Presentación

Videos: https://drive.google.com/file/d/1wL8Yo4MO-YtF0LlQjtSm_ggGAIijUzK9/view?usp=sharing / https://drive.google.com/file/d/1Uj3FplaKj4NIEg1P8sveDUHpakH0VPkJ/view?usp=sharing

Nombre: ANGEL CORCINO SANCHEZ

Matricula: 2024-2541

Profesor: Jhonatan Rondon

Materia: Seguridad de Redes

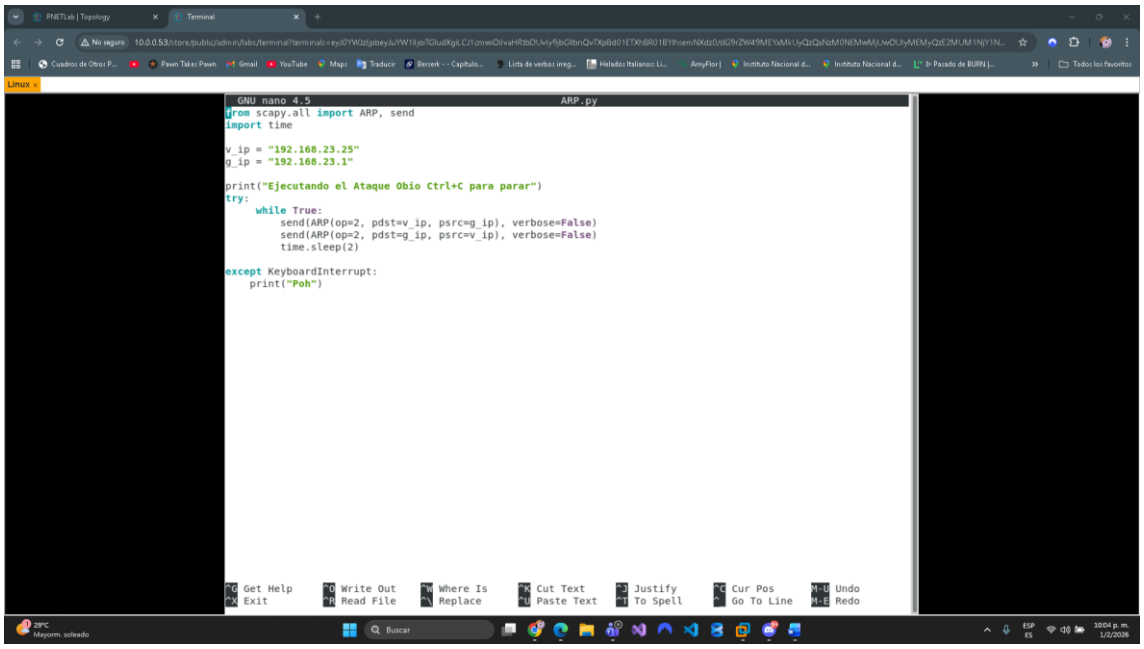
Institucion: ITLA

Reporte de la practica Num. 3

-Ataque ARP-

Realizacion del script 1 gracias a ChatGPT :)

