



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto tecnológico de Cancún

Nombre:

Bartolo Cordova Rodríguez

Maestro:

Ing. Ismael Jiménez Sánchez

Asignatura:

FUNDAMENTOS DE TELECOMUNICACIONES

Actividad:

Investigación

MITM

Fecha

09 de diciembre de 2021

MITM

Definición de ataque MITM

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.

Variante

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.

Una variante más reciente de este tipo de ataque es el ataque man-in-the-browser. En este contexto, el ciberdelincuente usa una serie de métodos para insertar un código malicioso en el equipo de la víctima, el cual funciona dentro del navegador.

Este malware registra, silenciosamente, los datos enviados entre el navegador y las páginas. Estos ataques han ganado en popularidad porque permiten al delincuente atacar a un grupo mayor de víctimas sin la necesidad de estar cerca de éstas.

Defensa

Existen diferentes formas efectivas para defendernos de los ataques MiTM, pero la mayoría de ellas usan un router/ servidor y no permiten que el usuario controle la seguridad de la transacción que realiza. Este método de defensa usa un sistema de cifrado fuerte entre el cliente y el servidor. 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.

Cómo prevenir los ataques MITM

Por norma general es casi imposible que los afectados puedan reconocer la presencia de un ataque de intermediario, por lo que la prevención se convierte en la mejor forma de protección. A continuación, presentamos una recopilación de los consejos más importantes para que los usuarios de Internet y operadores de páginas web puedan minimizar el riesgo de convertirse en blanco de un ataque MITM.

Bibliografía

<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/>