**Layer 2 Security Lab**

**CYBR3010**

**Cybersecurity Foundations**

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

[**Introduction** 1](#_Toc210924279)

[**Network Diagram** 1](#_Toc210924280)

[**Explanation of vulnerabilities and potential impact** 2](#_Toc210924281)

[**MAC Flooding** 2](#_Toc210924282)

[**ARP Spoofing** 2](#_Toc210924283)

[**Spanning Tree Protocol (STP) Manipulation** 3](#_Toc210924284)

[**Test results (before and after scenarios)** 3](#_Toc210924285)

[**MAC flooding before launching the attack in Kali Linux VM** 3](#_Toc210924286)

[**MAC flooding after launching the attack in Kali Linux VM** 4](#_Toc210924287)

[**ARP flooding before launching the attack in Kali Linux VM** 7](#_Toc210924288)

[**ARP flooding after launching the attack in Kali Linux VM** 7](#_Toc210924289)

[**STP before launching the attack** 7](#_Toc210924290)

[**STP after launching the attack** 7](#_Toc210924291)

[**Configuration steps for security measures** 7](#_Toc210924292)

[**MAC flooding attack – security measures** 7](#_Toc210924293)

[**Questions and answers** 11](#_Toc210924294)

[What role does the Spanning Tree Protocol (STP) play in a Layer 2 network? Analyze how STP manipulation attacks could be leveraged to cause denial-of-service or traffic interception. Recommend a security-hardening plan that preserves redundancy while minimizing attack vectors. 11](#_Toc210924295)

[What is Dynamic ARP Inspection and what does it protect against? 11](#_Toc210924296)

[How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy? 11](#_Toc210924297)

# **Introduction**

This document is about Data Link Layer (layer 2 of the OSI model). This layer is responsible for the reliable transmission of data between two directly connected nodes on the same local area network (LAN) via MAC addresses. Common network devices operating here are switches and bridges. Additionally, it will tackle vulnerabilities in Data Link Layer, compare results before and after the attack, and apply security measures to mitigate the vulnerabilities effectively.

# **Network Diagram**

This is the network layout which consists of multiple virtual machines (VMs) with MAC address running on different operating systems (Windows, Linux), as well as a virtual cisco switch configured to communicate with other network devices.

A diagram of a computer program

AI-generated content may be incorrect.

Figure 1: Network Diagram for Layer 2 Security Lab.

# **Explanation of vulnerabilities and potential impact**

## **MAC Flooding**

It is a cyberattack that targets network switches on a Local Area Network (LAN) and tries to steal user data. Every device has a MAC address, a unique numerical signifier used to identify the device within a network. The attacker uses the command “**macof**”, which floods the local network with random fake MAC addresses, causing some switches to fail open in repeating mode which in turn facilitate sniffing.

As a result, sensitive data can be intercepted by attackers and can lead to data breaches, financial losses, and damage to an organization’s reputation. By overloading a network switch, attackers can disrupt its functionality and block legitimate traffic. This causes serious issues like efficiency, increased delays, or even a complete denial of service for authorized users. Furthermore, when network traffic is broadcast to all devices, attackers can intercept sensitive information they wouldn’t normally have access to. This includes login credentials, private data, or communications meant for restricted systems. Such unauthorized access can compromise the security of the entire network and lead to further exploitation.

## **Spanning Tree Protocol (STP) Manipulation**

## **ARP Spoofing**

ARP (Address Resolution Protocol) spoofing is a type of attack in which a malicious actor sends falsified ARP messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

# **Test results (before and after scenarios)**

## **MAC flooding before launching the attack in Kali Linux VM**

* In CML, right-click the switch then press “Start”.
* Right-click the switch again then press “Console”.
* Click “Open Console”.
* In the console, type “enable” then press enter.
* Type “configure” then press enter.
* If you see “Configuring from terminal, memory, or network [terminal]”, just press enter.
* Inside the config, type the word “hostname” plus name of the device to enter to the device configuration, then press enter. Ex. “hostname SW01”.
* Type “exit”.
* Considering all the virtual machines were turned-on, type “show mac address-table” in switch.
* MAC address table will display MAC addresses that are connected to the switch.

