Introduction to Cybersecurity

Hamideh Baharlouei

PhD Candidate at Dalhousie University

Cybersecurity, Machine Learning, and Vehicular Networks Specialist

Enhancing Security in VANETs and IoT

Where you can find me?

www.linkedin.com/in/hamideh-baharlouei-510a0441

hm729953@dal.ca

Introduction to the Course Structure and Objectives

- **Session1: Introduction to Cybersecurity**
  - **Objective:** To introduce students to the fundamentals of cybersecurity, including terminology, types of threats, and basic defense mechanisms.
- **Session 2: Network Security Fundamentals**
  - **Objective:** To understand network security concepts and practice securing network infrastructure.
- **Session 3: System Security and Secure Configuration**
  - **Objective:** To explore system security, identify common vulnerabilities, and practice securing the systems.
- **Session 4: Incident Response and Penetration Testing**
  - **Objective:** To understand the importance of incident response, develop incident handling skills, and learn best practices in penetration testing.

Goals

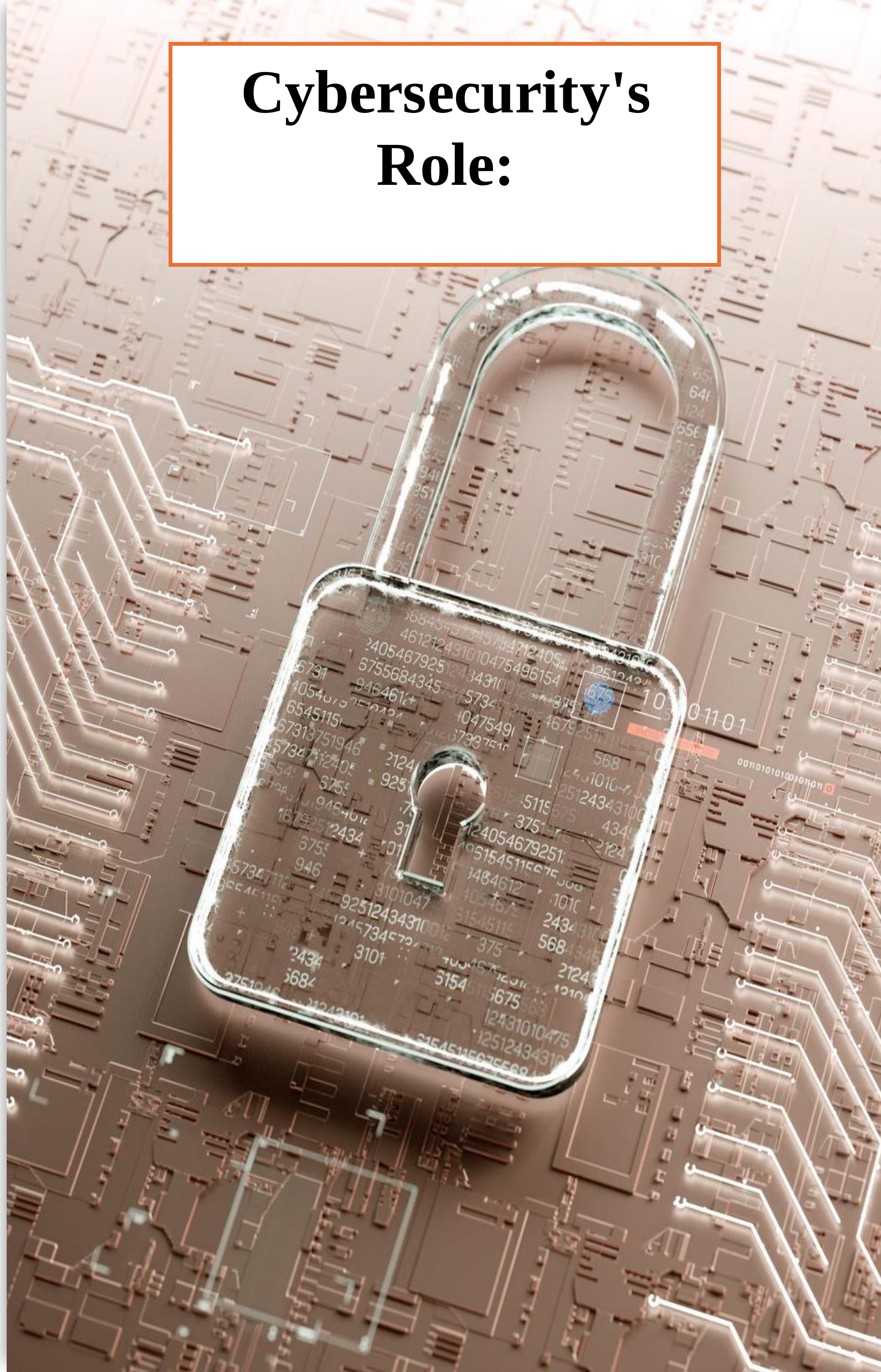
- **Knowledge Acquisition:**
  - Gain a foundational understanding of cybersecurity concepts and practices.
- **Practical Skills:**
  - Develop hands-on skills in network scanning, system hardening and penetration testing.
- **Awareness:**
  - Increase awareness of the current threat landscape and the importance of cybersecurity in protecting information and systems.

