Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

“Tarea: Investigación MITM”

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

ATAQUE MAN-IN-THE-MIDDLE

El término Man-In-The-Middle (hombre en el medio en inglés) denota un ataque de encriptación en una red de ordenadores. Es un tercer host que reenvía de forma transparente la información digital como una pasarela entre dos o más socios de comunicación y espías simultáneamente. El remitente y el destinatario no saben que hay un tercer host entre los dos y que en realidad no se están comunicando directamente. Este tipo de ataque se llama ataque de Man-In-The-Middle (abreviado ataque MITM). Los objetivos más comunes son las conexiones SSL seguras, como en la banca en línea.

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.

Ejemplos

- Dos interlocutores enlazados A y B están en la misma subred. El "MITM" envía su propia dirección MAC a los dos hosts con la dirección IP de la otra parte respectiva. Los ordenadores de los dos hosts A y B se conectan al ordenador del atacante. Los dos socios de comunicación A y B creen que están conectados directamente.
- 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".