Fecha

13/2/2026

Nombre

Jose Alfredo

Apellidos

Daniel Castro

Matrícula

2024-1346

Carrera

Seguridad informática

Materia

Seguridad De Redes

Docente

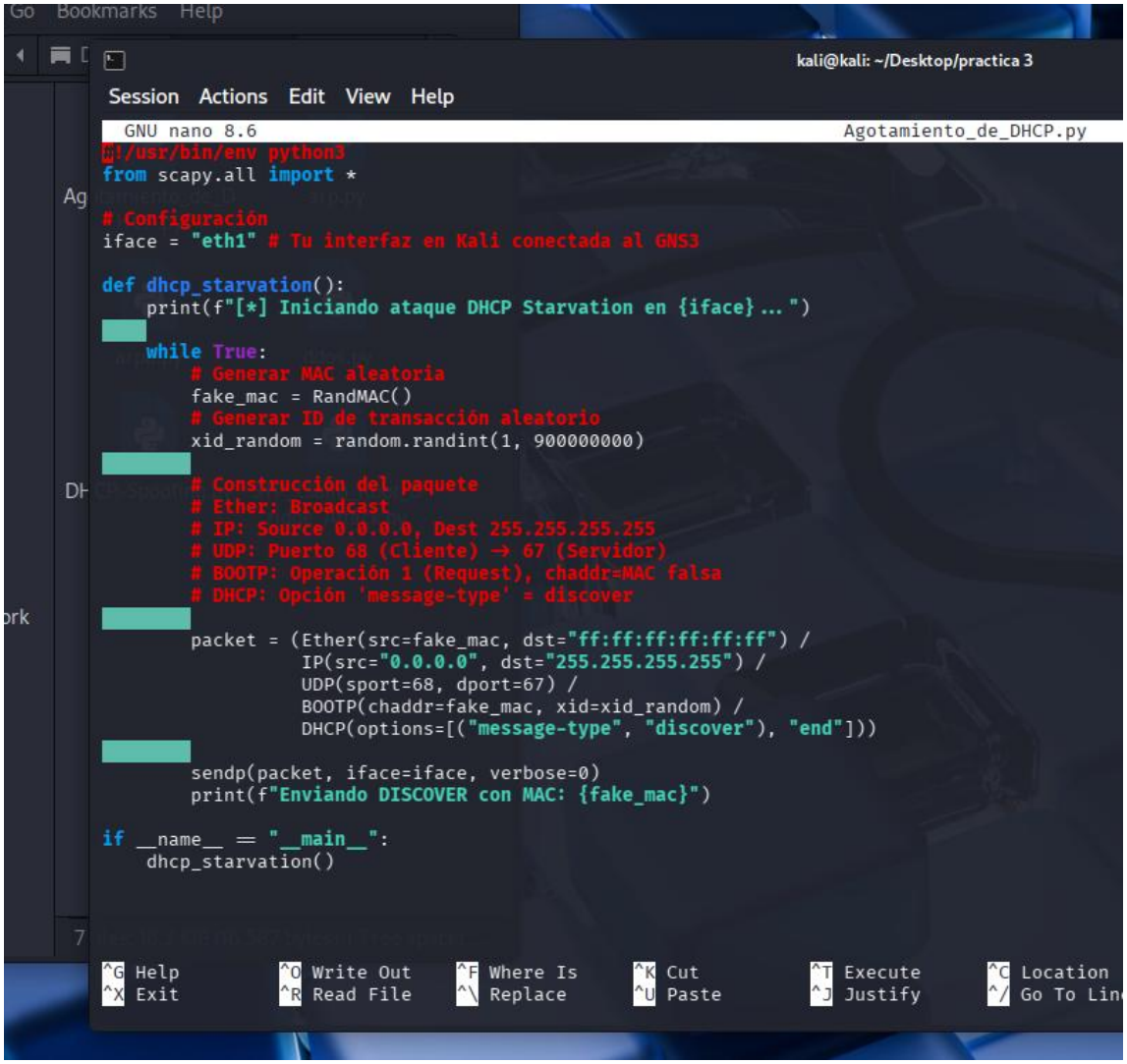
Jonathan Rondon

Video: https://youtu.be/OhtWDl9uVVI

Repositorio: https://github.com/castromenaenrrique-cell/Ataque_DHCP-starvation_DHCP-Spoofing_STP-Root-Bridge

Objetivo de los scripts y como mitigarlos ataques:

