**CYBR3010**

**Cybersecurity Foundations**

**Layer 2 Security Lab**

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

[**Introduction** 1](#_Toc210724131)

[**Network Diagram** 1](#_Toc210724132)

[**Vulnerabilities and potential impact** 1](#_Toc210724133)

[MAC Flooding 1](#_Toc210724134)

[**Test results (before and after scenarios)** 2](#_Toc210724135)

[Mac Flooding before launching the attack in Kali Linux 2](#_Toc210724136)

[Mac Flooding after launching the attack in Kali Linux 3](#_Toc210724137)

[**Configuration steps for security measures** 4](#_Toc210724138)

[Mac Flooding security measures 4](#_Toc210724139)

[**Questions and answers** 4](#_Toc210724140)

[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. 4](#_Toc210724141)

[What is Dynamic ARP Inspection and what does it protect against? 4](#_Toc210724142)

[How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy? 4](#_Toc210724143)

# **Introduction**

This lab is all about layer 2 of the OSI model which is the Data Link Layer. This layer is responsible for the reliable transmission of data between two directly connected nodes on the same local area network (LAN), framing data into frames, and using MAC addresses for addressing. Additionally, this lab will tackle vulnerabilities in Data Link Layer and apply security measures to mitigate the vulnerabilities effectively.

# **Network Diagram**

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

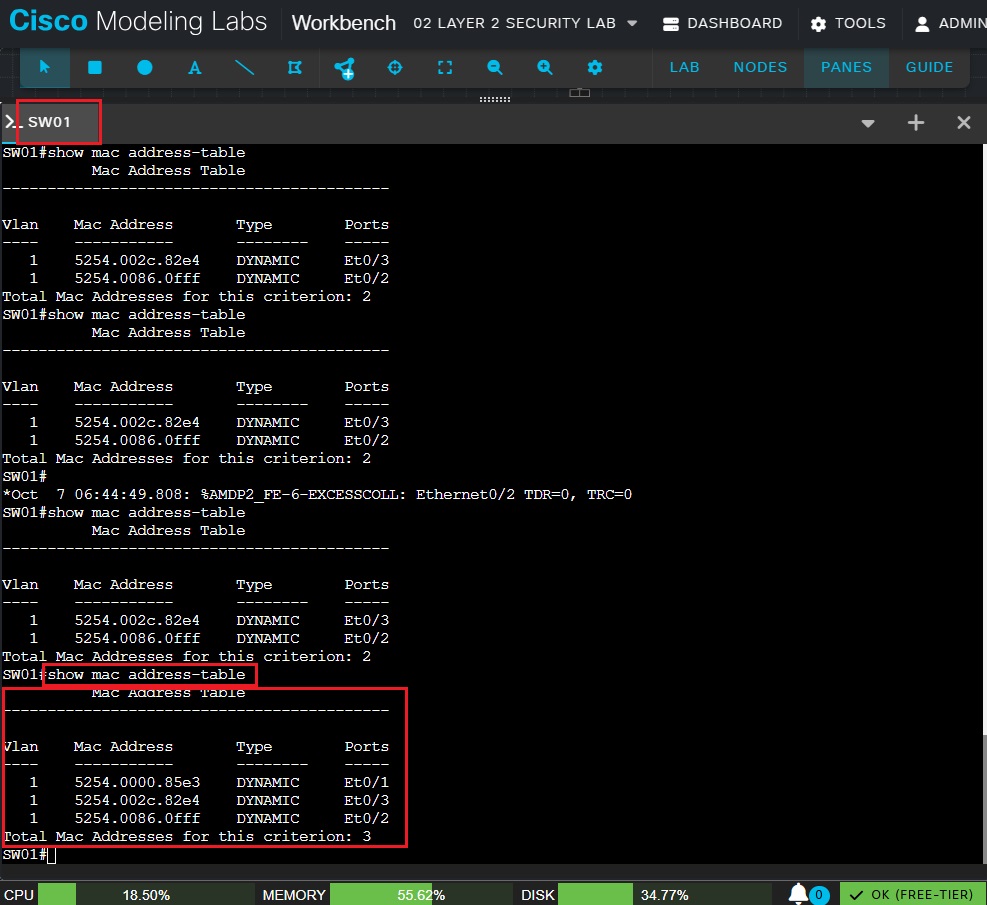
*(Screen label) A Visio diagram of the final network.*

