Más información sobre el modelo TCP/IP

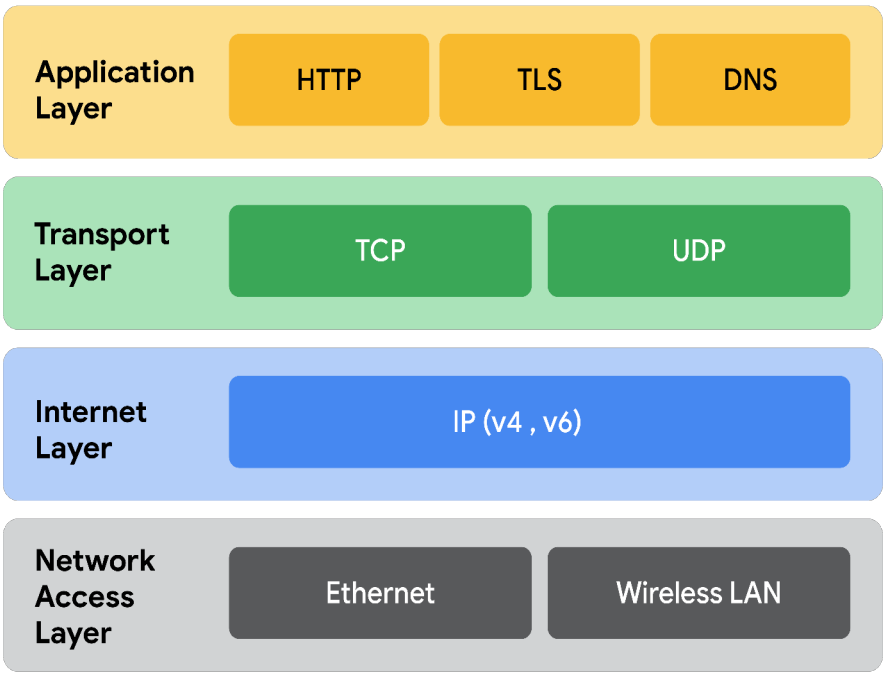
En esta lectura, profundizarás lo que has aprendido sobre el modelo de protocolo de control de transmisión/protocolo de Internet (TCP/IP), analizarás las diferencias entre el modelo de Interconexión de Sistemas Abiertos (OSI, por sus siglas en inglés) y el modelo TCP/IP, y comprenderás cómo se relacionan. Luego, revisarás cada capa del modelo TCP/IP y repasarás los protocolos comunes utilizados en cada capa.

Como profesional de la seguridad, es importante que entiendas el modelo TCP/IP porque toda la comunicación en una red está organizada mediante protocolos de red. Los protocolos de red son un lenguaje que los sistemas utilizan para comunicarse entre sí. Para que dos sistemas de red se comuniquen con éxito, deben usar el mismo protocolo. Los dos modelos más comunes disponibles son el TCP/IP y el OSI. Estos modelos son una guía representativa de cómo las comunicaciones de red trabajan de forma conjunta y se mueven a través de la red y el host (anfitrión). Los ejemplos proporcionados en este curso seguirán el modelo TCP/IP.

El modelo TCP/IP

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

El modelo TCP/IP tiene cuatro capas: de acceso a la red, de Internet, de transporte y de aplicación. Al solucionar problemas en la red, las y los profesionales de seguridad pueden analizar y deducir en qué capa o capas se produjo el ataque, basándose en los procesos involucrados en un incidente.



Capa de acceso a la red

La **capa de acceso a la red**, a veces llamada capa de enlace de datos, organiza el envío y la recepción de paquetes de datos dentro de una sola red. Esta capa corresponde al hardware físico involucrado en la transmisión de red. Los hubs, módems, cables y cableado se consideran parte de esta capa. El protocolo de resolución de direcciones (ARP, por sus siglas en inglés) forma parte de la capa de acceso a la red. El ARP ayuda a la IP a dirigir paquetes de datos al mapear direcciones IP a direcciones MAC en la misma red física.

Capa de Internet

La **capa de Internet**, a veces denominada capa de red, es responsable de garantizar la entrega al host de destino, que potencialmente puede residir en una red diferente. La capa de Internet determina qué protocolo es el encargado de entregar los paquetes de datos. A continuación, se presentan algunos de los protocolos comunes que operan en la capa de Internet:

- **Protocolo de Internet (IP)**. Envía los paquetes de datos al destino correcto y se basa en el protocolo de control de transmisión/protocolo de datagramas de usuario (TCP/UDP) para entregarlos al servicio correspondiente. Los paquetes de IP posibilitan la comunicación entre dos redes, ya que se enrutan desde la red de origen hasta la de destino. El IP retransmite cualquier dato que se haya perdido o dañado.
- **Protocolo de mensajes de control de Internet (ICMP)**. Comparte información de errores y actualizaciones de estado de los paquetes de datos. Resulta útil para detectar y solucionar errores de red y, además, informa sobre paquetes que fueron descartados o desaparecieron durante el tránsito, problemas de conectividad de red y paquetes redirigidos a otros enrutadores.

