ITCANCUN

ALUMNO: LÓPEZ HERNÁNDEZ JAVIER ISAC

PROFESOR: ISMAEL JIMENEZ SANCHEZ

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

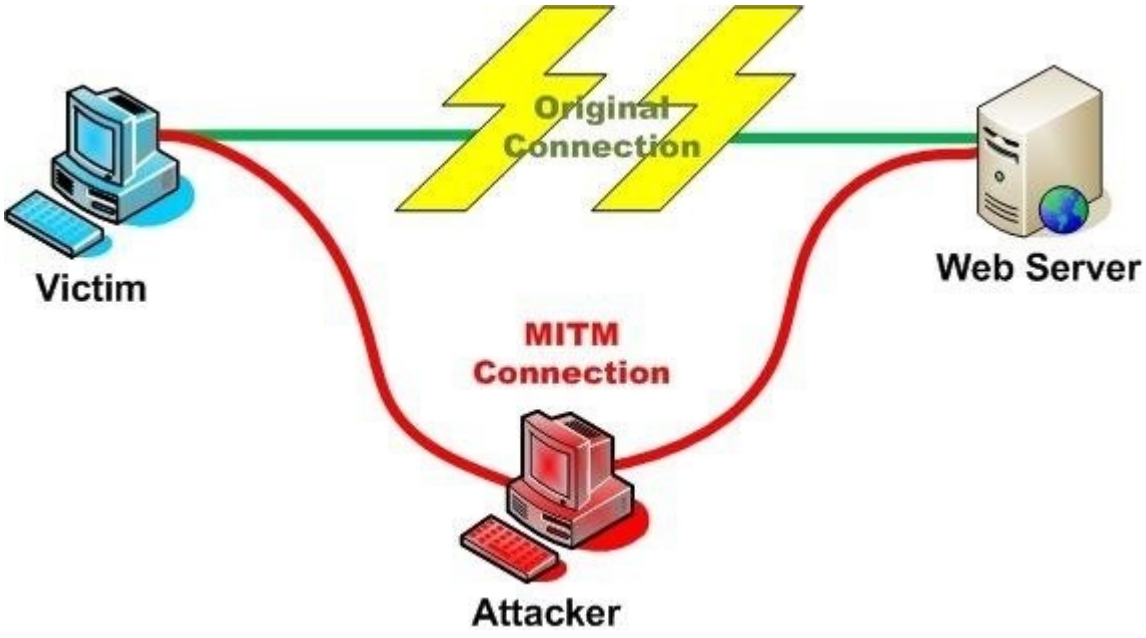
CURSO: FUNDAMENTOS DE TELECOMUNICACIONES

INVESTIGACIÓN SOBRE MITM Y TIPOS DE PROXY

MITM

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. 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. 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. La posibilidad de un ataque de intermediario sigue siendo un problema potencial de seguridad serio, incluso para muchos criptosistemas basados en clave pública

En un ataque de MITM, el atacante tiene control total de la información entre dos o más socios de enlace. Esto permite al atacante leer, influir y manipular la información. El atacante está reflejando la identidad del primero y del segundo interlocutor de comunicación, de modo que puede participar en el canal de comunicación.



El hombre en el medio es una forma de secuestro de sesiones. Otras formas de secuestro de sesiones similares al hombre en el medio son:

SideHacking - Este ataque implica oler paquetes de datos para robar cookies de sesión y secuestrar la sesión de un usuario. Estas cookies pueden contener información de inicio de sesión sin cifrar, incluso si el sitio era seguro.
Evil Twin - Esta es una red Wi-Fi pícara que parece ser una red legítima. Cuando los usuarios se unen sin saberlo a la red no autorizada, el atacante puede lanzar un ataque de tipo "man-in-the-middle", interceptando todos los datos entre usted y la red.
Sniffing - Esto implica un actor malicioso que utiliza software fácilmente disponible para interceptar los datos que se envían desde, o a, su dispositivo.

Usa siempre HTTPS: muchos sitios web ofrecen desde hace tiempo comunicaciones cifradas a través de SSL, siempre que visites una página asegúrate de que la dirección muestre HTTPS en lugar de HTTP, y si no lo hace, escríbelo manualmente.

Activar la verificación de dos pasos: muchos servicios han comenzado a ofrecer verificación de dos factores en sus servicios para aumentar la seguridad del acceso a las cuentas de usuario.
Usar una red VPN: de esta manera la conexión se cifra entre un cliente VPN y un servidor VPN, estableciéndose a través de un túnel de comunicación seguro.

