MARCH EVENTS

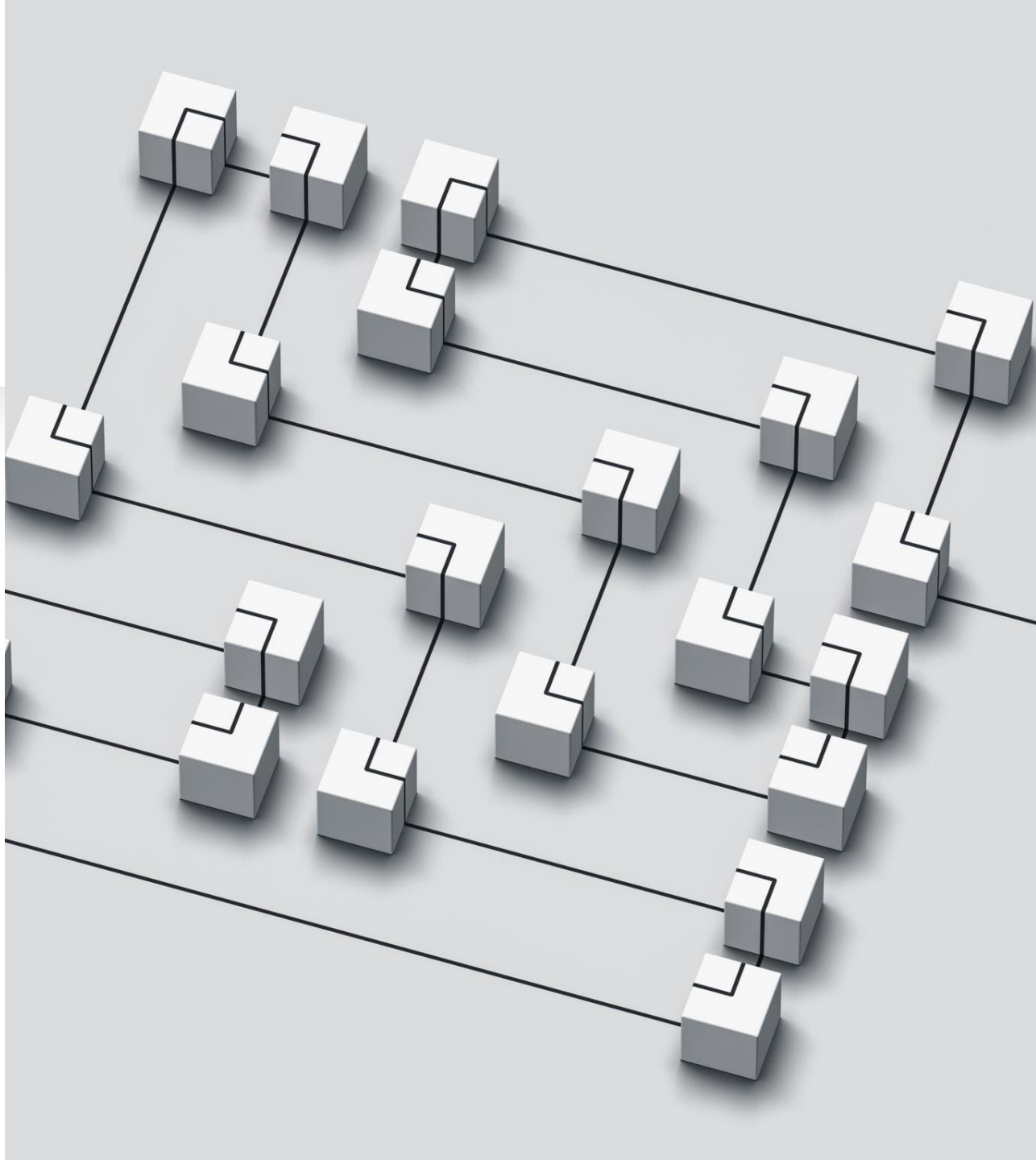
MAR 4	**ACADEMY UP: CLOUD FOUNDATIONS** 6:00pm to 8:00m Kenneth C Rowe Management Building
MAR 4	**SHIFTKEY LOUNGE: ENTREPRENEURSHIP** 6:00pm-7:00pm Goldberg Computer Science Building
MAR 5	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 6	**WOMEN'S EXCELLENCE GALA** 5:00pm to 7:00pm Dalhousie Student Union Building
MAR 12	**INDUSTRY SHOWCASE: AVANADE** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 12	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 13	**INDUSTRY SHOWCASE: RBC** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 15	**SNOWBALL AWARDS** 5:00pm to 11:30pm The Westin Nova Scotian
MAR 17	**HAPPY SAINT PATRICK'S DAY**
MAR 18	**SHIFTKEY LOUNGE: FINTECH** 6:00pm to 7:00pm Goldberg Computer Science Building
MAR 19	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 20	**SPEECH CRAFT WORKSHOP** 5:30pm to 8:30pm Goldberg Computer Science Building
MAR 22	**CONSULTING 101 WORKSHOP** 1:00pm to 5:00pm Goldberg Computer Science Building
MAR 24	**ALUMNI SPEAKS: ANDRES COLLART** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 26	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 28	**INDUSTRY SHOWCASE: VOLTA** 4:00 pm to 5:30pm Goldberg Computer Science Building

