INVESTIGACIÓN MITV Y TIPOS DE PROXY.

TELECOMUNICACIONES

Alumno: Manuel Alfonso Alonzo Chi

12 DE NOVIEMBRE DE 2020

¿QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE?

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. 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 plugin 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.

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.

Es importante que nuestras cuentas en Internet estén perfectamente protegidas. Solo así podremos evitar intrusos que puedan interceptar nuestras comunicaciones.

Qué es un proxy

En primer lugar, vamos a empezar hablando de qué es un 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.

Qué tipos de proxys existen

Hay que tener en cuenta que existen diferentes tipos de proxys. Vamos a ver cuáles son los más comunes.

Proxy web

Sin duda uno de los servidores proxy más populares son los webs. 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 los proxys 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.

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.