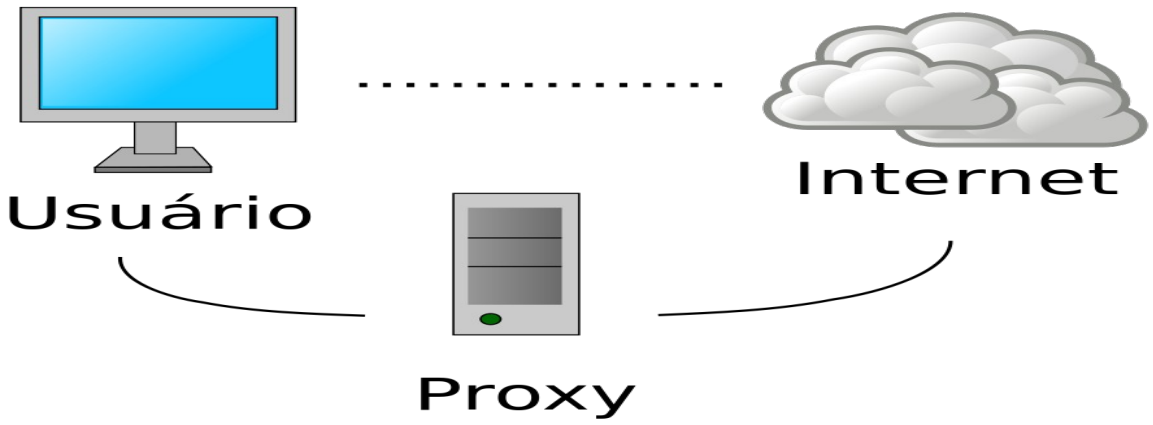
Herramientas de ataque MITM
Hay varias herramientas para realizar un ataque MITM. Estas herramientas son particularmente eficientes en entornos de red LAN, ya que implementan funcionalidades adicionales, como las capacidades de suplantación de arp que permiten la interceptación de la comunicación entre hosts.

1. PacketCreator
2. Ettercap
3. Dsniff
4. Caín e Abel

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.
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.

Los proxys son utilizados muy a menudo para acceder a servicios que tienen bloqueado su contenido en determinado país. Por ejemplo, si una web no ofrece determinado contenido en tu país pero sí en otro, haciéndote pasar por un internauta de ese otro país puedes acceder a él.
Como muchos de estos servicios de proxy bloquean también cookies, scripts y otros objetos que están alojados en las webs, también son útiles para poder navegar de una manera mucho más privada y anónima.

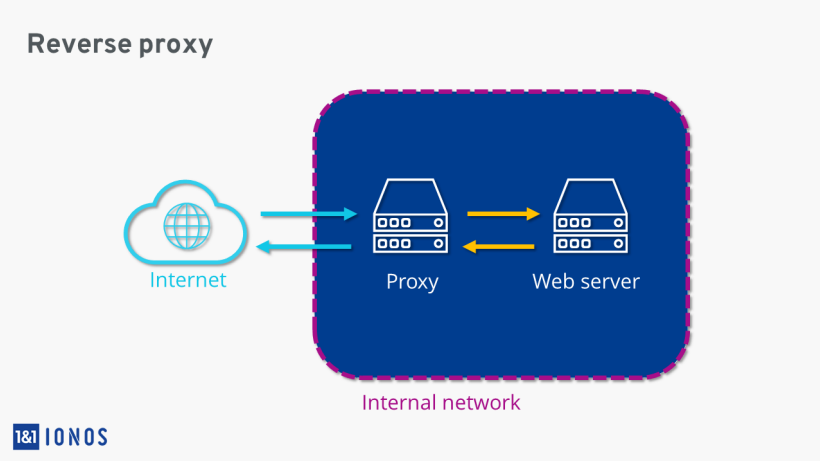


Proxy web
Sin duda uno de los servidores proxy más populares son los web. Estamos ante una opción en la que los usuarios pueden acceder a través de una página web.
A través de esa página web podremos navegar por otros sitios. Toda esa navegación pasa a través del proxy web que estamos utilizando.

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.
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.

