Ataques Man-in-the-Middle

Juan Aparicio

Universidad de la Empresa

21 de julio de 2018

Temario

Introducción

Un ataque Man-in-the-Middle, es un ataque que se basa en posicionar una computadora entre medio de otras 2 computadoras que se están comunicando.
Al estar en el medio de la comunicación de 2 computadoras, el atacante puede escuchar y potencialmente cambiar el contenido de los mensajes que se están enviando en el canal.

ARP cache Poisoning I

Como el switch solo va a enviar los paquetes a la computadora que le corresponden, lo que se hace es *engañar* a la computadora objetivo o switch, para que piense que la computadora del atacante es la computadora atacada.
Cuando se desea establecer comunicación con otra máquina en la red, se usa su dirección IP (también se puede usar le hostname).
Para saber que máquina física tiene esa dirección IP, se envía un mensaje tipo broadcast que pregunta *"Who has IP address x.x.x.x"*.
La máquina con esa dirección IP responde *Ï have IP address x.x.x.x and my MAC is y:y:y:y:y:y"*
La máquina luego guarda en su cache ARP ese mapeo de IP - MAC.

ARP cache Poisoning II

Lo que se hace entonces es enviar constantemente paquetes de respuesta falsos que digan que mi MAC corresponde a la IP del destino.
Luego la máquina atacada va a pensar que la máquina del atacante es en realidad la máquina destino, y envía su tráfico a la máquina del atacante.

Denial of Service I

Una vez que se efectuó el ataque Man-in-the-Middle, si se quiere hacer un denial of service, no hay que hacer nada mas, si no se quiere hacer un denial of service, se tiene que hacer un forwardeo de IP.
Si no se hace el forwardeo de IP, entonces el tráfico que quiere enviar la máquina atacada, va a *morir* cuando llegue a la máquina del atacante, porque la máquina del atacante no va a saber que hacer con el tráfico que tiene como destino otra IP.
Si se hace el forwardeo de IP, entonces los paquetes que llegan a la máquina del atacante que van destinado a otra IP (la que en realidad se quiere enviar), van a ser forwardeados a la dirección correcta.

Captura de tráfico de red I

Una vez habilitado el forwardeo de IP, los paquetes que pasan por la máquina del atacante pueden ser capturados en un archivo para su posterior análisis.
Los paquetes capturados contienen toda la información que se ha transmitido por el canal. Los datos que se pueden ver por ejemplo son:

- Consultas a los servidores DNS (historial de sitios accedidos)
- Tráfico de páginas web ya sea encriptado o desencriptado.
- Si se accedió a algún sitio HTTP (no encriptado) y se hizo un inicio de sesión se pueden ver las credenciales ingresadas (usuario y contraseña).

DNS spoofing I

Una vez que la máquina del atacante se encuentra posicionada en el medio del canal de comunicación, lo que se hace es interceptar las respuesta del servidor DNS (puerto 53) y se modifica el contenido de la respuesta (Por ejemplo 64.233.190.106 que es la dirección de uno de los servidores de google por 192.168.0.107 que puede ser la ip de un apache de una pc en la red).
Luego la máquina atacada recibe la respuesta modificada y va a pensar que google.com se encuentra en una de las máquinas en la red.

Demostración

Fin