INSTITUTO TECNOLOGICO DE CANCUN

LEON QUEB MIGUEL ANGEL

ISMAEL JIMENEZ SANCHEZ

FUND. TELECOMUNICACIONES

HORARIO

17:00 – 18:00

MAN IN THE MIDDLE

-Definición

El ataque man in the middle describe un patrón de ataque en internet en el que un atacante se infiltra, entre el sistema de la víctima y un recurso de internet utilizado por la víctima, un sistema que el controla de forma física o lógica. El objetivo de este ataque es interceptar, leer o manipular la comunicación entre la víctima y el recurso de internet sin ser descubierto.

Por ataque MitM se entiende aquel método por el que un hacker interviene en el tráfico de datos entre dos participantes en una comunicación, haciéndose pasar por uno o por otro. Este tipo de ataques se llevan a cabo, sobre todo, en redes informáticas con el fin de anular la codificación SSL/TLS y poder acceder a información confidencial ya sean datos de usuario, contraseñas y cuentas bancarias.

-Modos de ataque Man in the Middle

Para infiltrarse en el tráfico de datos entre dos o más sistemas, una práctica común es recurrir a diversas técnicas que se centran en las debilidades de la comunicación por internet.

Algunos de estos modos de ataque están centrados en los protocolos DHCP (Dynamic Host Configuration Protocol), responsable de la concesión de direcciones IP locales, ARP (Address Resolution Protocol) el cual sirve para determinar las direcciones de hardware (Media Access Control) es decir MAC. Todos estos protocolos son vulnerables al ataque MitM. Así mismo los ataques de este tipo pueden ser realizados manipulando los servidores DNS. Así mismo los atacantes aprovechan las brechas de seguridad en softwares de navegación anticuados.

Ataques basados en servidores DHCP

En esta modalidad el atacante coloca su propio ordenador o cualquier equipo que este en su control en una LAN a modo de servidor DHCP. Con esto el atacante puede controlar la adjudicación de direcciones IP locales mediante el servidor DHCP simulado, puede registrar las puertas de acceso que se deseen y desviar el tráfico de datos salientes a cualquier ordenador para interceptar y manipular contenidos.

Ya que este tipo de ataque se basa en la manipulación de un sistema DHCP, la terminología correcta en este caso es la de DHCP spoofing. La condición para poder llevar a cabo este tipo de ataque es que el atacante utilice la misma red de área local que la víctima. Si un atacante quiere infiltrarse en una red corporativa que funciona por cable, primero tendrá que buscar un punto de acceso físico a la red LAN.

ARP Cache Poisoning

Este modo de ataque se basa en el funcionamiento del protocolo ARP el cual resuelve las direcciones IP de redes LAN, en direcciones MAC. De esta manera, la asignación de direcciones MAC a IP locales se guarda en forma de tabla en el caché ARP del ordenador que solicita la información. Es aquí donde se lleva acabo el ARP cache poisoning, el objetivo de este tipo de ataque es manipular las tablas ARP de los diversos ordenadores de la red por medio de respuestas ARP falsas para que, por ejemplo, un ordenador que está bajo el control del atacante actúe como punto de acceso inalámbrico o puerta de entrada a internet.

Si un ataque de ARP spoofing tiene éxito, el o los atacantes tienen la posibilidad de leer a totalidad los datos salientes de los ordenadores que hayan sido engañados, pero también de registrarlos o de manipularlos antes de transmitirlos a la verdadera puerta de acceso.

El ataque ARP cache poisoning solo es posible si el atacante está en la mima red LAN que la víctima.

Ataques basados en servidores DNS

Este tipo de ataques como su nombre lo indica está basado en servidores DNS el cual es el sistema de nombres de dominio de internet, el cual es responsable de la resolución de URL en direcciones IP públicas. En este tipo de ataque, el atacante manipula las entradas en el caché de un servidor DNS; con el objetivo de persuadirlas para que respondan a solicitudes con direcciones de destino falsas. Si este ataque es realizado correctamente el usuario puede derivar a otros usuarios de internet a una página web de la red.

Uno de los puntos de partida para los ataques de este tipo reside en, que los servidores utilizan una versión muy antigua del software DNS en los cuales por lo general aceptan y guardan los datos solicitados de manera explícita.

Simulación de un punto de acceso inalámbrico

Este tipo de ataque está principalmente dirigido a los usuarios de dispositivos móviles, para llevar a cabo este tipo de ataque, el atacante configura su ordenador de tal manera que se convierta en una vía adicional para acceder a internet. Si el atacante consigue engañar a los usuarios este puede acceder y manipular la totalidad de los datos de su sistema antes de que se transmitan al verdadero Access point. En caso de requerirse una autenticación, el atacante recibe el nombre de usuario y contraseñas que se utilizan en el registro.

Ataque Man in the browser

Variante del ataque MitM, en este ataque el hacker instala malware en el navegador de los usuarios de internet, con el objetivo de interceptar sus datos. Los ordenadores que no están

correctamente actualizados son lo que más ofrecen brechas de seguridad que permite la infiltración de atacantes. Si se introducen programas en el navegador de un usuario de forma clandestina, estos registran en un segundo plano todos los datos que se intercambian entre el sistema de la persona que ha sido víctima del ataque y las diferentes páginas web.

Esta modalidad de ataque, permite que el atacante pueda interceptar una gran cantidad de sistemas con relativamente poco esfuerzo.

Human assisted attack

Esta forma de ataque consiste en ser realizado por uno o varios atacantes simultáneamente en tiempo real. Uno de estos ataques MitM tendría lugar de la siguiente manera: en cuanto un usuario de Internet inicia sesión en la página web de su banco, el hacker, que se ha colocado entre el navegador del usuario y el servidor del banco, recibe una señal. Esto le da la posibilidad de robar las cookies de sesión y la información de la autenticación en tiempo real y de conseguir, así, los nombres de usuario, las contraseñas y los códigos TAN.