P1 – DHCP STARVATION

Viensy Pérez

2024-1203

Asignatura: Seguridad de Redes

Prof. Jonathan Rondón

Fecha: 13-02-2026

Introducción

El ataque DHCP Starvation consiste en enviar múltiples solicitudes DHCP falsas utilizando direcciones MAC aleatorias, con el objetivo de agotar el pool de direcciones del servidor legítimo. Al saturar el servidor DHCP, los clientes reales de la red no pueden obtener una dirección IP válida, lo que provoca una denegación de servicio.

El propósito de esta práctica es comprender cómo funciona este ataque, analizar su impacto en la red y reforzar la importancia de implementar contramedidas como DHCP Snooping para proteger la infraestructura.

Objetivo del script (P1 – DHCP Starvation)

El objetivo del script es ejecutar un ataque de DHCP Starvation contra el servidor DHCP legítimo de la red.

El script envía múltiples solicitudes DHCP falsas utilizando direcciones MAC aleatorias, con el fin de agotar el pool de direcciones disponibles.

De esta manera, los clientes legítimos (como el PC1) no pueden obtener una dirección IP válida, generando una denegación de servicio en la red.

Medidas de mitigación (P1 – DHCP Starvation)

- Para proteger la red contra ataques de DHCP Starvation se recomiendan las siguientes contramedidas:
- DHCP Snooping: Permite identificar puertos confiables y no confiables, bloqueando solicitudes falsas.
- Port Security: Limita el número de direcciones MAC que pueden conectarse a un puerto del switch.
- IP Source Guard: Evita que dispositivos no autorizados usen direcciones IP falsas.
- Monitoreo de logs y alertas: Detectar actividad anómala en el servidor DHCP.

Escenario de laboratorio

Para la práctica se configuró un entorno de laboratorio con los siguientes elementos:

- **Router (R1):** Servidor DHCP legítimo.
- **Kali Linux:** Equipo atacante que ejecuta el script en Python con Scapy.
- **VPCS (PC1):** Cliente víctima que solicita una dirección IP.
- **Switch:** Dispositivo de interconexión que distribuye el tráfico entre los nodos.

El direccionamiento IP se definió en base a la matrícula: 2024-1203

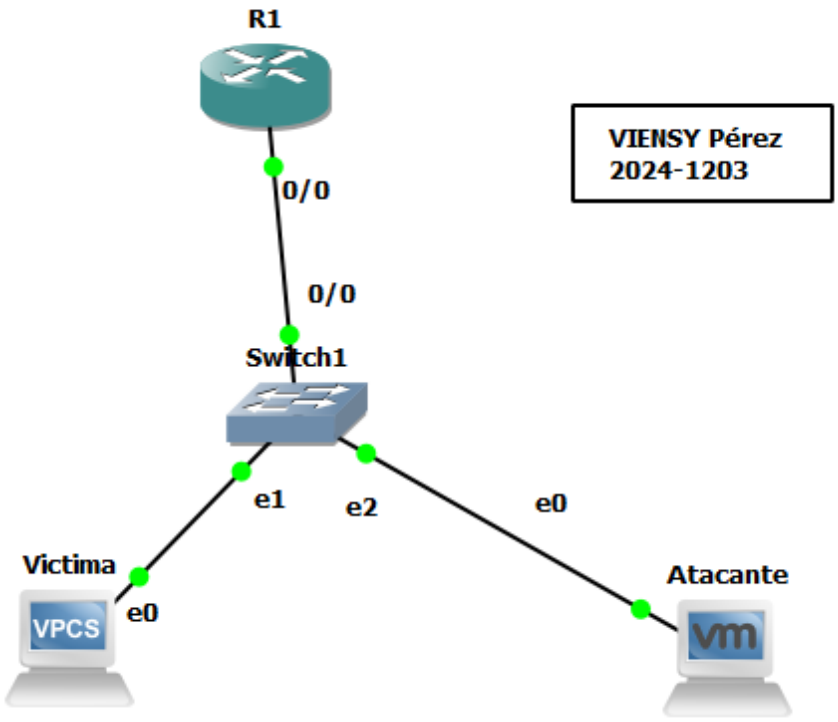
• **Red:** 192.168.120.0/24

•**Router (R1):** 192.168.120.1

•**Kali:** 192.168.120.99

•**VPCS (PC1):** 192.168.120.6 (asignado por DHCP)

Este escenario permite simular un entorno real en el que un atacante puede afectar la disponibilidad de servicios de red mediante el agotamiento del pool DHCP.