Capa de transporte

La **capa de transporte** es responsable de entregar datos de manera confiable entre dos sistemas o redes. El protocolo de control de transmisión (TCP) y el de datagramas de usuario (UDP) son los dos protocolos de transporte que se producen en esta capa.

Protocolo de control de transmisión (TCP)

El **TCP** garantiza que los datos se transmitan de forma segura al servicio de destino. Contiene el número de puerto del servicio de destino previsto, que reside en el encabezado TCP de un paquete TCP/IP.

Protocolo de datagramas de usuario (UDP)

Las aplicaciones que no están afectadas por la confiabilidad de la transmisión usan el protocolo **UDP**. Los datos enviados a través de UDP no son objeto de un seguimiento tan exhaustivo como los enviados mediante TCP. Debido a que el UDP no establece conexiones de red, se utiliza principalmente para aplicaciones sensibles al rendimiento que operan en tiempo real, como la transmisión de video.

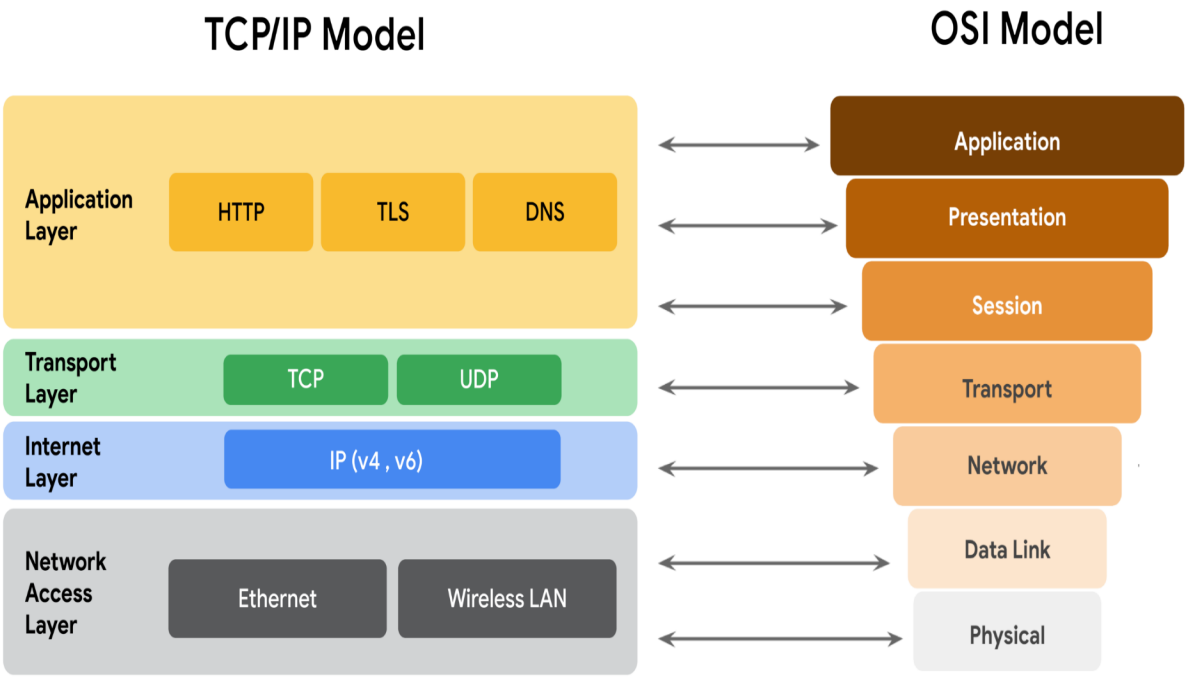
Capa de aplicación

La **capa de aplicación** en el modelo TCP/IP es similar a las capas de aplicación, presentación y sesión del modelo OSI. Es la responsable de realizar solicitudes de red o de responder a solicitudes. Además, esta capa define a qué servicios y aplicaciones de Internet puede acceder cualquier usuario. Algunos de los protocolos comunes utilizados en esta capa son:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Secure Shell o shell seguro (SSH)
- Protocolo de transferencia de archivos (FTP)
- Sistema de nombres de dominio (DNS)

Los protocolos de capa de aplicación se basan en capas subyacentes para transferir los datos a través de la red.

Comparación del modelo TCP/IP con el modelo OSI



El modelo **OSI** organiza visualmente los protocolos de red en diferentes capas. Las y los profesionales de redes suelen usar este modelo para comunicarse entre sí sobre posibles fuentes de problemas o amenazas de seguridad.

