

Cybersecurity Engineer – 100+ Lab Exercises (Basic, Intermediate, Advanced)

□ Basic Level (30+ Exercises)

Objective: Establish foundational knowledge of cybersecurity principles, threat landscape, and essential defensive practices.

Cybersecurity Fundamentals

- Understand cybersecurity concepts and terminologies.
- Explore the CIA triad (Confidentiality, Integrity, Availability).
- Identify common attack types: phishing, malware, ransomware.
- Study network basics: IP, TCP/IP, DNS, ports, and protocols.
- Use basic tools: Wireshark, Nmap for network scanning.

Operating System Security

- Understand Windows and Linux security fundamentals.
- Practice user and permission management.
- Secure file systems and disk encryption.
- Configure firewalls and security policies.
- Analyze system logs for suspicious activity.

Authentication & Access Control

- Implement strong password policies.
- Use multi-factor authentication (MFA).
- Study access control models: DAC, MAC, RBAC.
- Understand session management and timeout.
- Explore identity and access management (IAM) basics.

□ Intermediate Level (40+ Exercises)

Objective: Develop skills in penetration testing, vulnerability assessment, and incident response.



TRAINING TRAINS

IT Services and IT Consultancy \ Internship-Inplant Training \ Software Training Institute

96985 48633
90250 10144

உங்கள் கடை மற்றும் வியாபாரத்திற்கு ஏற்ற **Website & Andriod App** மற்றும் **Software** மிகச்சிறந்த முறையில் செய்து கொடுக்கப்படும்.

Expertise : **AI, Machine Learning & Data Science \ Cybersecurity & Ethical Hacking**
IoT, Blockchain & Cloud Computing \ Full Stack Web & Mobile Development
Digital Marketing & SEO

W3 App Developers 332, MULLAMPARAPPU, N.G.PALAYAM POST
ERODE - 638 115 **DomainHostly.COM**

Penetration Testing & Ethical Hacking

- Setup Kali Linux environment.
- Perform reconnaissance and footprinting.
- Conduct scanning and enumeration.
- Exploit common vulnerabilities (SQLi, XSS, CSRF).
- Use Metasploit framework for exploitation.

Vulnerability Management

- Perform vulnerability scanning using Nessus/OpenVAS.
- Prioritize vulnerabilities based on CVSS.
- Patch management strategies.
- Study OWASP Top 10 web vulnerabilities.
- Harden web servers and databases.

Network Security

- Configure VPNs and secure remote access.
- Implement IDS/IPS systems.
- Set up and analyze firewall rules.
- Detect and mitigate DDoS attacks.
- Use packet filtering and traffic analysis.

Incident Response & Forensics

- Develop incident response playbooks.
- Perform log analysis and threat hunting.
- Use forensic tools (Autopsy, FTK Imager).
- Recover compromised systems.
- Conduct root cause analysis and reporting.

□ Advanced Level (40+ Exercises)

Objective: Master advanced cybersecurity architecture, threat intelligence, and proactive defense strategies.

Advanced Threat Detection

- Implement Security Information and Event Management (SIEM).



TRAINING TRAINS

IT Services and IT Consultancy \ Internship-Inplant Training \ Software Training Institute

96985 48633
90250 10144

உங்கள் கடை மற்றும் வியாபாரத்திற்கு ஏற்ற **Website & Andriod App** மற்றும் **Software** மிகச்சிறந்த முறையில் செய்து கொடுக்கப்படும்.

Expertise : **AI, Machine Learning & Data Science \ Cybersecurity & Ethical Hacking**
IoT, Blockchain & Cloud Computing \ Full Stack Web & Mobile Development
Digital Marketing & SEO

W3 App Developers

332, MULLAMPARAPPU, N.G.PALAYAM POST
ERODE - 638 115

DomainHostly.COM

- Automate threat detection with SOAR platforms.
- Use threat intelligence feeds and indicators of compromise (IoCs).
- Analyze advanced persistent threats (APT).
- Develop honeypots and deception techniques.

Cryptography & Secure Communications

- Implement symmetric and asymmetric encryption.
- Use TLS/SSL certificates and PKI.
- Study blockchain security fundamentals.
- Secure email with PGP/GPG.
- Develop secure APIs using OAuth2 and JWT.

Cloud & Application Security

- Secure cloud environments (AWS, Azure, GCP).
- Implement container security best practices.
- Conduct secure code reviews and static analysis.
- Use DevSecOps tools for pipeline security.
- Study zero trust architecture.

Governance, Risk & Compliance

- Understand regulatory standards: GDPR, HIPAA, PCI-DSS.
- Develop risk management frameworks.
- Conduct security audits and compliance assessments.
- Design security policies and training programs.
- Manage third-party risk.

Capstone Projects

- Perform a full penetration test on a web application.
- Design and deploy a SOC (Security Operations Center).
- Create a cloud security monitoring solution.
- Develop an enterprise incident response and recovery plan.
- Implement a zero trust network architecture.

□ Tools & Technologies

- Kali Linux, Metasploit, Nessus, OpenVAS



TRAINING TRAINS

96985 48633
90250 10144

IT Services and IT Consultancy \ Internship-Inplant Training \ Software Training Institute

உங்கள் கடை மற்றும் வியாபாரத்திற்கு ஏற்ற **Website & Andriod App** மற்றும் **Software** மிகச்சிறந்த முறையில் செய்து கொடுக்கப்படும்.

Expertise : **AI, Machine Learning & Data Science \ Cybersecurity & Ethical Hacking**
IoT, Blockchain & Cloud Computing \ Full Stack Web & Mobile Development
Digital Marketing & SEO

W3 App Developers

332, MULLAMPARAPPU, N.G.PALAYAM POST
ERODE - 638 115

DomainHostly.COM

- Wireshark, Nmap, Burp Suite
- SIEM (Splunk, ELK Stack, QRadar)
- Cloud Security (AWS Security Hub, Azure Security Center)
- Cryptography Libraries (OpenSSL, GPG)