Instituto Politécnico Nacional

Escuela Superior De Cómputo

Ingeniería En Sistemas Computacionales

Redes de computadoras

Profesor: Puebla Lomas Jaime Hugo

Alumno:

Olguín Martínez José Arturo

Proyecto

Analizador de protocolos de red con Scapy

Índice

[Estado del arte 3](#_Toc187147540)

[Detection and Prevention of Poisoning Targets with ARP Cache using Scapy 3](#_Toc187147541)

[SentinelScan: Advanced Network Scanner and Packet Detection Suite 4](#_Toc187147542)

[Visualization of DDoS Attack using Python Libraries 5](#_Toc187147543)

[Scapy Scripting to Automate Testing of Networking Middleboxes 6](#_Toc187147544)

[SCAPY- A powerful interactive packet manipulation program 7](#_Toc187147545)

[Introducción 8](#_Toc187147546)

[Scapy como librería de Python 8](#_Toc187147547)

[Características principales de Scapy 8](#_Toc187147548)

[Objetivo 9](#_Toc187147549)

[Desarrollo 10](#_Toc187147550)

[Requisitos para Scapy 10](#_Toc187147551)

# Estado del arte

## Detection and Prevention of Poisoning Targets with ARP Cache using Scapy

Debido a sus vulnerabilidades, ARP se convierte en un objetivo para atacantes que buscan ejecutar falsificación o envenenamiento de ARP, lo cual permite manipular la caché ARP de los dispositivos en red, generando problemas de integridad y confidencialidad de datos.

La amenaza principal son los ataques de envenenamiento ARP explotan la falta de autenticación en el protocolo, permitiendo a un atacante interceptar, modificar, o redirigir tráfico de red mediante paquetes ARP falsificados. Estos ataques pueden llevar a consecuencias serias, como ataques de hombre en el medio (MITM) y denegación de servicio (DoS), que afectan a dispositivos específicos o a toda la red.

Propuesta de solución planteada

1. Simulación del Ataque: Utilizando la biblioteca de Python Scapy, se elabora un "spoofer" de ARP que fabrica y envía paquetes ARP falsificados, simulando ataques de envenenamiento a la caché ARP.
2. Algoritmo de Detección de Ataques ARP: Un sistema implementado en Python y Scapy que monitorea constantemente los paquetes ARP, verificando discrepancias en las direcciones MAC y los patrones de tráfico anómalos. Este proceso clasifica diferentes tipos de ataque, incluyendo DoS y MITM.
3. Medidas Preventivas: Además del sistema de detección, se incluye una estrategia de protección preventiva mediante la incorporación de entradas ARP estáticas en los dispositivos de red para mitigar la posibilidad de envenenamiento.

## SentinelScan: Advanced Network Scanner and Packet Detection Suite

La ciberseguridad de redes destaca la importancia de herramientas avanzadas de detección y defensa proactiva, como SentinelScan, en la protección contra una creciente gama de amenazas cibernéticas. La integración de técnicas como olfateo de paquetes (packet sniffing) y manipulación de paquetes se ha vuelto crucial para la detección temprana de vulnerabilidades y el bloqueo de ataques.

SentinelScan, se basan en frameworks y bibliotecas que permiten el análisis y manipulación de tráfico en capas profundas de la red. La biblioteca Scapy, se ha consolidado como una opción robusta para el manejo de paquetes en Python, permitiendo la creación, el envío y la captura de paquetes personalizados para analizar patrones de tráfico. Este enfoque se combina con técnicas de criptografía y autenticación de red para asegurar la integridad y autenticidad de los datos.

SentinelScan también se construye sobre protocolos fundamentales, abordando desde los niveles de transporte, con TCP y UDP que permiten la transmisión fiable de datos, hasta los protocolos de aplicación, como los protocolos de correo y web, que exigen una mayor precisión en la detección de amenazas.

SentinelScan, se propone un modelo de múltiples capas que abarca diferentes protocolos y verifica de forma continua la legitimidad de los patrones de tráfico en la red. Los algoritmos criptográficos y mecanismos de autenticación integrados facilitan el manejo seguro de datos sensibles y la verificación de identidad, asegurando que cada conexión sea autenticada y confiable.

