INSTITUTO TECNOLÓGICO DE CANCÚN

ALUMNO: GONGORA JIMENEZ FRANCISCO DAVID.

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ.

MATERIA: FUNDAMENTOS DE TELECOMUNICACIONES.

TAREA:

INVESTIGAR SOBRE LOS TIPOS DE MITM

HORARIO: 5PM-6PM.

FECHA DE ENTREGA:

12 DE NOVIEMBRE DEL 2020

INVESTIGAR SOBRE LOS TIPOS DE MITM

Qué son los ataques Man in the Middle

Man in the Middle significa “hombre en el medio”. Básicamente eso nos indica qué es este tipo de ataque. Consiste en una persona que es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía. Una especie de “pinganillo” capaz de escuchar todo lo que se transfiere entre dos puntos.

Un ataque Man in the Middle puede ser tanto online como offline. Los piratas informáticos pueden llevar a cabo diferentes tipos de ataques para lograr su objetivo. Siempre intentarán interceptar los mensajes pasando desapercibido.

Si hablamos de uno de los ejemplos más habituales y claros, podemos mencionar cuando se utiliza un router Wifi. En este caso el atacante lo que hace es configurar un dispositivo malicioso para que parezca legítimo. De esta forma buscará interceptar toda la información que pase por él, todos los datos que envía el usuario. Puede utilizar un ordenador, por ejemplo, para crear una red Wi-Fi a la que se conecta la víctima.

TIPOS

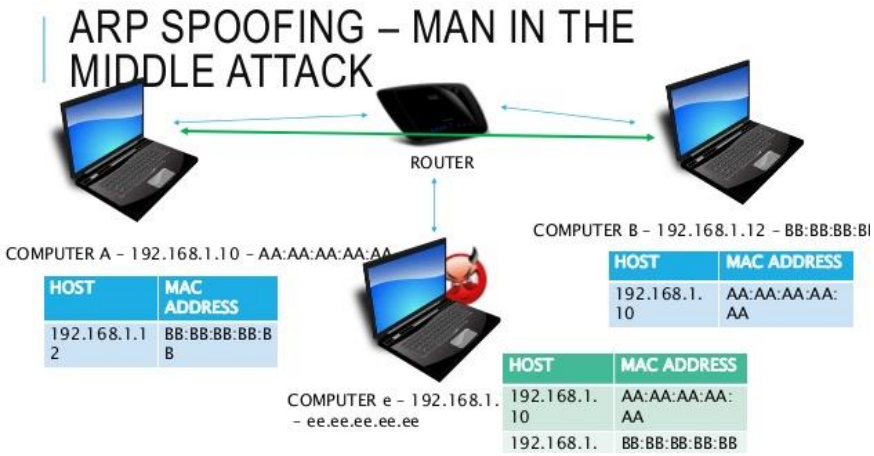
ROUGE ACCESS POINT

Los dispositivos equipados con tarjetas inalámbricas a menudo intentan conectarse automáticamente al punto de acceso que emite la señal más fuerte. Los atacantes pueden configurar su propio punto de acceso inalámbrico y engañar a los dispositivos cercanos para unirse a su dominio. Todo el tráfico de red de la víctima ahora puede ser manipulado por el atacante. Esto es peligroso porque el atacante ni siquiera tiene que estar en una red confiable para hacer esto. El atacante simplemente necesita una proximidad física lo suficientemente cercana.

ARP SPOOFING

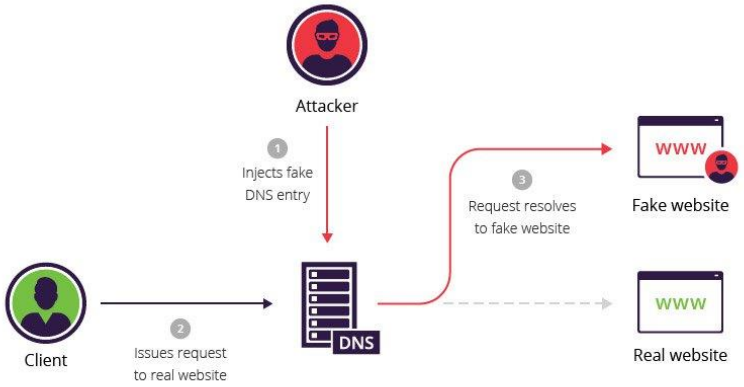
ARP es el protocolo de resolución de direcciones. Se utiliza para resolver direcciones IP en direcciones físicas MAC en una red de área local. Cuando un host necesita hablar con un host con una dirección IP determinada hace referencia a la cache ARP para resolver la dirección IP en una dirección MAC. Si no se conoce la dirección se realiza una solicitud solicitando la dirección MAC del dispositivo con la dirección IP.

