Fundamentos de telecomunicaciones

Arturo alexander felipe lopez
Noviembre 2020
Profesor: ING. Ismael Jiménez

Instituto tecnológico de Cancún
Ing. En sistemas computacionales
investigación

MITM

El objetivo de la mayoría de los ciberdelincuentes es robar la información valiosa para los usuarios. Los ataques pueden ser dirigidos a usuarios individuales, páginas web famosas o bases de datos

El objetivo de la mayoría de los ciberdelincuentes es robar la información valiosa para los usuarios. Los ataques pueden ser dirigidos a usuarios individuales, páginas web famosas o bases de datos financieros. Aunque la metodología sea diferente en cada situación, el fin siempre es el mismo. En la mayoría de los casos, los criminales intentan, en primer lugar, insertar algún tipo de malware en el equipo de la víctima, ya que ésta es la ruta más corta entre ellos y los datos que tanto desean. Si esto no les resulta posible, otra forma común es el ataque Man-in-the-Middle. Como sugiere su nombre en inglés, en este método se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente: una página de banca online o una cuenta de correo electrónico. Estos ataques son realmente efectivos y, a su vez, muy difíciles de detectar por el usuario, quien no es consciente de los daños que puede llegar a sufrir.

El concepto de un ataque MiTM es muy sencillo. Además, no se limita únicamente al ámbito de la seguridad informática o el mundo online. 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

Por su nombre en inglés, un intermediario, normalmente el cibercriminal o un software malicioso, se incrusta entre la víctima y la fuente de datos (cuentas bancatias, email…etc). El objetivo es interceptar, leer o manipular de forma efectiva la comunicación entre la víctima y sus datos sin que nadie se dé cuenta de que hay una tercera persona incluida en la operación.

Para que os hagáis una idea de cómo funciona, imaginad tres sistemas: A, B y C. El sistema A intenta conectarse con B, pero realmente lo hace con el sistema C, que intercede desviando la conexión codificada, de forma que A envía todos los datos a C y luego C transmite a B. Es decir, C suplanta la identidad y se hace con el control de los datos antes de que lleguen a B, pudiendo hacer con ellos lo que quiera sin que nadie se entere.

¿Qué tipos de ataque Man in the Middle existen?

Para infiltrarse en los sistemas, los hackers tienen varias técnicas para buscar cualquier debilidad. Por norma, suelen automatizarse los ataques empleando software específico.

-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.

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.

-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.

-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.

-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.

-Consejos para navegar por Internet

Nadie está libre de pecado y haber cometido un error que cree más de un problema, o estar cerca de cometerlo. Para ello, si quieres prevenir y limitar al mínimo las posibilidades de ser atacado, sigue estos consejos de seguridad cuando entres en la Red:

*Asegúrate de acceder siempre a cualquier web que utilice un certificado SSL. Las direcciones que empiezan con “https” son seguras y puedes acceder a ellas con plena libertad, mientras que las que solo tienen “http” pueden provocarte quebraderos de cabeza.

*Tener siempre actualizado tu navegador a la última versión disponible además de tener el sistema operativo también al día.

*Evita usar redes VPN de acceso libre o servidores proxy.

*Actualiza tus contraseñas y utiliza diferentes claves para cada web.

*Evita conectarte, en la medida de lo posible, a redes wifi abiertas (hoteles, estaciones de tren, tiendas, etc.).

*Evita descargar información confidencial o transmitir datos de inicio de sesión en redes públicas, y por supuesto no uses tu tarjeta de crédito en estas redes.

*Si ves un correo electrónico cuyo remitente no te suena, elimínalo. Pueden contener malware y fastidiarte el día.

BIBLIOGRAFIA:

https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/#:~:text=Un%20ataque%20Man%20in%20the%20Middle%20(en%20adelante%20MitM)%20o,cuando%20en%20realidad%20es%20el