IICIS

6-Month Course

Cyber Security

www.iicis.org

24 Weeks (6 Months)

Job-ready skills in Cybersecurity, Ethical Hacking, SOC, and Digital Forensics

Instructor-led Classes + Hands-on Labs + Assignments + Case Studies

Module	Module Title
1	Foundations of Cybersecurity
2	Networking & Security Essentials
3	Ethical Hacking & Penetration Testing
4	SOC Operations
	Revision & Internal Assessment
5	Digital Forensics
6	Cloud & Advanced Security
7	Capstone Project & Final Exam
	Final Evaluation

Module 1: Foundations of Cybersecurity (Week 1–2)

Content:

- Introduction to Cybersecurity & Threat Landscape
- Security Triad: Confidentiality, Integrity, Availability (CIA)
- Cybersecurity Governance, Risk & Compliance (ISO 27001, GDPR, HIPAA basics)
- Linux & Windows Basics for Security Professionals
- Cybersecurity Terminology & Roles (SOC Analyst, Pen Tester, Forensic Investigator)

Labs:

1. Harden a Linux server (disable root login, configure SSH).
2. Create and enforce Group Policies in Windows.
3. Patch vulnerabilities using OpenVAS & WSUS.
4. Deploy and test EDR solutions.
5. Simulate privilege escalation attack & mitigation.

Module 2: Networking & Security Essentials (Week 3–4)

Content:

- Networking Fundamentals: TCP/IP, OSI Model, Routing, Switching
- Firewalls, IDS/IPS, VPNs, Proxy Servers, Load Balancers
- Common Attack Vectors: Phishing, Malware, Ransomware, Insider Threats
- Network Segmentation & Security Best Practices

Labs:

1. Packet analysis using Wireshark
2. Simulate firewall rules & network access control
3. Identify anomalies in sample network traffic

Module 3: Ethical Hacking & Penetration Testing (Week 5–10)

Content:

- Introduction to Ethical Hacking: Phases & Legal Scope
- Reconnaissance & Footprinting: OSINT, Whois, Shodan, Maltego
- Scanning & Enumeration: Nmap, Nessus, OpenVAS
- Exploitation Tools: Metasploit, Burp Suite, SQLMap
- Privilege Escalation & Maintaining Access
- Web Application Security: OWASP Top 10, SQLi, XSS, CSRF
- Wireless & IoT Security Basics

Labs:

1. Capture the Flag (CTF) Challenges
2. Vulnerability scanning & exploitation exercises
3. Web app hacking in controlled lab environment

Module 4: SOC Operations (Week 11–14)

Content:

- Introduction to Security Operations Center (SOC)
- SIEM Tools: Splunk, ELK Stack, QRadar, Azure Sentinel
- Incident Response Workflow & Playbooks
- Threat Intelligence & Log Analysis Basics
- Threat Hunting & Alert Prioritization

Labs:

1. Simulate attacks and monitor in SIEM
2. Create dashboards & alerts in Splunk/ELK
3. Incident handling exercises

Module 5: Digital Forensics (Week 15–18)

Content:

- Computer Forensics & Chain of Custody
- File System & Disk Forensics (NTFS, FAT32, Ext4)
- Memory Forensics & Volatile Data Capture: FTK, Autopsy, Volatility
- Email & Network Forensics
- Investigating Logs & Artifacts

Case Study:

- Investigating a ransomware attack in an enterprise environment

Labs:

1. Disk imaging & forensic analysis using Autopsy
2. Memory dump analysis with Volatility
3. Recover deleted files & track user activity

Module 6: Cloud & Advanced Security (Week 19–22)

Content:

- Cloud Security Fundamentals: AWS, Azure, GCP
- Cloud Threats, Misconfigurations & Best Practices
- Identity & Access Management (IAM)
- Endpoint Detection & Response: CrowdStrike, Defender ATP
- Zero Trust Security Architecture & Principles
- Advanced Malware & Threat Hunting Techniques

Labs:

1. Secure a cloud VM instance (AWS/Azure)
2. Simulate phishing & ransomware mitigation
3. Configure IAM policies and access control

Module 7: Capstone Project & Final Exam (Week 23–24)

Capstone Project Options (Choose 1):

1. Perform Penetration Test on a simulated enterprise environment
2. Set up and monitor a SOC using SIEM tools
3. Investigate a forensic case study & submit report

- **Present findings & recommendations**
- **Final Assessment: Practical + Theoretical Exam**
- **Certification Awarded**