Objetivo del Proyecto

"Desarrollar una herramienta de prueba de concepto (PoC) en Python utilizando la librería Scapy para analizar las vulnerabilidades del protocolo ARP (Address Resolution Protocol). El objetivo principal es demostrar la falta de autenticación en las actualizaciones ARP y comprender cómo un atacante podría posicionarse como intermediario (Man-in-the-Middle) para interceptar o analizar el tráfico en una red local con fines de auditoría de seguridad."

Este script automatiza el proceso de envenenamiento de caché ARP entre dos nodos (víctima y gateway) para fines de estudio académico. Sus funciones principales incluyen:

- **Discovery: Identificación automática de direcciones MAC mediante solicitudes ARP Request.**
- **Poisoning: Envío de respuestas ARP no solicitadas (unsolicited ARP replies) para redirigir el tráfico.**
- **Self-Healing: Mecanismo de restauración automática de las tablas ARP de los nodos afectados al finalizar la ejecución (Ctrl+C).**