El modelo TCP/IP combina múltiples capas del modelo OSI. Ambos modelos comparten muchas similitudes, ya que definen estándares para las redes y dividen el proceso de comunicación de red en diferentes capas. Sin embargo, el modelo TCP/IP es una versión simplificada del modelo OSI.

Conclusiones clave

Los modelos TCP/IP y OSI son marcos conceptuales que ayudan a las y los profesionales de redes a visualizar los procesos y protocolos con respecto a la transmisión de datos entre dos o más sistemas. El modelo TCP/IP contiene cuatro capas, y el modelo OSI, siete.

El modelo OSI

Hasta ahora, en esta sección del curso, aprendiste sobre los componentes y dispositivos de redes y cómo se produce la comunicación a través de una red.

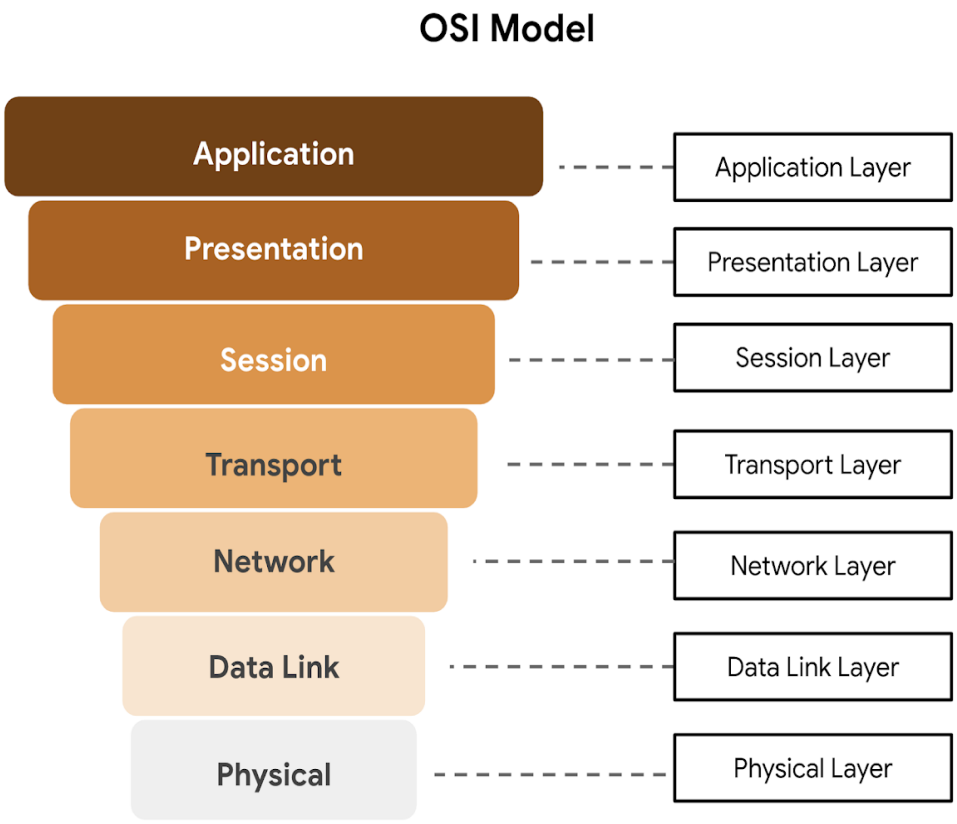
En una red, toda la comunicación se organiza mediante protocolos de red. Anteriormente, aprendiste sobre el protocolo de control de transmisión (TCP), que establece conexiones entre dos dispositivos, y sobre el protocolo de Internet (IP), que se utiliza para enrutar y direccionar paquetes de datos mientras viajan entre dispositivos en una red. Esta lectura continuará explorando las siete capas del modelo de interconexión de sistemas abiertos (OSI) y los procesos que ocurren en cada una de ellas. Trabajaremos en sentido inverso, desde la capa siete hasta la uno, yendo desde los procesos que involucran al usuario cotidiano de la red, hasta aquellos que involucran los componentes de red más básicos, como cables de red y switches. También revisaremos las principales diferencias entre los modelos TCP/IP y OSI.

Comparación entre el modelo TCP/IP y el modelo OSI

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

El modelo TCP/IP tiene cuatro capas: de acceso a la red, de Internet, de transporte y de aplicación. Al analizar los eventos de la red, las y los profesionales de seguridad pueden determinar en qué capa o capas se produjo el ataque, basándose en los procesos involucrados en el incidente.