Expectations

- **Participation:**
  - Actively participate in discussions, hands-on exercises, and group activities.
- **Application:**
  - Apply the knowledge and skills learned in real-world scenarios and projects.
- **Continuous Learning:**
  - Stay curious and keep learning about new threats and security practices even after the course.

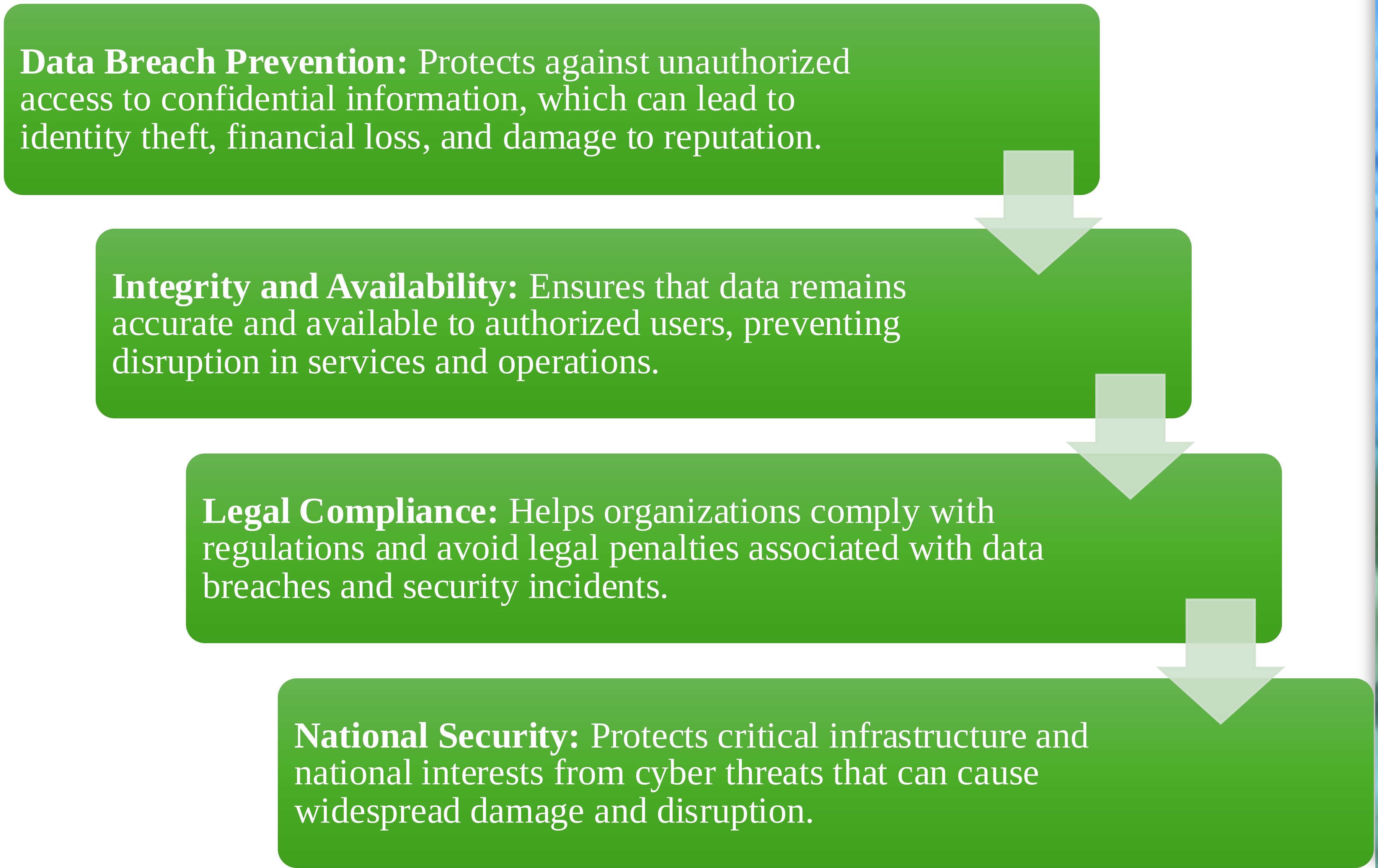
Importance of Cybersecurity in Today's Digital World