Visualizacion del script en el entorno de Kali

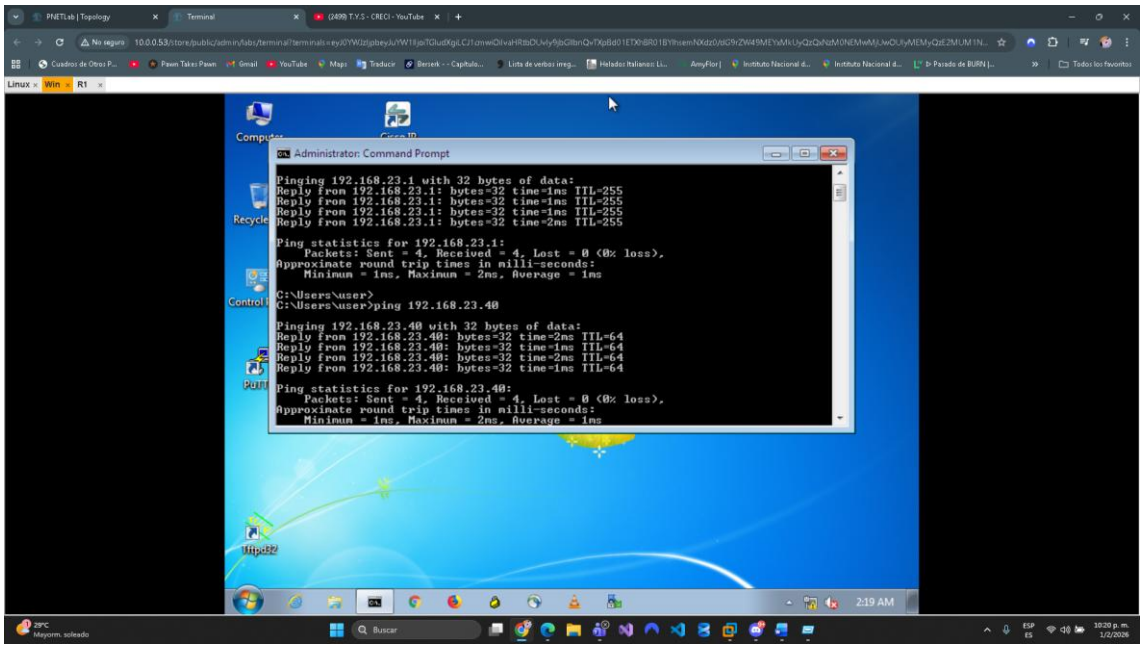


Ahora podemos visualizar en el script el cual declaramos en 2 variables las direcciones ip las cuales son v_ip: 192.168.23.25 / g_ip 192.168.23.1 el cual el primero es de la victima y el segundo es el del router, ya después se ejecuta un bucle el

cual utiliza parámetros de la librería que se llamo al principio para generar el ataque

Parte numero 2: Verificacion de la conectividad de los dispositivos

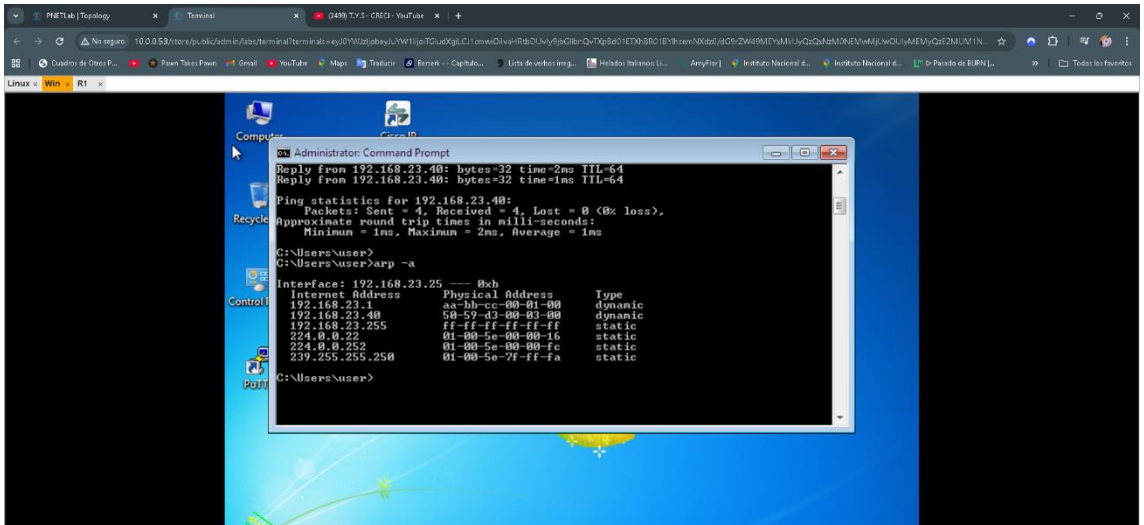
_____*Parte2.1*_____



Ahora ingresamos desde la PC de la victima y realizamos un ping el cual ira de desde el router a la pc atacante para probar la conectividad de los dispositivos finales.

