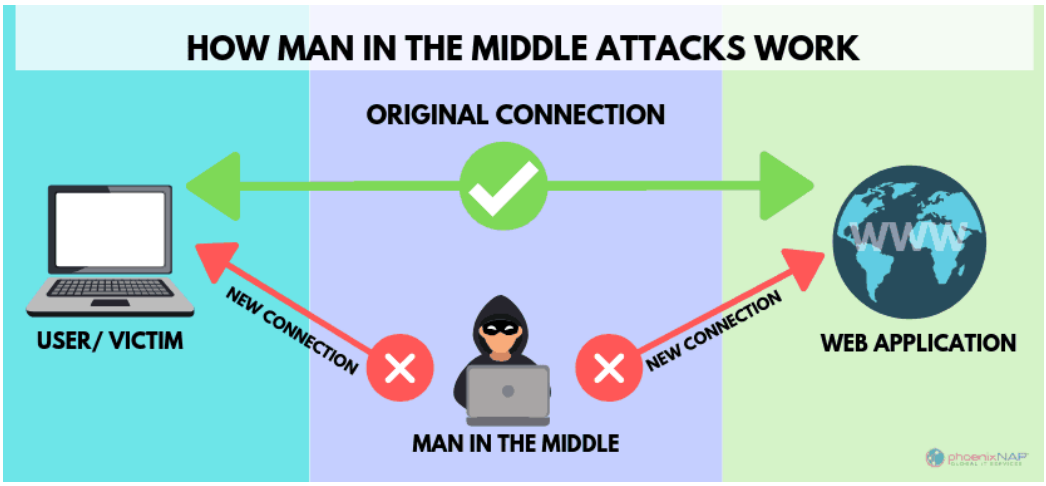
INSTITUTO TECNOLOGICO DE CANCUN

INVESTIGACION MITM



ALUMNO:
PEREZ ALEGRIA ALVARO FERNANDO.

PROFESOR:
ING. ISAMEL JIMENEZ SANCHEZ

INGENIERÍA EN SISTEMAS COMPUTACIONALES.

INVESTIGACIÓN MITM

Definición de ataque Man-in-the-Middle

El ataque MITM (Man in the middle), del inglés “Hombre en el medio”, es muy popular entre los ciberdelincuentes por la cantidad de información a la que pueden llegar a acceder en caso de que tengan éxito. Es un tipo de ataque basado en interceptar la comunicación entre 2 o más interlocutores, pudiendo suplantar la identidad de uno u otro según lo requiera para ver la información y modificarla a su antojo, de tal forma que las respuestas recibidas en los extremos pueden estar dadas por el atacante y no por el interlocutor legítimo.

Básicamente, consiste en interceptar la comunicación entre 2 o más interlocutores. Para ello, alguien anónimo llamado “X” se sitúa entre ambos e intercepta los mensajes de A hacia B, conociendo la información y a su vez dejando que el mensaje continúe su camino. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas. Por ejemplo, en el mundo offline, se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos. En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente; pasando totalmente desapercibido para poder alcanzar con éxito la meta.

Los ciberdelincuentes pueden utilizar los ataques Man in the Middle con el objetivo de robar credenciales de acceso o información personal, espiar a una víctima, sabotear comunicaciones o alterar datos. Por ejemplo, podrían exfiltrar la información de un teléfono móvil que está conectado a una red wifi de un hotel que previamente han comprometido.

Tipos de ataque

Para infiltrarse en los sistemas, los hackers tienen varias técnicas para buscar cualquier debilidad. Por norma, suelen automatizarse los ataques empleando software específico. Veamos ahora algunos de los ataques más comunes relacionados con el Man in the Middle.

Ataques basados en servidores DHCP

En este ataque, el hacker usa su propio ordenador en una red de área local a modo de servidor DHCP, que en resumidas cuentas sirve para asignar dinámicamente una dirección IP y configuración adicional a cada dispositivo dentro de una red para que puedan comunicarse con otras redes. En cuanto un ordenador establece la conexión con una red de área local, el cliente DHCP reclama datos como la dirección IP local o la dirección de la puerta de acceso predeterminada, entre otros.

Lo que buscan los hackers por esta vía es controlar las direcciones IP locales mediante el servidor DHCP simulado, para utilizar en su favor las puertas de acceso y el servidor DNS en los ordenadores víctimas y poder desviar el tráfico de datos saliente para interceptar y manipular su contenido.

Por darle un nombre propio a este ataque, se le conoce en el mundillo como DHCP spoofing. Pero la clave para que hablemos de un ataque MitM es usar la misma LAN que su víctima, porque sino hablaríamos directamente de un ataque basado en un servidor DHCP.

ARP cache poisoning

En este caso nos referimos al protocolo ARP, que permite resolver IPs en redes LAN siempre que un ordenador quiera enviar paquetes de datos en una red. Para ello, es imprescindible que conozca el sistema del destinatario. Cuando hace una petición ARP, está enviando al mismo tiempo las direcciones MAC y la IP del ordenador que solicita la información, como la dirección IP del sistema solicitado. Si es correcta toda la petición, la asignación de direcciones MAC a IP locales se guarda en la caché ARP del ordenador solicitante.

