1-Year Advanced Diploma

Cyber Security and Digital Forensics

www.iicis.org

48 Weeks (1 Year)

Advanced Cybersecurity Specialist ready for roles like SOC Analyst, Penetration Tester, Digital Forensic Investigator.

Deep-dive + Hands-on Labs + Projects + Industry Internship

Module	Module Title
1	Cybersecurity & Networking Fundamentals
2	Operating Systems Security
3	Ethical Hacking & Penetration Testing
4	SOC & Incident Response
	Revision & Internal Assessment
5	Digital Forensics & Investigation
6	Advanced Security Domains
7	Emerging Technologies & Cyber Defense
8	Capstone, Internship & Career Prep
	Final Evaluation

Semester 1 (Month 1–6)– Core Cybersecurity Skills

Module 1 – Cybersecurity & Networking Fundamentals (Month 1)

Content:

- Cybersecurity Principles, CIA Triad, Security Models
- International Standards & Compliance (ISO 27001, NIST, GDPR, HIPAA, PCI-DSS)
- Networking Basics (TCP/IP, OSI Model, Routing & Switching)
- Perimeter Security: Firewalls, IDS/IPS, VPNs, Proxies
- Threat Intelligence, Risk Management & Threat Modeling
- Security Policies, Governance & Real-world Attack Case Studies

Labs:

1. Configure and test a Firewall (pfSense/iptables).
2. Set up an IDS/IPS using Snort or Suricata.
3. Create & test a VPN connection.
4. Perform Risk Assessment on a small simulated network.

Module 2: Operating Systems Security (Month 2)

Content:

- Linux Hardening & Security (SELinux, iptables, auditd)
- Windows Security (Group Policies, Active Directory Security)
- Patch & Vulnerability Management (WSUS, SCCM, OpenVAS)
- Endpoint Security (EDR, Antivirus, DLP, USB Control)
- Secure Shell, Privilege Escalation Prevention & Admin Controls

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 3: Ethical Hacking & Penetration Testing (Month 3–4)

Content:

- Phases of Ethical Hacking (Recon → Exploitation → Reporting)
- Recon & Scanning (Nmap, Shodan, OSINT tools)
- Vulnerability Assessment (Nessus, OpenVAS)
- Exploitation & Post Exploitation (Metasploit, Hydra, Empire)
- Web App Security (OWASP Top 10: SQLi, XSS, CSRF, RCE, File Uploads)
- Wireless & Mobile Security (Aircrack-ng, Wireshark, MobSF)
- Password Cracking, Social Engineering & Phishing Campaigns
- Bug Bounty Hunting Methodologies

Labs:

1. Perform Nmap scans on a target system.
2. Conduct OSINT using Maltego & Recon-ng.
3. Run a Vulnerability Scan using Nessus/OpenVAS.
4. Exploit a vulnerable web app (DVWA / Juice Shop).
5. Capture and crack Wi-Fi passwords with Aircrack-ng.
6. Create a phishing simulation using SEToolkit.
7. Write a penetration testing report.

Module 4: SOC & Incident Response (Month 5–6)

Content:

- SOC Design, Tiers, and Workflows
- SIEM Tools: Splunk, ELK Stack, IBM QRadar, Microsoft Sentinel
- Threat Hunting, IOC & IOA Identification
- Malware Analysis Basics (Static & Dynamic Analysis)
- Incident Response Lifecycle & Playbooks
- MITRE ATT&CK Framework & Cyber Kill Chain
- Case Studies of Major Breaches

Labs:

1. Deploy ELK/Splunk and create custom dashboards.
2. Ingest logs and detect suspicious activity.
3. Perform threat hunting using MITRE ATT&CK mapping.
4. Analyze a malware sample in a sandbox.
5. Create & execute an Incident Response Playbook.
6. Blue Team vs Red Team Simulation.

Semester 2 (Month 7–12): Advanced Cybersecurity & Forensics

Module 5: Digital Forensics & Investigation (Month 7–8)

Content:

- Cyber Laws, Chain of Custody & Forensic Standards
- Evidence Collection, Preservation & Reporting
- File System Analysis (Windows, Linux, FAT/NTFS/EXT)
- Disk Imaging & Data Recovery (Autopsy, FTK Imager, EnCase)
- Network Forensics (Wireshark, Zeek, Packet Analysis)
- Mobile Forensics (Android/iOS Tools – Cellebrite, Magnet AXIOM)
- Cloud Forensics & Logs Investigation
- Memory Forensics (Volatility)
- Anti-Forensics Techniques & Countermeasures

Labs:

1. Create disk images using FTK Imager.
2. Analyze deleted files with Autopsy.
3. Extract data from an Android device (MobSF).
4. Investigate insider threat logs.

Module 6: Advanced Security Domains (Month 9–10)

Content:

- Cloud Security & Shared Responsibility Model
- Security in AWS, Azure, GCP (IAM, Key Management, Logging)
- Identity & Access Management (IAM, MFA, PAM, SSO)
- Zero Trust Security & Threat Modeling
- Container & Kubernetes Security Basics
- DevSecOps & Secure CI/CD Practices
- Cloud Security Posture Management (CSPM)
- Red Team vs Blue Team Advanced Simulation

Labs:

1. Set up IAM roles & MFA in AWS.
2. Deploy secure storage using S3 with encryption.
3. Implement role-based access control in Azure.
4. Configure Zero Trust policies.
5. Secure a Kubernetes cluster.
6. Integrate DevSecOps security scans in CI/CD pipeline.

Module 7: Emerging Technologies & Cyber Defense (Month 11)

Content:

- AI & ML in Cybersecurity (Anomaly Detection, SOC Automation)
- Blockchain Security (Smart Contract Vulnerabilities, Crypto Forensics)
- Threat Intelligence Platforms & Dark Web Monitoring
- Cybersecurity in OT/ICS & IoT Security (SCADA, Smart Devices)
- Quantum Computing & its Impact on Cybersecurity
- AI-Powered Malware & Evasion Techniques

Labs:

1. Train a simple ML model for malware detection.
2. Perform smart contract vulnerability analysis.
3. Use a Dark Web monitoring tool (OnionScan).
4. Analyze logs from IoT devices for anomalies.
5. Simulate an attack on SCADA/ICS systems.

Module 8: Capstone, Internship & Career Prep (Month 12)

Content:

- Capstone Project (Choose 1):
    1. Full-Scale Penetration Test Report
    2. SOC Monitoring & Threat Hunting Project
    3. Forensic Investigation Report.
- Internship / Virtual Labs with Industry Scenarios
- Resume Building & Interview Preparation
- Certifications Mapping (CEH, CHFI, CompTIA Security+, SOC Analyst, Azure Security Engineer, OSCP/Practical Labs)
- Soft Skills for Cybersecurity Professionals (Communication, Documentation, Teamwork)
- Mock Interviews & Industry Mentorship

Labs:

1. Perform an end-to-end Penetration Test and submit a report.
2. Build SOC dashboards and threat hunting cases.
3. Conduct a complete forensic investigation of a compromised system.
4. Defend against a simulated APT attack.
5. Resume workshop & mock interviews.