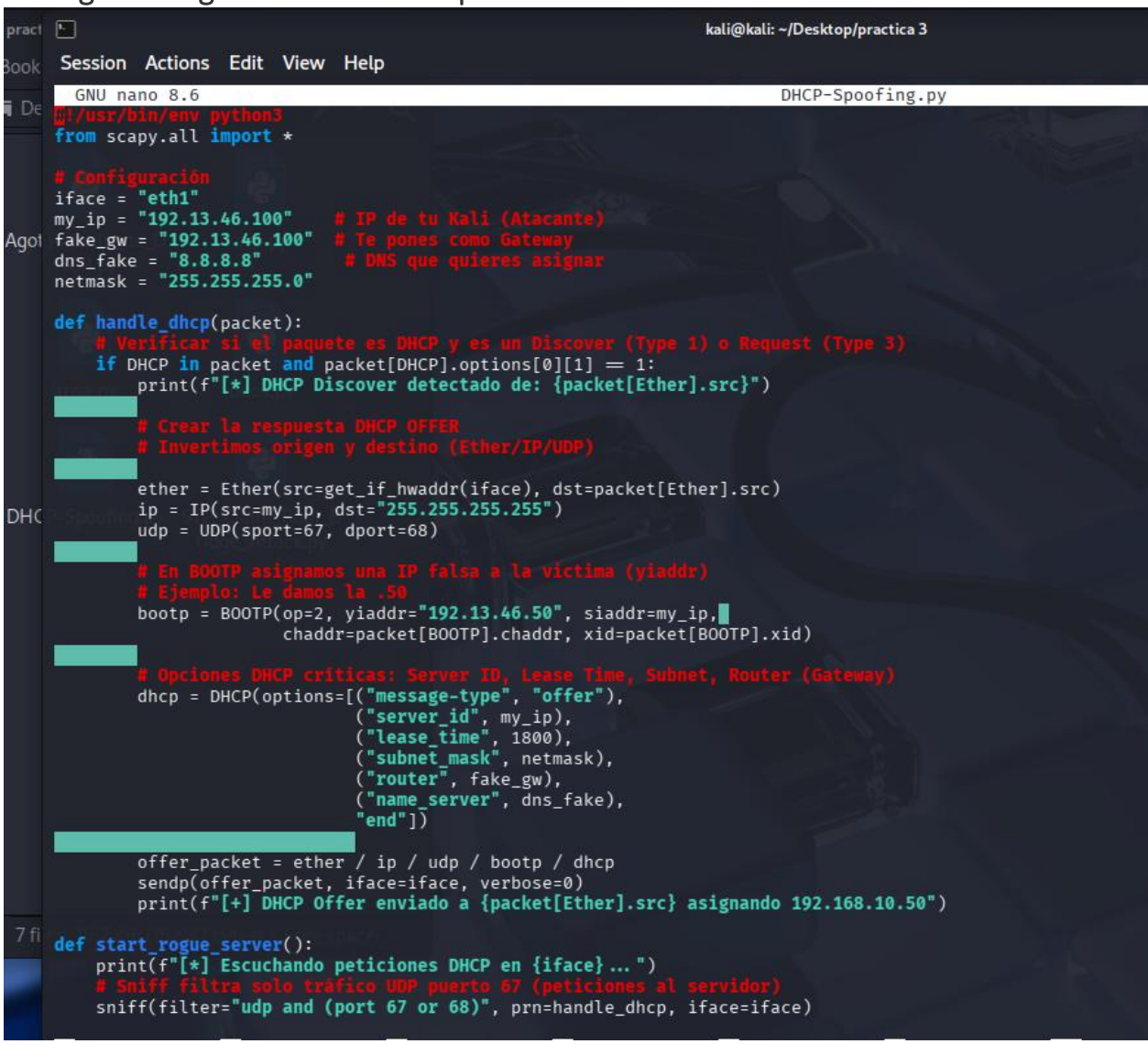
1. DHCP starvation.
    a. Objetivo: agotar el pool de direcciones IP disponibles de un servidor DHCP para impedir que los dispositivos legítimos puedan obtener una dirección IP válida.



b. Mitigación: DHCP Snooping Previene (DHCP Starvation, Servidores DHCP falsos (Rogue DHCP)), Port Security evita que un atacante genere múltiples MAC falsas desde un mismo puerto, Limitar tasa de solicitudes DHCP (Rate Limiting), Segmentar la red mediante VLANs.

