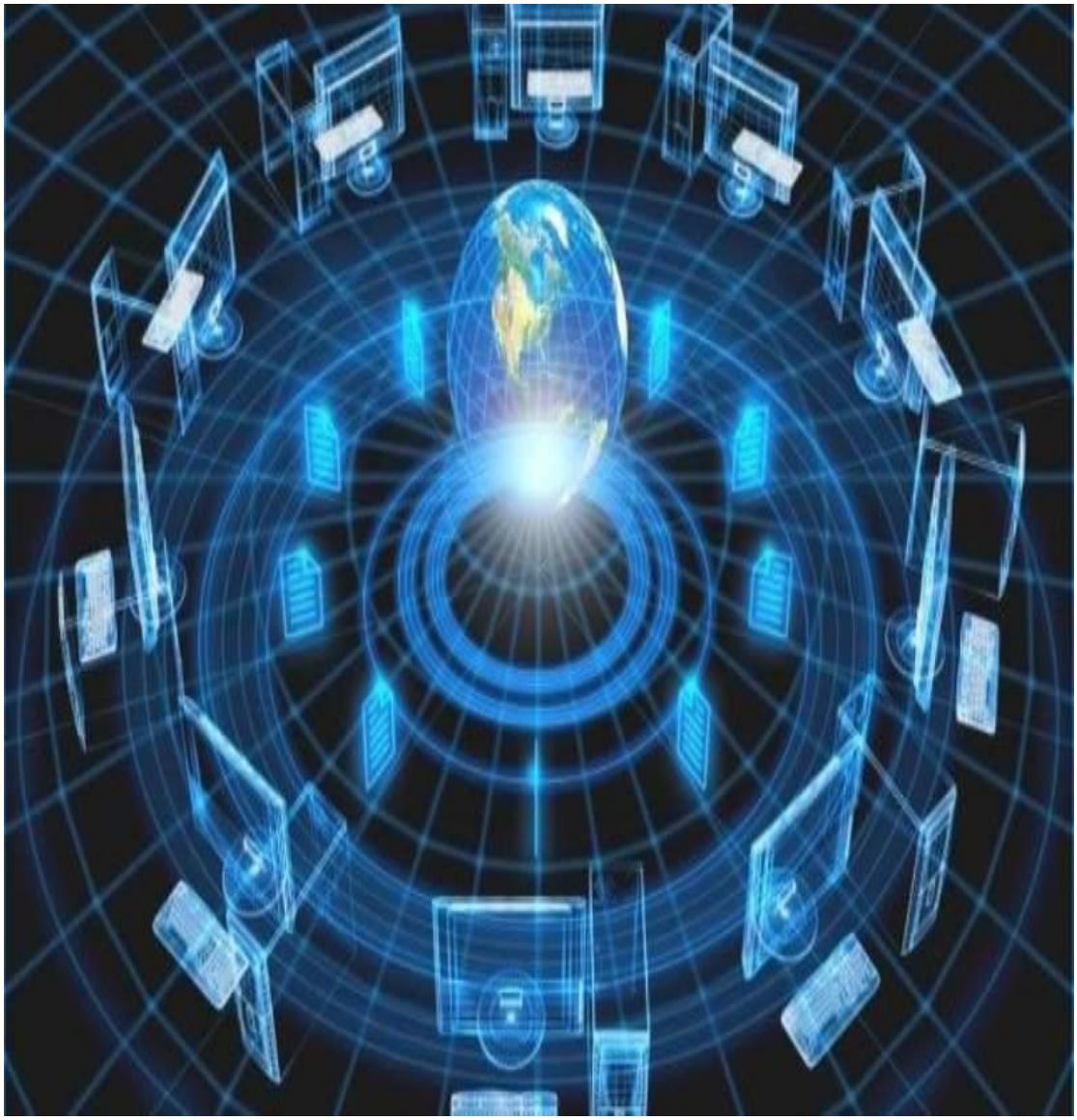


Investigar sobre MITM

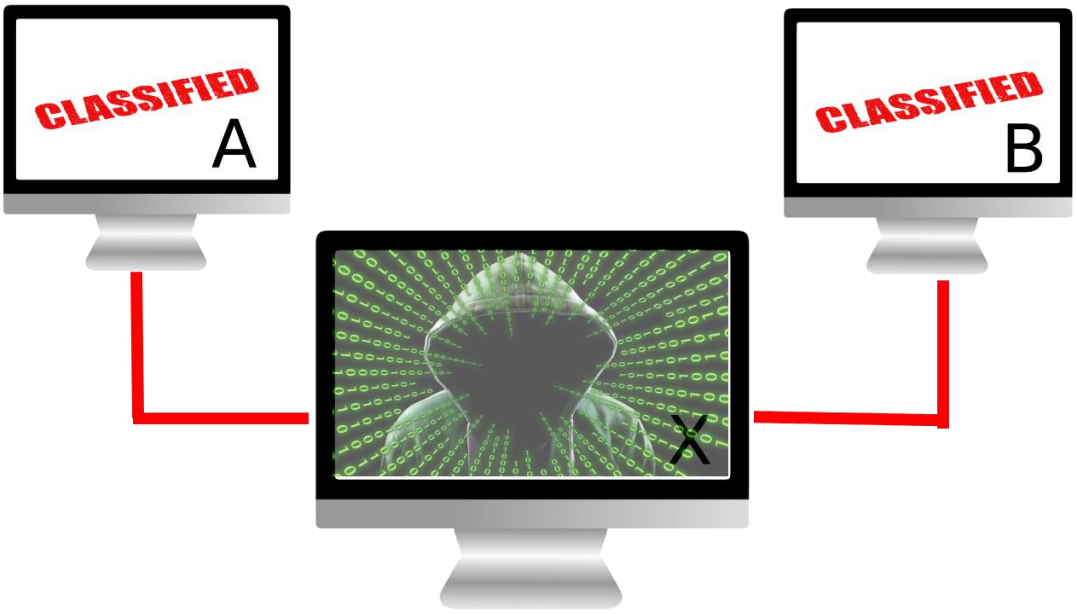
IBARRA SABIDO JOSE MARIA | **Fundamentos de Telecomunicaciones** | 12-11-2020

MITM

El ataque MITM (Man in the middle), del inglés “Hombre en el medio”, es muy popular entre los ciberdelincuentes por la cantidad de información a la que pueden llegar a acceder en caso de que tengan éxito. Es un tipo de ataque basado en interceptar la comunicación entre 2 o más interlocutores, pudiendo suplantar la identidad de uno u otro según lo requiera para ver la información y modificarla a su antojo, de tal forma que las respuestas recibidas en los extremos pueden estar dadas por el atacante y no por el interlocutor legítimo. Pero veamos exactamente en qué consiste para entenderlo mejor.

¿En qué consiste?

Básicamente, consiste en interceptar la comunicación entre 2 o más interlocutores. Para ello, alguien anónimo llamado “X” se sitúa entre ambos e intercepta los mensajes de A hacia B, conociendo la información y a su vez dejando que el mensaje continúe su camino.



Generalmente este tipo de ataques son muy peligrosos y difíciles de detectar, ya que precisamente uno de los objetivos del atacante es evitar ser descubierto, para ello emplean diversas técnicas que complican la detección.

Por si fuera poco, con el sigilo, la comunicación entre A y B transcurre normal como si fuera legitima, sin embargo, el atacante puede decidir si el mensaje interceptado continuará, si lo hará con la misma información o si lo hará con otro contenido modificado que pudiera suponerle una ventaja o beneficio.

Tipos de ataques

Los ataques MITM tienen diferentes modalidades que dependen de la técnica empleada, por lo tanto, más que hablar de los tipos de ataques vamos a hablar de los escenarios de ataque.

puntos de acceso wifi abiertos o con baja seguridad,