Instructor: Aman Bhalla

Learning Objectives

By the end of this session, you will:

- Understand **network security principles** (firewalls, IDS/IPS, VPNs).
- Differentiate between **encryption methods** (symmetric vs. asymmetric).
- Learn best practices for **authentication & secure communication**.
- **Analyze encrypted vs. unencrypted network traffic** using online tools.



What is Network Security?

Definition: Network security is the practice of **protecting data, devices, and systems** from cyber threats by controlling access and monitoring network activity.

- Prevents **unauthorized access** to sensitive data.
- Ensures **data integrity** (no tampering).
- Maintains **availability** (systems stay online).

Example:

- **A remote data centre** without security cameras or alarms. **Network security** is the digital equivalent—without it, attackers can easily steal or manipulate data.

Key Network Security Components

1. **Firewalls** – Act as **digital barriers** between networks.
2. **Intrusion Detection/Prevention Systems (IDS/IPS)** – Detect & block malicious activities.
3. **Virtual Private Networks (VPNs)** – Encrypt internet traffic for **secure remote access**.
4. **Secure Communication Protocols (HTTPS, SSL/TLS)** – Protects data in transit.

Firewalls – The First Line of Defense

Definition: A **firewall** is a security system that **monitors** and **controls** incoming and outgoing network traffic based on security rules.

- **Blocks unauthorized access** while allowing legitimate communication.
- Can be **hardware**, **software-based** or **cloud-based**.
- Protects against **malware, hackers,** and **phishing attacks**.

IDS vs. IPS

What's the Difference?

- **IDS (Intrusion Detection System):** Monitors & **Alerts** – Detects suspicious activity but **does not block it**.
- **IPS (Intrusion Prevention System):** Monitors & **Blocks** – Detects and **automatically stops threats**.

How They Work:

- **IDS**: Passive – Logs threats, alerts security teams.
- **IPS**: Active – Blocks malicious traffic in real time.

Example:

- **IDS:** Notifies about a hacker scanning the network.
- **IPS:** Detects & **blocks** the hacker's attempt instantly.

Which One is Better?

- **IDS** = Great for monitoring & analysis.
- **IPS** = Better for real-time attack prevention.
- **Best practice?** Use **both** for layered security.

Discussion: *Would you rather detect or prevent threats? Why?*

Encryption & Data Security

Definition: Encryption converts readable data (**plaintext**) into an unreadable format (**ciphertext**) to prevent unauthorized access.

Types of Encryption:

- **Symmetric Encryption** – Uses the **same key** for encryption & decryption (e.g., AES).
- **Asymmetric Encryption** – Uses a **public key for encryption** and a **private key for decryption** (e.g., RSA).

Introduction to VPNs – What & Why?

What is a VPN?

- A **Virtual Private Network (VPN)** encrypts internet traffic, making it unreadable to hackers.
- It creates a **secure "tunnel"** between your device and the internet.
- Hides your **IP address**, keeping your online activity private.

Why Use a VPN?

- **Protects data on public Wi-Fi** – Prevents hackers from stealing your information.
- **Hides your online identity** – Websites and advertisers can't track your real location.
- **Encrypts your internet traffic** – Even if intercepted, data is unreadable.

Example:

- Logging into **your bank account on public Wi-Fi** without a VPN can expose your credentials.

How VPNs Work & When to Use One

How Does a VPN Work?

- Encrypts your internet traffic so **hackers can't see what you're doing**.
- Routes your connection through a **secure VPN server** before reaching the internet.
- **Changes your IP address** to protect your location and identity.

When Should You Use a VPN?

- **On Public Wi-Fi** (cafés, airports, hotels).
- **When Accessing Sensitive Accounts** (banking, work emails).
- **When Bypassing Geo-Blocked Content** (e.g., restricted websites).

VPN Limitations:

- VPNs don't protect against **malware or phishing attacks**.
- Some **free VPNs log** and **sell your data** – use trusted providers!
- VPNs can slow down your internet speed due to encryption.

