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/ZVodf3atLXs

https://github.com/Laboa09/Emmanuelbello_2024-1369_P1/tree/main

---

1. Descripción del Ataque

Este proyecto implementa un ataque de **Man-in-the-Middle (MitM)** utilizando la técnica de **ARP Spoofing**.

El script envenena las tablas ARP de la víctima y del router, haciéndose pasar por el otro dispositivo. Esto permite al atacante interceptar, modificar o detener el tráfico de red entre la víctima e Internet. Además, se habilita el **IP Forwarding** en Linux para que la víctima no pierda conexión y el ataque sea invisible.

2. Entorno de Laboratorio (Topología)

Atacante: Ubuntu Desktop 20.04 (IP: Dinámica, Interfaz: `ens3`).

Víctima: Ubuntu Desktop (IP: `192.168.10.3`).

Gateway: Router Cisco (IP: `192.168.10.1`).

3. Requisitos y Ejecución

Prerrequisitos

Se requiere Python 3, Scapy y permisos de superusuario.

Comando de Ejecución

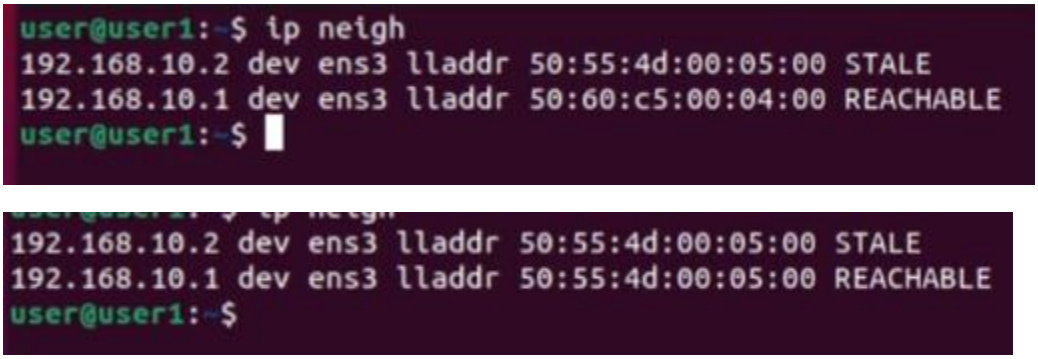
```bash

sudo python3 arp_mitm.py

El script automáticamente activa el reenvío de paquetes en el kernel (/proc/sys/net/ipv4/ip_forward) al iniciar y lo desactiva al terminar.

## 4. Evidencia de Funcionamiento

El éxito del ataque se verifica en la máquina víctima mediante el comando:







Se observa que la dirección MAC asociada a la IP del Router (192.168.10.1) cambia y se vuelve idéntica a la MAC del atacante, confirmando la suplantación.

## 5. Medidas de Mitigación (Defensa)

**Dynamic ARP Inspection (DAI):** Característica de seguridad en switches Cisco que intercepta y valida los paquetes ARP contra una base de datos de confianza (DHCP Snooping).
```

Entradas ARP Estáticas: Configurar manualmente las direcciones MAC del router en servidores críticos (poco escalable).

Uso de Cifrado: ***Utilizar HTTPS, SSH o VPNs para asegurar que, aunque el tráfico sea interceptado, la información sensible permanezca ilegible.***