Un atacante que desee hacerse pasar por otro host podría responder a las solicitudes a las que no debería responder con su propia dirección MAC. Con algunos paquetes colocados con precisión un atacante puede detectar el tráfico privado entre dos hosts. Se puede extraer información valiosa del tráfico como el intercambio de tokens de sesión, proporcionando acceso completo a las cuentas de la aplicación a las que el atacante no debería poder acceder.



MDNS SPOOFING

El DNS de multidifusión es similar al DNS, pero se realiza en una red de área local (LAN) mediante



trasmisión como ARP. Esto lo convierte en un objetivo perfecto para los ataques de suplantación de identidad. Se supone que el sistema local de resolución de nombres hace que la configuración de los dispositivos de red sea extremadamente simple. Los usuarios no tienen que saber exactamente con que direcciones deben comunicarse sus dispositivos. Dejan que el sistema lo resuelva por ellos. Los dispositivos como televisores impresoras y sistemas de entretenimiento hacen uso de este protocolo ya que generalmente se encuentran en redes confiables.

Cuando una aplicación necesita conocer la dirección de un determinado dispositivo como TV. local, un atacante puede responder fácilmente a esa solicitud con datos falsos indicándole que resuelva en una dirección que tiene control. Dado que los dispositivos mantienen un cache local de direcciones la victima ahora vera el dispositivo del atacante como confiable por un periodo de tiempo.

SUPLANTACIÓN DE DNS

Al igual que ARP resuelve las direcciones IP en direcciones MAC en una LAN, DNS resuelve los nombres de dominio en direcciones IP. Cuando se usa un ataque de suplantación de DNS el atacante intenta introducir información corrupta de cache de DNS a un host en un intento de acceder a otro host utilizando su nombre de dominio.

Esto lleva a la víctima a enviar información confidencial a un host malicioso con la creencia de que está enviando información a una fuente confiable. Un atacante que ya haya falsificado una dirección IP podría tener mucho más fácil falsificar DNS simplemente resolviendo la dirección de un servidor DNS a la dirección del atacante.

TÉCNICAS DE ATAQUE MAN IN THE MIDDLE

SNIFFING

Los atacantes usan herramientas de captura de paquetes para inspeccionar paquetes a un nivel bajo. El uso de dispositivos inalámbricos específicos que se pueden poner en modo de monitoreo o promiscuo puede permitir que un atacante vea los paquetes que no están destinados a ver como los paquetes dirigidos a otros hosts.

INYECCIÓN DE PAQUETES

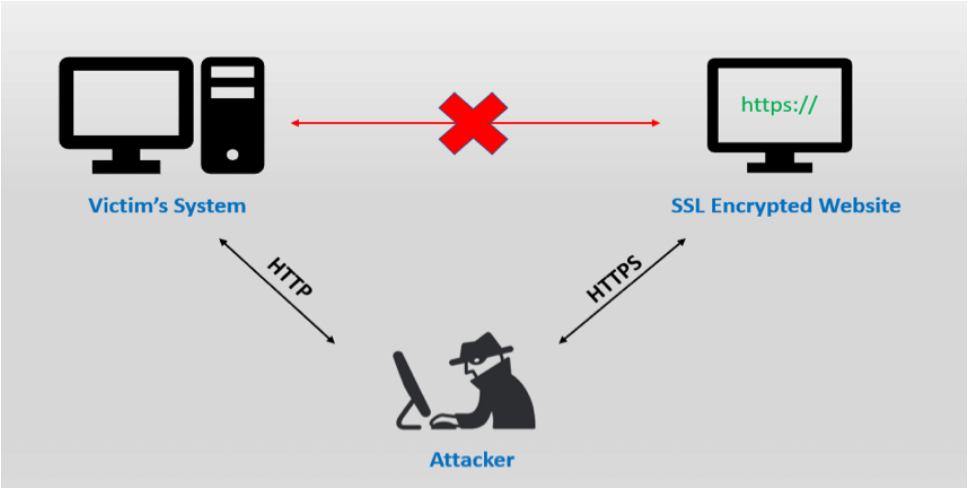
Un atacante también puede aprovechar el modo de monitoreo de su dispositivo para inyectar paquetes maliciosos en los flujos de comunicación de datos. Los paquetes pueden combinarse con flujos de comunicación de datos validos que parecen ser parte de la comunicación, pero de naturaleza maliciosa. La inyección de paquetes generalmente implica primero sniffar para determinar cómo y cuándo elaborar y enviar paquetes.