Secure Communication Protocols (HTTPS, SSL/TLS)

HTTPS (Hypertext Transfer Protocol Secure): Ensures data exchanged between a browser and website **remains encrypted**.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Encrypts data during online transactions.

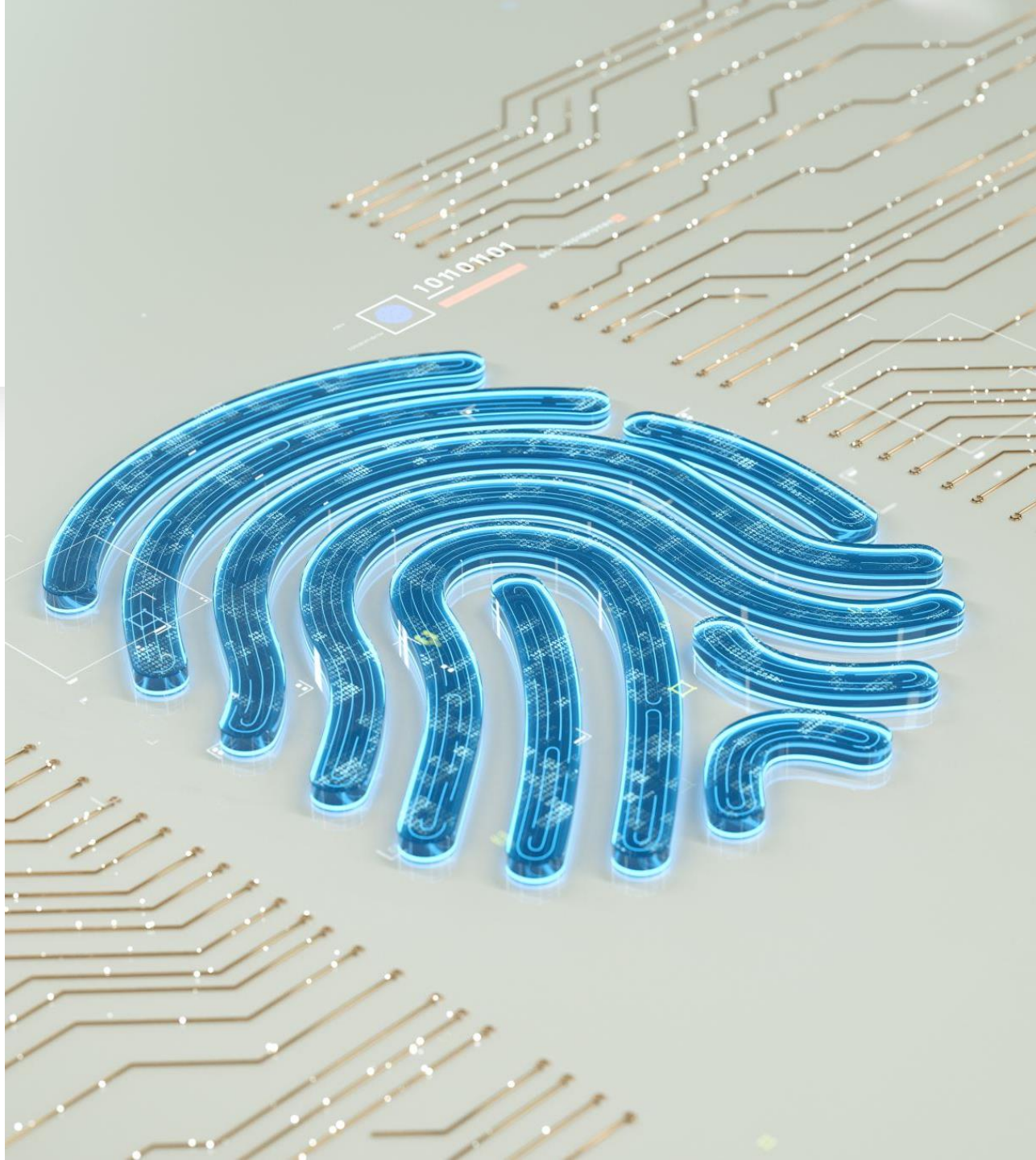
Example: Websites with a 🔒 **lock symbol** use HTTPS, protecting login credentials from being stolen.

Team Activity – Build A Secure Network

Authentication & Multi-Factor Authentication (MFA)

Definition: Authentication ensures **only authorized users** can access a system.

- **Single-Factor Authentication (SFA):** Password-only login (least secure).
- **Multi-Factor Authentication (MFA):** Requires an extra security step (e.g., phone code).
- **Biometric Authentication:** Uses fingerprints or facial recognition.



