INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN
SISTEMAS COMPUTACIONALES

MATERIA:
FUNDAMENTOS DE TELECOMUNICACIONES

TAREA:
INVESTIGAR MITM Y LOS TIPOS DE PROXY

NUMERO DE CONTROL Y NOMBRE DEL ALUMNO:
18530369 CRUZ GÓNGORA FERNANDO JÓSE

HORARIO:
LUNES A JUEVES
17:00 PM – 18:00 PM

MAESTRO:
ING. ISMAEL JIMÉNEZ SÁNCHE

MITM

es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso wifi sin cifrar, donde este se puede insertar como intermediario.

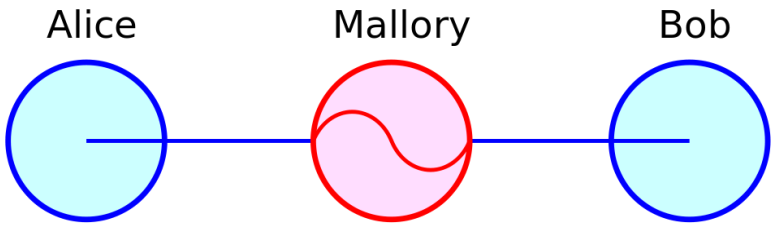
EJEMPLO DE UN ATAQUE:

Suponga que Alice quiere comunicarse con Bob. Mientras tanto, Mallory quiere interceptar la conversación para escuchar y posiblemente alterar (aunque este paso no es necesario) el mensaje que recibe Bob.

En primer lugar, Alice le pregunta a Bob por su clave pública. Si Bob envía su clave pública a Alice, pero Mallory es capaz de interceptarla, un ataque de intermediario puede comenzar. Mallory envía un mensaje falsificado a Alice que dice ser de Bob, pero en cambio incluye la clave pública de Mallory. Alice, creyendo que esta clave pública sea de Bob, cifra su mensaje con la clave de Mallory y envía el mensaje cifrado de nuevo a Bob. Mallory intercepta otra vez, descifra el mensaje utilizando su clave privada, posiblemente altera si ella quiere, y vuelve a cifrar con la clave pública de Bob que fue enviada originalmente a Alice. Cuando Bob recibe el nuevo mensaje cifrado, él cree que vino de Alice.

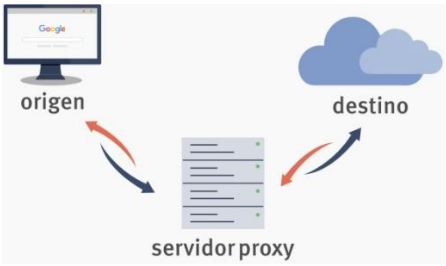
1. **Alice envía un mensaje a Bob, que es interceptado por Mallory:**
   Alice ***"Hola Bob, soy Alice. Dame tu clave."*** → **Mallory** **Bob**
2. **Mallory reenvía este mensaje a Bob; Bob no puede decir que no es realmente de Alice:**
   Alice **Mallory** ***"Hola Bob, soy Alice. Dame tu clave."*** → **Bob**
3. **Bob responde con su clave de cifrado:**
   Alice **Mallory** ← ***[clave de Bob]*** **Bob**
4. **Mallory reemplaza la clave de Bob con la suya, y transmite esto a Alice, afirmando que es la clave de Bob:**
   Alice ← ***[clave de Mallory]*** **Mallory** **Bob**
5. **Alicia encripta un mensaje con lo que ella cree que es la clave de Bob, pensando que sólo Bob puede leer:**
   Alice ***"¡Nos vemos en la parada de autobús!" [Cifrada con la clave de Mallory]*** → **Mallory** **Bob**

6. **Sin embargo, debido a que en realidad estaba cifrada con la clave de Mallory, Mallory puede descifrarlo, leerlo, modificarlo (si se desea), volver a cifrar con la clave de Bob, y lo remitirá a Bob:**
   Alice Mallory "¡*Nos vemos en la furgoneta de al lado del río!" [Cifrada con la clave de Bob]* → Bob
7. **Bob cree que este mensaje es una comunicación segura de Alice.**
8. **Bob va a la furgoneta sin ventanas y Mallory le atraca.**



Este ejemplo muestra la necesidad de que Alice y Bob tengan alguna manera de asegurarse de que están realmente utilizando mutuamente claves públicas, en lugar de la clave pública de un atacante. De lo contrario, este tipo de ataques son generalmente posibles, en principio, contra cualquier mensaje enviado utilizando la tecnología de clave pública. Afortunadamente, hay una variedad de técnicas que ayudan a defenderse de los ataques MITM.

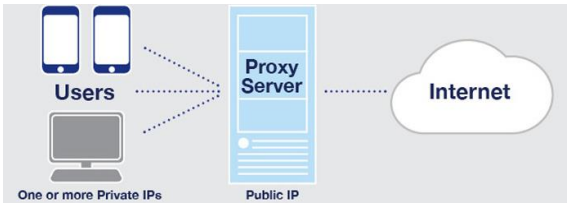
PROXY



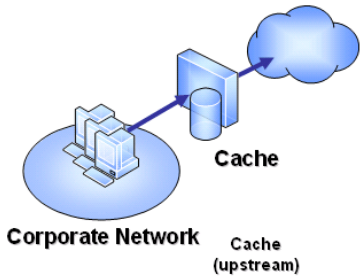
Un servidor proxy es un servidor (puede ser tanto un programa como un dispositivo físico) que actúa como un intermediario. Se sitúa entre la solicitud que realiza un cliente y otro servidor que da la respuesta. Si queremos acceder desde un móvil a un servidor de Internet donde está alojada una página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

TIPOS DE PROXY

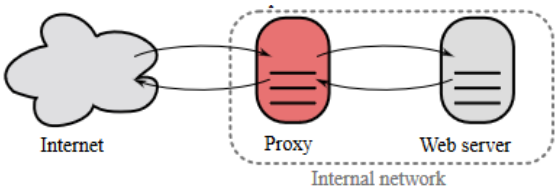


PROXY WEB: Sin duda uno de los servidores proxy más populares son los webs. Estamos ante una opción en la que los usuarios pueden acceder a través de una página web. Esa web es la que actúa como proxy. Está basado en HTTP y HTTPS y actúa como intermediario para acceder a otros servicios en Internet.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