IP/MAC Spoofing y ARP Flooding

Arroyo G. Diego, Castañeda F. Juan, y Gómez M. David

Resumen - Este proyecto consiste en el desarrollo e implementación de dos herramientas de red que permiten la inundación de una red LAN mediante la generación de GARP y la suplantación de identidad para realizar un ataque de *Man in the middle*.

I. INTRODUCCIÓN

En el proyecto se plantea la creación de una herramienta que a través de la generación de ARP gratuitos (GARP), logre desbordar la tabla CAM del host de una red LAN, con el fin de generar un trabajo inesperado del switch, donde este comienza a comportarse como un hub permitiendo la lectura de información a todos los nodos de la red o incluso finalizando en un ataque de *Denial of Service* (DoS).

En la segunda parte del proyecto se implementa una herramienta con la capacidad de realizar una suplantación de la dirección MAC de dos máquinas que se encuentren en comunicación mediante FTP, con el fin de ejecutar un ataque de *Man in The Middle (MiTM)*

Para la correcta compresión se deben aclarar algunos conceptos claves utilizados en el desarrollo del proyecto como son ARP, este se trata de un protocolo encargado de la resolución de direcciones IP a direcciones de red físicas (MAC), a su vez, MAC del inglés *Media Access Control*, se trata de un identificador único por tarjeta de red conformado por 48 bits, donde, los primeros 24 bits hacen referencia a el fabricante de dicha tarjeta y los siguientes 24 son configurados por el IEEE.

En consecución a lo planteado, se debe aclarar que este proyecto asume la existencia de una red LAN (*Local Access Network)* donde podemos identificar un *Switch,* que podremos definir como un dispositivo anfitrión que tiene la capacidad de prestar servicios orientados a la comunicación de los usuarios y todo lo que esto abarca, una de las características más importantes para este desarrollo es la existencia de tablas CAM (Tabla de direcciones MAC) que son utilizadas como un recopilatorio del contenido direccionable de la red.

Gracias a la posibilidad de comunicación dentro de la red LAN podemos hacer uso de ciertos protocolos, como puede ser el protocolo de transferencia de archivos (FTP), que es un protocolo basado en la comunicación Cliente-Servidor estándar para la transferencia de archivos.

II. ESTADO DEL ARTE

A. Tipos de ataques

Los ataques dentro del contexto de la Seguridad de la Información, son todo aquello tipo de actividades que están dirigidas a disminuir o corromper la seguridad de una red. En otras palabras, un ataque es cualquier amenaza sistemática generada de manera artificial, de manera deliberada y negligente.[3]

Los ataques más comunes que son usados dentro de este marco son los siguientes:

- •Ingeniería social
- •DoS
- •Ataque a protocolos
- •Ataque a servidores
- •Captura de archivos

Según Kaspersky, ingeniería social puede definirse como un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.[6]

Para los siguientes cuatro ítems podremos generar definiciones desde la práctica, pues, en este proyecto existe la integración de los mismos.

B. ARP Flooding

Una inundación de MAC o ARP, que pueden entender con el mismo ataque, tienen el fin de comprometer la seguridad de un *Switch*.

La manera de proceder en este tipo de ataque, es la generación indiscriminada de paquetes ARP hasta sobrecargar la red, esto puede, además de inundar la tabla CAM, desencadenar una denegación de servicio (*DoS)* por la sobrecarga de tráfico.

C. IP/MAC Spoofing

Identificando el significado de MAC, se puede explicar la suplantación como el engaño a los demás usuarios de una red sobre un cambio de tarjeta de red en las máquinas víctimas.

En esencia, la técnica aplicada en este tipo de ataque es, manteniendo las direcciones IP constantes, cambiar la dirección MAC a la que son direccionadas, como si de un cambio de tarjeta de red se tratara, de esta manera el atacante puede cambiar su dirección IP y su MAC, luciendo ante las víctimas como si él fuese la misma máquina con que se comunicaban pero con una tarjeta de red diferente.

III. Propuesta final

En la primera parte del proyecto realizamos un ARP flooding, para esto solicitamos al usuario cuantos hilos y cuantos mensajes por hilo desea enviar, seguido a esto el programa detecta cuál es la puerta de enlace de la máquina del atacante y comienza a crear paquetes ARP.

Para la creación de paquetes ARP el programa se soporta en una lista de MAC en formato txt donde se pueden encontrar los distintos códigos usados por los fabricantes, los 24 bits restantes son creados de manera aleatoria por el programa.

Para el empaquetamiento se identifican las cuatro variables necesarias en la construcción, la IP fuente, que en este caso es una IP al azar, la IP destino, que se identificó como la puerta de enlace, la MAC fuente, que fue creada a partir de la lista de MAC de fabricantes y MAC destino que se define como de broadcast (ff:ff:ff:ff:ff:ff); finalmente se empaqueta ARP dentro de Ethernet.

Para la segunda parte del proyecto, hicimos un IP/MAC Spoofing, el cual funciona como un hombre en el medio, entre una puerta de enlace y una máquina objetivo.

El programa funciona de la siguiente manera:se ingresa por consola la dirección IP de la máquina objetivo y la dirección IP de la puerta de enlace, el programa obtiene la dirección MAC de la máquina a atacar tanto como la de la puerta de enlace mediante solicitudes ARP. Luego se toma la dirección MAC de la máquina atacante y se envía a la puerta de enlace muchos mensajes ARP para que actualiza su tabla ARP - IP con la dirección MAC del atacante para que la asocie con la ip de la máquina objetivo. Al mismo tiempo también se envían mensajes a la máquina objetivo con la MAC del atacante, para que este también haga la relación. Este proceso, se repite varias veces para mantener “actualizada” la IP en relación a la MAC falsa en ambos casos y que todo el tráfico pase por la maquina del atacante.

IV. Conclusiones

- La capa de enlace es vulnerable a ataques, que se debe por tener acceso en gran parte a la red interna.
- En la capa de enlace es sencillo falsificar las direcciones MAC y utilizar el protocolo ARP para conseguirlo.
- Realizar una inundación en la capa de enlace ralentiza o inhibe por completo la comunicación de una red interna.

References

[1] Neo.lcc.uma.es. 2020. *Protocolo ARP*. [online] Available at: <http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/arp.html> [Accessed 22 April 2020]..

[2] Es.wikipedia.org. 2020. *Host*. [online] Available at: <https://es.wikipedia.org/wiki/Host> [Accessed 22 April 2020].

[3] G. S. Medero, “El ciberespionaje”, Derecom, num. 13 (mar-may), p. 9,2013.

[4] Itesa.edu.mx. 2020. 5.3.1.2 Tabla De Direcciones MAC Del Switch. [online] Available at: <https://www.itesa.edu.mx/netacad/introduccion/course/module5/5.3.1.2/5.3.1.2.html> [Accessed 22 April 2020].

[5] Speedcheck.org. 2020. ¿Qué Es FTP?. [online] Available at: <https://www.speedcheck.org/es/wiki/ftp/> [Accessed 22 April 2020].

[6] Latam.kaspersky.com. 2020. Ingeniería Social: Definición. [online] Available at: <https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering> [Accessed 22 April 2020].

[7] En.wikipedia.org. 2020. MAC Flooding. [online] Available at: <https://en.wikipedia.org/wiki/MAC_flooding> [Accessed 22 April 2020].

[8] Es.wikipedia.org. 2020. MAC Spoofing. [online] Available at: <https://es.wikipedia.org/wiki/MAC_spoofing> [Accessed 22 April 2020].