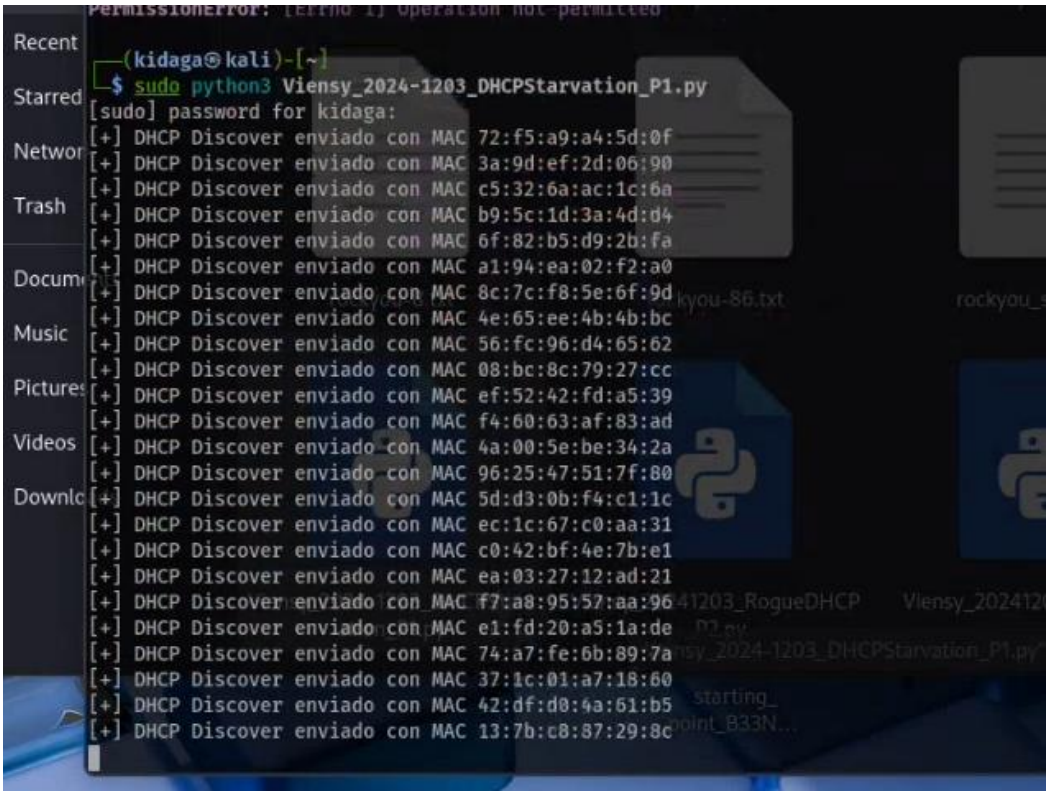


Desarrollo

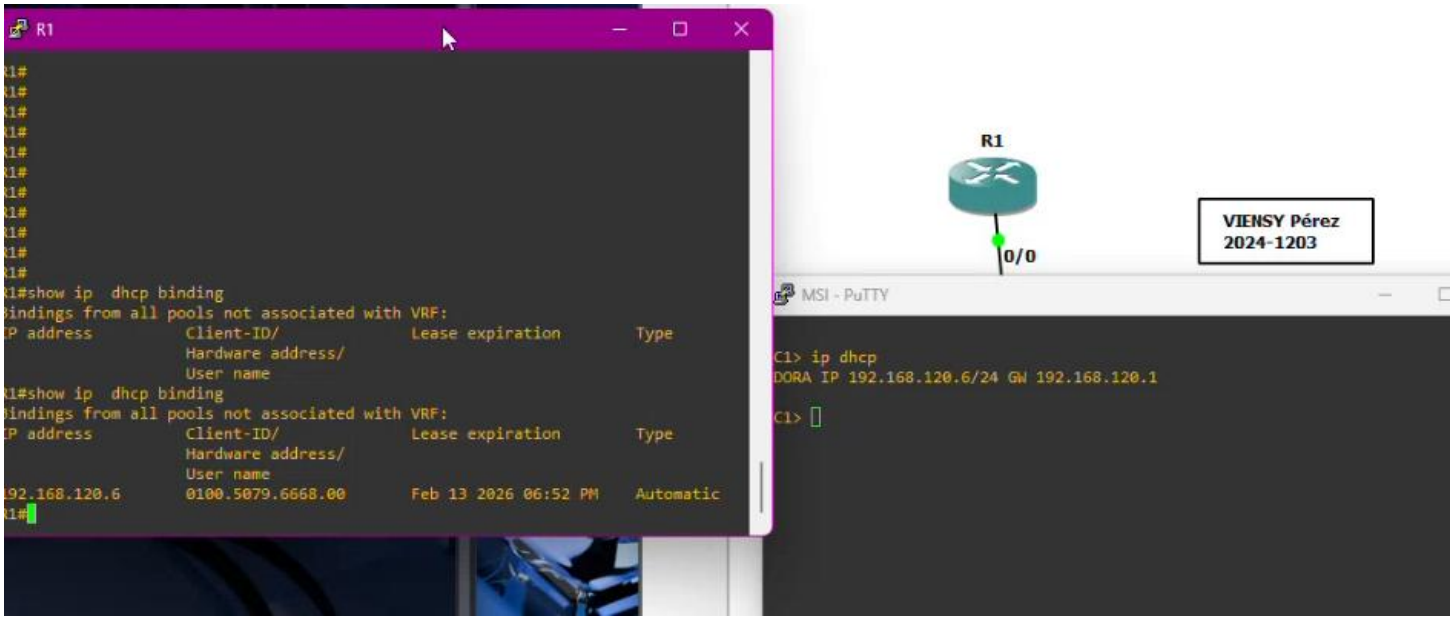
Se adjuntan capturas que muestran el script en ejecución, el agotamiento del pool de direcciones en el router, el estado de las interfaces , pruebas de conectividad mediante ping y la verificación de que el servidor DHCP dejó de asignar direcciones válidas a los clientes.

