Instituto Tecnológico de las Américas

Nombre: Emmanuel Bello Sierra

Matricula: 2024-1369

Profesor: Jonathan Rondon

Asignatura: Seguridad de Redes

Tema: Tarea Semana 3 (Practica 2)

Fecha: 5 / 2 / 2026

Video de Demostración

https://youtu.be/zPP2iGL8FP4

---

1. Descripción del Ataque

Este proyecto implementa un ataque de **Denegación de Servicio (DoS)** dirigido al protocolo CDP (Cisco Discovery Protocol).

El script genera miles de paquetes CDP falsificados con direcciones MAC de origen y nombres de dispositivo aleatorios (`FakeDevice_XXXX`). Esto satura la tabla de vecinos del Switch objetivo, consumiendo su memoria y dificultando la administración de la red.

2. Entorno de Laboratorio (Topología)

Atacante: Ubuntu Desktop 20.04 (Virtualizado en PNETLab).

Herramienta: Python 3 + Scapy.

Interfaz: `ens3`.

Víctima: Switch Cisco vIOS (L2).

Red: 192.168.10.0/24.

3. Requisitos y Ejecución

Prerrequisitos

Se requiere tener instalada la librería Scapy:

```bash
sudo pip3 install scapy
```

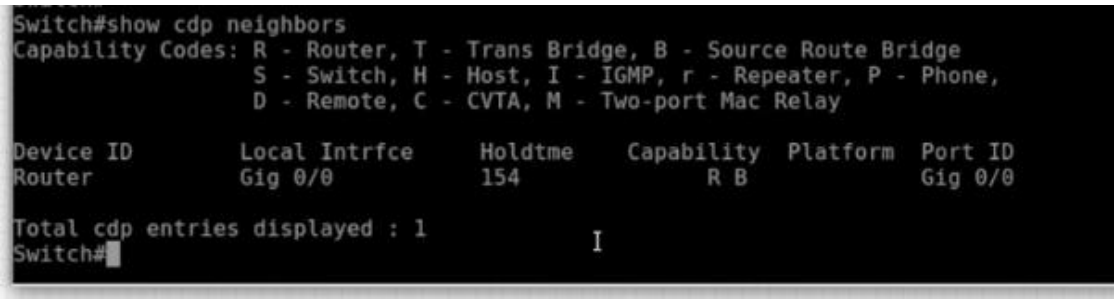
Comando de Ejecución

El script debe ejecutarse con privilegios de superusuario para poder inyectar paquetes en la interfaz de red:

sudo python3 cdp_dos.py

4. Evidencia de Funcionamiento

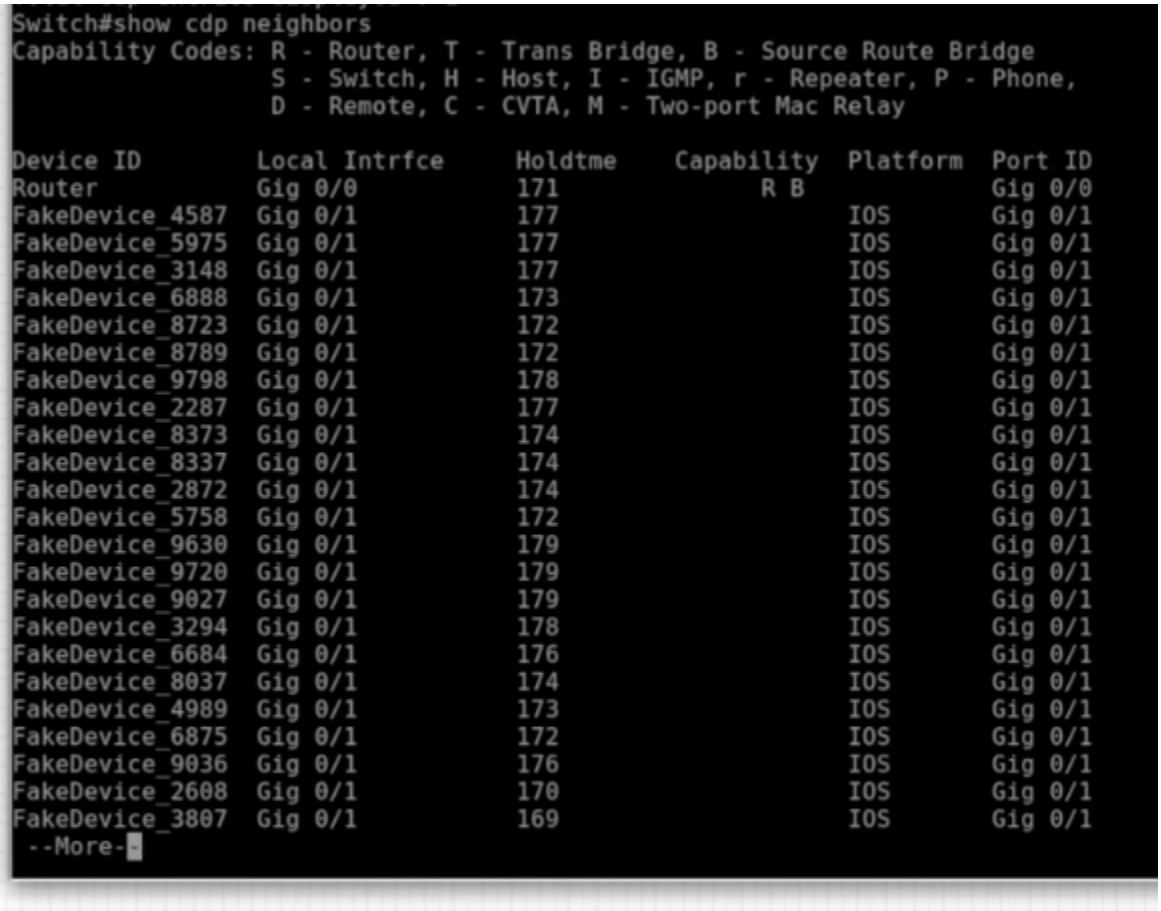
Antes del ataque, la tabla de vecinos del Switch muestra solo los dispositivos legítimos. Durante la ejecución del script, la tabla se inunda con entradas falsas:



```
Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router           Gig 0/0           154              R B            Gig 0/0

Total cdp entries displayed : 1
Switch#
```



```
Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router           Gig 0/0           171              R B            Gig 0/0
FakeDevice_4587  Gig 0/1           177                     IOS       Gig 0/1
FakeDevice_5975  Gig 0/1           177                     IOS       Gig 0/1
FakeDevice_3148  Gig 0/1           177                     IOS       Gig 0/1
FakeDevice_6888  Gig 0/1           173                     IOS       Gig 0/1
FakeDevice_8723  Gig 0/1           172                     IOS       Gig 0/1
FakeDevice_8789  Gig 0/1           172                     IOS       Gig 0/1
FakeDevice_9798  Gig 0/1           178                     IOS       Gig 0/1
FakeDevice_2287  Gig 0/1           177                     IOS       Gig 0/1
FakeDevice_8373  Gig 0/1           174                     IOS       Gig 0/1
FakeDevice_8337  Gig 0/1           174                     IOS       Gig 0/1
FakeDevice_2872  Gig 0/1           174                     IOS       Gig 0/1
FakeDevice_5758  Gig 0/1           172                     IOS       Gig 0/1
FakeDevice_9630  Gig 0/1           179                     IOS       Gig 0/1
FakeDevice_9720  Gig 0/1           179                     IOS       Gig 0/1
FakeDevice_9027  Gig 0/1           179                     IOS       Gig 0/1
FakeDevice_3294  Gig 0/1           178                     IOS       Gig 0/1
FakeDevice_6684  Gig 0/1           176                     IOS       Gig 0/1
FakeDevice_8037  Gig 0/1           174                     IOS       Gig 0/1
FakeDevice_4989  Gig 0/1           173                     IOS       Gig 0/1
FakeDevice_6875  Gig 0/1           172                     IOS       Gig 0/1
FakeDevice_9036  Gig 0/1           176                     IOS       Gig 0/1
FakeDevice_2608  Gig 0/1           170                     IOS       Gig 0/1
FakeDevice_3807  Gig 0/1           169                     IOS       Gig 0/1
 --More--
```

5. Medidas de Mitigación

Para proteger la infraestructura de red contra este tipo de ataques, se recomiendan las siguientes configuraciones en los dispositivos Cisco:

Deshabilitar CDP Globalmente: Si el protocolo no es estrictamente necesario. “**no cdp run”**

Deshabilitar CDP por Interfaz: En puertos conectados a usuarios finales o dispositivos no confiables.

“Interface gig0/1

no cdp Enable”