Exploración Scapy

S. Rodríguez Camargo sarodriguezca@unal.edu.co

***Resumen*— Scapy es una herramienta de creación y manipulación de paquetes de red basada en Python. Esta herramienta tiene gran potencial y múltiples utilidades. La idea de este trabajo es crear un notebook en Python que explore algunas de esas utilidades, que cubra las capacidades básicas de captura y manipulación de paquetes, así como una aplicación concreta de un ataque de Man in the Middle usando envenenamiento de paquetes ARP.**

***Abstract*-- Scapy is a Python-based tool for creating and manipulating network packets. This tool has great potential and multiple utilities. The idea of this work is to create a Python notebook that explores some of these utilities, covering the basic capabilities of packet capture and manipulation, as well as a concrete application of a Man in the Middle attack using ARP packet poisoning., how it was done, principal results, and their significance.**

I. Introducción

Como parte del trabajo de clase de la materia de Ciberseguridad, dentro del capítulo ataques cibernéticos, realizamos un taller para entender los conceptos de *sniffing* y *spoofing*, usando Scapy para capturar y enviar paquetes. Como proyecto final decidí profundizar un poco sobre esta herramienta y organizar un notebook de Python a manera de guía que permita explorar sus utilidades y que quizá incluso puede servir como complemento del taller de sniffing de la clase en versiones futuras.

Para cerrar el notebook se implementó una aplicación de Scapy que recrea un ataque de Man in the Middle utilizando spoofing para envenenar paquetes ARP y suplantar dispositivos en una red. Dicha aplicación ilustra lo fácil que es robar información, intervenir el tráfico de red y las capacidades a las que puede llegar un software como Scapy.

II. MARCO TEÓRICO

A. Sniffing

El sniffing de paquetes es la captura de los paquetes que viajan por una red para su estudio, ya sea con motivos, educativos, de monitoreo o maliciosos para robar información o conocer lo que viaja en la red de un tercero. Existen múltiples programas capaces de hacer esta captura y son denominados sniffers, ejemplos de ellos son WireShark y SmartSniff.[1]

Como se dijo, el sniffing de paquetes se usa con fines tanto positivos, como negativos, y su impacto depende de la intención de la persona que hace la captura. Dentro de los usos positivos que pueden atribuirse a este tipo de rastreo están la identificación de problemas de una red, como la congestión, la pérdida de paquetes y errores de configuración, también puede ser usado para identificar posibles brechas de seguridad o ataques a la red, posibles errores de configuración u organización e incluso en materia más académica, el estudio de los protocolos y su estructura con aras de entenderlos y optimizarlos. [1]

Sin embargo, así como hay usos positivos de este tipo de herramientas, el sniffing de paquetes es ampliamente utilizado para fines maliciosos como violar la privacidad de usuarios al interceptar información de cómo navegan estos, y peor aun exponiendo información sensible. Existen múltiples formas en las que los atacantes pueden explotar este tipo de vulnerabilidad para ganar beneficios y robar información de los usuarios, afortunadamente la encriptación de los paquetes que viajan en la red es una medida de protección efectiva, puesto que a pesar de que un atacante logre capturar el tráfico de red de un usuario, si la información que este contiene está encriptada, le será imposible al atacante saber a ciencia cierta qué información contienen los paquetes. De esta forma puede protegerse a los usuarios de los ataques de sniffing. [2]

B. Spoofing

Spoofing hace referencia a la acción de crear paquetes y enviarlos por la red, pero específicamente cuando estos paquetes han sido modificados para cambiar su dirección de origen modificada, para ocultar el verdadero origen. En materia de ciberseguridad el spoofing se usa para realizar ataques de diferente tipo, como DDoS que no pueden ser rastreados pues las direcciones de origen no son reales, o la suplantación de dispositivos específicos dentro de una red. [3]

Diferentes softwares permiten la creación y envío de paquetes personalizados a los que se les pueden modificar múltiples parámetros (incluyendo las direcciones de envío y origen, puertos, protocolos etc.), abriendo un mundo de posibilidades tanto positivas (como el testeo de servicios) como negativas.

Una de las estrategias más usadas para protegerse del spoofing es el filtrado de paquetes, que consiste en verificar la información interna de los paquetes para tratar de identificar irregularidades o amenazas y bloquear por completo la recepción de paquetes modificados o dañinos. [3]

C. Scapy

Scapy es una librería escrita en Python usada para la manipulación de paquetes de red. Dentro de sus funcionalidades se enumeran la creación y codificación de

* Revista Argentina de Trabajos Estudiantiles. Patrocinada por la IEEE.

paquete de múltiples protocolos, la capacidad de enviar dichos paquetes a través de la red, la captura de tráfico entre otras aplicaciones dentro del campo de los paquetes de red. En conjunto, Scapy es una herramienta muy útil para el escaneo, estudio, seguimiento y ataque de redes de computadores. [4]

