Desarrollo de sistema de software detector de ataques de ARP Spoofing

Christian Leonardo Muñoz Cardenas – 20141020111

Redes de comunicaciones II.

Universidad Distrital Francisco José de Caldas

Bogotá

2020

INTRODUCCIÓN

En la actualidad, el fenómeno de la globalización ha inundado el mundo con ingreso a internet, tanto que el 51% de la población mundial cuenta con acceso a internet (ABC, 2019), la mayoría de estas se conectan vía Wifi, un método inalámbrico de conexión a Internet que, aunque muy práctico, resulta más inseguro que una conexión física, ya que le da la oportunidad a presuntos atacantes en la misma red Wifi de realizar ataques de hombre en el medio (MITM).

Uno de los ataques preferidos, por su versatilidad y simplicidad, son los ataques de personificación por medio del protocolo de red ARP, el cual permite que los equipos sepan que dispositivos hay en la red y ligar su dirección física (MAC) con la dirección IP asignada por el enrutador. Los atacantes pueden enviar paquetes ARP maliciosos para personificar al enrutador y hacer de intermediario entre la comunicación del equipo víctima y el enrutador (Imperva, 2016).

CONTEXTUALIZACIÓN

El protocolo de red objetivo en este trabajo escrito es el protocolo de resolución de direcciones (ARP, por sus siglas en ingles), este es un protocolo perteneciente a la capa de enlace del modelo OSI, cuya función tiene resolver cada IP asignada en la red, enlazandola con la dirección física MAC del dispositivo, permitiendo a una red manejar los distintos dispositivos conectados a la red independientemente (LifeWire, 2019), este protocolo no fue pensado para la seguridad, por lo que no realiza ninguna verificación en caso de algún agente malicioso presente en la red (Imperva, 2016).

Para que exista una comunicación entre dos dispositivos de una red, antes debe haber un mapeo de la dirección física a la dirección IP entre ambos, esta relación MAC-IP estaría guardada en la memoria caché en cada dispositivo, de no existir información acerca del dispositivo a comunicarse, el dispositivo debe realizar una petición ARP broadcast para realizar un mapeo de cada dispositivo que responda a la petición con una respuesta ARP, la cual contendrá las direcciones IP y MAC del dispositivo que responde (LifeWire, 2019).

El poco análisis que se hace a un posible envenenamiento intencionado a esta memoria caché es lo que le hace la vida tan fácil a los atacantes informáticos, ya que solo se requiere de un poco de discreción para realizar el ataque ARP con dirección a cualquier maquina pasando totalmente desapercibido.

Los ataques de este tipo funcionan así (Veracode, 2020), el atacante debe enviar al equipo víctima paquetes ARP maliciosos, donde enviará la dirección MAC de equipo de salida de la red (generalmente, el enrutador) en vez de la suya, haciendo que el equipo enlace la dirección IP del atacante como la dirección IP del enrutador, por lo que todo su tráfico en la red lo enviará a la maquina del atacante, permitiendole ver, alterar o destruir dicho tráfico, teniendo control total del acceso de la máquina a internet, lo que permite al atacante escalar fácilmente a ataques de robo de sesión, denegación de servicios, phishing y otros ataques MITM.

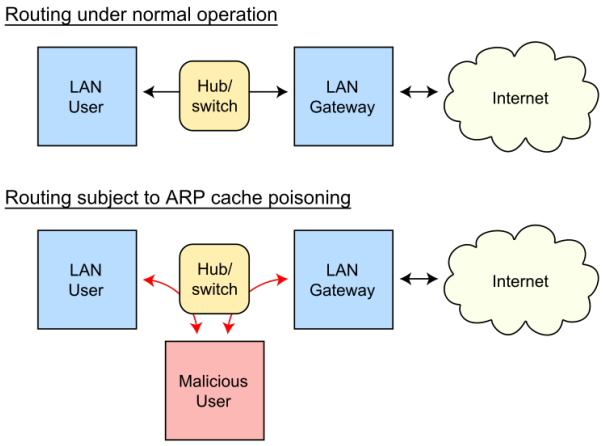

Figura 1: Ilustración comparativa de cómo funciona una conexión a internet ininterrumpida (arriba) y cómo altera a este las acciones de un usuario malicioso (abajo)[1].

Estos ataques son muy fáciles de detectar, un software detector de ataques de ARP spoofing deben filtrar los paquetes ARP que reciba el equipo y si detecta que el equipo que envió el paquete tiene una

1 https://en.wikipedia.org/wiki/ARP_spoofing#/media/File:ARP_Spoofing.svg

dirección MAC distinta a la que dice tener en el paquete ARP, será identificado como un usuario malicioso. Esto también puede verse en la caché, si en la caché ARP existen dos equipos con la misma dirección MAC, se sabrá con certeza que alguno de estos es un atacante.