Script: **Viensy_2024-1203_DHCPStarvation_P1.py**

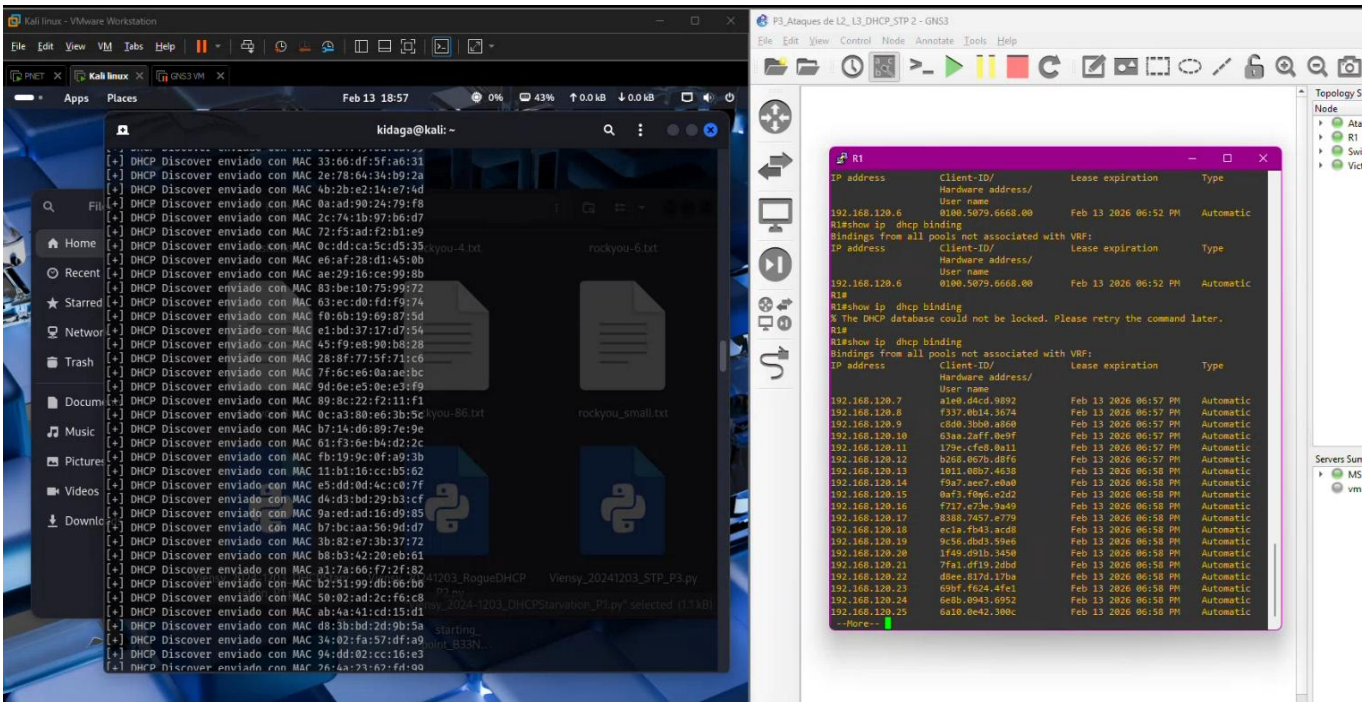
- Ejecución en Kali:



Verificación de funcionamiento del DHCP



Resultado de show ip dhcp binding luego del Ataque



verificación de red y conexión antes de iniciar

```
R1#ping 192.168.120.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.120.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/19/36 ms
R1#ping 192.168.120.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.120.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/24 ms
R1#
```

```
!
interface FastEthernet0/0
 ip address 192.168.120.1 255.255.255.0
```

```
ip dhcp pool LABPOOL
   network 192.168.120.0 255.255.255.0
   default-router 192.168.120.1
   dns-server 8.8.8.8 1.1.1.1
!
```

```
R1#
R1#
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.120.1   YES manual up                    up
R1#
```

Comandos de verificación:

Router: show ip dhcp binding

VPCS: ip dhcp

Resultados

- El pool DHCP se saturó con solicitudes falsas.
- El PC1 no logró obtener una dirección IP válida.
- El router mostró múltiples bindings ocupados.

Conclusiones

El ataque DHCP Starvation demuestra cómo un atacante puede provocar una denegación de servicio en la red. La práctica evidencia la necesidad de implementar medidas de seguridad como DHCP Snooping y Port Security para proteger la infraestructura.

Medidas de mitigación

- DHCP Snooping
- Port Security
- IP Source Guard
- Monitoreo de logs

Enlace de repositorio

https://github.com/Bee-nc/Dhcp_starvation-p1/tree/main

Enlace de Video

https://youtu.be/pTHRTvgymaA