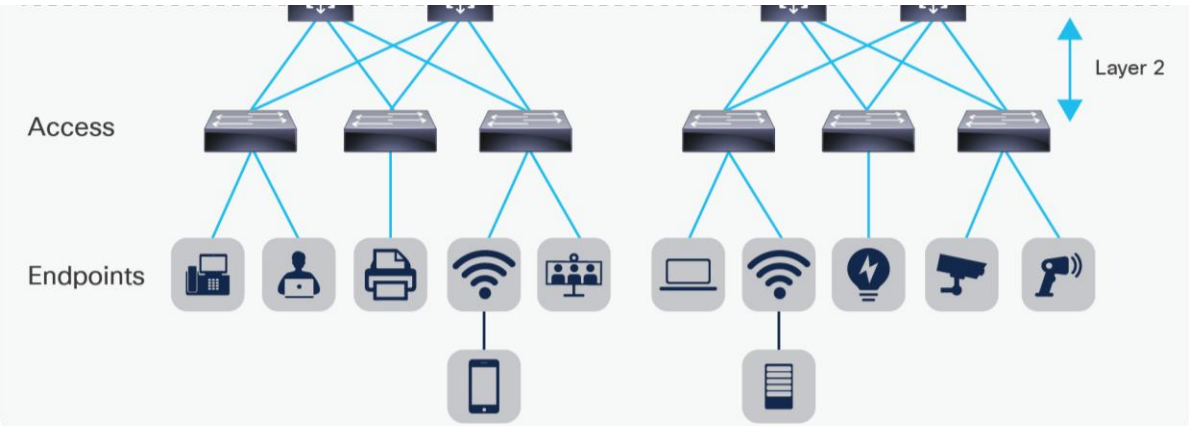
NAIT

Edmonton **Alberta**

CYBR3010

Cybersecurity Foundations

Layer 2 Security



Student:_____

Layer 2 Security

Objectives

This assignment is a practical lab to understand the vulnerabilities in layer 2 of the OSI model and apply security measures to mitigate these vulnerabilities effectively.

At the end of this activity, students will be able to demonstrate their abilities to protect a network by implementing some layer 2 security measures to protect against specific layer 2 attacks, as well as document their work.

Equipment and Materials:

For this lab use the following:

- CML Environment
- Virtual Network Switch
- Multiple virtual machines (VMs) running different operating systems (e.g., Windows, Linux)

Instructions:

1. **Create a network with the specifications below and perform the following attacks on the network created:**

- Configure a network topology with a network switch and several virtual machines (VMs) as end devices.
- Display the switch's MAC table, compare it with devices MAC addresses and explain how each device is assigned to its corresponding port.
- In your lab environment, intentionally introduce at least **three** different Layer 2 vulnerabilities. Examples include:
    - MAC flooding, MAC spoofing | VLANs | ARP spoofing | DHCP spoofing | STP attacks | CDP/LLDP reconnaissance
- Document the methods used to create these vulnerabilities.
- For each identified vulnerability, implement the appropriate security measures to mitigate the risk. Use Layer 2 security features provided by the switch.
- Describe the security measures you apply in detail, including configurations and settings.
- Test the effectiveness of each security measure by attempting to exploit the vulnerability observing the results and verifying that the vulnerabilities are mitigated successfully.

2. **Answer the following questions (With your own words):**

- 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?

Deliverables

PDF Document with screenshots and explanations:

- An introduction to provide an overview of your network build.
- An explanation of each identified vulnerability and its potential impact.
- A Visio diagram of the final network.
- Configuration steps for security measures.
- Test results, including before and after scenarios.
- Questions and answers listed above.

DISCLAIMER

This cybersecurity lab involves hands-on learning experiences, including the use of various tools and techniques to explore security vulnerabilities and threats. While the purpose of these activities is purely educational and designed to enhance your understanding of cybersecurity, it is essential to emphasize responsible and ethical use of the knowledge gained during this lab.

Please be aware of the following:

Educational Purpose: This lab is intended solely for educational purposes within the controlled virtual environment built in the previous lab. The knowledge and skills acquired here are to be used responsibly and legally.

Ethical Conduct: Under no circumstances should the tools, techniques, or knowledge gained from this lab be applied to compromise, harm, or intrude upon any legitimate systems or networks without proper authorization. Unauthorized access or malicious actions against real-world systems are illegal and unethical.

Responsible Use: Always respect the privacy and security of individuals, organizations, and systems. Any attempt to engage in hacking or unauthorized activities outside of this educational context is strictly prohibited.

Authorization: If you wish to test or assess the security of any system or network, it is imperative to obtain explicit permission from the system owner or responsible authority. Unauthorized testing, even with good intentions, can lead to legal consequences.

Legal Compliance: Ensure that you are familiar with and abide by all applicable laws and regulations related to cybersecurity, computer misuse, and data protection. Ignorance of the law is not an excuse.

Maintain Confidentiality: Do not share sensitive information or lab findings outside of the educational environment. Always protect the privacy and confidentiality of data encountered during lab exercises.

Seek Guidance: If you have any questions or uncertainties regarding the ethical and legal aspects of cybersecurity activities, consult with your instructor for guidance.

By participating in this lab, you acknowledge and agree to abide by these principles of ethical and responsible conduct. It is our collective responsibility to ensure that our knowledge and skills in cybersecurity are used to enhance security and protect digital assets, not to harm or exploit them.

Remember that cybersecurity professionals play a critical role in safeguarding the digital world, and our commitment to ethical behavior and responsible use is fundamental to the cybersecurity community.