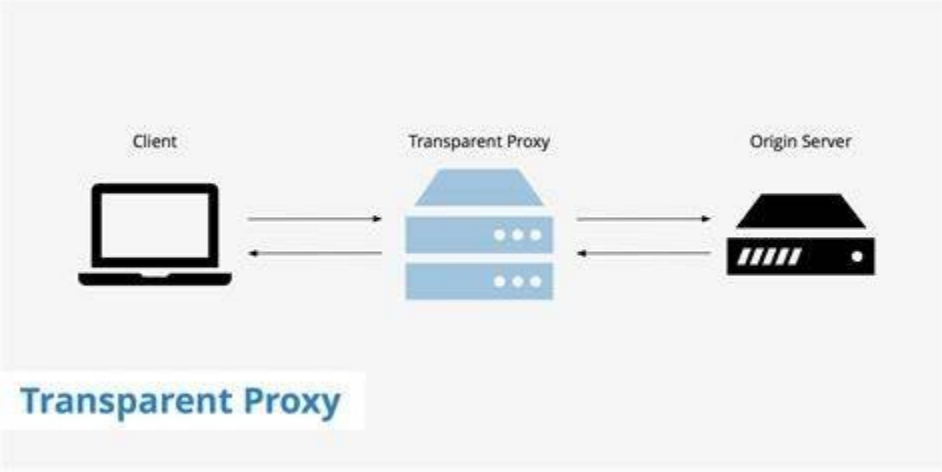
Proxy reverso

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. También están los proxy reversos. Puede utilizarse para brindar acceso a Internet a un usuario en concreto dentro de la red.

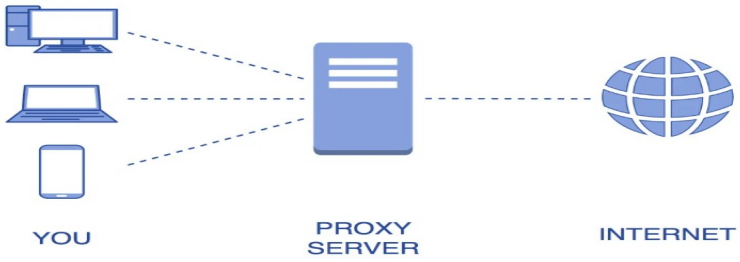


Proxy transparente

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. combina un servidor proxy con NAT (Network Address Translation) demanera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia.



Proxy NAT
Una opción más en cuanto a proxys son los proxy NAT. Principalmente se utilizan para enmascarar la identidad de los usuarios.



FreeProxy
FreeProxy te permite compartir una única conexión a Internet con varios ordenadores en una misma red local: muy útil si necesitas conectar varios ordenadores pero dispones de un único punto de conexión.

inProxy
Con este programa, todos los ordenadores de una red local se pueden conectar a través de una sola conexión de módem. Ofrece "logging" y seguridad para múltiples usuarios

Ana o Proxy
Si tienes varias máquinas en red local, pero una sola conexión a Internet, aquí tienes la solución perfecta para compartir la conexión entre todas ellas.

Bibliografías

Serge Malenkovich. (2013). ¿QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE?. 2020, de kaspersky daily Sitio web: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

Autor desconocido. (2020). Ataque de intermediario. 2020, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Ataque_de_intermediario#Defensas_contra_el_ataque

Javier Jiménez. (2019). Tipos de proxys y qué usos tienen. 2020, de Redes Zone Sitio web: https://www.redeszone.net/tutoriales/redes-cable/tipos-proxys-internet/

Autor desconocido. (Año de publicación desconocido). EL HOMBRE EN EL ATAQUE MEDIO (MITM). 2020, de Veracode Sitio web: https://www.veracode.com/security/man-middle-attack

Gabriela González. (2014). Qué es un ataque «Man in The Middle». 2020, de Hipertextual Sitio web: https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/

Autor desconocido. (Año de publicación desconocido). Ataque de hombre en el medio. 2020, de Owasp Sitio web: https://owasp.org/www-community/attacks/Man-in-the-middle_attack

Autor desconocido. (Año de publicación desconocido). Proxy. 2020, de Asociación que publica el artículo desconocida Sitio web: https://cursosasir.files.wordpress.com/2015/07/tema-5-proxy.pdf

YÚBAL FERNÁNDEZ. (2017). Qué es un proxy y cómo puedes utilizarlo para navegar de forma más anónima. 2020, de Xataca basics Sitio web: https://www.xataka.com/basics/que-es-un-proxy-y-como-puedes-utilizarlo-para-navegar-de-forma-mas-anonima