- **Protection of Information:** Safeguarding sensitive information from unauthorized access and breaches.
- **Business Continuity:** Ensuring that businesses can continue to operate smoothly without disruptions caused by cyber-attacks.
- **Trust:** Maintaining the trust of customers, partners, and stakeholders by protecting their data and privacy.
- **Economic Stability:** Protecting the economy from the financial impacts of cybercrime, which can amount to billions of dollars annually.



Cybersecurity's Role:

Importance of Protecting Information and Systems:



Data Breach Prevention: Protects against unauthorized access to confidential information, which can lead to identity theft, financial loss, and damage to reputation.

Integrity and Availability: Ensures that data remains accurate and available to authorized users, preventing disruption in services and operations.

Legal Compliance: Helps organizations comply with regulations and avoid legal penalties associated with data breaches and security incidents.

National Security: Protects critical infrastructure and national interests from cyber threats that can cause widespread damage and disruption.

Overview of Cybersecurity Domains 1

- **Network Security:**
  - Protects the integrity, confidentiality, and availability of data as it is transmitted over or accessed through a network.
  - Techniques include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and virtual private networks (VPNs).
- **Application Security:**
  - Ensures that applications are secure from threats throughout their lifecycle.
  - Involves practices like secure coding, code reviews, and penetration testing.
- **Information Security:**
  - Protects data from unauthorized access, disclosure, alteration, and destruction.
  - Encompasses encryption, access controls, and data masking.

Overview of Cybersecurity Domains 2

- **Operational Security:**
  - Focuses on the processes and decisions for handling and protecting data assets.
  - Includes incident response planning, disaster recovery, and business continuity planning.
- **Identity and Access Management (IAM):**
  - Manages users' identities and their access to systems and data.
  - Involves authentication, authorization, and accounting (AAA) mechanisms.
- **Endpoint Security:**
  - Protects individual devices such as computers, mobile devices, and IoT devices.
  - Techniques include antivirus software, endpoint detection and response (EDR), and mobile device management (MDM).

Definition of Cybersecurity

- **Cybersecurity**: Protecting systems, networks, and programs from digital attacks that aim to access, alter, or destroy sensitive information, extort money, or disrupt business processes.

- **Threat**: Any circumstance or event capable of causing harm to a system or organization, such as malware, phishing, insider threats, or natural disasters.

