

Cyber Security Curriculum

Cyber security Fundamentals

- **Introduction to Cyber security:**
 - The evolution of Cyber security
 - Cyber security & situational awareness
 - The Cyber security skills gap
- **Difference between Information Security & Cyber security:**
 - Protecting digital assets
- **Cyber security objectives:**
 - Confidentiality, integrity, & availability
 - Nonrepudiation
- **Cyber security Roles:**
 - Governance, risk management, & compliance
 - What does a Cybersecurity professional do?
 - Information Security roles
 - Board of Directors
 - Executive management
 - Senior Information security management
 - Cyber security practitioners
- **Ethical Hacking:**
 - Types of Hackers
 - Phases of Ethical Hacking
- **NMAP:**
 - Basics of Networking
 - TCP and UDP protocols
 - 3-Way TCP Handshake
 - Ping and Ping Scan
 - Basics of NMAP
 - Shortcuts to save time in nmap



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

✓ **Hands-On /Demo:**

- How to spin up KALI Linux as virtual machine
- Dirbuster
- Gobuster
- Gathering information about Domain through Reon-ng Tool in Kali Linux
- Gathering information about Sub-domain through Sublist3r and dnsmap tool in Kali linux
- Host, nslookup and dig
- Gathering information about Domain through Maltego Tool
- DNS Footprinting using DNS Interrogation Tools

Cyber security Concepts

- **Risk:**

- Approaches to Cybersecurity
- Key terms & definitions
- Likelihood & impact
- Approaches to risk
- Third-party risk
- Risk management

- **Common Attack Types & Vectors:**

- Threat agents
- Attack attributes
- Generalized attack process
- Non-adversarial threat events
- Malware & attack types

- **Policies & Procedures:**

- Cyber Security Standards
- Business Continuity and Disaster Recovery
- Policy life cycle
- Guidelines
- Policy frameworks
- Types of Information Security policies
- Access control policy
- Personnel Information Security policy
- Security incident response policy



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Cyber security Controls:**
 - Identity management
 - Provisioning & de-provisioning
 - Authorization
 - Authentication
 - MBSA (Practical)
 - Tripwire (Practical)
 - Privileged user management
 - Change management
 - Configuration management
 - Patch management

Security Architecture Principles

- **Overview of security architecture:**
 - The security perimeter
 - Interdependencies
 - Security architectures & frameworks
 - SABSA & the Zachman framework
 - The open group architecture framework (TOGAF)
- **Computer Networks:**
 - Introduction to Computer Network
 - Computer Networks - Architecture
 - Layered architecture
- **The OSI model:**
 - TCP/IP
- **Hands-On/Demo:**
 - Identify the Network Routes in the System
 - DNS lookup and reverse lookup
 - Network Path tracing
 - Network Analysis
 - Network scanning
 - Enumeration



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Defense in Depth:**
- **Firewalls:**
 - Firewall general features
 - Network firewall types
 - Packet filtering firewalls
 - Stateful inspection firewalls
 - Stateless vs. stateful
 - Examples of firewall implementations
 - Firewall issues
 - Firewall platforms
 - Introduction to Honeypots
- **Isolation & segmentation:**
 - VLANs
 - Security zones & DMZs
- **Monitoring, Detection, and Logging:**
 - Ingress, egress, & data loss prevention (DLP)
 - Antivirus & anti-malware
 - Intrusion detection systems
 - IDS limitations
 - IDS policy
 - Intrusion prevention systems
 - Malware and its propagation ways
 - Malware components
 - Types of malware
 - Concept of sniffing
 - Types of sniffing attacks
 - SQL injection
 - DoS attack
 - DDoS attack
 - Common symptoms of DoS/DDoS attack
 - Categories of DoS/DDoS Attack Vectors
 - DoS/DDoS detection techniques
 - Session hijacking
 - Application level session hijacking
 - Network level session hijacking
 - Evading IDS



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- ✓ **Hands-On/Demo:**
 - DoS Attack using LOIC Tool
 - Cross-site Scripting attack
- ✓ **Hands-On/Demo:**
 - Create a trojan by using msfvenom
 - Sniff network packets Using Wireshark
 - MAC Flooding Using macof
 - DHCP attack using Yersinia
 - Bypass Authentication using SQL Injection
 - Determine how the hackers may get the database of a website and steal the credentials of users from website vulnerability
- **Cryptography Fundamentals:**
 - Key elements of cryptographic systems
 - Key systems
- **Encryption Techniques:**
 - Symmetric (private) key encryption
 - Asymmetric (private) key encryption
 - Elliptical curve cryptography
 - Quantum cryptography
 - Advanced encryption standard
 - Digital signature
 - Attacks on cryptosystems
 - Virtual private network
 - Wireless network protections
 - Stored data
 - Public key infrastructure
- **Encryption Applications:**
 - Applications of cryptographic systems
- ✓ **Hands-On/Demo:**
 - Generating and identifying hashes
 - Signing a file with digital signatures



