

Investigar sobre MITM

UNIDAD II



FECHA: 11 – nov – 2020
Wilmer Rodríguez
Jiménez
Fundamentos de
telecomunicaciones
Prof. Ismael Jimenez
Sanchez
Periodo Ago – Dic

Investigar sobre Man-In-The-Middle

El ataque 'Man in the middle', traducido a español como 'El hombre en el medio', es un ataque PASIVO, que se lleva a cabo tanto en redes LAN como WLAN. Pongamos un simple ejemplo para poner de manifiesto en qué consiste este ataque: Supongamos que tenemos 3 hosts dentro de una red, host A, host B, y host C. El host A quiere intercambiar información con el host B (éste host puede o no estar en la misma red), para ello, los paquetes deben enviarse a través del router que los dirige hacia B. Ahora, si el host C tiene intención de 'escuchar' el mensaje que A envía a B, sólo tiene que adoptar un papel de puente entre A y el router.

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.

Si hablamos de uno de los ejemplos más habituales y claros, podemos mencionar cuando se utiliza un router Wi-Fi. En este caso el atacante lo que hace es configurar un dispositivo malicioso para que parezca legítimo. De esta forma buscará interceptar toda la información que pase por él, todos los datos que envía el usuario. Puede utilizar un ordenador, por ejemplo, para crear una red Wi-Fi a la que se conecta la víctima.

Esto es algo que suele estar presente en lugares muy concurridos. Por ejemplo en aeropuertos, centros comerciales, estaciones de tren... Sitios donde los usuarios van a conectarse a redes inalámbricas para poder tener Internet. El problema es que en realidad no se están conectando a un router legítimo, sino que están entrando en una red configurada en un ordenador u otro dispositivo de forma maliciosa.

Otro ejemplo de ataque 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. Estamos, una vez más, en un intermediario.