



Tecnológico Nacional de México

Instituto Tecnológico de Cancún

Sergio Eleazar Barahona Chulim

Carrera:

Ingeniería en Sistemas Computacionales

Materia:

Fundamentos de Telecomunicaciones

Profesor:

ING ISMAEL JIMÉNEZ

Horario:

5 a 6 PM

TAREA: INVESTIGAR SOBRE MITM

¿QUÉ ES 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.

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.

DEFINICIÓN DE ATAQUE MAN-IN-THE-MIDDLE

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.

VARIANTES DE ATAQUE MITM

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.

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.