Q&A & Discussion

Do you use Multi-Factor Authentication (MFA)? Why or why not?

What happens if an attacker steals unencrypted data?

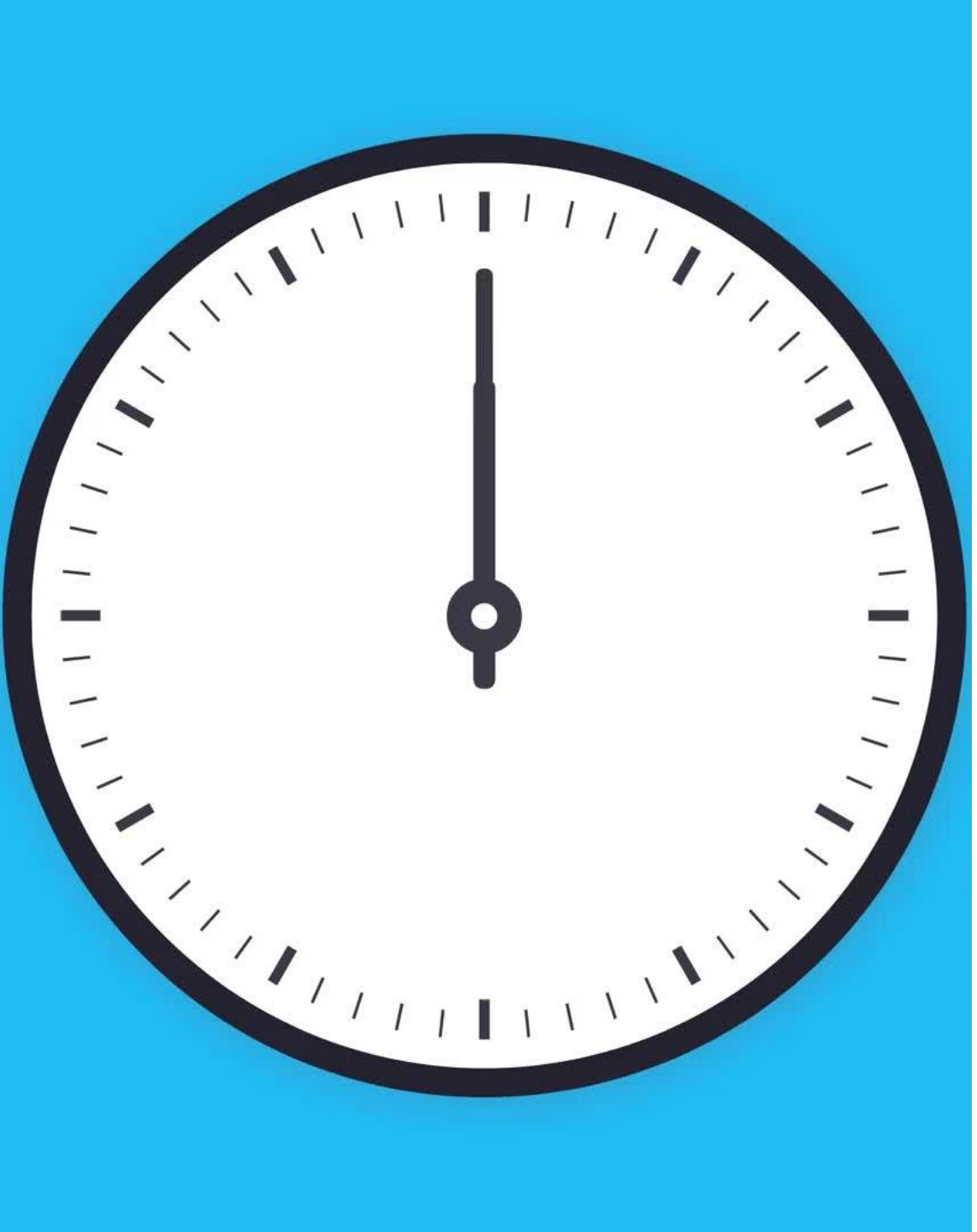
What was the most interesting aspect of Network Security to you? Why?

Key Takeaways

- Firewalls & IDS/IPS protect networks from cyber threats.
- Encryption ensures data security, both in transit & at rest.
- MFA and strong authentication prevent unauthorized access.

Week 3 Preview

- Secure Software Development & **OWASP Top 10**
- Incident Response & Threat Intelligence
- Practical Activity: **Web Application Scanning with OWASP ZAP**



Quiz Time!

- Time Limit – 15 Minutes. Quiz begins at 7:45 pm and will close at 8:00 pm.
- Questions: MCQ’s, True or False and Short Answer.