Nombre de la materia: Fundamentos de Telecomunicaciones

Nombre de la licenciatura: Ingeniería en Sistemas Computacionales

Nombre del alumno(a):

William Adrien Sarragot Pastrana

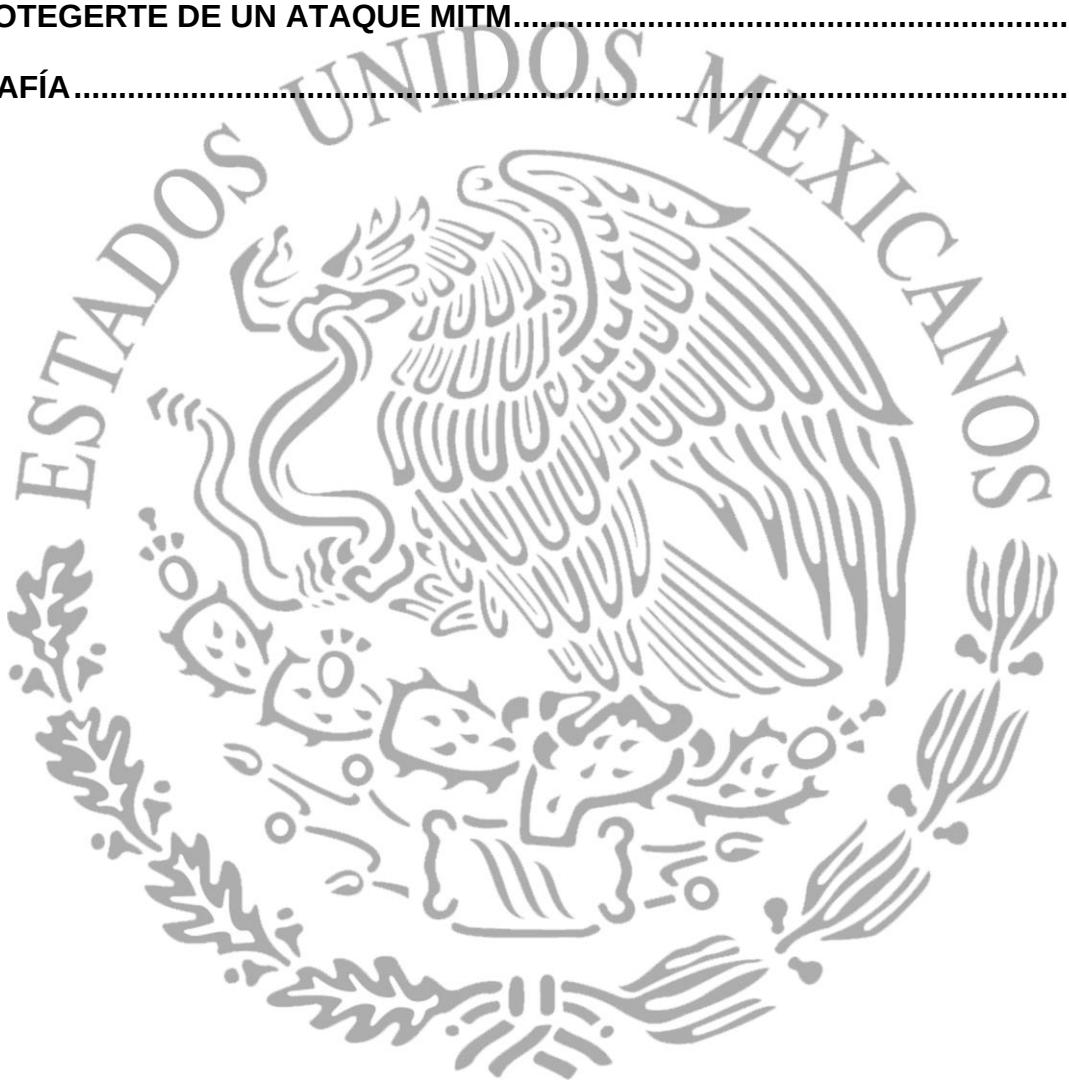
Unidad 2: Tarea : Investigar MITM

Nombre del profesor(a):

Ing. Ismael Jiménez Sánchez

Fecha: 11 noviembre del 2020

INDICE



MITM Definición:

Traducimos literalmente al español, Man in the Middle significa “hombre en el medio”. Básicamente eso nos indica qué es este tipo de ataque. Consiste en una persona que es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía. Una especie de “pinganillo” capaz de escuchar todo lo que se transfiere entre dos puntos.

