Instituto Tecnológico de Cancún.

Investigación:

Ataques Man in the middle.

.

Kanxoc Ek Felix Gerardo.

Fundamentos de Telecomunicaciones.

Ismael Jiménez Sánchez.

Ingeniería en Sistemas Computacionales.

Noviembre 2020.

Ataques Man in the middle.

Un ataque man-in-the-middle describe un patrón de ataque en Internet en el que un atacante infiltra, entre el sistema de la víctima y un recurso de Internet utilizado por la víctima, un sistema que él controla de forma física o lógica. El objetivo del atacante es interceptar, leer o manipular la comunicación entre la víctima y el recurso de Internet sin que nadie se dé cuenta de ello.

Modalidades de ataque man-in-the-middle.

Para infiltrase en el tráfico de datos entre dos o más sistemas, los hackers recurren a diversas técnicas que se centran en las debilidades de la comunicación por Internet. El servicio DHCP (Dynamic Host Configuration Protocol), responsable de la concesión de direcciones IP locales, o el protocolo de resolución de direcciones conocido como ARP o Address Resolution Protocol y que sirve para determinar las direcciones de hardware (Media Access Control, MAC), son vulnerables, por ejemplo, para ataques de intermediario en redes de área local internas. En términos generales, estos ataques pueden llevarse a cabo mediante la manipulación de servidores DNS, que son los encargados de la resolución de direcciones de Internet en IP públicas. Además, los hackers hacen uso de las brechas de seguridad en software de navegación anticuado o ponen a disposición de los usuarios más ingenuos accesos corruptos a redes de área local inalámbricas.

Ataques basados en servidores DHCP

En el caso de los ataques basados en un servidor DHCP, es un hacker el que coloca su propio ordenador (o uno que esté bajo su control) en una red de área local (LAN) a modo de servidor DHCP. Este es un componente esencial de una red local y se encarga de la asignación de la configuración de red a otros ordenadores de la red local. Esta tiene lugar, por lo general, de manera automática: en cuanto un ordenador establece la conexión con una red de área local, el cliente DHCP del sistema operativo reclama datos como la dirección IP local, la máscara de red, la dirección de la puerta de acceso predeterminada, o la dirección del servidor DNS competente. Asimismo, este envía un mensaje de transmisión a todos los dispositivos

conectados a la red de área local, aguarda a la respuesta de un servidor DHCP y acepta la primera que entre.

ARP cache poisoning

Por ARP (Address Resolution Protocol) se entiende aquel protocolo de red que sirve para resolver direcciones IP de redes LAN en direcciones de hardware (direcciones MAC). Para que un ordenador pueda enviar paquetes de datos en una red, tiene que conocer las direcciones de hardware del sistema del destinatario. Para ello, se envía una petición de ARP en calidad de transmisión de direcciones MAC a todos los sistemas de la red de área local. Dicha petición contiene tanto las direcciones MAC e IP del ordenador que solicita la información, como la dirección IP del sistema solicitado. Si un ordenador de la red recibe una petición ARP de tales características, el paso siguiente es que este compruebe si el paquete contiene la dirección IP propia en calidad de dirección IP del destinatario. Si es así, se le enviará una respuesta ARP con la dirección MAC al sistema solicitante.

Esta asignación de direcciones MAC a IP locales se guarda en forma de tabla en el caché ARP del ordenador que solicita la información. Es aquí donde actúa el llamado ARP cache poisoning (envenenamiento de caché ARP). El objetivo de este tipo de ataque es manipular las tablas ARP de los diversos ordenadores de la red por medio de respuestas de ARP falsas para que, por ejemplo, un ordenador que está bajo el control del atacante actúe como punto de acceso inalámbrico o puerta de entrada para Internet.

