INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN

SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

TEMA: MITM.

NOMBRE DEL ALUMNO:

COLLÍ CHEL WILLIAM BLADIMIR

HORARIO

LUNES A JUEVES

5:00 PM – 6:00 PM

PROFESOR

ISMAEL JIMENEZ SANCHEZ

¿Qué es un ataque Man in the Middle?

Por su nombre en inglés, un intermediario, normalmente el cibercriminal o un software malicioso, se incrusta entre la víctima y la fuente de datos (cuentas bancatias, email…etc). El objetivo es interceptar, leer o manipular de forma efectiva la comunicación entre la víctima y sus datos sin que nadie se dé cuenta de que hay una tercera persona incluida en la operación.

¿Qué tipos de ataque Man in the Middle existen?

Para infiltrarse en los sistemas, los hackers tienen varias técnicas para buscar cualquier debilidad. Por norma, suelen automatizarse los ataques empleando software específico. Veamos ahora algunos de los ataques más comunes relacionados con el Man in the Middle.

Ataques basados en servidores DHCP

En este ataque, el hacker usa su propio ordenador en una red de área local a modo de servidor DHCP, que en resumidas cuentas sirve para asignar dinámicamente una dirección IP y configuración adicional a cada dispositivo dentro de una red para que puedan comunicarse con otras redes. En cuanto un ordenador establece la conexión con una red de área local, el cliente DHCP reclama datos como la dirección IP local o la dirección de la puerta de acceso predeterminada, entre otros.

ARP cache poisoning

En este caso nos referimos al protocolo ARP, que permite resolver IPs en redes LAN siempre que un ordenador quiera enviar paquetes de datos en una red. Para ello, es imprescindible que conozca el sistema del destinatario. Cuando hace una petición ARP, está enviando al mismo tiempo las direcciones MAC y la IP del ordenador que solicita la información, como la dirección IP del sistema solicitado. Si es correcta toda la petición, la asignación de direcciones MAC a IP locales se guarda en la caché ARP del ordenador solicitante.

Ataques basados en servidores DNS

Este ataque tiene como objetivo manipular las entradas en la caché de un servidor DNS haciendo que den direcciones de destino falsas. Si ha tenido éxito, los hackers pueden mandar a los usuarios de Internet a cualquier página web sin que nadie se dé cuenta.

El proceso se inicia cuando los datos del sistema de nombres de dominio se distribuyen por diferentes ordenadores de la red. Cuando alguien quiere acceder a una web lo suele hacer usando un nombre de dominio. También necesita una dirección IP, determinada por el router que tenga el usuario, para enviar la solicitud.

Si hay entradas en la caché, el servidor DNS emite la respuesta a la solicitud con la IP que proceda, y si no las hay el servidor decidirá la IP con ayuda de otros servidores.

Simulación de un punto de acceso inalámbrico

Centrado en los usuarios de dispositivos móviles, este ataque consiste en recrear un punto de acceso inalámbrico en una red pública, como pueden ser las de una cafetería, un aeropuerto, etc. El atacante prepara su ordenador para que actúe como una vía adicional de acceso a Internet, intentando engañar a los usuarios para que le proporcionen los datos de su sistema antes de que se den cuenta.

Ataque Man in the Browser

Por último, el ataque Man in the Browser consiste en que el atacante instala malware en el navegador de los usuarios de Internet con la finalidad de interceptar sus datos. La principal causa para verse infectado por este ataque es el hecho de tener ordenadores que no están correctamente actualizados y que, por ello, ofrecen brechas de seguridad muy visibles que dan camino libre para infiltrarse en el sistema.

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.

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.

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.