasa a niveles superiores del Modelo OSI.

Claves

Tanto el modelo TCP/IP como el OSI son modelos conceptuales que ayudan a los profesionales de las redes a diseñar procesos y protocolos de red en relación con la transmisión de datos entre dos o más sistemas. El Modelo OSI contiene siete capas de Comunicación. Los profesionales de las redes y la seguridad utilizan el modelo OSI para comunicarse entre sí sobre las posibles fuentes de problemas o amenazas a la seguridad cuando se producen. Los ingenieros de redes y los analistas de seguridad de redes utilizan los modelos TCP/IP y OSI para conceptualizar los procesos de red y comunicar la ubicación de las interrupciones o amenazas.