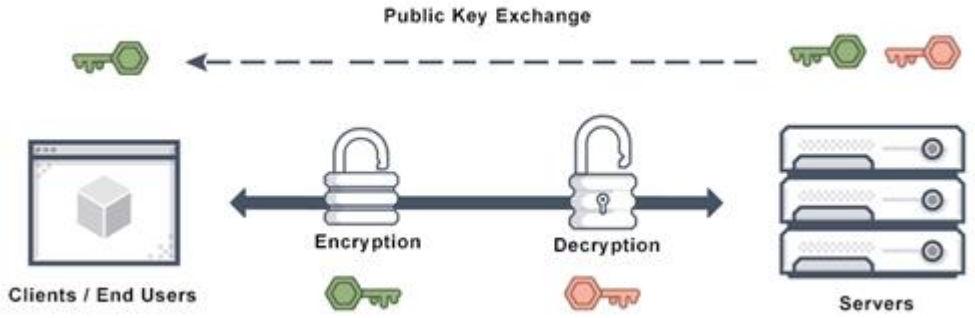
NAIT

Edmonton **Alberta**

CYBR3010

Cybersecurity Foundations

Application Layer Security



Student:_____

Application Layer Security

Objectives

This lab is a practical exercise in configuring SSL inspection using a virtual firewall appliance.

At the end of this activity students will be able to demonstrate their abilities to create SSL rules and understand how traffic is decrypted, then inspected, again encrypted, and sent to end client on a firewall appliance of your choosing.

For this lab, use the following components:

- **Virtual Network Environment**: Use either **CML** or **VMware** for your virtualized setup. The **Lab3 environment** can be used as a starting point for this lab.
- **Windows Client**: Set up a Windows client environment with appropriate configurations.
- **Virtual Firewall**: Configure a virtual firewall to manage and inspect SSL traffic in the network.

Instructions:

1- **Design and implement a network to set up and demonstrate SSL inspection, including the following steps:**

- Con figure IP addressing all VMs and verify network connectivity.
- Set up SSL inspection on the firewall.
- Show case client web browser response before and after injecting the certificate to the client.
- Use Wireshark to capture any SSL traffic and demonstrate how it can be decrypted.

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

- Explain the process of SSL/TLS interception and include how certificates are handled and the role of root certificate authorities in maintaining trust.
- What technical challenges can occur during SSL/TLS inspection (e.g., certificate pinning, encrypted SNI, performance overhead)? Propose potential solutions or workarounds for these issues.
- How does SSL/TLS inspection intersect with data privacy laws and compliance requirements such as GDPR, HIPAA, or PIPEDA? Provide examples of scenarios where SSL inspection might be restricted or prohibited.

Deliverables

PDF Document with screenshots and explanations:

- **An introduction:** briefly describe the goal of the lab and outline what the lab will cover.
- **Step-by-Step Configuration:** An explanation of steps performed to configure your environment.
- A network diagram of the final build.
- SSL Inspection: Include screenshots **before** and **after** applying the firewall's SSL certificate.
- Wireshark SSL Decryption: Provide Wireshark screenshots **before** and **after** decryption, highlighting SSL traffic and the decrypted payload.
- Answers to the questions 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.