## Visualization of DDoS Attack using Python Libraries

El crecimiento de los servicios en línea ha expuesto a las organizaciones a mayores riesgos de ataques de Denegación de Servicio Distribuido (DDoS), los cuales pueden saturar la infraestructura de red, provocando la interrupción de servicios, pérdidas económicas y daño reputacional.

Los ataques DDoS han evolucionado tanto en volumen como en complejidad, usando múltiples métodos de inundación como ACK, SYN, PUSH y RESET para maximizar el tráfico de red y obstruir las defensas tradicionales, como cortafuegos y sistemas de detección de intrusiones.

Se han implementado técnicas de análisis y visualización utilizando Python y bibliotecas como Scapy, que permite la captura y manipulación de paquetes. Además, el uso de Wireshark para recopilar archivos “pcap” permite analizar patrones de tráfico en busca de actividad anómala. Estas herramientas, junto con la visualización de datos en HTML y gráficos personalizados, permiten al usuario monitorear múltiples parámetros de tráfico en tiempo real, logrando una visión integral del comportamiento de la red.

La metodología de este enfoque se centra en la detección visual de patrones irregulares, como picos repentinos en el tráfico o el uso anómalo de determinados protocolos, que son indicativos de un ataque en curso.

La capacidad de predecir y visualizar ataques DDoS mejora la seguridad, permitiendo a las organizaciones adaptar sus estrategias de defensa en tiempo real. Al ofrecer una visualización clara y accesible, los analistas pueden tomar decisiones informadas, lo que reduce la dependencia de sistemas automatizados propensos a errores y facilita una respuesta rápida y eficiente.

Este enfoque contribuye significativamente a la ciberseguridad al ofrecer una herramienta visual en tiempo real, basada en Python y Scapy, que permite identificar patrones sospechosos en el tráfico de red.

## Scapy Scripting to Automate Testing of Networking Middleboxes

La adopción de middleboxes como los balanceadores de carga en las corporaciones responde a la necesidad de gestionar y respaldar sus infraestructuras. Estos dispositivos procesan diariamente grandes volúmenes de ancho de banda, abarcando desde protocolos de red hasta protocolos de capa de aplicación. Sin embargo, este tráfico puede incluir datos dañinos o maliciosos, lo cual podría llevar a que estos dispositivos fallen o se vuelvan vulnerables a explotaciones

Para abordar la seguridad y la fiabilidad de estos dispositivos, se utiliza Scapy, una herramienta poderosa e interactiva de manipulación de paquetes desarrollada como un módulo en Python. Python, por su versatilidad como lenguaje de scripting, facilita el uso de Scapy en múltiples aplicaciones. En este caso, se estudia el funcionamiento de Citrix NetScaler ADC mediante la creación de un modelo cliente-servidor para protocolos como FTP, HTTPS y TFTP. Estos scripts, desarrollados con Scapy y compatibles con IPv4 e IPv6, han sido publicados como software de código abierto para facilitar su aplicación en distintas pruebas de red.

Scapy se basa en dos funciones fundamentales: enviar paquetes y recibir respuestas, lo que permite construir paquetes personalizados que abarcan detalles desde la capa de transporte TCP/UDP hasta configuraciones de bajo nivel como el tamaño de ventana o el número de acuse de recibo. Una ventaja significativa de Scapy frente a herramientas como Nmap o hping es que no se limita a paquetes conocidos, sino que permite al usuario escuchar, filtrar, modificar y redirigir paquetes en la red.

## SCAPY- A powerful interactive packet manipulation program

Scapy admite múltiples protocolos de red, desde las capas bajas (como IP y ARP) hasta protocolos de aplicación. Además, permite manipular de manera precisa las características de los paquetes, lo que es útil en diversas tareas de seguridad, como pruebas de penetración y detección de vulnerabilidades.

Scapy también es compatible con herramientas de monitoreo de red como Wireshark, permitiendo a los investigadores rastrear en tiempo real los paquetes enviados y recibidos en un entorno visual y detallado.

Entre sus puntos fuertes, Scapy destaca por su capacidad para manejar tareas complejas de redes que suelen requerir herramientas dedicadas, como filtrado avanzado, trazado de rutas y pruebas de conectividad. Sin embargo, Scapy tiene un soporte limitado para protocolos más nuevos y enfrenta restricciones de rendimiento cuando se utiliza en redes de gran escala.