DISEÑO

Para este problema, se desarrolló un sistema de software capaz de filtrar los paquetes ARP que el equipo donde se este corriendo reciba, procesará cada uno de estos paquetes y, en caso de detectar un paquete malicioso, la aplicación alertará al usuario por medio de una ventana emergente con información acerca del ataque informático, además de esto, la aplicación permitirá el escaneo broadcast de la subred especificada por el usuario y mostrará el resultado de este escaneo en una tabla, junto con una columna que indique si se repite o no su dirección MAC, siendo indicativo de atacante o de equipo personificado.

La aplicación se realizó con Python v3.6.8, con ayuda de la librería Scapy, una herramienta de manipulación de paquetes para redes de computadores, esta contiene funciones para filtrar tráfico de protocolos especificados y diseñar y enviar paquetes por internet (PyPI, 2019).

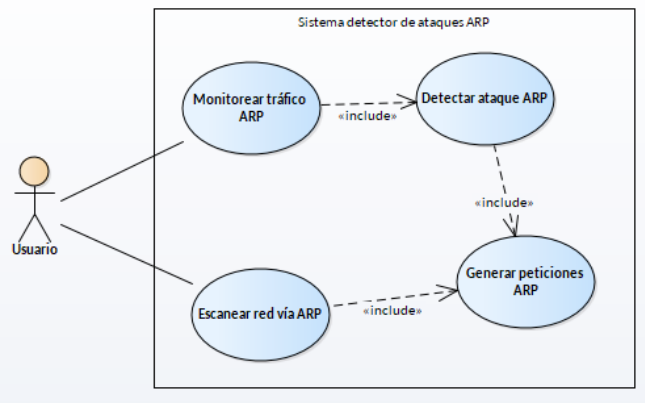

Figura 2: Diagrama de casos de uso de sistema de software detector de ataques ARP.

Debido a que se espera que el sistema pueda realizar distintas tareas independientes al mismo tiempo, se debe diseñar un sistema de software multihilo, para impulsar el uso de este tipo de aplicacioes por personas sin conocimiento en redes y computación se diseño una interfaz gráfica sencilla e intuitiva.

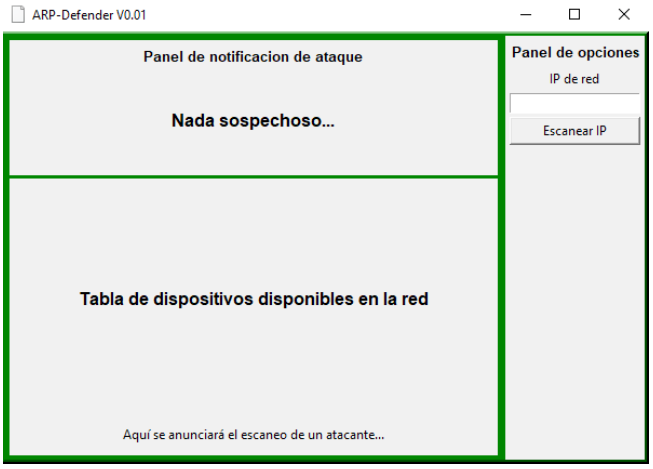

Figura 3: Interfaz gráfica de usuario del sistem de sofotware detector de ataques ARP

El fondo de la interfaz, el cual es de color verde y separa los paneles de la ventana, es el indicador gráfico del estado del tráfico ARP que llega al equipo, cuando se encuentra verde significa que no hay nada sospechoso en el tráfico recibido, en caso contrario, este cambiará a color rojo, indicando tráfico malicioso recibido.

RESULTADOS

Al escanear la red por medio de pings ARP, utilizando la librería Scapy para crear y enviar peticiones broadcast ARP a la red, se obtiene un escaneo impreciso, ya que se deben realizar varios escaneos para obtener la lista completa de los equipos, y estos a veces se pierden de la lista en los escaneos posteriores, por lo que se debe seguir la investigación para realizar escaneos ARP por medio de librerías o utilizando la misma consola de comandos del equipo, el cual realiza un escaneo bastante preciso con el comando "arp -a".

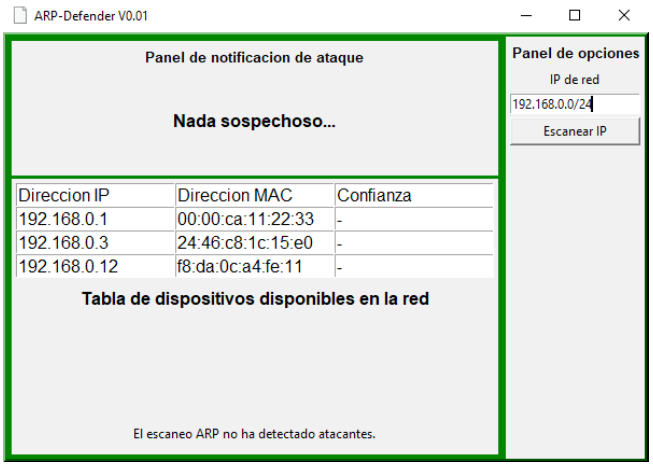

Figura 4: Resultado de escaneo ARP por medio de la aplicación.