2. DHCP Rogue/Spoofing.

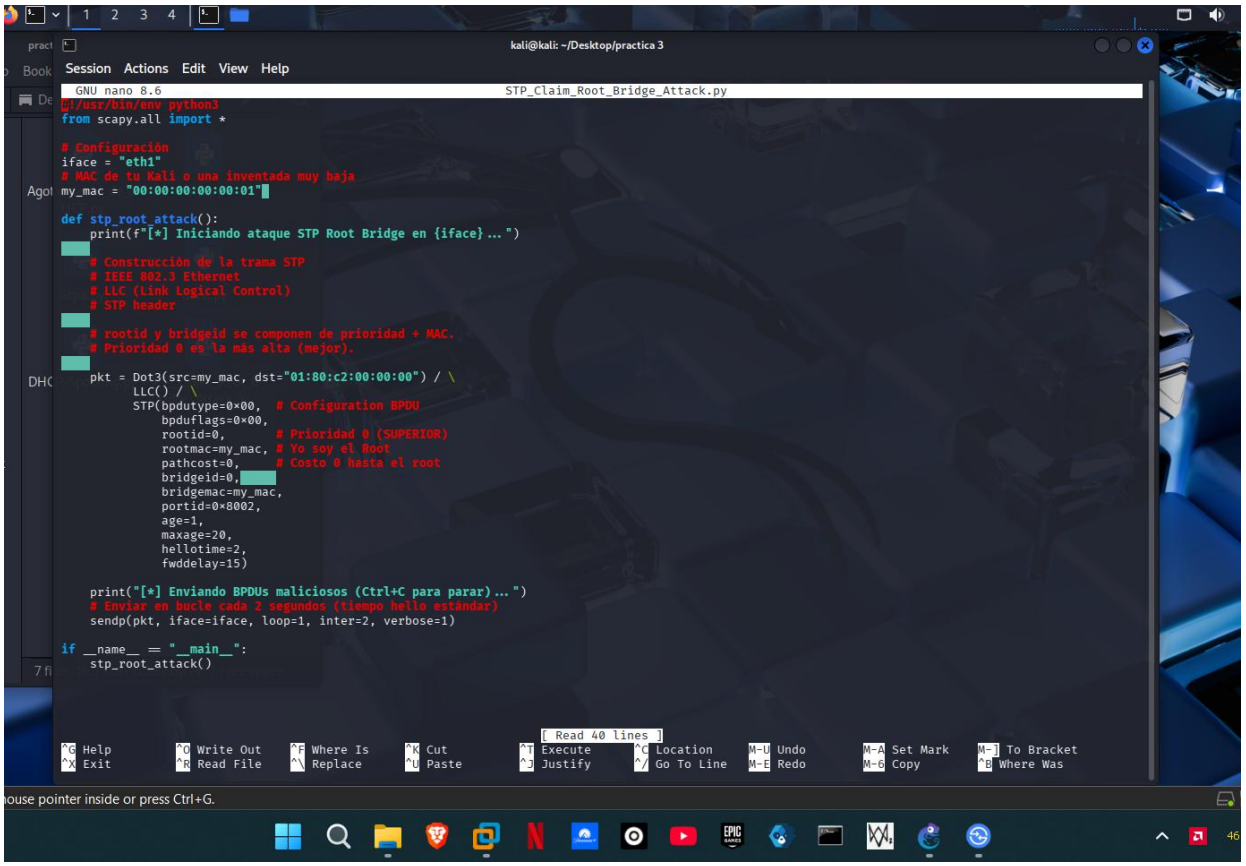
   a. Objetivo: introducir un servidor DHCP falso dentro de la red para entregar configuraciones IP manipuladas a los clientes.



   b. Mitigación: DHCP Snooping previene servidores DHCP falsos, Port Security, Dynamic ARP Inspection, Segmentar la red mediante VLANs.

3. STP Claim Root Bridge.

    a. Objetivo: hacerse pasar por el Root Bridge (puente raíz) en una red que usa Spanning Tree Protocol (STP) para controlar el flujo del tráfico de la red.

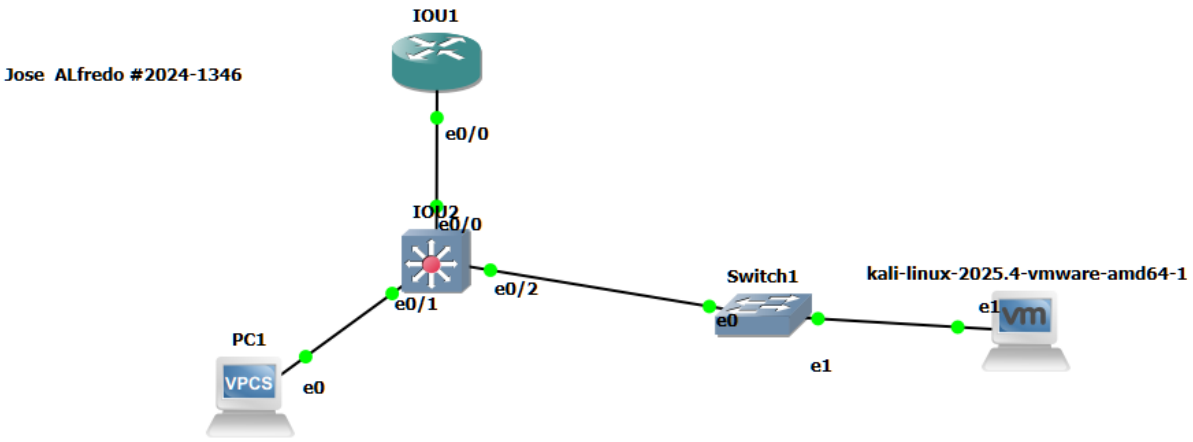


    b. Mitigación: Fijar manualmente el Root Bridge, Root Guard (Evita que un switch no autorizado se vuelva root).

Topología (interfaces, VLANs, direccionamiento IP)

Router		
Interfas e0/0.10	192.13.46.1	255.255.255.0

switch		
Vlan10	admin	
Vlan20	native	
Interfas 0/0	trunk	10,20
Interfas range 0/1-2	acces	10



Requisitos para utilizar la herramienta:

1. Sistema operativo Linux
2. Tener instalado python3