# Introducción

Un sniffer de red, también conocido como analizador de paquetes, es una herramienta de software o hardware diseñada para monitorizar y capturar el tráfico de datos que circula por una red. Su función principal es permitir a los administradores y profesionales de TI observar y analizar la información que se envía y recibe a través de la red.

## Scapy como librería de Python

Scapy destaca debido a su enfoque en el control preciso de paquetes. Mientras que otras librerías como socket y requests permiten establecer conexiones y manejar protocolos a nivel de aplicación, Scapy opera en un nivel más bajo, ofreciendo capacidades de construcción y manipulación de paquetes a nivel de red.

## Características principales de Scapy

Scapy permite realizar múltiples tareas en redes, como:

1. Construcción y manipulación de paquetes: Scapy facilita la creación de paquetes personalizados, especificando cada campo de los diferentes protocolos (TCP, UDP, IP, ARP, ICMP, etc.).
2. Envió y recepción de paquetes: Scapy permite enviar y recibir paquetes directamente desde Python, lo que es ideal para realizar pruebas de conexión y análisis de red en tiempo real.
3. Sniffing de red: Con Scapy, es posible ver o escuchar el tráfico de red, filtrando y capturando paquetes específicos, lo cual es muy valioso para el análisis de tráfico en ciberseguridad y la detección de intrusiones.
4. Análisis y manipulación: Ofrece funciones para modificar y analizar los paquetes recibidos, permitiendo realizar transformaciones, reenviar tráfico, o investigar patrones específicos.

# Objetivo

El objetivo de este proyecto es crear un Sniffer implementado con Python y la librería Scapy, aplicando los conocimientos previos de programación y el conocimiento sobre los protocolos de transmisión en específico los protocolos UDP y TCP que están montados sobre IP, además de esto, el Sniffer deberá de ser capaz de poder filtrar por protocolos cambiando una ejecución en el main del programa y este podrá desplegar en terminal la información básica de la transmisión de datos y exportara los resultados en un archivo pcap que podrá ejecutarse con Wireshark para una mejor visualización.