redes locales (LAN),

software de navegación anticuado.

Los puntos de acceso wifi públicos o con bajo nivel de seguridad pueden suponer un riesgo en el que un atacante de forma deliberada permite la conexión para poder efectuar un ataque de "Man in the middle". Otra modalidad consiste en imitar el nombre de una red cercana (SSID) para crear confusión y que algunas personas conecten por error a ella, además muchos dispositivos están configurados por defecto para conectar sin preguntar, conectándose automáticamente a las redes abiertas más cercanas o cuyo nombre SSID es igual.

Las redes locales (Local Area Network LAN) de las empresas también son vulnerables a este tipo de ataques. El atacante deberá tener acceso a la red local corporativa, donde podrá lanzar un ataque que consistirá en engañar a los equipos de la red local haciéndoles creer que es un dispositivo legítimo de la misma y forzando a que todo el tráfico generado pase a través del dispositivo controlado por el ciberdelincuente. El acceso a las redes locales puede ser llevado a cabo de forma física, por ejemplo, con un ordenador o mediante malware, infectando por ejemplo determinados servidores y pudiendo manipular sus respuestas.

Por otro lado, los atacantes también aprovechan las vulnerabilidades de los navegadores obsoletos o no actualizados, por lo que debemos prestar especial atención.

Prevención

Generalmente, es muy difícil detectar cuándo se está sufriendo un ataque de intermediario (Man In The Middle), por tanto, la prevención es la primera medida de protección. Para poder minimizar el riesgo de convertirse en blanco de un ataque de este tipo, podemos llevar a cabo algunas acciones específicas:

Acceso a sitios web seguros con certificado. (Aquellos que empiezan por HTTPS, comprobando que el certificado pertenece a la compañía o entidad que corresponde).

