Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

MITM y Proxy

Prof. Ismael Jiménez Sánchez

Alumno(a). Laury del Rosario Mex Martin

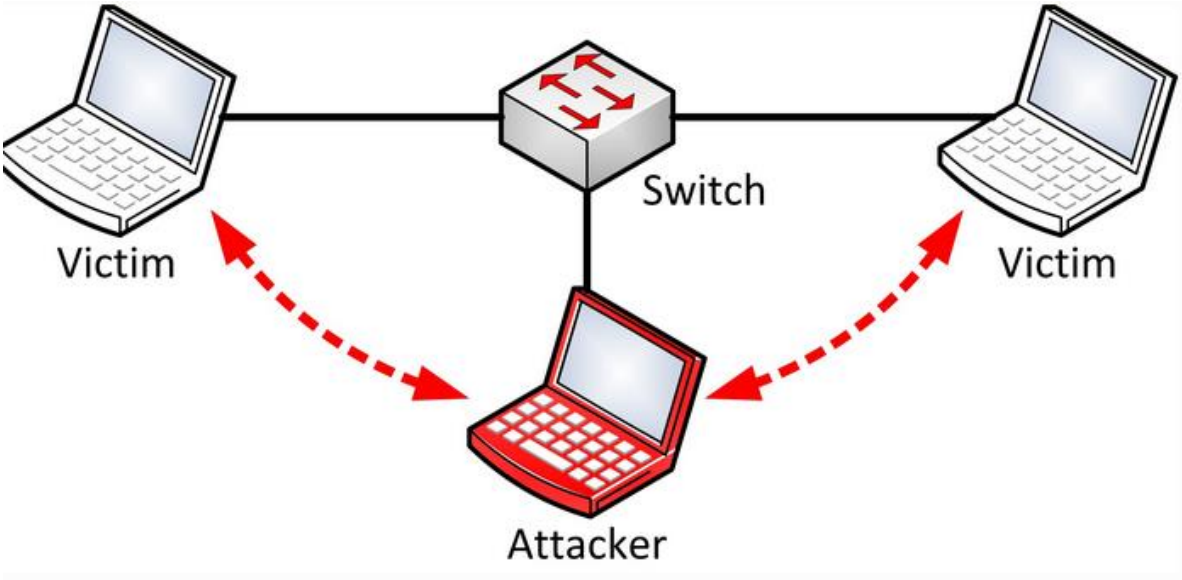
Ciclo 2020-B

Fecha de Entrega: 12 de Noviembre de 2020

MITM (Ataques Man-In-The-Middle.)

En la criptografía y la seguridad informática , un ataque de hombre en el medio (a menudo abreviado a MITM , MitM , MIM , MiM o MITMA) es un ataque donde el atacante secretamente transmite y posiblemente altera la comunicación entre dos partes que creen que son comunicándose directamente entre sí . A través de una analogía de ajedrez se pueden pensar los ataques de hombre en el medio .
Alguien que apenas sabe jugar al ajedrez , afirma que puede jugar dos grandes maestros simultáneamente y ganar un juego o sacar ambos . Espera a que el primer gran maestro haga un movimiento y luego hace este mismo movimiento contra el segundo gran maestro . Cuando el segundo gran maestro responde , Mallory hace el mismo juego contra el primero. Él juega todo el juego de esta manera y no puede perder.

Un ataque de hombre en el medio (MITM) es una estrategia similar y puede utilizarse contra muchos protocolos criptográficos . Un ejemplo de ataques de hombre en el medio es la escucha activa , en la que el atacante establece conexiones independientes con las víctimas y transmite mensajes entre ellos para hacerles creer que están hablando directamente entre sí a través de una conexión privada , cuando de hecho la toda la conversación es controlada por el atacante . El atacante debe ser capaz de interceptar todos los mensajes relevantes que pasan entre las dos víctimas e inyectar nuevos . Esto es sencillo en muchas circunstancias ; por ejemplo , un atacante dentro del rango de recepción de un punto de acceso inalámbrico Wi - Fi no cifrado , puede insertarse como un hombre en el medio.
Esta es una descripción genérica, sobre todo porque (si estamos hablando de ataques MITM de red), la lógica y los detalles dependen en gran medida de la técnica que se está utilizando (más en la sección de spoofing).
Sin embargo, podemos simplificar el concepto con un ejemplo. Cuando se conecta a alguna red (su red doméstica, WiFi público, Starbucks, etc.), el router / switch es responsable de reenviar todos sus paquetes al destino correcto, durante un ataque MITM "forzamos" a la red a considerar nuestro dispositivo como el enrutador (nosotros "spoofeamos/suplantamos" la dirección original del ranurador / del interruptor de cierta manera):



Una vez que esto ocurre, todo el tráfico de la red pasa a través de su computadora en lugar del enrutador/switch legítimo y en ese momento usted puede hacer prácticamente todo lo que quiere, desde sólo sniffear datos específicos (correos electrónicos, contraseñas, cookies, etc de otras personas en su red) hasta interceptar y procesar activamente todas las peticiones de algún protocolo específico con el fin de modificarlas (puede, por ejemplo, reemplazar todas las imágenes de todos los sitios web visitados por todos, eliminar conexiones, etc.).
BetterCap es responsable de proporcionar al investigador de seguridad todo lo que necesita en una sola herramienta que funciona simplemente en sistemas GNU/Linux, Mac OS X y OpenBSD.

