Universidad del Istmo

Campus Tehuantepec

Carrera: Ingeniería en computación

Grupo: 704

Alumno:

Juan Emmanuel Becerril Nolasco

Materia: Redes II

Profesor: Carlos Mijangos Jimenéz

1er Parcial

Trabajo: “Investigación sobre tipos de ataque Man-in-the-Middle”

Santo Domingo Tehuantepec, a 27 de octubre del 2025

Ataques Man-in-the-Middle

Consiste en un ataque donde una persona es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía. Un ataque Man in the Middle puede ser tanto online como offline. Los piratas informáticos pueden llevar a cabo diferentes tipos de ataques para lograr su objetivo. Siempre intentarán interceptar los mensajes pasando desapercibido. Los principales tipos de ataques MitM son los siguientes:

DNS Spoofing

La suplantación de identidad del sistema de nombres de dominio (DNS), o envenenamiento de caché DNS, ocurre cuando los registros DNS manipulados se utilizan para desviar el tráfico legítimo en línea a un sitio web falso o falsificado creado para parecerse a un sitio web que el usuario probablemente conocería y en el que confiaría.

Al igual que con todas las técnicas de suplantación de identidad, los atacantes solicitan a los usuarios que inicien sesión involuntariamente en el sitio web falso y los convenzan de que deben realizar una acción específica, como pagar una tarifa o transferir dinero a una cuenta específica. Los atacantes roban tantos datos como puedan de las víctimas en el proceso.

HTTPS Spoofing

En este caso el ataque tiene como objetivo que el usuario, la víctima en definitiva, termine en una página sin cifrar. Esto lo pueden lograr a través de un enlace en algún sitio de terceros, a través del correo electrónico, etc.

La víctima cree que va a entrar en una página cifrada, HTTPS, pero en realidad está accediendo a una copia en versión HTTP, sin cifrar. Allí pondrá sus datos, iniciará sesión o incluso realizará algún pago, pero todo eso va a ser controlado por el atacante, que va a tener acceso a todo el contenido ingresado.

Secuestro de correo electrónico

Como su nombre lo indica, en este tipo de ataque, los cibercriminales toman el control de las cuentas de correo electrónico de bancos, instituciones financieras u otras empresas de confianza que tienen acceso a datos sensibles y dinero. Una vez dentro,

los atacantes pueden monitorear las transacciones y la correspondencia entre el banco y sus clientes.

En escenarios más maliciosos, los atacantes falsifican o falsifican la dirección de correo electrónico del banco y envían a los clientes correos electrónicos que les indican que vuelvan a enviar sus credenciales, o peor aún, envían dinero a una cuenta controlada por los atacantes. En esta versión de ataque MitM, la ingeniería social o el desarrollo de confianza con las víctimas es clave para el éxito.

Robo de cookies del navegador

En informática, una cookie es una pequeña información almacenada. Una cookie de navegador, también conocida como cookie HTTP, son datos recopilados por un navegador web y almacenados localmente en la computadora de un usuario. La cookie del navegador ayuda a los sitios web a recordar información para mejorar la experiencia de navegación del usuario. Por ejemplo, con las cookies habilitadas, un usuario no tiene que seguir completando los mismos elementos en un formulario, como el nombre y el apellido.

El robo de cookies del navegador se debe combinar con otra técnica de ataque MitM, como el espionaje Wi-Fi o el secuestro de sesiones, para llevar a cabo. Los cibercriminales pueden obtener acceso al dispositivo de un usuario utilizando una de las otras técnicas de MitM para robar cookies del navegador y aprovechar todo el potencial de un ataque de MitM. Con el acceso a las cookies del navegador, los atacantes pueden obtener acceso a contraseñas, números de tarjetas de crédito y otra información confidencial que los usuarios almacenan regularmente en sus navegadores.

Envenenamiento de caché ARP

El Protocolo de resolución de direcciones (ARP) es un protocolo de comunicación utilizado para descubrir la dirección de la capa de enlace, como una dirección de control de acceso a medios (MAC), asociada con una dirección de capa de Internet determinada. El ARP es importante porque traduce la dirección de la capa de enlace a la dirección del protocolo de Internet (IP) en la red local.

En este esquema, la computadora de la víctima es engañada con información falsa del cibercriminal para que piense que la computadora del estafador es la puerta de enlace de la red. Como tal, la computadora de la víctima, una vez conectada a la red, envía esencialmente todo su tráfico de red al actor malicioso en lugar de a través de la puerta de enlace de red real. Luego, el atacante utiliza este tráfico desviado para analizar y robar toda la información que necesita, como la información de identificación personal (PII) almacenada en el navegador.