Simulación de un punto de acceso inalámbrico

Un modelo de ataque dirigido sobre todo a los usuarios de dispositivos móviles se basa en la simulación de un punto de acceso inalámbrico en una red inalámbrica pública, como las de las cafeterías o las de los aeropuertos. En ello, un atacante configura su ordenador de tal manera que este se convierta en una vía adicional para acceder a Internet (probablemente una con una calidad de señal mejor que el propio punto de acceso). De esta manera, si el atacante consigue engañar a los usuarios más ingenuos, este puede acceder y manipular la totalidad de los datos de su sistema antes de que estos se transmitan al verdadero access point o punto de acceso. Si este requiere autenticación, el hacker recibe para ello los nombres de usuario y contraseñas que se utilizan en el registro. El peligro de convertirse en el blanco de estos

ataques man-in-the-middle se da particularmente cuando los dispositivos de salida se configuran de tal manera que se pueden comunicar automáticamente con los puntos de acceso con mayor potencia de señal.

Ataque man-in-the-browser

El ataque man-in-the-browser es una variante del ataque MitM. En él, el atacante instala malware en el navegador de los usuarios de Internet con el objetivo de interceptar sus datos. Los ordenadores que no están correctamente actualizados son los que, sobre todo, ofrecen brechas de seguridad que permiten a los atacantes infiltrarse en el sistema. Si se introducen programas en el navegador de un usuario de forma clandestina, estos registran en un segundo plano todos los datos que se intercambian entre el sistema de la persona que ha sido víctima del ataque y las diferentes páginas web.

Human assisted attack

Se puede hablar de human assisted attack cuando una de las modalidades de ataque anteriores no se realiza de manera automática, sino de la mano de uno o varios atacantes en tiempo real. En la práctica, uno de estos man-in-the-middle attacks tendría lugar del siguiente modo: en cuanto un usuario de Internet inicia sesión en la página web de su banco, el hacker, que se ha colocado entre el navegador del usuario y el servidor del banco, recibe una señal. Esto le da la posibilidad de robar las cookies de sesión y la información de la autenticación en tiempo real y de conseguir, así, los nombres de usuario, las contraseñas y los códigos TAN.

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 usuarios de Internet

- Asegúrate de acceder siempre a los sitios web con una conexión segura SSL/TLS. Mientras que las direcciones de Internet que empiezan con https son seguras, las que lo hacen con http suponen un riesgo para la seguridad.

- Antes de introducir las credenciales, comprueba si el certificado SSL de un sitio web está actualizado y ha sido emitido por una autoridad de certificación de confianza.
- El navegador ha de utilizarse siempre en su última versión y el sistema debe estar al día con las actualizaciones.
- Evita usar redes VPN de acceso libre o servidores proxy.
- Mantén las contraseñas actualizadas, utiliza para cada aplicación una contraseña diferente y evita utilizar contraseñas antiguas.
- Evita conectarte a redes wifi abiertas, por ejemplo, en hoteles, estaciones de tren o tiendas.
- Si no tienes más remedio que acceder a una red pública, evita descargar información, transmitir datos de inicio de sesión (por ejemplo, para la bandeja de entrada del correo electrónico o redes sociales) y realizar algún pago.
- Si el operador de un sitio web ofrece métodos adicionales para iniciar sesión de forma segura, utilízalos. Entre ellos pueden citarse la autenticación multifactor (MFA) a través de un token, por SMS o vía app en el Smartphone.
- No cliques en los enlaces de correos de remitentes desconocidos, pues pueden dirigirte a un sitio web con malware.

Consejos para operadores de sitios web

- Protege siempre los datos de tus clientes con un certificado SSL actualizado de una autoridad fiable en páginas web con acceso para clientes.
- Ofrece a tus usuarios métodos adicionales para que puedan iniciar sesión de forma segura. Por ejemplo, con una autenticación multifactor a través del correo.
- Haz saber a los clientes que, en principio, nunca vas a pedir los datos de acceso a través del email y evita los enlaces en los correos que les envíes.