Tipos de Proxy

Un servidor proxy es un servidor (puede ser tanto un programa como un dispositivo físico) que actúa como un intermediario. Se sitúa entre la solicitud que realiza un cliente y otro servidor que da la respuesta. Si queremos acceder desde un móvil a un servidor de Internet donde está alojada una página web, un proxy puede actuar de intermediario.

Esto permite ganar más control de acceso, registrar el tráfico o incluso restringir determinados tipos de tráfico. De esta forma podremos mejorar en seguridad y también en rendimiento, así como tener anonimato al acceder a determinados servicios.

Una de las funciones más comunes para lo que los usuarios utilizan los proxys es para **saltarse la restricción geográfica**. Es decir, un proxy puede actuar como intermediarios y hacer que nuestra conexión aparezca en otro lugar. De esta forma podemos acceder a contenido disponible únicamente para un determinado país o poder ver contenido que no esté disponible en el nuestro.

Proxy web

Sin duda uno de los servidores proxy más populares son la web. Estamos ante una opción en la que los usuarios pueden acceder a través de una página web. Esa web es la que actúa como proxy. Está basado en HTTP y HTTPS y actúa como intermediario para acceder a otros servicios en Internet.

A través de esa página web podremos navegar por otros sitios. Toda esa navegación pasa a través del proxy web que estamos utilizando.

Proxy caché

Otra opción es la de un servidor **proxy caché**. En este caso este servidor actúa como intermediario entre la red e Internet para cachear contenido. Puede ser contenido de tipo estático como HTML, CSS, imágenes… Se utiliza para acelerar el contenido de un sitio al navegar.

Si una persona entra en una página por segunda vez, esa información que está cargando ya puede estar cacheada. De esta forma no necesita descargarla de nuevo y va más rápido.

Proxy reverso

También están los **proxys reversos**. Puede utilizarse para brindar acceso a Internet a un usuario en concreto dentro de la red, ofrecer algún tipo de caché o incluso actuar como firewall y ayudar a mejorar la seguridad.

Proxy transparente

En este caso lo que hace el proxy es obtener la petición que hemos dado y darle una redirección sin necesidad de modificar nada previamente. Básicamente actúa como un intermediario sin modificar nada, de ahí el nombre que obtiene.

Proxy NAT

Una opción más en cuanto a proxys es el proxy **NAT**. Principalmente se utilizan para enmascarar la identidad de los usuarios. Esconde la verdadera dirección IP para acceder a la red. Cuenta con variadas configuraciones.

En definitiva, estos son los principales tipos de proxys que podemos encontrarnos. Como vemos hay una variedad de opciones y cada uno de ellos puede tener un uso diferente de cara a los usuarios. Todos ellos actúan como intermediarios entre el usuario (dispositivo móvil, ordenador…) y un servidor. Pueden ayudar para mejorar la seguridad y privacidad, así como para obtener diferentes funciones a la hora de navegar por la red.

Proxy Anónimo

Este tipo de proxy web permite realizar actividades en Internet de forma anónima. El acceso es realizado por el servicio de proxy, protegiendo la información de IP y ocultando la identificación del ordenador de origen. Es un gran obstáculo para las redes, pues a través de éstos, se hace posible el bypass de políticas de seguridad.

Aunque este tipo de proxy puede ser utilizado con fines legítimos, desafortunadamente la mayoría de los accesos son para burlar las políticas de seguridad existentes en las empresas. Otro aspecto importante es que esto termina siendo una fuente utilizada por criminales y mal intencionados para capturar información sensible de los usuarios.

Mientras el usuario está utilizando el servicio para burlar la seguridad local, puede automáticamente estar exponiendo información que genera un riesgo personal e incluso corporativo. Por lo tanto, mucho cuidado con este tipo de proxy.

Proxy abierto

Estos tipos de proxies están abiertos a todo tipo de conexiones y cualquier usuario puede utilizarlos. Si utilizas un servicio así, puede que los servidores te bloqueen porqué detecten que están realizando SPAM, ya que no controlan quien se conecta.