Espionaje Wi-Fi

En el espionaje Wi-Fi, los cibercriminales hacen que las víctimas se conecten a una red inalámbrica cercana con un nombre de sonido legítimo. Pero en realidad, la red está configurada para participar en actividades maliciosas. La red inalámbrica puede parecer propiedad de una empresa cercana a la que el usuario frecuenta o podría tener un nombre genérico, aparentemente inofensivo, como “Red Wi-Fi pública gratuita”. En algunos casos, el usuario ni siquiera necesita ingresar una contraseña para conectarse.

Una vez que las víctimas están conectadas al Wi-Fi malicioso, el atacante tiene opciones: monitorear la actividad en línea del usuario o raspar las credenciales de inicio de sesión, la información de la tarjeta de crédito o pago y otros datos sensibles.

Para protegerse contra este ataque, los usuarios siempre deben verificar a qué red están conectados. Con los teléfonos móviles, deben desactivar la función de conexión automática Wi-Fi al moverse localmente para evitar que sus dispositivos se conecten automáticamente a una red maliciosa.

Ejemplos de ataques MitM famosos

En 2013, Edward Snowden filtró documentos que obtuvo mientras trabajaba como consultor en la Administración de Seguridad Nacional (NSA). Los documentos mostraron que la NSA fingía ser Google al interceptar todo el tráfico con la capacidad de falsificar la certificación de cifrado SSL. La NSA utilizó este ataque MitM para obtener los registros de búsqueda de todos los usuarios de Google, incluidos todos los estadounidenses, que era espionaje doméstico ilegal contra ciudadanos estadounidenses.

El proveedor de servicios de Internet Comcast utilizó JavaScript para sustituir sus anuncios por anuncios de sitios web de terceros. Este tipo de ataque MitM se denomina inyección de código. El tráfico web que pasaba a través del sistema Comcast le dio a Comcast la capacidad de inyectar código e intercambiar todos los anuncios para cambiarlos a anuncios de Comcast o insertar anuncios de Comcast en contenido de otro modo libre de anuncios.

Un famoso ejemplo de ataque de hombre en el medio es Equifax, una de las tres empresas más grandes de informes de historial crediticio. La empresa tuvo una filtración de información de MitM en 2017 que expuso los datos financieros de más de 100 millones de clientes a criminales durante muchos meses.

Una falla en una aplicación bancaria utilizada por HSBC, NatWest, Co-op, Santander y Allied Irish Bank permitió a los criminales robar información personal y credenciales, incluidas contraseñas y códigos PIN.

Los ataques de MitM contribuyeron a violaciones masivas de datos. Las mayores violaciones de datos en 2021 incluyeron Cognyte (cinco mil millones de registros), Twitch (cinco mil millones de registros), LinkedIn (700 millones de registros) y Facebook (553 millones de registros).

0-day exploit

Un ataque de día cero (en inglés: zero-day attack) es un ataque contra una aplicación o sistema informático que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Esto supone que aun no hayan sido arregladas. Es frecuente la venta en el mercado negro de exploits que aprovechan estas vulnerabilidades. Su precio se establece con base a su impacto y el número de dispositivos vulnerables. Un ataque de día cero se considera uno de los más peligrosos instrumentos de una guerra informática.

El término "día cero" se refería originalmente al número de días desde que se lanzó al público una nueva pieza de software, por lo que el "software de día cero" se obtenía pirateando la computadora de un desarrollador antes de su lanzamiento. Finalmente, el término se aplicó a las vulnerabilidades que permitieron esta piratería y al número de días que el proveedor ha tenido para solucionarlas. Una vez que el proveedor se entera de la vulnerabilidad, generalmente creará parches o recomendará soluciones para mitigarla.

Los ataques día cero ocurren cuando una vulnerabilidad tiene una ventana de tiempo existente entre el tiempo en el que se publica una amenaza y el tiempo en el que se publican los parches que las solucionan. Normalmente estos parches son preparados por los propios responsables del programa «defectuoso» en cuestión (sobre todo con los programas de pago).

La línea de tiempo que se emplea para virus y troyanos, entre otros, es la siguiente:

- Publicación del ataque o exploit al mundo
- Detección y estudio del problema
- Desarrollo de una solución al mismo

- Publicación del parche (o firma del virus si procede), para evitar el exploit.
- Distribución e instalación del parche en los sistemas de los usuarios y actualización de los antivirus.

Este proceso puede durar horas o incluso días. Todo el tiempo que dura este proceso es el que dura la ventana de vulnerabilidad.