Scapy destaca de otros programas similares en que aporta mayor libertad a la hora de crear paquetes, que se ajustan más a los deseos del usuario y no están limitados por las capacidades del software o sus reglas. Aun cuando dichos paquetes no cumplan estándares o la lógica de los protocolos, Scapy puede crearlos. Scapy también agrupa os mensajes de peticiones y respuestas para que sean más fácil de interpretar. El uso de Python permite la facilidad del manejo de la aplicación, al igual que elimina la necesidad de aprender nuevos lenguajes específicos, saltándose también el uso de templates o métodos predeterminados. Al contrario, Scapy construye los paquetes por capas y permite al usuario apilar las capas de la manera que desee, cambiando los atributos que desee. [5]

Finalmente, Scapy retorna y decodifica toda la información de los paquetes al usuario y no interpreta los que encuentra. Otros programas similares pretenden simplificar o ayudar a el entendimiento de los paquetes interpretando los resultados y dando juicios sobre la información encontrada. Aunque esto puede ser útil en muchos casos, Scapy se aleja de esa funcionalidad pues la interpretación debe ser llevada a cabo por la persona que estudia los paquetes y no generada de forma automática por el programa; no es raro que se pierda información valiosa o incluso se comentan errores en la interpretación automática, en especial al disponer de un único punto de vista para estudiar los resultados. Scapy no quiere sesgar o imponer análisis, por lo que deja ese paso al usuario. [5]

D. Man in the Middle

El ataque de Man in the Middle ocurre cuando un atacante se sitúa en medio de la comunicación de dos partes e intercepta el paso de información entre ellos, manteniendo la conexión para evitar ser detectado. En concreto el atacante suplanta la identidad de una página, un servidor o dispositivo y recibe los paquetes enviados al receptor original, para después redirigirlos al destino original. [6]

El principal objetivo de este ataque es robar información sensible del tránsito de información, sin ser descubierto (robo de contraseña, credenciales, información de tarjetas etc.)

Existen múltiples métodos en los que se puede lograr, pero la suplantación se da usualmente a nivel de IP, DNS u ARP, engañando a las víctimas que creen estar navegando de manera segura, conectados a portales y servidores legítimos, pero que en realidad han sido sustituidos. [6]

Tal como en el caso del sniffing convencional, la información puede ser protegida gracias a la encriptación, pues a pesar de que el atacante se encuentre en medio y pueda ver toda la comunicación entre dos víctimas, si los datos están encriptados, no entenderá realmente qué se está transportando por la red y el ataque será en vano. Desafortunadamente los atacantes tienen métodos para sobrepasar la encriptación y descifrar los mensajes enviados, principalmente manipulado y explotando vulnerabilidades SSL y HTTPS para degradar las conexiones a HTTP y hacer pasar una conexión insegura por una segura.

Es por eso que es muy importante saber cómo prevenir este tipo de ataques, evitando conectarse a redes no seguras, públicas, que no están protegidas por contraseñas, asegurarse que los sitios que se visitan son seguros, legítimos y están protegidos con encriptación, limitar el paso de información sensible y operaciones delicadas en redes que no sean 100% confiables. [7]

E. Envenenamiento ARP

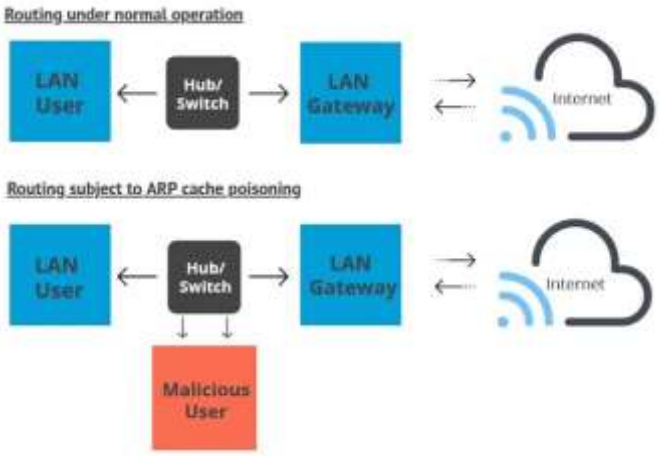
Dentro de las múltiples modalidades de ataques Man in the Middle se encuentra una llamada envenenamiento ARP o ARP spoofing.

