CYBER SECURITY SYLLABUS

Module 1: Foundation for Cyber Security

- Hacker
- Ethical Hacker
- Cyber-attacks:
    - Network Infrastructure Attacks
    - Operating System Attacks
    - Application and Other Specialized Attacks
- Security Assessment Principles

Module 2: Hacking Methodology

- Scanning the Systems and Network
- Attack Tree Analysis
- Assessing Vulnerabilities
- Penetration Testing
- Security Testing Tools

Module 3: Social Engineering

- Social Engineering Implications
- Performing Social Engineering Attacks
- Social Engineering Countermeasures:
    - Policies
    - User Awareness and Training
- Social Engineering Toolkit
- Physical Security

Module 4: Password Security

- Password Vulnerabilities
- Password Cracking Tools
  - Brute-force Attacks
  - Rainbow Attacks
- Password Cracking Countermeasures:
  - Password Policy
  - Securing Operating Systems
  - Keyloggers Tools

Module 5: Wireless and Mobile Security

- Wireless and Mobile Vulnerabilities and Attacks
- Encrypted Traffic and Countermeasures
- Rogue Wireless Devices and Countermeasures
- MAC Spoofing and Countermeasures
- Securing Wireless Workstations, Wi-Fi, and Internet of Things

Module 6: Operating System Security

- OS Vulnerabilities: Windows, Linux, and Mac
- Detecting Null Sessions
- Exploiting Missing Patches
  - Metasploit
  - Burp Suite
  - Overflow and NFS Attacks
- Countermeasures Against Buffer Overflow

Module 7: Web Application and Databases Security

- Web App Security:
  - Seeking Out Web Vulnerabilities

    - Directory Traversal
    - Input-Filtering Attacks
    - Code Injection, SQL Injection, Cross-Site Scripting
- Countermeasures
- Database Security:
    - Database Vulnerabilities
    - Minimizing Database Security Risks and Storage Security Risks
- Countermeasures and Tools