TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico De Cancún

Fundamentos de Telecomunicaciones

Tarea: Investigar sobre MITM

Ingeniería En Sistemas Computacionales

Alumno: Pérez Ovalle Alan

Docente: Ing. Ismael Jiménez Sánchez

Horario 05:00 Pm – 06:00 Pm

Qué Son Los Ataques Man In The Middle

Si traducimos literalmente al español, Man in the Middle significa “hombre en el medio”. Básicamente eso nos indica qué es este tipo de ataque. Consiste en una persona que es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía. Una especie de “pinganillo” capaz de escuchar todo lo que se transfiere entre dos puntos.

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.

Si hablamos de uno de los ejemplos más habituales y claros, podemos mencionar cuando se utiliza un router Wi-Fi. En este caso el atacante lo que hace es configurar un dispositivo malicioso para que parezca legítimo. De esta forma buscará interceptar toda la información que pase por él, todos los datos que envía el usuario. Puede utilizar un ordenador, por ejemplo, para crear una red Wi-Fi a la que se conecta la víctima

Esto es algo que suele estar presente en lugares muy concurridos. Por ejemplo, en aeropuertos, centros comerciales, estaciones de tren… Sitios donde los usuarios van a conectarse a redes inalámbricas para poder tener Internet. El problema es que en realidad no se están conectando a un router legítimo, sino que están entrando en una red configurada en un ordenador u otro dispositivo de forma maliciosa.

Otro ejemplo de ataque Man in the Middle es el que se lleva a cabo en los navegadores. Lo que hacen los atacantes es insertar código malicioso en el sistema de la víctima y actúa como intermediario. El objetivo aquí es ir recopilando todos los datos que se introducen en el navegador, las páginas visitadas, etc. Estamos, una vez más, en un intermediario.

Cómo protegernos de ataques Man in the Middle

Por suerte los usuarios podemos llevar a cabo diferentes acciones o el uso de herramientas para protegernos de ataques Man in the Middle. De esta forma podremos mantener la seguridad de nuestros sistemas y no corregir ningún tipo de riesgo. Vamos a explicar cuáles son los métodos más aconsejables y habituales para protegernos de este tipo de ataques.

Evitar las redes públicas y abiertas

Como hemos visto, una de las técnicas más utilizadas para llevar a cabo ataques Man in the Middle es a través de redes configuradas de forma maliciosa. Por tanto hay que intentar evitar las redes públicas y aquellas que tengan un cifrado débil o que estén abiertas. De esta forma tendremos más garantías de que nuestras conexiones están aseguradas. Debemos asegurarnos de que las redes a las que accedemos son reales, seguras y que no van a ser un problema para nuestra seguridad. Así podremos proteger la información a la hora de navegar.

Usar herramientas para navegar en HTTPS

Si navegamos por páginas HTTP nuestra información puede ser interceptada. Esto hace que algo básico para evitar ser víctimas de este tipo de ataques sea navegar solo a través de páginas HTTPS, que son aquellos sitios cifrados.

Ahora bien, podemos hacer uso de herramientas que nos ayudan a ello. Hay extensiones que nos permiten navegar únicamente por sitios HTTPS y de esta forma no comprometer nuestros datos.

Utilizar servicios VPN

El uso de servicios VPN puede ayudar a prevenir los ataques Man in the Middle cuando navegamos por páginas que no estén cifradas o desde redes Wi-Fi públicas. Hay muchas opciones tanto gratuitas como de pago y tienen como objetivo cifrar nuestras conexiones. Es un tipo de herramientas que debemos considerar.

Proteger nuestras cuentas

Para evitar intrusos que puedan llevar a cabo este tipo de ataques algo que debemos tener en cuenta es la protección de nuestras cuentas. Con esto nos referimos a utilizar contraseñas que sean fuertes y complejas, pero también el uso de métodos como la autenticación en dos pasos para evitar que alguien pudiera acceder.