Un ataque Man in the Middle puede ser tanto online como offline. Los piratas informáticos pueden llevar a cabo diferentes tipos de ataques para lograr su objetivo. Siempre intentarán interceptar los mensajes pasando desapercibido.

Ejemplo:

Man in the Middle es el que se lleva a cabo en los navegadores. Lo que hacen los atacantes es insertar código malicioso en el sistema de la víctima y actúa como intermediario. El objetivo aquí es ir recopilando todos los datos que se introducen en el navegador, las páginas visitadas, etc.

- Ataques de phishing a través de correos electrónicos que redirigen a sitios web falsos.
- Kits de phishing o banca electrónica
- Portales de viajes que en realidad no son portales de viajes pero que ofrecen vuelos baratos. El cliente introduce su número de cuenta y su código bancario en el sitio web falso.
- "Ataques con marcadores" son los clásicos "ataques de man-in-the-middle"

Características

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. La información entre los dos hosts está cifrada, pero es descifrada por el atacante y transmitida.

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.

Evitar las redes públicas y abiertas

Como hemos visto, una de las técnicas más utilizadas para llevar a cabo ataques Man in the Middle es a través de redes configuradas de forma maliciosa. Por tanto, hay que intentar evitar las redes públicas y aquellas que tengan un cifrado débil o que estén abiertas. De esta forma tendremos más garantías de que nuestras conexiones están aseguradas.

Cómo protegerte de un ataque MITM

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. Siempre que el mecanismo de verificación de los dos factores sea suficientemente fuerte, esta es otra linea de defensa contra atacantes.

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.

Bibliografía

Aguero, A. (18 de enero de 2019). *softwarelab.org/es/servidor-proxy/*. Obtenido de softwarelab.org/es/servidor-proxy/: https://softwarelab.org/es/servidor-proxy/

Carlos, D. J. (7 de Noviembre de 2018). *medium.com*. Obtenido de medium.com: https://medium.com/@xxxamin1314/t568a-vs-t568b-cu%C3%A1l-es-la-diferencia-entre-el-cable-directo-y-el-cable-cruzado-3da883c1bb62

Castrejon, M. (1 de Agosto de 2017). *blog.gruponovelec.com*. Obtenido de blog.gruponovelec.com: https://blog.gruponovelec.com/redes-vdi/cable-coaxial-tipos-y-caracteristicas/

community.fs.com. (9 de Febrero de 2018). *community.fs.com*. Obtenido de community.fs.com: https://community.fs.com/es/blog/t568a-vs-t568b-difference-between-straight-through-and-crossover-cable.html

Jimenez, J. (14 de diciembre de 2019). *redeszone.net*. Obtenido de redeszone.net: https://www.redeszone.net/tutoriales/seguridad/ataques-man-in-the-middle-evitar/

Leyva, A. (8 de noviembre de 2018). *bricoladores*. Obtenido de bricoladores: https://bricoladores.simonelectric.com/bid/379675/tipos-de-cable-y-tipos-de-aislamiento-del-cable-coaxial

monografias. (17 de enero de 2014). Obtenido de https://www.monografias.com/trabajos14/estruct-datos/estruct-datos.shtml

Osorio, F. (9 de agosto de 2018). *ibiblio.org*. Obtenido de ibiblio.org: https://www.ibiblio.org/pub/linux/docs/LuCaS/Tutoriales/doc-servir-web-escuela/doc-servir-web-escuela-html/enmascaramiento.html

Sanchez, R. (31 de junio de 2016). *ionos.mx*. Obtenido de ionos.mx: https://www.ionos.mx/digitalguide/servidores/know-how/que-es-un-servidor-proxy-inverso/