**CYBR3010**

**Cybersecurity Foundations**

**Layer 2 Security Lab**

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

[Introduction 1](#_Toc210644541)

[Network Diagram 1](#_Toc210644542)

[Vulnerabilities and its potential impact 1](#_Toc210644543)

[Subtopic 2.1 1](#_Toc210644544)

[Configuration steps for security measures 1](#_Toc210644545)

[Subtopic 2.1 1](#_Toc210644546)

[Test results (before and after scenarios) 1](#_Toc210644547)

[Subtopic 2.1 1](#_Toc210644548)

[Questions and answers 2](#_Toc210644549)

[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. 2](#_Toc210644550)

[What is Dynamic ARP Inspection and what does it protect against? 2](#_Toc210644551)

[How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy? 2](#_Toc210644552)

# Introduction

This lab is to understand the vulnerabilities in Layer 2 (Data Link) of the OSI model 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 its potential impact

## Subtopic 2.1

# Configuration steps for security measures

## Subtopic 2.1

# Test results (before and after scenarios)

## Subtopic 2.1

# 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?

END