DHCP Starvation Attack – Scapy

👨‍🎓 Autor

Nombre: Juan isai Casado De Oleo

Matrícula: 2024-1580

Video demostrativo

[Ver video demostrativo] (https://youtu.be/j-XN6hBOSqk?si=FO2LdQtP_8S63AQy)

🎯 Objetivo

Desarrollar un script en Python utilizando Scapy para ejecutar un ataque DHCP Starvation en un entorno controlado de laboratorio, demostrando cómo un atacante puede agotar el pool de direcciones IP del servidor DHCP.

🖥️ Topología del Laboratorio

- Router: R1

- Switch: SW1

- Host Atacante: Kali Linux

- Host Víctima: Windows 10

- Red basada en matrícula

Red utilizada:

10.15.80.0/24

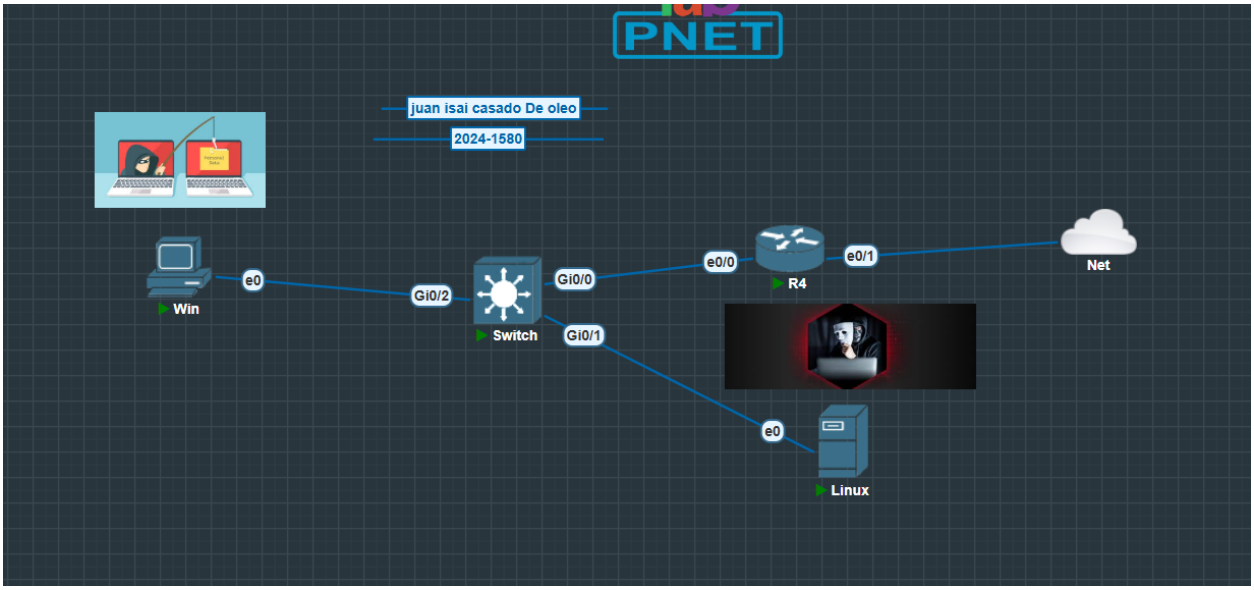
Direccionamiento

- Default gateway 10.15.80.0

- PC Kali Linux 10.15.80.3

- PC Window 10.15.80.2

Diagrama de Topología



⚙ Requisitos

- Python 3

- Scapy

- Permisos root

- Entorno virtualizado (VMware / PnetLab)

🔧 **Instalación de Scapy**

```bash
pip install scapy
```

🚀 **Ejecución del Script**

Desde la máquina atacante (Kali Linux):

```bash
sudo python3 starvation.py
```

🔍 **Funcionamiento del Script**

El script genera múltiples direcciones MAC aleatorias y envía paquetes DHCP Discover al servidor DHCP.

Cada solicitud simula un cliente diferente dentro de la red.

El servidor DHCP responde asignando direcciones IP hasta que el pool disponible se agota.

Cuando el pool se llena, los dispositivos legítimos ya no pueden obtener una dirección IP válida, provocando una denegación de servicio (DoS).

📊 **Resultados Obtenidos**

- Se enviaron múltiples solicitudes DHCP Discover.
- El servidor asignó direcciones IP a clientes falsos.
- El pool DHCP se saturó.
- El equipo víctima no pudo obtener dirección IP.

🛡 **Medidas de Mitigación**

Para prevenir este tipo de ataque se pueden implementar:

- DHCP Snooping
- Port Security en switches
- Limitación de solicitudes DHCP por puerto
- Monitoreo de tráfico anómalo
- Segmentación de red

⚠ Este laboratorio fue realizado únicamente en un entorno controlado con fines académicos.