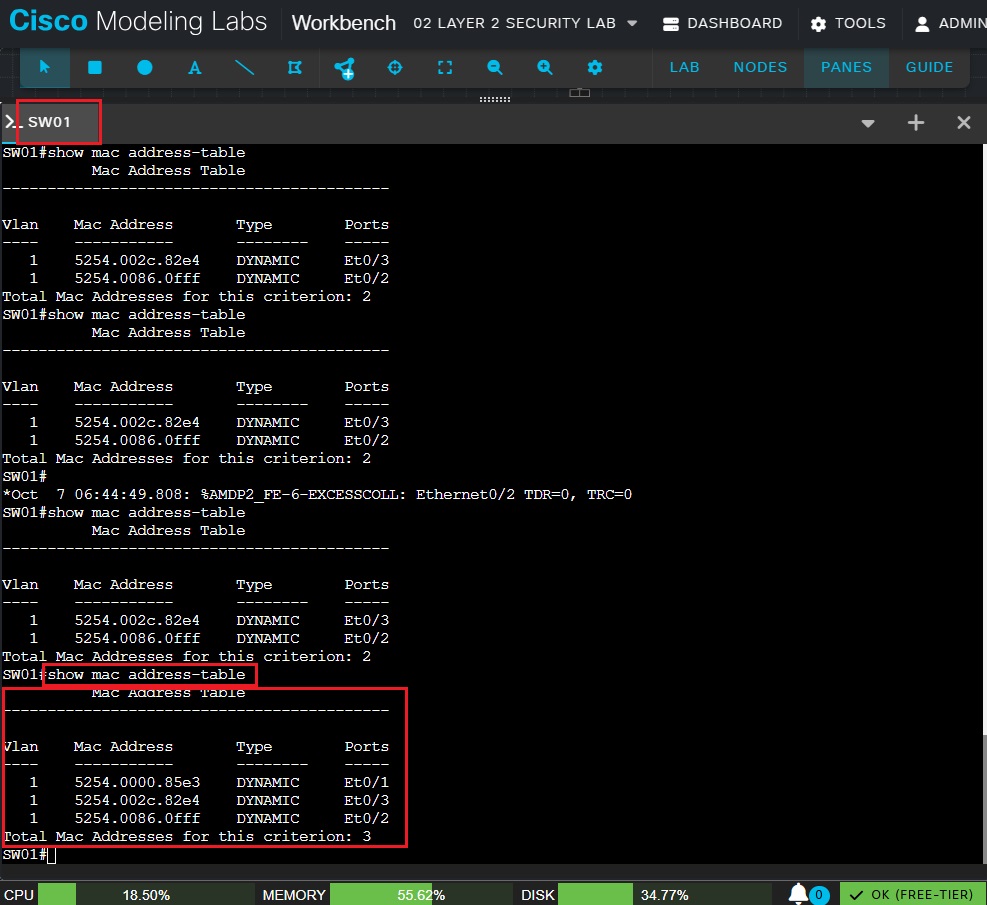


Figure 2 Before the attack, there are 3 MAC addresses connected to the switch.

## **MAC flooding after launching the attack in Kali Linux VM**

* To launch an attack, type “sudo macof -1 eth0” in Kali Linux terminal and press enter.
* Type the password and press enter.
* Mac flooding will take effect at this moment of time. Several frames with different MAC addresses will be displayed continuously.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 After the attack, notice in Kali Linux terminal that all frames with different MAC addresses will keep showing up.

* In switch console, type “show mac address-table” then press enter.
* This will display the total entries of MAC addresses after the attack.

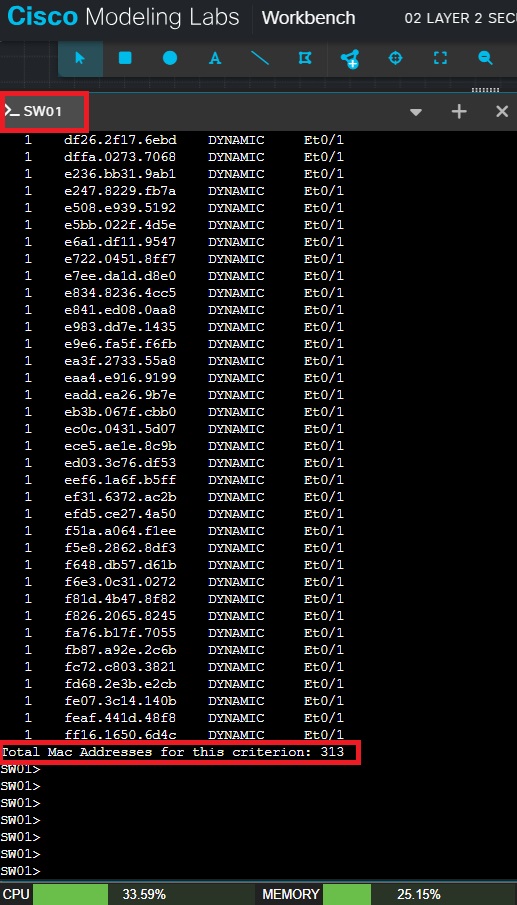


Figure 4 After the attack, there are total of 313 MAC addresses in the MAC address table as opposed to 3 MAC addresses before the attack.

