Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

Ing. Sistemas Computacionales

“INVESTIGACIÓN SOBRE MITM”

Profesor: Ismael Jiménez Sánchez

Alumno: Ángel Eduardo Hernández Pimentel

Fecha: jueves 12 noviembre del 2020

INVESTIGAR SOBRE MITM (MAN-IN-THE-MIDDLE)

Definición MITM

Un ataque de intermediario (Man in the middle en inglés) es un nombre genérico para definir un ciberataque en el que alguien se coloca entre usted y lo que sea que esté haciendo en línea, por ejemplo, entre usted y sus transacciones bancarias en línea, entre usted y el chat con su madre, entre sus correos electrónicos de trabajo y la persona que los tenga que recibir o los envíe, o bien entre usted y el cuadro en que introduce su información de pago, entre otras muchas situaciones.

Cada segundo que permanecemos navegando dentro de la red estamos bajo riesgo de un ataque cibernético. Entre los más reconocidos, y que suponen una alerta, se encuentra el ataque Man-in-the-Middle, también conocido como MitM o ataque intermediario. Consiste en una persona o software interfiriendo en la comunicación entre ordenadores o dispositivos, lo que permite que un tercero tenga acceso a la información que se transmite. La idea de este ataque es desviar los datos y controlarlos.

Tipos de ataques Man-in-the-Middle

El riesgo de sufrir un ataque MitM está latente en todo momento. La realidad es que no existe una sola manera de lograr **irrumpir en la comunicación de datos**. El hacker no hace todo por casualidad, conoce a la víctima para poder implementar el método más adecuado y engañarla. Entre los tipos de ataques Man-in-the-Middle se encuentran:

Ataques basados en servidores DHCP: Cuando se habla de DHCP, este permite asignar dinámicamente una dirección IP y toda su configuración. Si se crea un servidor DHCP falso, entonces este se encargará del control de asignación de direcciones IP locales. Con esto, podrá desviar y manipular el tráfico de información gracias a que es capaz de utilizar las puertas de enlace y servidores DNS a su favor.

- **ARP cache poisoning:** El ARP o Address Resolution Protocol permite la resolución de direcciones IP de una red LAN en direcciones MAC. En el momento en que el protocolo empieza a trabajar, se realiza el envío de las direcciones IP y MAC de la máquina solicitante, así como la IP del solicitado. Finalmente, la información queda almacenada en el caché ARP. Para lograr tener acceso a estos datos, entonces el hacker creará un ARP falso. Esto permitirá que se conecte la dirección MAC del atacante con la IP de la red y poder recibir toda la información que se transmite.
- **Ataques basados en servidores DNS:** el DNS o Domain Name System está encargado de traducir los nombres de dominios a direcciones IP y almacenarlas en un caché para recordarlas. La idea del atacante es manipular la información de este caché, para cambiar los nombres de dominio y redirigir a un sitio diferente.

Tipos de descifrados en un MitM

Se ha interceptado la comunicación, llega el momento en que los datos obtenidos deben ser descifrados. En lo que respecta a los ataques Man-in-the-Middle, los atacantes suelen enfocarse en cuatro formas para tener acceso a la información:

- **Suplantación de HTTPS:** el HTTPS es un protocolo que te asegura que el sitio web que visitas mantiene tus datos seguros. Pero un hacker tiene la capacidad de romper esta seguridad. Instala un certificado de raíz de

seguridad falso. Se engaña al navegador, haciéndole creer que el sitio es seguro y le permite el acceso a la clave de cifrado.

- **BEAST en SSL:** en español se le conoce como vulnerabilidad del navegador en SSL/TLS. SSL y TLS son otros dos protocolos de seguridad que buscan proteger la información de los usuarios. En este caso, el hacker aprovecha las debilidades del cifrado por bloques para desviar y descifrar cada uno de los datos que se envían entre el navegador y el servidor web. De esta manera, conoce el tráfico de internet de la víctima.
- **Secuestro de SSL:** en el momento en que se ingresa a un sitio web, el navegador primero hace conexión con el protocolo HTTP para luego pasar al HTTPS. Esto permite proporcionar un certificado de seguridad, logrando así que el usuario navegue de forma segura. Si existe un atacante, entonces este desviará el tráfico a su dispositivo antes de que se logre la conexión al protocolo HTTPS. Así será capaz de acceder a la información de la víctima.
- **Stripping de SSL**: el atacante utiliza un ataque MitM de ARP cache poisoning. A través de este, logrará que el usuario ingrese a una versión HTTP del sitio. Con esto, tendrá acceso a todos los datos descifrados.

CÓMO DEFENDERSE

En este caso, el servidor se verifica a sí mismo presentando un certificado digital y se establece un canal cifrado entre el cliente y el servidor a través del que se envía la información confidencial. Además, los usuarios pueden protegerse de estos ataques evitando conectarse a routers WiFi abiertos o usando plugins de navegador como HTTPS Everywhere o ForceTLS; los cuales establecen una conexión segura siempre que sea posible. Sin embargo, cada una de estos métodos tiene sus límites y existen ejemplos de ataques como SSLStrip o SSLSniff que pueden invalidar la seguridad de las conexiones SSL

Bibliografía

Carlos, A. (18 de noviembre de 2018). *analfatecnicos.net*. Obtenido de analfatecnicos.net: https://www.analfatecnicos.net/archivos/79.ConexionesRJ45-Wikipedia.pdf

Cruz, J. A. (27 de agosto de 2018). *penta.ufrgs.br*. Obtenido de penta.ufrgs.br: http://penta.ufrgs.br/gereseg/unlp/t17ahome.htm

Marchan, E. (9 de junio de 2016). *mi.certerus.com/*. Obtenido de mi.certerus.com/: https://mi.certerus.com/knowledgebase/124/iQue--es-un-Proxy-y-para-que-sirve-.html

Moreno, A. (7 de Agosto de 2018). *akubica.com*. Obtenido de akubica.com: https://akubica.com/ataques-mitm/

Torres, D. (7 de Agosto de 2018). *blog.masmovil.es*. Obtenido de blog.masmovil.es: https://blog.masmovil.es/glosario/definicion-proxy/

Vargas, P. (9 de febrero de 2019). *tsitio.com*. Obtenido de tsitio.com: https://www.itsitio.com/us/que-es-un-ataque-man-in-the-middle-mitm-2/