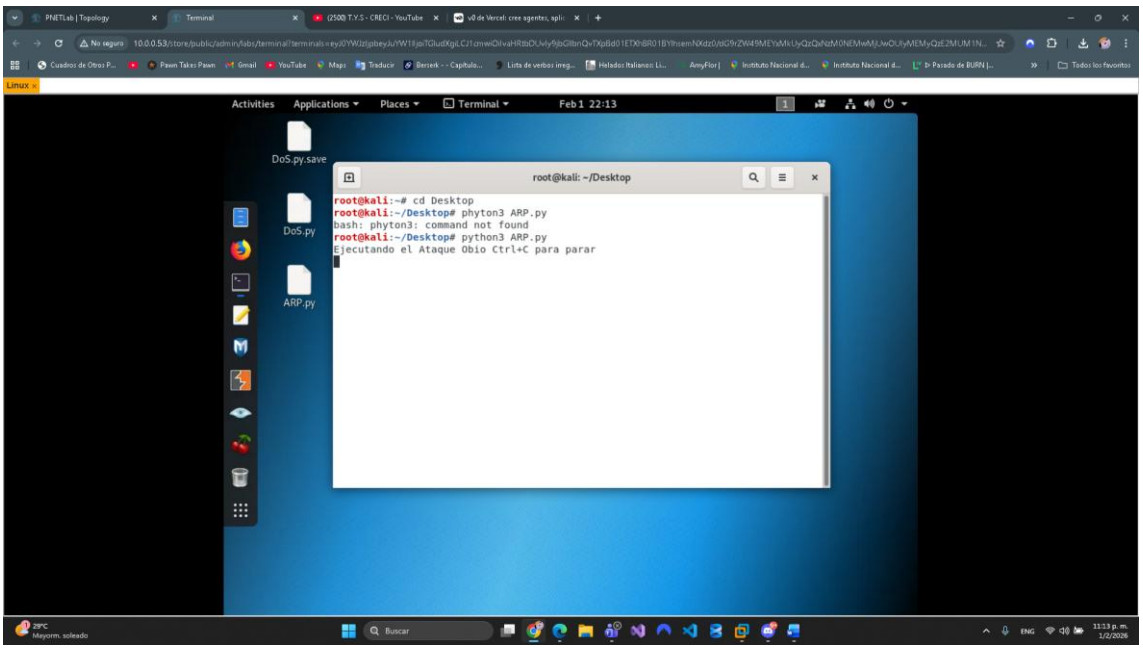
_____*Parte2.2*_____

ARP Verification: Desde la maquina victima



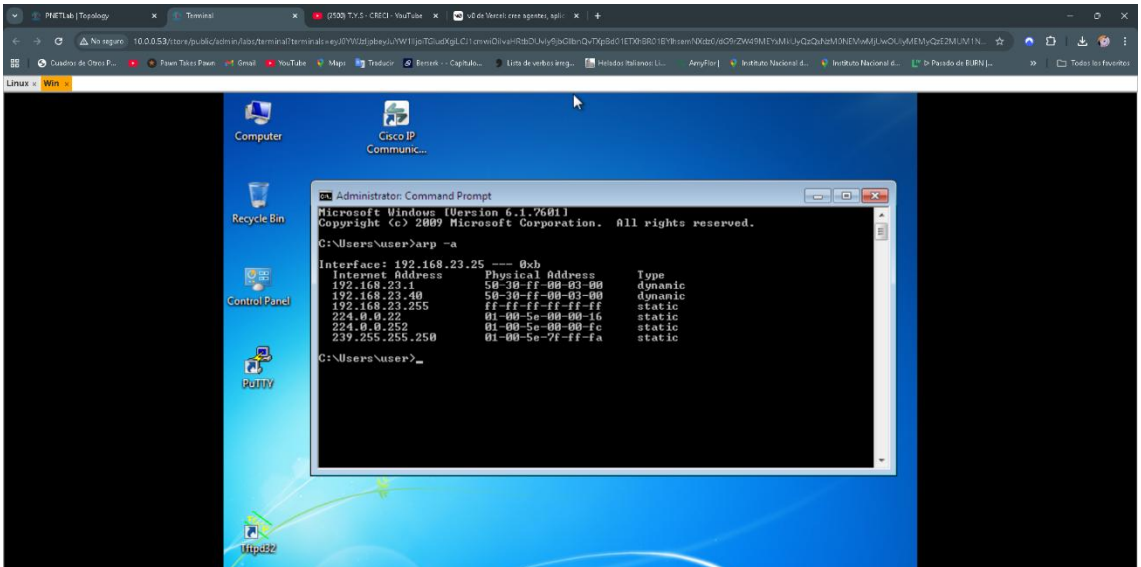
Ahora podemos realizar la visualización de la tabla Arp para verificar las direcciones MAC de los dispositivos antes de realizar el ataque.