A diferencia de este, la funcionalidad de detección de ataques ARP en tiempo real es satisfecha en el desarrollo de la aplicación, ya que puede detectar un ataque de ARP Spoofing segundos después de haberse ejecutado, avisando por medio de una ventana emergente y el cambio de color de fondo en la aplicación.

Para probar esto, se simuló un ataque de ARP Spoofing al equipo donde se está ejecutando la aplicación con ayuda de la herramienta ARPSpoof, una herramienta nativa del sistema operativo Kali Linux 2020.1

```
kali@kali:~$ sudo arpspoof -i eth0 -r 192.168.0.1 -t 192.168.0.6
0:c:29:e7:96:1d 0:c0:ca:98:37:df 0806 42: arp reply 192.168.0.1 is-at 0:c:29:e7:96:1d
0:c:29:e7:96:1d 0:0:ca:11:22:33 0806 42: arp reply 192.168.0.6 is-at 0:c:29:e7:96:1d
0:c:29:e7:96:1d 0:c0:ca:98:37:df 0806 42: arp reply 192.168.0.1 is-at 0:c:29:e7:96:1d
0:c:29:e7:96:1d 0:0:ca:11:22:33 0806 42: arp reply 192.168.0.6 is-at 0:c:29:e7:96:1d
```

Figura 5: Ataque de ARP Spoofing, intentando personificar el enrutador (dirección IP 192.168.0.1) para la maquina víctima (192.168.0.6).

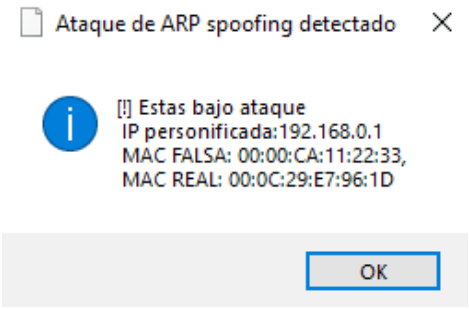

Figura 6: Ventana emergente que anuncia el ataque ARP

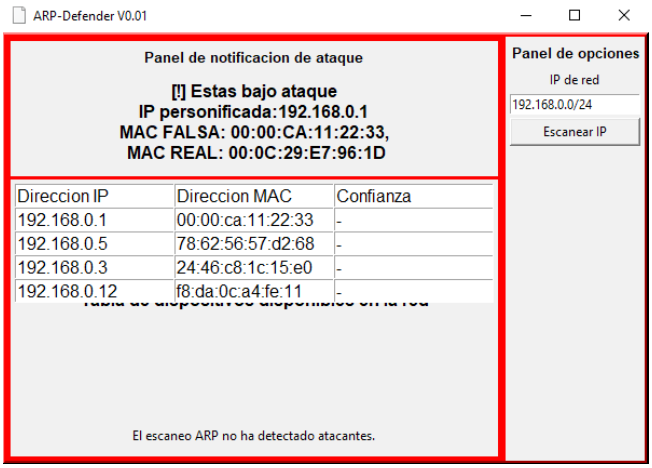

Figura 7: Interfaz gráfica de usuario de aplicación, al detectar un ataque ARP.

La aplicación mantiene el anuncio de ataque unos segundos más antes de que confirme que el ataque ha finalizado.

CONCLUSIONES

Del trabajo investigativo, se puede deducir que el poco conocimiento general acerca del tema de la computación y las redes de comunicaciones lleva a la gente a ignorar este tipo de ataques informáticos, siendo víctimas potenciales de ataques tan fácilmente ejecutables y detectables como los ataques de ARP Spoofing.

Del desarrollo de la aplicación de software se puede concluir que la programación de herramientas de redes es un trabajo complejo, donde se debe tener en cuenta la información accesible de un equipo a los demás equipos de la red y cómo este se comunica con los demás equipos de la red.

Para trabajos futuros, se puede continuar la investigación de escaneos broadcast, implementando otros tipos de escaneos de red que sean más precisos y puedan dar más información acerca de los equipos encontrados, además de diseñar una medida de protección (contra-ataque) que el usuario pueda ejecutar contra el atacante detectado.

REFERENCIAS

1. https://en.wikipedia.org/wiki/ARP_spoofing
2. https://www.lifewire.com/address-resolution-protocol-817941
3. https://www.veracode.com/security/arp-spoofing
4. https://www.imperva.com/learn/application-security/arp-spoofing/
5. https://en.wikipedia.org/wiki/Address_Resolution_Protocol
6. https://pypi.org/project/scapy/
7. https://www.thepythoncode.com/article/detecting-arp-spoof-attacks-using-scapy
8. https://www.shellvoide.com/python/how-to-build-an-arp-scanner-python-using-scapy/
9. https://www.tutorialspoint.com/python_penetration_testing/python_penetration_testing_arp_spoofing.htm
10. https://www.w3schools.in/python-tutorial/network-programming/