Month 1: Foundations of Cybersecurity

Week 1: Introduction to Cybersecurity

- **Topics:**
  - What is Cybersecurity?
  - Importance of Cybersecurity in the Modern World
  - Cybersecurity Domains (Confidentiality, Integrity, Availability)
- **Activities:**
  - Group discussion on recent cybersecurity incidents.
  - Introduction to key cybersecurity terms and concepts.

Week 2: Threat Landscape

- **Topics:**
  - Types of Cyber Threats (Malware, Phishing, Social Engineering)
  - Attack Vectors (Network, Application, User)
  - Understanding the Adversary: Cybercriminals, Hacktivists, Nation-States
- **Activities:**
  - Case studies on common cyber threats.
  - Analyzing attack vectors through examples.

Week 3: Introduction to Cybersecurity Frameworks and Standards

- **Topics:**
  - Overview of Cybersecurity Frameworks (NIST, ISO 27001)
  - Security Controls and their Importance
  - Compliance and Regulatory Requirements (GDPR, HIPAA)
- **Activities:**
  - Discussion on the importance of compliance.
  - Analyzing case studies on compliance failures.

Week 4: Basics of Networking for Cybersecurity

- **Topics:**
  - Network Fundamentals (TCP/IP, DNS, Firewalls)
  - Network Security Basics (VPNs, Intrusion Detection Systems)
  - Common Network Attacks (DDoS, Man-in-the-Middle)
- **Activities:**
  - Lab: Simulating a simple network attack.

Month 2: Core Cybersecurity Concepts

Week 5: Introduction to Cryptography

- **Topics:**
    - What is Cryptography?
    - Encryption and Decryption Methods
    - Symmetric vs Asymmetric Encryption
- **Activities:**
    - Lab: Using encryption tools (e.g., AES encryption).
    - Group activity: Analyzing encrypted messages.

Week 6: Secure System Design

- **Topics:**
    - Principles of Secure Design
    - Access Control Models (RBAC, MAC, DAC)
    - Secure Software Development Lifecycle(SDLC)
- **Activities:**
    - Case study: Analyzing a secure software design.
    - Discussion: Secure coding practices.

Week 7: Identity and Access Management (IAM)

- **Topics:**
    - Importance of IAM in Cybersecurity
    - Authentication and Authorization Methods
    - Multi-Factor Authentication (MFA)
- **Activities:**
    - Lab: Implementing MFA.
    - Group discussion on IAM best practices.

Week 8: Cybersecurity Tools and Techniques

- **Topics:**
    - Overview of Common Cybersecurity Tools (Antivirus, SIEM, IDS/IPS)
    - Basics of Vulnerability Scanning and Penetration Testing
    - Incident Response Overview
- **Activities:**
    - Lab: Running a vulnerability scan.
    - Introduction to penetration testing tools.

Month 3: Application of Cybersecurity Knowledge

Week 9: Risk Management and Incident Response

- **Topics:**
    - Introduction to Risk Management (Risk Assessment, Mitigation)
    - Incident Response Lifecycle (Preparation, Detection, Containment, Recovery)

    - Incident Handling Best Practices
- **Activities:**
    - Presentation: Conducting a mock risk assessment.
    - Incident response simulation exercise.

Week 10: Security Awareness and Training

- **Topics:**
    - Importance of Security Awareness
    - Phishing Awareness and Email Security
    - Building a Security-Aware Culture
- **Activities:**
    - Creating a security awareness campaign.
    - Role-playing common social engineering scenarios.

Week 11: Legal, Ethical, and Social Implications of Cybersecurity

- **Topics:**
    - Cybersecurity Laws and Regulations (Data Protection, Cybercrime)
    - Ethical Hacking and its Importance
    - Privacy Concerns in Cybersecurity
- **Activities:**
    - Presentation on privacy vs. security.
    - Case study: Analyzing legal and ethical cybersecurity issues.

Week 12: Capstone Project and Review

- **Capstone Project:**
    - Students will work on a small project where they identify and propose solutions to a cybersecurity problem.
- **Review:**
    - Recap of the key concepts learned throughout the course.
    - Final Q&A session.
    - Presentation of capstone projects