El protocolo ARP (Address Resolution Protocol), en términos simples es el encargado de conectar las direcciones IP de una red (que son dinámicas) con las direcciones MAC de sus correspondientes dispositivos (que son fijas). Entonces el protocolo se encarga de mantener un registro que indica qué dirección IP corresponde actualmente a cada dirección MAC en una red. Este registro se llena preguntando: un dispositivo envía una petición sobre una dirección IP que no tiene asignada una dirección MAC a todos los dispositivos de la red, esperando que el dispositivo correcto con la IP dada responda con su dirección MAC para así completar el registro ARP. [8]

El protocolo ARP tiene algunos problemas de seguridad, principalmente el hecho de que no cuenta con un sistema de validación delas peticiones y respuestas ARP; en otras palabras, cualquier dispositivo dentro de la red puede responder un mensaje ARP aun cuando el mensaje original no fuera dirigido a él. [9]

Esta vulnerabilidad es explotada para “envenenar” los registros ARP y permitir la suplantación de direcciones y situarse en medio del tráfico de dos dispositivos en una red para llevar a cabo un ataque de Man in the Middle.

En primera instancia el atacante debe tener acceso a la red y conocer las direcciones IP de las víctimas, a manera de ejemplo un usuario y el Gateway de dicha red. Luego se usan técnicas de spoofing para crear un paquete ARP que responda las peticiones de identificación y así hacer cree a las víctimas que la dirección IP con la que se están comunicando corresponde a la dirección MAC del atacante. Los dispositivos actualizarán sus registros ARP con la información falsa y al intentar comunicarse entre sí, realmente estarán enviando todos los mensajes al atacante primero, que se encargará de redirigir los paquetes a sus destinos correctos después de haberlos capturado, para así mantener el funcionamiento de la red y no alertar del ataque a las víctimas. [9]



Envenenamiento ARP [9]

III. NOTEBOOK

Como entregable del proyecto de ciberseguridad se incluye un notebook de Jupyter en Python que explora varias de las posibles funcionalidades de Scapy a nivel tanto de sniffing como spoofing. El notebook incluye instrucciones para realizar la captura, construcción y envío de diferentes tipos de paquetes, el modificado de sus capas y atributos, así como capturas de los resultados vistos a través de un sniffer gráfico como WireShark. Adicionalmente, al final de notebook se incluye un ejemplo de programa para realizar un ataque de Man in the Middle basado en envenenamiento ARP como se ha descrito en la sección anterior.

El notebook puede ejecutarse casi en su totalidad en un ambiente de nube como Google Colab, pero se recomienda ejecutarlo localmente en VS Code o similares, para así poder hacer uso completo de la herramienta y poder capturar el tráfico fácilmente con otras herramientas como WireShark.

El notebook se encuentra en el siguiente repositorio: https://github.com/sarodriguezcam/Cibersecurity2024.git

IV. CONCLUSIONES

Scapy es una librería de manipulación de paquetes altamente adaptable que permite trabajar sobre las diferentes capas de los paquetes de red y manipularlos a conveniencia con relativa facilidad.

Las herramientas de sniffing y spoofing tienen múltiples aplicaciones tanto positivas, para hacer diagnósticos y estudiar las características de la red, como negativas, principalmente como parte de ciberataques que buscan robar información de víctimas.

Una de las manifestaciones de ataques relacionados a sniffing y spoofing es el ataque de Man in the Middle, que se basa en suplantar la identidad de un componente de la red para recibir tráfico con un destino diferente y poder robar la información. Una de las aplicaciones de este tipo de ataque se logra con el envenenamiento ARP, que se basa en ligar incorrectamente direcciones IP y MAC para suplantar dispositivos de red y endpoints y situarse en el medio de la transmisión de información sin ser detectados.

REFERENCIAS

[1] "What is packet sniffing ?," GeeksforGeeks, https://www.geeksforgeeks.org/what-is-packet-sniffing/ (accessed May 30, 2024).
[2] E. Farrier, "¿Qué es el sniffing de paquetes? Definición, tipos y protección," ¿Qué es el sniffing de Paquetes? Definición, Tipos y Protección, https://www.avast.com/es-es/c-packet-sniffing (accessed May 30, 2024).
[3] Kaspersky, "IP spoofing: How it works and how to prevent it," www.kaspersky.com, https://www.kaspersky.com/resource-center/threats/ip-spoofing (accessed May 30, 2024).
[4] Scapy, https://scapy.net/ (accessed May 30, 2024).
[5] P. Biondi, "Introduction," Introduction - Scapy 2.6.0 documentation, https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy (accessed May 30, 2024).
[6] K. Yasar and M. Cobb, "What is a man-in-the-Middle Attack (MITM)? - definition from Iotagenda," IoT Agenda, https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM (accessed May 30, 2024).
[7] "What is MITM (man in the middle) attack: Imperva," Learning Center, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (accessed May 30, 2024).
[8] "What is address resolution protocol (ARP)?," Fortinet, https://www.fortinet.com/resources/cyberglossary/what-is-arp (accessed May 30, 2024).
[9] N. Pubudu, "Understanding arp poisoning & MITM attack," Medium, https://medium.com/geekculture/understanding-arp-poisoning-mitm-attack-7b12a3b061bd (accessed May 30, 2024).