- **Vulnerability**: A weakness in a system, network, or application that can be exploited to gain unauthorized access or cause harm, like unpatched software or weak passwords.

- **Risk**: The potential for loss or damage when a threat exploits a vulnerability, assessed by the likelihood and impact of the event.

Current State of the Cybersecurity Industry

- **Increasing Cyber Threats:** Cyber threats are becoming more sophisticated and frequent, with attackers using advanced techniques to bypass security measures.

- **Skill Shortage:** There is a significant shortage of skilled cybersecurity professionals, making it challenging for organizations to defend against threats effectively.

- **Regulatory Pressure:** Governments and regulatory bodies are imposing stricter regulations to ensure organizations protect their data and systems adequately.

- **Technological Advancements:** Rapid advancements in technology, such as cloud computing, IoT, and AI, are creating new security challenges and opportunities.

- **Awareness and Education:** Increasing awareness and education efforts are crucial in building a culture of cybersecurity within organizations and society at large.

CIA Triad (Confidentiality, Integrity, Availability)

- **Confidentiality:**
  - Ensures that information is accessible only to those authorized to have access.
  - Techniques: encryption, access controls, and authentication methods.
  - **Example:** Encrypting sensitive emails to prevent unauthorized reading.
- **Integrity:**
  - Ensures that information is accurate, reliable, and not tampered with.
  - Techniques: hash functions, checksums, digital signatures, and backups.
  - **Example:** Using digital signatures to ensure a software update has not been tampered with.
- **Availability:**
  - Ensures that information and resources are accessible to authorized users when needed.
  - Techniques: redundancy, fault tolerance, load balancing, and disaster recovery planning.
  - **Example:** Redundant servers ensures service availability during hardware failure.

Balancing CIA Principles in Real-World Scenarios

Hospital:

- It must ensure the availability of patient records (availability) while protecting sensitive patient information (confidentiality) and ensuring the accuracy of medical data (integrity).
- **Case Study:** During the COVID-19 pandemic, many organizations had to rapidly shift to remote work. This required balancing the confidentiality of sensitive information (ensuring secure remote access), the integrity of data being shared and stored remotely, and the availability of services and data to remote employees.

Threat Landscape: Malware

Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.

- **Viruses:** Programs that attach to legitimate files and spread upon execution.
- **Worms:** Self-replicating programs that spread through networks without file attachment.
- **Trojans:** Malicious programs posing as legitimate software that create backdoors for attackers.
- **Ransomware:** Malware that encrypts a user's files and demands a ransom to restore access.
- **Spyware:** Software that secretly gathers information about a person or organization.
- **Adware:** Software that automatically displays or downloads advertising material.

Threat Landscape: Phishing

Definition: Phishing is a technique used by cybercriminals to trick individuals into providing sensitive information by masquerading as a trustworthy entity.

- **Techniques:**
  - **Email Phishing:** Fraudulent emails that appear to come from reputable sources.
  - **Spear Phishing:** Targeted phishing aimed at specific individuals or organizations.
  - **Whaling:** Phishing attacks aimed at senior executives and high-profile individuals.
  - **Smishing:** Phishing via SMS text messages.
  - **Vishing:** Phishing through voice calls.
- **Recognition:**
  - Look for suspicious email addresses and domain names.
  - Be wary of urgent or threatening language.
  - Check for spelling and grammatical errors.
  - Hover over links to check their actual URLs.
- **Prevention:**
  - Use email filters and anti-phishing software.
  - Educate employees on recognizing phishing attempts.
  - Implement multi-factor authentication (MFA).
  - Regularly update and patch software.

Threat Landscape: Ransomware

Ransomware encrypts the victim's files or locks them out of their systems, then demands a ransom, usually in cryptocurrency, for the decryption key or access restoration.

