Man in the middle (MitM)

Medio se una de las principales amenazas cibernéticas que recibe su nombre del hecho de que un atacante se inserta entre 2 partes comunicantes. Si todas las comunicaciones pasan a través del atacante en ruta a su destino, esto crea la posibilidad de que el atacante deje caer, lea o modifique los mensajes antes de que lleguen al destino final.

¿Cómo funciona?

Primero, necesita insertarse en la comunicación de una manera que les permita interceptar el tráfico en ruta hacia su destino, algunas de las formas en que el atacante podría lograr es:

- **Wi-Fi malicioso:** Todo el tráfico fluye a través de un punto de acceso inalámbrico que el atacante controla y puede engañar a los usuarios para que se conecten a él.
- **Spoofing ARP:** ARP se utiliza para asignar direcciones IP a direcciones MAC. Al usar mensajes ARP falsos, un atacante asigna la dirección IP del objetivo a su dirección MAC, lo que hace que el tráfico del objetivo se envíe a ellos en su lugar.
- **Suplantación de DNS:** El DNS asigna nombres de dominio a direcciones IP. Envenenar una caché DNS con registros DNS falsos puede hacer que el tráfico al dominio de destino se enrute a la dirección IP del atacante.

Una vez en medio de una comunicación, el atacante necesita poder leer los mensajes; sin embargo, un gran porcentaje de trafico de internet se encripta mediante SSL/TLS. Si el tráfico está cifrado, la lectura y modificación de los mensajes requieren la capacidad de suplantación o interrupción de la conexión SSL/TLS.

Ejemplos

Certificaciones digitales falsas

SSL/TLS están diseñados para proteger contra ataques de MitM proporcionado confidencialidad, integridad y autenticación al tráfico de red. Sin embargo, depende de que el usuario solo acepte certificados digitales válidos para el dominio en particular.

Aplicaciones móviles/IoT vulnerable

Muchas aplicaciones móviles y dispositivos IoT, especialmente los más antiguos o de bajo costo, pueden carecer de cifrado robusto o utilizar protocolos inseguros como HTTP o Telnet. Si las aplicaciones o dispositivos IoT transmiten datos sensibles sin cifrar, un atacante en la misma red puede interceptar y leer fácilmente esa información.