Proteger la red wifi de la empresa. Asegurando como mínimo la red en modo WPA2-AES con contraseñas robustas y no adivinables, así evitaremos que los atacantes puedan colarse en la red local. Si es necesario que los clientes se

conecten a una red en nuestra empresa, habilitar una red de invitados con acceso restringido a la red corporativa y servicios de la empresa.

Tener actualizado el software de nuestros equipos, especialmente el sistema operativo y el navegador.

Utilizar contraseñas robustas y siempre que sea posible habilitar la autenticación en dos pasos.

Evitar conectar a redes wifi abiertas (las que podemos encontrar en cafeterías, hoteles, aeropuertos, centros comerciales, vecindarios, etc.), en caso de conexión utilizar una red privada virtual o VPN.

En caso de conexión a través de redes públicas sin utilizar una VPN (centros comerciales, aeropuertos, etc.), evitar difundir información personal conectándose a redes sociales o banca online, entre otros ejemplos.

Evita usar redes VPN gratuitas, ya que se desconoce quién está detrás de ellas y el uso que puedan darle a la información.

Evitar abrir enlaces de correo procedentes de fuentes desconocidas.

Emplear software de seguridad como antivirus y antimalware en los equipos corporativos y mantenerlo actualizado, realizando escaneos frecuentemente. Además, también es aconsejable proteger la red LAN mediante el uso de hardware especifico de seguridad como Firewalls o mUTM's con IPS/IDS (prevención y detección de intrusiones), mejorando así tanto la seguridad pasiva como la activa de la red corporativa.

Mantener el firewall por software activado en aquellos sistemas que lo permitan.

Proteger la página web corporativa mediante un certificado SSL.

Si, además, recientemente hemos sufrido alguna infección en nuestros equipos o sospechamos que podamos tenerla a causa de comportamientos extraños, ventanas emergentes, publicidad, etc., debemos realizar una limpieza del equipo antes de transmitir cualquier información sensible.

Con estos consejos y navegando en sitios web seguros reducimos sustancialmente el riesgo de sufrir ataques de este tipo.

Si tienes dudas, llama al 017, la Linea de Ayuda en Ciberseguridad de INCIBE. Expertos en la materia resolverán cualquier conflicto online relacionado con el uso de la tecnología y los dispositivos conectados.

Cómo prevenir los ataques Man in the Middle

Por norma general es casi imposible que los afectados puedan reconocer la presencia de un ataque de intermediario, por lo que la prevención se convierte en la mejor forma de protección. A continuación, presentamos una recopilación de los consejos más importantes para que los usuarios de Internet y operadores de páginas web puedan minimizar el riesgo de convertirse en blanco de un ataque MitM.

Consejos para navegar por Internet

Nadie está libre de pecado y haber cometido un error que cree más de un problema, o estar cerca de cometerlo. Para ello, si quieres prevenir y limitar al mínimo las posibilidades de ser atacado, sigue estos consejos de seguridad cuando entres en la Red:

Asegúrate de acceder siempre a cualquier web que utilice un certificado SSL. Las direcciones que empiezan con “https” son seguras y puedes acceder a ellas con plena libertad, mientras que las que solo tienen “http” pueden provocarte quebraderos de cabeza.

Tener siempre actualizado tu navegador a la última versión disponible además de tener el sistema operativo también al día.

Evita usar redes VPN de acceso libre o servidores proxy.

Actualiza tus contraseñas y utiliza diferentes claves para cada web.

Evita conectarte, en la medida de lo posible, a redes wifi abiertas (hoteles, estaciones de tren, tiendas, etc.).

Evita descargar información confidencial o transmitir datos de inicio de sesión en redes públicas, y por supuesto no uses tu tarjeta de crédito en estas redes.

Si ves un correo electrónico cuyo remitente no te suena, elimínalo. Pueden contener malware y fastidiarte el día.

Consejos para tener una página web fiable

Al igual que siendo usuario tienes que tomar medidas como las que hemos mencionado antes, si acabas de lanzar tu negocio al mundo online, ponte en su lugar. No puedes permitir que tu vida se arruine por no estar prevenido y no haber evitado un ataque fulminante a tus datos. Por ello:

No dudes en proteger los datos de tus clientes con un certificado SSL, que hará ver a tus clientes y visitantes que tienes una web segura.

Trata de darle a tus distintas formas de iniciar sesión de forma segura, por ejemplo, si habilitas la autenticación de dos pasos, o una validación de cuenta a través del correo electrónico.

Jamás solicites los datos de acceso de tus clientes (usuario y contraseña) por correo, pónselo por escrito para que no tengan dudas.