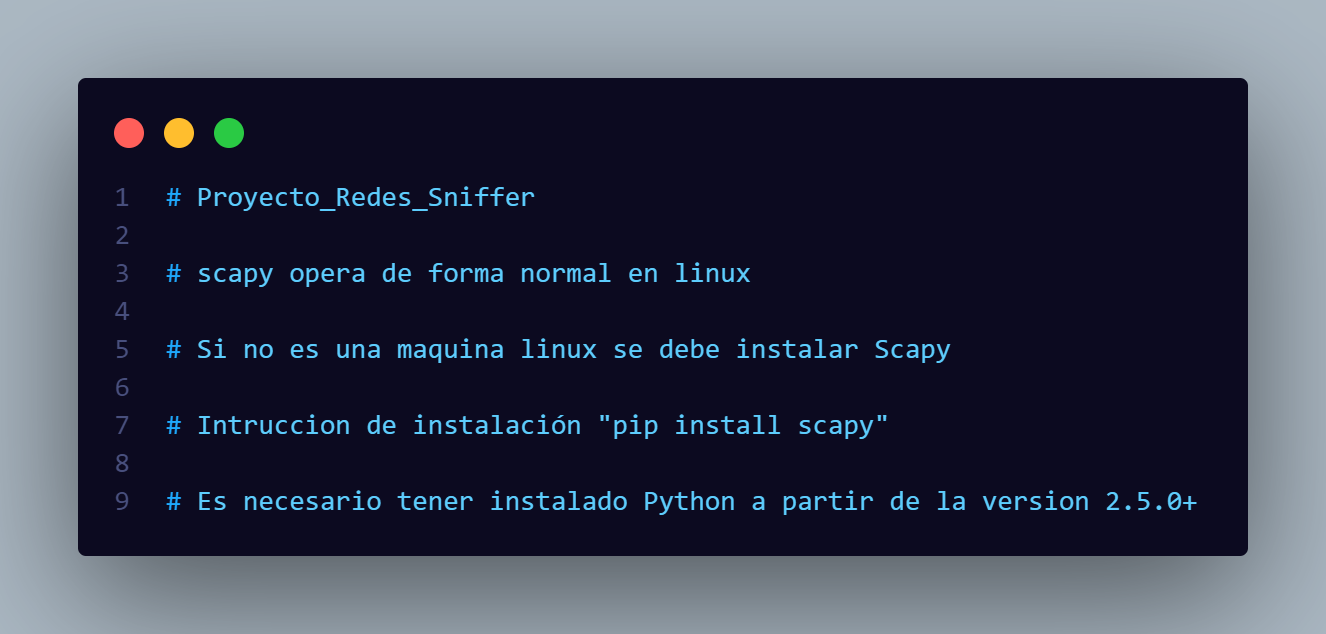
# Desarrollo

Para comenzar el proyecto se reviso la documentación de Scapy, en donde se decidió que el sistema operativo en donde se ejecutaría el Sniffer seria Kali Linux, pues en sistemas Linux Scapy viene precargado, sin embargo, para ejecutarlo en un sistema Windows se debe instalar la librería.

Texto

Descripción generada automáticamente

## Requisitos para Scapy



Importación de librerías

Texto

Descripción generada automáticamente

Como se observa de todo lo que es Scapy únicamente se utilizan 5 librerías:

Sniff: Esta librería permite capturar paquetes de en una interfaz específica.

PcaReader: Nos permite poder leer archivos con la extensión pcap, que son los mismos con los que trabaja Wireshark.

Wrpcap: Nos permite hacer la exportación de un archivo con extensión pcap, lo que lo hace ejecutable en Wireshark.

IP, TCP, UDP: Son los protocolos que se van a examinar.

## Definición de la clase Sniffer



Esta clase tendrá todas las funciones que se ejecutan para poder capturar los paquetes.

## Definiciones

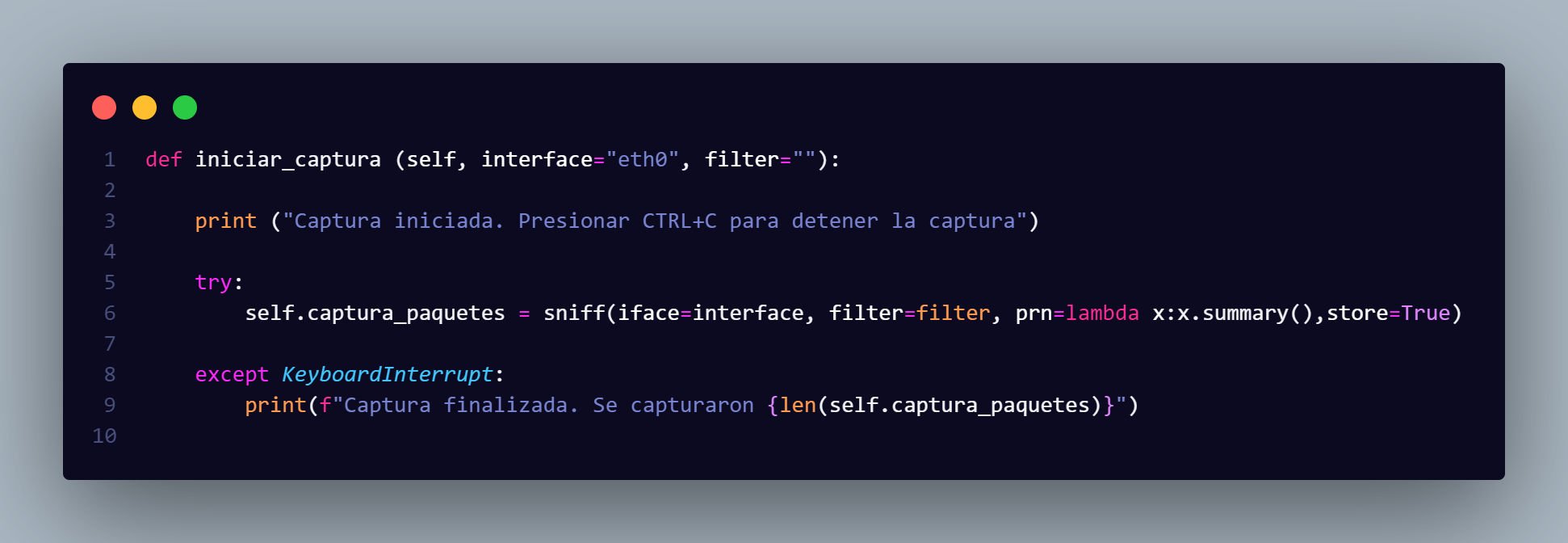
El programa inicia con la declaración de una lista vacía en donde se guardarán todos los paquetes capturados.