- **Impact on Businesses and Individuals:**
  - **Businesses:** Operational disruptions, financial loss, reputational damage, and potential legal consequences.
  - **Individuals:** Loss of personal data, financial loss, and emotional distress.
- **Prevention:**
  - Regularly back up data and store backups offline.
  - Keep software and systems updated with the latest patches.
  - Educate users on safe email and web browsing practices.
  - Implement strong security measures such as firewalls and endpoint protection.
- **Response:**
  - Isolate affected systems to prevent further spread.
  - Report the attack to relevant authorities.
  - Restore data from backups if available.
  - Consider paying the ransom as a last resort, understanding that it does not guarantee data recovery.

Threat Landscape: Other Threats

- **Insider Threats:**
  - **Definition**: Threats from within the organization, such as employees, contractors, or partners.
  - **Examples**: Data theft, sabotage, espionage.
- **DDoS Attacks (Distributed Denial of Service):**
  - **Definition**: Overwhelming a network or service with internet traffic, making it unavailable.
- **SQL Injection:**
  - **Definition**: Inserting malicious SQL statements into an entry field to access or manipulate the database.
- **Zero-Day Exploits:**
  - **Definition**: Exploiting unknown vulnerabilities before they are patched.

Attack Vectors and Methods1

Common Attack Vectors:

Email: Phishing, malicious attachments, and links.

Web: Drive-by downloads, cross-site scripting (XSS), and SQL injection.

Network: Man-in-the-Middle (MitM) attacks, IP spoofing, and network sniffing.

Social Engineering: Psychological manipulation to trick users into divulging information or performing actions.

Physical Access: Theft or tampering with physical devices.

Attack Vectors and Methods2

Methods Used by Attackers:

Exploitation: Taking advantage of vulnerabilities in software, hardware, or human behavior.

Privilege Escalation: Gaining higher levels of access to systems or data than initially authorized.

Lateral Movement: Moving within a network to gain further access and control over additional systems.

Example Scenarios Illustrating Different Attack Vectors:

Email Phishing Attack:

- An employee receives an email appearing to be from the IT department, requesting password confirmation. Clicking the link leads to a fake login page, capturing the employee’s credentials.

Web-Based Attack:

- A user visits a compromised website that downloads malware onto their system without their knowledge (drive-by download).

Network Attack:

- An attacker uses a MitM attack to intercept and alter communications between two parties, gaining access to sensitive information.

Social Engineering Attack:

- An attacker poses as a maintenance worker to gain physical access to an office, then installs keyloggers on computers to capture login credentials.

Notable Cyber-Attacks: Target Data Breach (2013)

- **Attack Timeline and Methods Used:**
  - **Initial Compromise:** Attackers gained access through a third-party vendor by stealing their credentials.
  - **Malware Deployment:** It was installed on Target's point-of-sale (POS) systems to collect payment card data.
  - **Data Exfiltration:** The stolen data was transferred to external servers controlled by the attackers.
- **Impact on the Organization and Affected Individuals:**
  - **Organization:** Target faced a massive financial impact, including costs related to legal fees, settlements, and security improvements, totaling over $200 million. The breach also damaged Target's reputation and led to executive resignations.
  - **Individuals:** Approximately 40 million credit and debit card accounts were compromised, along with personal information of 70 million customers.
- **Response and Mitigation Strategies:**
  - Target enhanced its security measures, including implementing chip-and-PIN technology for payment cards, increasing monitoring and detection capabilities, and conducting extensive security audits.
  - Publicly communicated the breach and cooperated with law enforcement agencies.

Notable Cyber-Attacks: Equifax Data Breach (2017)

- **Attack Timeline and Methods Used:**
  - **Initial Compromise:** Attackers exploited a vulnerability in the Apache Struts web application framework used by Equifax.
  - **Data Access:** Once inside, attackers accessed sensitive information, including names, Social Security numbers, birth dates, addresses, and some driver's license numbers.
  - **Data Exfiltration:** Data was extracted over several weeks before the breach was discovered.
- **Impact on the Organization and Affected Individuals:**
  - **Organization:** Equifax incurred costs exceeding $1.4 billion related to response efforts, settlements, and fines. The breach severely damaged Equifax’s reputation and trust.
  - **Individuals:** Around 147 million people were affected, one of the largest data breaches in history. The compromised information put individuals at risk of identity theft and fraud.
- **Response and Mitigation Strategies:**
  - Free credit monitoring services to affected customers and enhanced its cybersecurity infrastructure.
  - The company improved its patch management processes and security posture.

