Nombre de la Materia:
Fundamentos de Telecomunicaciones Aula

Nombre de la Licenciatura:
Ing. Sistemas Computacionales.

Nombre del Alumno(a):
Pool Ramírez Miguel Ángel.

Número de Control:
18530437.

Nombre de la Tarea:
MITM (Man in the Middle)

Unidad #3

Nombre de la Unidad: Modulación

Nombre del Profesor(a):

Ing. Ismael Jiménez Sánchez

Fecha: 12/11/20

Introducción

El objetivo número uno de cualquier hacker mínimamente capacitado es acceder a la información confidencial de una empresa para poder gestionarla a su gusto, ya sea mediante chantajes o simplemente eliminando los datos, provocando un auténtico caos informático en los sistemas. Aunque sean ataques diferentes para cada situación (pueden ser individuales u organizados entre varias personas de forma simultánea), el fin siempre es el mismo.

Lo más común para atacar una página web o un sistema informático es insertar código malicioso o malware en el equipo de la potencial víctima, intentando llegar lo antes posible a los datos que quiere lograr el atacante.

¿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 bancarias, 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.

"Un ataque Man in the Middle (en adelante MitM) o ataque de intermediario es el método por el cual un hacker interviene en el tráfico de datos de dos partes vinculadas entre sí en una comunicación haciéndose pasar por cualquiera de ellas, haciéndoles creer que se están comunicando entre ellos cuando en realidad es el intermediario quien recibe la comunicación."

¿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.

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.

El objetivo del ataque ARP cache poisoning es dar respuestas falsas en el proceso para lograr que el atacante use su ordenador como punto de acceso inalámbrico o entrada a Internet. Si es exitoso, el ataque permite leer todos los datos salientes de los ordenadores atacados, aparte de registrarlos o de manipularlos antes de enviarlos al lugar correcto.

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. El peligro real viene si tu dispositivo se configura para comunicarse automáticamente con los puntos de acceso con mayor potencia de señal.

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.

El malware incluye programas en el navegador de un usuario de forma clandestina, registrando todos los datos que intercambia la nueva víctima con las diferentes páginas web que visita. Los hackers obtienen con este método la información que buscaban de forma muy rápida y sin demasiado esfuerzo.

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. Para ello, si quieres prevenir y limitar al mínimo las posibilidades de ser atacado, sigue estos consejos de seguridad cuando entres en la Red:

- 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.
- Si ves un correo electrónico cuyo remitente no te suena, elimínalo. Pueden contener malware y fastidiarte el día.

Consejos para tener una página web fiable

Al igual que siendo usuario tienes que tomar medidas como las que hemos mencionado antes, si acabas de lanzar tu negocio al mundo online, ponte en su lugar. No puedes permitir que tu vida se arruine por no estar prevenido y no haber evitado un ataque fulminante a tus datos. Por ello:

- No dudes en proteger los datos de tus clientes con un certificado SSL, que hará ver a tus clientes y visitantes que tienes una web segura.
- Trata de darle a tus distintas formas de iniciar sesión de forma segura, por ejemplo, si habilitas la autenticación de dos pasos, o una validación de cuenta a través del correo electrónico.
- Jamás solicites los datos de acceso de tus clientes (usuario y contraseña) por correo, pónselo por escrito para que no tengan dudas.

Referencias.

- Andrés Rodríguez. (24/10/2019). ¿Qué es un ataque Man in the Middle? 12/11/2020, de GoDaddy Sitio web: https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/