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

Security of Networks, System, Application and Data:

- **Process Controls – Risk Assessments:**

- Attributes of risk
- Risk response workflow
- Risk analysis
- Evaluating security controls
- Risk assessment success criteria
- Managing risk
- Using the results of the risk assessment

- **Process Controls – Vulnerability Management:**

- Vulnerability management
- Vulnerability scans
- Vulnerability assessment
- Remediation
- Reporting & metrics

- ✓ **Hands-On/Demo:**

- Find the vulnerabilities of the host/website using the Nessus tool
- Find the vulnerabilities on target website/ host using Nikto scanner
- Password Breaking – Ophcrack
- Password Breaking - Konboot Tool
- Install keyloggers and configure the victim PC to monitor the system on keystrokes and screenshots

- **Process Controls – Penetration Testing:**

- Penetration testers
- Types of Penetration Test
- Penetration testing phases

- **Network Security:**

- Network management
- LAN/WAN security
- Network risks
- Wireless local area networks
- Wired equivalent privacy & Wi-Fi protected access (WPA/WPA2)
- Ports & protocols
- Port numbers
- Protocol numbers & assignment services
- Virtual private networks
- Remote access



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Operating System Security:**

- System/platform hardening
- Modes of operations
- File system permissions
- Credentials & privileges
- Command line knowledge
- Logging & system monitoring
- Virtualization
- Specialized systems

- **Application Security:**

- System development life cycle (SDLC)
- Security within SDLC
- Design requirements
- Testing
- Review process
- Separation of development, testing, & production environments
- OWASP top ten
- Wireless application protocol (WAP)

- **Data Security:**

- Data classification
- Data owners
- Data classification requirements
- Database security

- **Web server security:**

- Web server architecture
- Web server attacks
- Countermeasures and patch management
- Web application architecture
- Web application attacks

- ✓ **Hands-On/Demo:**

- Capturing session ID with Burp Suite
- Local File Inclusion on bWAPP



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Authentication:**

- Authentication and authorization
- Authentication and authorization principles
- Regulation of access
- Access administration
- IdAM
- Password protection
- Identity theft

- ✓ **Hands-On/Demo:**

- Adding and granting permissions to users in Linux
- Identifying phishing websites

Incident Response:

- **Event vs. Incident:**

- Events vs. incident
- Types of incidents

- **Security Incident Response:**

- What is incident response?
- Why do we need incident response?
- Elements of an incident response plan
- Security event management

- **Investigations, Legal Holds, & Preservation:**

- Investigations
- Evidence preservation
- Legal requirements

- **Forensics:**

- Data protection
- Data acquisition
- Imaging
- Extraction
- Interrogation
- Ingestion/normalization
- Reporting
- Network traffic analysis
- Log file analysis
- Time lines
- Anti-forensics



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Disaster recovery & business continuity plans**

- What is a disaster?
- Business continuity & disaster recovery
- Business impact analysis
- Recovery time objectives (RTO)
- Recover point objective (RPO)
- IS business continuity planning
- Recovery concepts
- Backup procedures

Security Implications & Adoption of Evolving Technology

- **Current Threat Landscape:**

- **Advanced persistent threats (APT's):**

- Evolution of the threat landscape
- Defining APTs
- APT characteristics
- APT targets
- Stages of an APT attack

- **Mobile Technology – Vulnerabilities, Threats, & Risk:**

- Physical risk
- Organizational risk
- Technical risk
- Activity monitoring & data retrieval
- Unauthorized network connectivity
- Web view/user interface (UI) impersonation
- Sensitive data leakage
- Unsafe sensitive data storage
- Unsafe sensitive data transmission
- Drive-by vulnerabilities

- **Consumerization of IT & Mobile Devices:**

- Consumerization of IT
- BYOD



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy

- **Cloud & Digital Collaboration:**

- Risk of cloud computing
- Web application risk
- Benefits of cloud computing
- Demo

KEY FEATURES



Instructor-led Sessions



Learn from Experts



Assignments



24 x 7 Support



Real-time Case Studies



Get Certified

For More Info:

www.slearn.academy

www.linkedin.com/company/slearnacademy

www.facebook.com/slearnacademy

www.instagram.com/slearnacademy



+44 (020) 3950 8881



+1 332-600-8899



+91 9581512555



trainings@slearn.academy