# **Vulnerabilities and potential impact**

## MAC Flooding

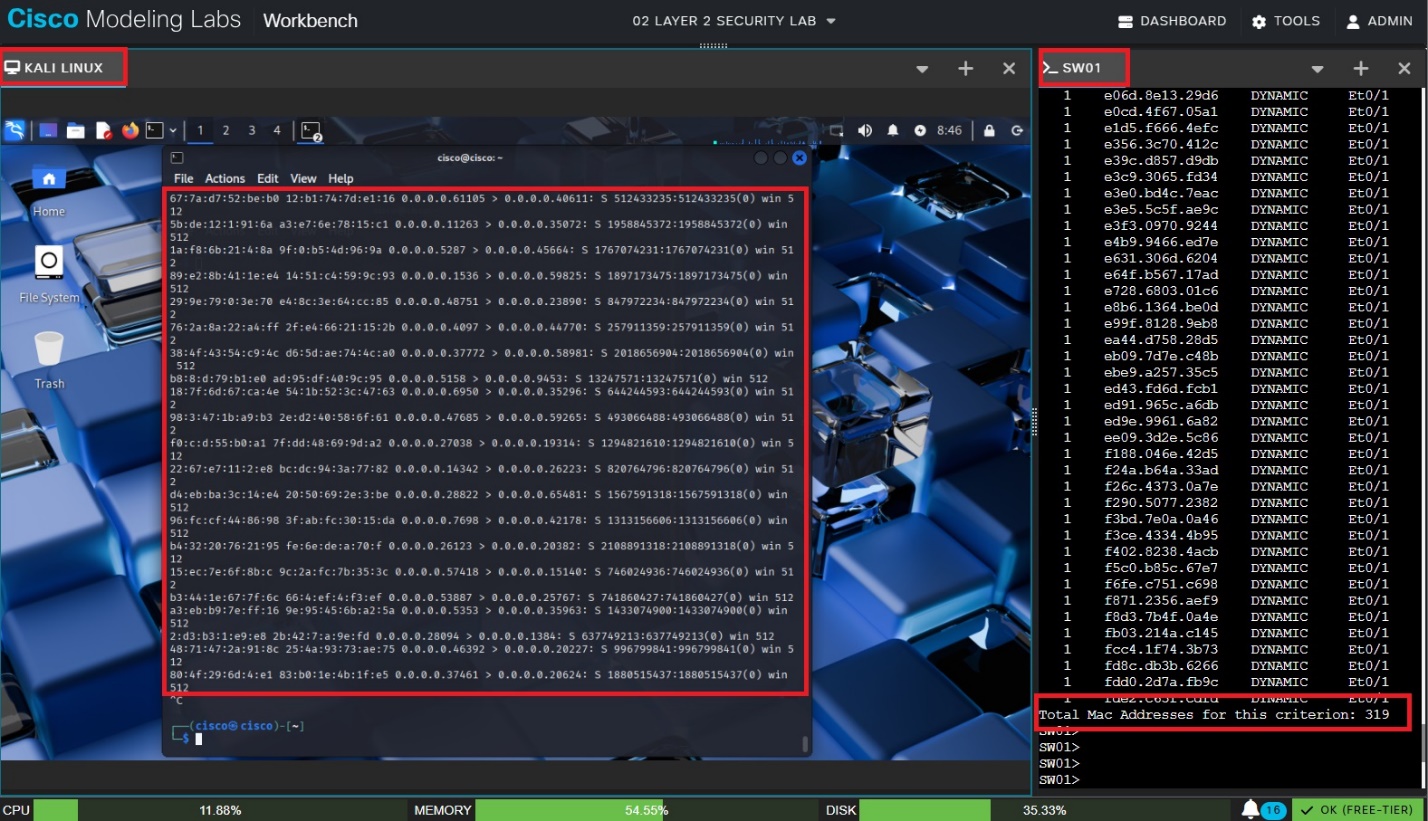
# **Test results (before and after scenarios)**

## Mac Flooding before launching the attack in Kali Linux



Before the attack, there were only 3 MAC addresses in the MAC address table

## Mac Flooding after launching the attack in Kali Linux



To launch an attack, run the command *sudo macof -i eth0* in Kali Linux terminal. Macof command floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

Notice in Kali Linux, it will display all the frames with different MAC address.

Notice in switch, there are total entries of 319 MAC addresses.

# **Configuration steps for security measures**

## Mac Flooding security measures

# **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