Paso Numero 3: *Activacion del .PY*



Parte3.2

En este punto Podemos ver el script en funcionamiento en el cual ya esta realizándose

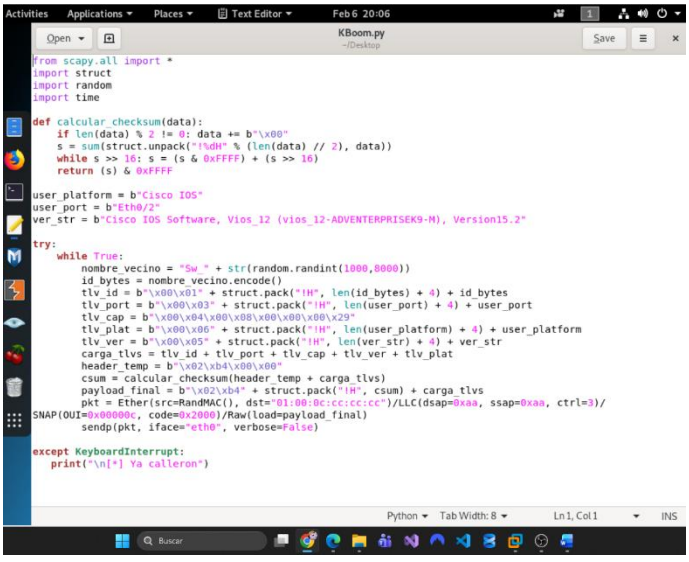


En esta parte final del primer ataque podemos ver de forma clara y sencilla que el router y la maquina Linux comparten la misma mac address y por ende hace cumplir su función.

Ataque Num: 2

Ataque DoS mediante Script Automatizado .PY

Visualización del Scrpit y desenglose del mismo



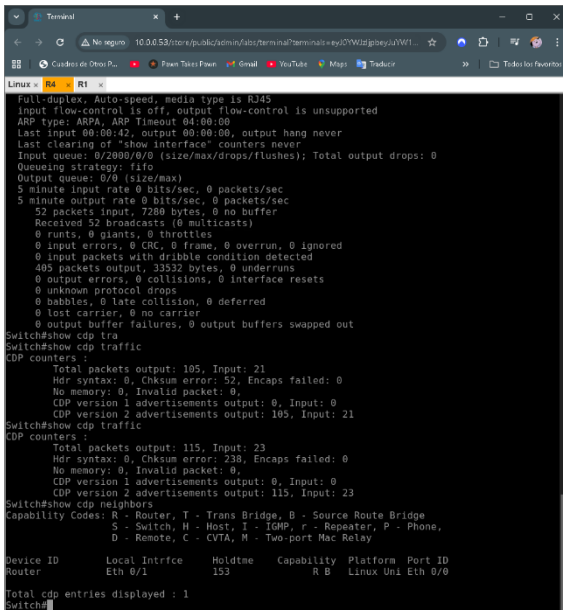
El script desarrollado en Python utiliza la librería Scapy para construir y enviar paquetes CDP (Cisco Discovery Protocol) de forma manual hacia un dispositivo Cisco, simulando un escenario de CDP flooding. El código genera diferentes campos TLV característicos del protocolo, como Device ID, Port ID, Platform y Version,

algunos de ellos con valores aleatorios, con el fin de simular múltiples anuncios de dispositivos falsos. Para garantizar el procesamiento del paquete a nivel de capa 2, este se encapsula correctamente en tramas Ethernet, LLC y SNAP.

Durante la ejecución, los paquetes CDP son enviados de manera continua a través de la interfaz de red especificada, lo que provoca un aumento en los contadores de tráfico CDP del dispositivo objetivo y la generación de errores de checksum, evidenciando el procesamiento de paquetes malformados. Aunque no se crean entradas adicionales en la tabla de vecinos, el ataque impacta el plano de control, permitiendo analizar el comportamiento del switch ante tráfico CDP inválido con fines estrictamente educativos y de laboratorio.

Vizualizando en los dispositivos

Switch:



Desenglose :

El ataque CDP flooding se ejecuta correctamente y los paquetes alcanzan el dispositivo Cisco, lo cual se evidencia por el incremento en los contadores de paquetes CDP de entrada y en los errores de checksum.
Aunque no se observe un aumento en la tabla de vecinos CDP, esto es un comportamiento esperado del protocolo, ya que el impacto del ataque se manifiesta en el plano de control y en el procesamiento interno del dispositivo