TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“MITM”

UNIDAD 2

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 (ver también servidor proxy).

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".

Ataques a conexiones https

Un atacante invisible puede incluso atacar conexiones https cifradas. En este caso, el atacante debe descifrar la información, leerla y transmitirla de forma encriptada a las dos direcciones respectivamente. Esta forma de ataque tiene éxito si el cifrado de los paquetes de datos se realiza sin certificados firmados (por ejemplo, mediante certificados SSL falsos).

Impacto en el SEO

Cada vez se anima más a los webmasters y SEOs a hacer sus webs más seguras. Así, Google ha incluido el cifrado SSL desde agosto de 2014 como factor de posicionamiento. Si se utiliza esta técnica de cifrado, el riesgo de un ataque de MITM es menor que sin cifrado.

Para asegurar que los usuarios estén suficientemente protegidos contra ataques, los operadores de sitios web también deben actualizar regularmente su software y servidores para que ningún tercero pueda piratear el tráfico entre servidores y clientes. Además del cifrado SSL, Google también supervisa las infracciones de seguridad y avisa a los webmasters si su sitio web ha sido pirateado, siempre que esté registrado en la Consola de Búsqueda de Google.