Texto

Descripción generada automáticamente con confianza baja

Posteriormente de inicia la captura, en donde se reciben como parámetros la lista vacía, la interfaz en donde se van a capturar los paquetes de información (Por defecto eth0) y por último el filtro (en este caso vacío porque se declara el protocolo buscado en la función main).

Además la forma de truncar el analizador y detener la captura hay que presionar la combinación Ctrl + C.



1.- Inicio de captura: El usuario solicita iniciar el sniffer a través de la UI

2.- Configuración: La UI pasa las configuraciones al núcleo del sniffer (Como filtros o puertos específicos)

3.- Captura de paquetes: El sniffer escucha en la red y captura los paquetes

4.- Procesamiento: Los paquetes capturados se envían al analizador para su decodificación

5.- Almacenamiento: Los datos procesados se guardan en la base de datos

6.- Visualización: Los resultados se muestran en la interfaz para el usuario.

Pasos del flujo

1. Inicio de captura:
   * El Usuario envía un mensaje a la UI solicitando iniciar el sniffer.
   * La UI envía una solicitud al Núcleo del sniffer para iniciar.
2. Configuración:
   * La UI envía configuraciones (filtros, puertos, etc.) al Núcleo del sniffer.
3. Captura de paquetes:
   * El Núcleo del sniffer empieza a escuchar la red y captura paquetes.
   * Por cada paquete capturado, el Núcleo envía los datos al Analizador.
4. Procesamiento:
   * El Analizador decodifica y procesa los paquetes capturados.
   * Los datos procesados se envían a la Base de datos para su almacenamiento.
5. Visualización:
   * La UI solicita los resultados procesados a la Base de datos.
   * Los datos son enviados a la UI y mostrados al Usuario.

Aplicado directamente a la librería de Scapy

Interfaz de usuario gráfica

Descripción generada automáticamente

Aquí podemos darnos cuenta de que el usuario únicamente puede ejecutar el sniffer si tiene acceso a internet. Una vez confirmado eso se filtraran solo los protocolos TCP Y UDP por lo que si no pertenecen a estos protocolos no serán guardados en la base de datos.

Bibliografía

* D. R. Thomas, P. V, W. Nancy, G. Sowmiya, A. T. P and V. Peroumal, "Detection and Prevention of Poisoning Targets with ARP Cache using Scapy," 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/IITCEE59897.2024.10467270. keywords: {Protocols;Machine learning algorithms;Network security;Maintenance engineering;Logic gates;Media Access Protocol;Reliability;ARP;MAC Address;Internet Protocols;ARP spoofing;Linux;MITM},
* T. Seshapriyan, S. M. Dinesh and J. Godwin Ponsam, "SentinelScan: Advanced Network Scanner and Packet Detection Suite," 2024 8th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2024, pp. 253-258, doi: 10.1109/ICISC62624.2024.00050. keywords: {Protocols;Documentation;Network security;User interfaces;Traffic control;Data transfer;Robustness;Network security;SentinelScan;Cyber threats;Packet manipulation;Real-time packet sniffing;Scapy;Cryptographic algorithms;Authentication mechanisms;Secure communication protocols;Security standards},
* S. T, M. G K y A. Santhosh R A, "Visualization of DDoS Attack using Python Libraries", 2024 Conferencia Internacional sobre Tendencias en Tecnologías de Computación Cuántica y Tecnologías Empresariales Emergentes, Pune, India, 2024, pp. 1-5, doi: 10.1109/TQCEBT59414.2024.10545204. palabras clave: Economía;Computación de Cuantum;Visorización de datos;Seguridad de la red;Ataque de la vida de servicio;Investigación de mercados;Bibliotes;Atapas deDDodios;Python librarys;Scapy;Intruyección,
* Moharir, M., Adyathimar, K. B., Shobha, G., & Soni, V. (2020). Scapy scripting to automate testing of networking middleboxes. *Advances in Science, Technology and Engineering Systems Journal*, *5*(2), 293-298.
* R. R. S, R. R, M. Moharir and S. G, "SCAPY- A powerful interactive packet manipulation program," 2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS), Bangalore, India, 2018, pp. 1-5, doi: 10.1109/ICNEWS.2018.8903954. keywords: {capture;packet;protocol;python;scapy;tool},