SECUESTRO DE SESIÓN

La mayoría de las aplicaciones web utilizan un mecanismo de inicio de sesión que genera un token de sesión temporal para usar en futuras solicitudes para evitar que el usuario escriba una contraseña en cada página. Un atacante puede detectar tráfico confidencial para identificar el token de sesión de un usuario y utilizarlo para realizar solicitudes como usuario. El atacante no necesita falsificar una vez que tiene un token de sesión.

SSL STRIPPING

Dado que el uso de HTTPS es una protección común contra la falsificación de ARP o DNS los atacantes usan la eliminación de SSL para interceptar paquetes y alterar sus solicitudes de dirección basadas en HTTPS para ir a su punto final equivalente HTTP lo que obliga al host a realizar solicitudes al servidor sin cifrar. La información confidencial se puede filtrar en texto sin formato.



PREVENCIÓN DE ATAQUES MAN IN THE MIDDLE

ENCRIPTACION FUERTE

Tener un fuerte mecanismo de encriptación en los puntos de acceso inalámbrico evita que usuarios no deseados se unan a su red simplemente estando cerca. Un mecanismo de cifrado débil puede permitir que un atacante ingrese a la red por fuerza bruta y comience a atacar en el medio. Cuanto más fuerte sea la implementación de cifrado más seguro.

RED PRIVADA VIRTUAL (VPN)

Las VPN se pueden usar para crear un entorno seguro para la información confidencial dentro de una red de área local. Utilizan cifrado basado en claves para crear una subred para una comunicación segura. De

esta manera incluso si un atacante llega a una red compartida no podrá descifrar el tráfico en la VPN.

HTTPS

Se puede utilizar para comunicarse de forma segura a través de HTTP mediante el intercambio de claves público-privadas. Esto evita que un atacante tenga uso de los datos que pueda estar Snifando. Los sitios web solo deben usar HTTPS y no proporcionar alternativas HTTP. Los usuarios pueden instalar complementos del navegador para aplicar siempre el uso de HTTPS en las solicitudes.

AUTENTICACION BASADA EN CLAVE PUBLICA

Los ataques Man In the Middle generalmente implican falsificación de algo. La autenticación basada en pares de claves públicas como RSA se puede usar en varias capas de la pila para ayudar a garantizar si las cosas con las que se está comunicando son en realidad las cosas con las que desea comunicarse.

Proteger nuestras cuentas

Para evitar intrusos que puedan llevar a cabo este tipo de ataques algo que debemos tener en cuenta es la protección de nuestras cuentas. Con esto nos referimos a utilizar contraseñas que sean fuertes y complejas, pero también el uso de métodos como la autenticación en dos pasos para evitar que alguien pudiera acceder. Es importante que nuestras cuentas en Internet estén perfectamente protegidas. Solo así podremos evitar intrusos que puedan interceptar nuestras comunicaciones.

Cuidado con los correos electrónicos

A través del correo electrónico podría llevarse a cabo un ataque de este tipo. Podrían, por ejemplo, enviar un documento haciéndose pasar por la otra parte simplemente para obtener información sobre un tema determinado. Debemos tomar precauciones a la hora de abrir, leer o responder correos que recibimos. Siempre hay que asegurarse de que el emisor es realmente quien dice ser y no es un impostor que pueda recopilar nuestra información.

Mantener los sistemas actualizados

Por supuesto algo que no puede faltar es tener los sistemas y aplicaciones actualizados. Con esto nos referimos al sistema operativo, al navegador, así como a cualquier otro tipo de herramientas que utilicemos.