En cambio, el **modelo OSI** es un concepto estandarizado que describe las siete capas que las computadoras utilizan para comunicarse y enviar datos a través de la red. Las y los profesionales de seguridad y de redes suelen utilizarlo para comunicarse entre sí sobre posibles fuentes de problemas o amenazas de seguridad.



Algunas organizaciones dependen en gran medida del modelo TCP/IP, mientras que otras prefieren usar el modelo OSI. Como analista de seguridad, es importante conocer los dos modelos, dado que ambos son útiles para comprender cómo funcionan las redes.

Capa 7: Capa de aplicación

La capa de aplicación incluye procesos que involucran directamente al/a la usuario/a cotidiano/a. Esta capa incluye todos los protocolos de red que las aplicaciones de software utilizan para conectarlo/a a Internet. Esta característica es la que identifica a la capa de aplicación: conexión de usuarios/as a la red a través de aplicaciones y solicitudes.

Un ejemplo de un tipo de comunicación que ocurre en la capa de aplicación es el uso de un navegador web. 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 transferencia de correo (SMTP) para transmitir información de correo electrónico. Además, los navegadores web utilizan el protocolo del sistema de nombres de dominio (DNS) para traducir los nombres de dominio del sitio web en direcciones IP, que identifican el servidor web que aloja la información del sitio.

Capa 6: Capa de presentación

Las funciones en la capa de presentación incluyen la traducción de datos y el cifrado para la red. Esta capa agrega y reemplaza datos con formatos que pueden ser entendidos por las aplicaciones (capa 7), en los sistemas de envío y recepción. Los formatos que están más cerca del usuario final, es decir, donde se encuentra la aplicación o dispositivo que utiliza el/la usuario/a para interactuar con la red o

recibir información, 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 se producen en la capa 6 incluyen cifrado, compresión y confirmación de que el conjunto de caracteres puede ser interpretado en el sistema receptor. Un ejemplo de cifrado que se da en esta capa es SSL, que cifra los datos entre los servidores web y los navegadores como parte de sitios web con HTTPS.

Capa 5: Capa de sesión

Una sesión indica cuando se establece una conexión entre dos dispositivos. Una sesión abierta permite que los dispositivos se comuniquen entre sí. El objetivo de los protocolos de la capa de sesión es mantener la sesión abierta mientras se transfieren datos y cerrarla una vez que se completa la transmisión.

La capa de sesión también es responsable de actividades como la autenticación, reconexión y establecimiento de puntos de control durante una transferencia de datos. Si la sesión se interrumpe, los puntos de control aseguran que, cuando se restablece la conexión, la transmisión se retome desde el último punto de control de la sesión. Las sesiones incluyen una solicitud y respuesta entre aplicaciones. Las funciones en la capa de sesión responden a solicitudes de servicio de procesos en 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 la responsable de enviar datos entre dispositivos. Además, esta capa maneja la velocidad y el flujo de transferencia, y divide los datos en segmentos más pequeños para facilitar el envío. La segmentación es el proceso de dividir una gran transmisión de datos en piezas más pequeñas que puedan ser procesadas por el sistema receptor. Para que se puedan procesar en la capa de sesión (capa 5), estos segmentos tienen que volverse a ensamblar en su destino. La velocidad y la tasa de 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 los paquetes desde la capa de enlace de datos (capa 2) y las entrega al destino previsto. El destino previsto puede encontrarse en función de la dirección que reside en el marco de los paquetes de datos. Estos paquetes incluyen direcciones IP, que indican a los routers dónde enviarlos y se enrutan desde la red de envío hacia la red de recepción.

Capa 2: Capa de enlace de datos

La capa de enlace de datos organiza el envío y la recepción de paquetes de datos dentro de una sola red. Esta capa incluye los switches en la red local y las tarjetas de interfaz de red en 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 sincrónico (SDLC).

Capa 1: Capa física

Como su nombre lo indica, la capa física corresponde al hardware físico utilizado en la transmisión de la red. Los hubs, los módems y el cableado que los conecta se consideran parte de esta capa. Para viajar a través de un cable Ethernet o coaxial, un paquete de datos debe ser traducido en una secuencia de ceros y unos, que se envía a través de los cables y conexiones físicas, se recibe y, luego, pasa a los niveles superiores del modelo OSI.

Conclusiones clave

Los modelos TCP/IP y OSI son marcos conceptuales que ayudan a las y los profesionales de redes a diseñar procesos y protocolos para la transmisión de datos entre dos o más sistemas. El modelo OSI incluye siete capas. Las y los profesionales de seguridad y de redes usan el modelo OSI para comunicarse entre sí sobre posibles fuentes de problemas o amenazas de seguridad. En tanto, los/las ingenieros/as de redes y los/las analistas de seguridad de redes utilizan los modelos TCP/IP y OSI para conceptualizar los procesos de red y notificar la ubicación de interrupciones o amenazas.