## **STP before launching the attack**

## **STP after launching the attack**

## **ARP spoofing before launching the attack in Kali Linux VM**

## **ARP spoofing after launching the attack in Kali Linux VM**

# **Configuration steps for security measures**

## **MAC flooding attack – security measures**

Below are the **main commands** that would limit MAC addresses and block unknown devices in a MAC flooding attack:

* Make sure you are in SW01#, otherwise type “enable” and press enter.
* Type “**configure terminal**” and press enter.
* In the switch configuration, type “**interface range e0/1-3**”and press enter. This command means going to interfaces range from e0/1, e0/2, and e0/3.
* Type “**switchport mode access**”.
* Type “**switchport port-security**”.
* Type “**switchport port-security mac-address sticky**”.
* Type “**switchport port-security maximum 2**”.
* For violation, we will use the default option which is to shutdown. As an alternative, type “**switchport port-security violation restrict**”.

A screenshot of a computer

AI-generated content may be incorrect.

*Main commands to configure security measures of Mac flooding attack.*

Below are additional helpful commands:

* If you type “switchport port-security ?”, this will display available configuration options.

A computer screen with white text

AI-generated content may be incorrect.

*This command is to control which MAC addresses are allowed on a port and what happens when an unauthorized device attempts to connect. Aging is an option to set the time for how long a secure MAC address remains in the switch's table before it's removed.*

*Mac-address allows you to statically define specific MAC addresses that are permitted on the port.*

*Maximum sets the highest number of unique MAC addresses allowed on that specific port.*

*Violation determines the switch's response when the maximum number of secure MAC addresses is exceeded or a violation occurs.*

* If you type “switchport port-security mac-address ?”, you will see configuration options for mac-address.

A computer screen with white text

AI-generated content may be incorrect.

*For MAC flooding security measures, we are only concerned about “sticky”. Sticky feature automatically learns and saves these MAC addresses.*

* If you type “switchport port-security violation ?”, you will see configuration options for violation.

A screenshot of a computer

AI-generated content may be incorrect.

*A switchport port-security violation is an event where a network switch's port security feature detects an unauthorized device or action, such as a MAC address that exceeds the configured limit for a port. When a violation occurs, the switch takes a specific action based on the configured violation mode, which can be to disable the port and requires network admin to manually re-enable it (shutdown, this is the default option), block the violating traffic while logging the event (restrict), or silently drop the violating traffic without logging (protect).*

* To check what is going on after the implementation of port security, exit the configuration and type “**show port-security**”.

A screenshot of a computer

AI-generated content may be incorrect.

* To show the status of all the interfaces, type “show ip interface brief”.

A screenshot of a computer

AI-generated content may be incorrect.

*Right now, the status of all the interfaces is up because MAC flood is not launched.*

*A screenshot of a computer

AI-generated content may be incorrect.*

*In this screenshot, MAC flooding is in place. Since port security is implemented, status of interface e0/1 is set to “down”. Therefore, MAC flooding attack is unsuccessful.*

* To return the affected interface (e0/1) from “down” status to “up” status
* Type “config terminal” and press enter.
* Type “int e0/1” and press enter.
* Type “shutdown” and press enter.
* Type “no shutdown” and press enter.
* Type “exit” and press enter (or ctrl+Z).
* Type “exit” and press enter (or ctrl+Z) again.
* Lastly, type “show ip interface brief” and press enter.

A screenshot of a computer

AI-generated content may be incorrect.

*Affected interface e0/1 is now back up after running the command.*

# **Questions and answers**

## What role does the Spanning Tree Protocol (STP) play in a Layer 2 network? Analyze how STP manipulation attacks could be leveraged to cause denial-of-service or traffic interception. Recommend a security-hardening plan that preserves redundancy while minimizing attack vectors.

## What is Dynamic ARP Inspection and what does it protect against?

## How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy?

REFERENCES

<https://linux.die.net/man/8/macof>

<https://www.howtonetwork.com/technical/security-technical/port-security/>

<https://jumpcloud.com/it-index/what-is-a-mac-flooding-attack>

ARP spoofing:

<https://www.veracode.com/security/arp-spoofing/>