Notable Cyber-Attacks: WannaCry Ransomware Attack (2017)

- **Attack Timeline and Methods Used:**
  - **Initial Spread:** It utilized a vulnerability in the Windows OS to quickly spread through networks.
  - **Malware Execution:** Encrypted files on infected systems and demanded ransom payments in Bitcoin to decrypt the files.
  - **Propagation:** The worm-like behavior allowed it to spread quickly to unpatched systems globally.
- **Impact on the Organization and Affected Individuals:**
  - **Organizations:** impacted numerous organizations globally, such as the UK’s National Health Service, severe operational disruptions and financial losses. Global damages: billions of dollars.
  - **Individuals:** Data loss and potential financial losses if they chose to pay the ransom.
- **Response and Mitigation Strategies:**
  - Organizations implemented emergency patching and used backup systems to restore affected data.
  - Microsoft released patches for unsupported versions of Windows to help contain the spread.
  - Collaboration with law enforcement and cybersecurity firms to mitigate the impact and prevent further infections.

Key Takeaways from Each Case Study:

- **Target Data Breach:**
  - Third-party vendors can be a significant risk; ensure they follow strong security practices.
  - Implement network segmentation to limit attackers' lateral movement.
  - Early detection and response capabilities are crucial to mitigating damage.
- **Equifax Data Breach:**
  - Patch management is critical; promptly apply security patches to prevent exploitation.
  - Continuous monitoring and threat detection can help identify breaches early.
  - Transparency and effective communication with stakeholders are essential in managing breach response.
- **WannaCry Ransomware Attack:**
  - Regularly update and patch systems to protect against known vulnerabilities.
  - Maintain robust backup solutions and ensure they are tested regularly.
  - Need for global cooperation and information sharing in response to widespread cyber-attacks.

How to Apply These Lessons to Improve Cybersecurity Posture:

- **Third-Party Risk Management:**
  - Conduct thorough security assessments of third-party vendors and continuously monitor them.
- **Patch Management and Vulnerability Remediation:**
  - Implement an effective patch management process to ensure all systems are up-to-date.
  - Use automated tools to identify and remediate vulnerabilities quickly.
- **Network Segmentation and Isolation:**
  - Segment networks to limit the spread of malware and restrict access to sensitive data.
  - Implement access controls and monitor network traffic for unusual activity.
- **Continuous Monitoring and Incident Response:**
  - Deploy advanced monitoring tools to detect and respond to threats in real-time.
  - Develop and regularly test incident response plans to ensure quick and effective response.
- **Employee Education and Awareness:**
  - Conduct regular cybersecurity training and awareness programs to educate employees.
  - Promote a security-conscious culture within the organization.

Key Takeaways:

- **Fundamentals of Cybersecurity:**
    - Importance of protecting information, systems, and networks from digital attacks.
    - Key terms: threats, vulnerabilities, risks.
- **Types of Cyber Threats:**
    - Common threats include malware, phishing, man-in-the-middle attacks, and denial-of-service attacks.
    - Real-world examples illustrate the impact of these threats.
- **Basic Defense Mechanisms:**
    - Essential security measures: firewalls, antivirus software, intrusion detection systems, encryption.
    - Importance of secure configuration and regular updates.
- **Importance of Cybersecurity:**
    - Ensuring confidentiality, integrity, and availability of data.
    - Implications of breaches: financial loss, reputational damage, legal consequences.
    - **Looking Ahead:**
- **Next Session:** Network Security Fundamentals.

White Hat Hacker

Hands-on exercise:

- Kali Linux
- GNS3
- Wireshark
- Other tools...