El objetivo del ataque ARP cache poisoning es dar respuestas falsas en el proceso para lograr que el atacante use su ordenador como punto de acceso inalámbrico o entrada a Internet. Si es exitoso, el ataque permite leer todos los datos salientes de los ordenadores atacados, aparte de registrarlos o de manipularlos antes de enviarlos al lugar correcto.

Ataques basados en servidores DNS

Este ataque tiene como objetivo manipular las entradas en la caché de un servidor DNS haciendo que den direcciones de destino falsas. Si ha tenido éxito, los

hackers pueden mandar a los usuarios de Internet a cualquier página web sin que nadie se dé cuenta.

El proceso se inicia cuando los datos del sistema de nombres de dominio se distribuyen por diferentes ordenadores de la red. Cuando alguien quiere acceder a una web lo suele hacer usando un nombre de dominio. También necesita una dirección IP, determinada por el router que tenga el usuario, para enviar la solicitud. Si hay entradas en la caché, el servidor DNS emite la respuesta a la solicitud con la IP que proceda, y si no las hay el servidor decidirá la IP con ayuda de otros servidores.

Para los hackers es fundamental centrarse en aquellos servidores que utilizan una versión muy antigua del software de DNS, ya que si logran acceder a un servidor con estas características, les resulta muy fácil dar registros falsos con cada dirección IP correcto, “envenenando” la caché del servidor DNS. Para evitar estos ataques, los administradores de sistemas tratan por todos los medios de actualizar el software de los servidores y que estén protegidos como es debido.

Simulación de un punto de acceso inalámbrico

Centrado en los usuarios de dispositivos móviles, este ataque consiste en recrear un punto de acceso inalámbrico en una red pública, como pueden ser las de una cafetería, un aeropuerto, etc. El atacante prepara su ordenador para que actúe como una vía adicional de acceso a Internet, intentando engañar a los usuarios para que le proporcionen los datos de su sistema antes de que se den cuenta. El peligro real viene si tu dispositivo se configura para comunicarse automáticamente con los puntos de acceso con mayor potencia de señal.

Ataque Man in the Browser

Por último, el ataque Man in the Browser consiste en que el atacante instala malware en el navegador de los usuarios de Internet con la finalidad de interceptar sus datos. La principal causa para verse infectado por este ataque es el hecho de tener ordenadores que no están correctamente actualizados y que, por ello, ofrecen brechas de seguridad muy visibles que dan camino libre para infiltrarse en el sistema.

El malware incluye programas en el navegador de un usuario de forma clandestina, registrando todos los datos que intercambia la nueva víctima con las

diferentes páginas web que visita. Los hackers obtienen con este método la información que buscaban de forma muy rápida y sin demasiado esfuerzo.

Variantes de ataque MiTM

En el ataque MiTM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario. Esto se puede realizar configurando el router malicioso para que parezca legítimo o atacando un error del mismo e interceptando la sesión del usuario. En el primero de los casos, el atacante configura su ordenador u otro dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería). Después, el usuario se conecta al “router” y busca páginas de banca o compras online, capturando el criminal las credenciales de la víctima para usarlas posteriormente. En el segundo caso, un delincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router. Éste es el método más complejo de los dos, pero también el más efectivo; ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.

Tipos de ataques

Los ataques MITM tienen diferentes modalidades que dependen de la técnica empleada, por lo tanto, más que hablar de los tipos de ataques vamos a hablar de los escenarios de ataque.

- puntos de acceso wifi abiertos o con baja seguridad,
- redes locales (LAN),
- software de navegación anticuado.

Prevención

Generalmente, es muy difícil detectar cuándo se está sufriendo un ataque de intermediario (Man In The Middle), por tanto, la prevención es la primera medida de protección.

- Evitar conectarse a redes wifi públicas y la difusión de información personal a través de estas redes.

- Tener actualizado el software de todos los dispositivos, especialmente el del sistema operativo y el navegador web.
- Utilizar contraseñas seguras y en la medida de lo posible activar la autenticación en dos pasos.
- Acceder a sitios web seguros cuya URL comience por “https”.
- A nivel empresarial, sería interesante contar con dos redes. Una de ellas destinada al uso propio y otra habilitada para invitados, restringiendo así el acceso a la red corporativa y otros servicios.
- Tener cuidado con los posibles ataques de correo electrónico conocidos como phishing y evitar abrir enlaces procedentes de fuentes desconocidas.
- En caso de sospecha, realizar una limpieza de los equipos afectados antes de transmitir información de carácter sensible.

BIBLIOGRAFIAS

Soto, P. (2021, 28 junio). Ataques ‘Man in the Middle’: cómo detectarlos y prevenirlos. Redseguridad. Recuperado 28 de octubre de 2021, de https://www.redseguridad.com/actualidad/ciberseguridad/ataques-man-in-the-middle-como-detectarlos-y-prevenirlos_20210628.html

INCIBE. (2020, 16 julio). El ataque del “Man in the middle” en la empresa, riesgos y formas de. Recuperado 28 de octubre de 2021, de https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

Malenkovich, S. (2020, 26 febrero). ¿QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE? Blog oficial de Kaspersky. Recuperado 28 de octubre de 2021, de https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

Rodríguez, A. (2019, 24 octubre). ¿Qué es un ataque Man in the Middle? Garage. Recuperado 28 de octubre de 2021, de https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/