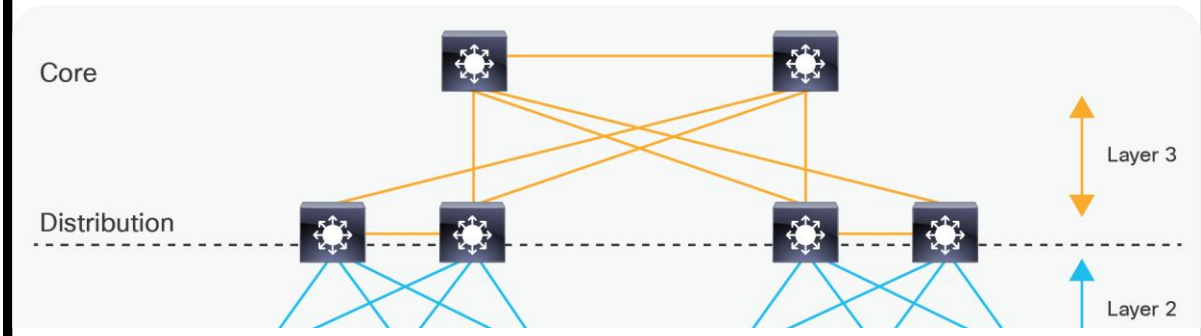
NAIT

Edmonton **Alberta**

CYBR3010

Cybersecurity Foundations

Layer 3 and Layer 4 Security



Student:_____

Layer 3 and Layer 4 Security

Objectives

This assignment is a practical lab to understand the vulnerabilities in layer 3 and layer 4 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 3 and layer 4 security measures to protect against specific layer 3 attacks, as well as document their work.

Equipment and Materials:

For this lab use the following:

1. CML Environment
2. Virtual Firewall
3. 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:**
   - Set up a network topology that includes a network switch and multiple VMs representing end devices.
   - Configure VLANs on the switches to segment the network for better control and security.
   - Configure Virtual firewall with proper VLAN interfaces.
   - Configure IP addressing on the firewall.
   - Configure DHCP Pools for each VLAN.
   - Show DHCP IP obtained by each VM (from each VLAN).
   - Configure NAT to allow VMs access to the internet.
   - In your lab environment, intentionally introduce at least **one** different Layer 3/4 vulnerabilities. Examples include:
     - IP Spoofing| VLANs Hopping | Port Scan | TCP SYN flood | ICMP attacks

2. **Answer the following questions (With your own words):**
   - What is IP spoofing, and how is it commonly used in network attacks? Discuss multiple mitigations explaining their benefits and limitations in different network environments.
   - How do ACLs operate at Layer 3/4 to filter traffic based on IP addresses, protocols, and ports? Evaluate their strengths and weaknesses as security control in large, distributed networks, and suggest how they should be combined with other defenses for layered security.
   - What are SYN flood attacks, and how do they exploit the TCP three-way handshake? Compare multiple mitigation approaches such as SYN cookies, connection rate-limiting, and load balancer filtering, and discuss their operational trade-offs.
     How does Deep Packet Inspection differ from traditional packet filtering at Layers 3 and 4? Analyze its advantages and privacy concerns and propose scenarios where DPI should or should not be implemented in enterprise environments.

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 network diagram of the final network.
- Configuration steps for each device and the security measures.
- Test results, including before and after scenarios.
- Answers to the above questions.

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.