

A Revolutionary Learning in IT

www.slearn.academy

Cyber Security Curriculum

Cyber security Fundamentals

- Introduction to Cyber security:
 - The evolution of Cyber security
 - o Cyber security & situational awareness
 - o The Cyber security skills gap
- Difference between Information Security & Cyber security:
 - o Protecting digital assets
- Cyber security objectives:
 - o Confidentiality, integrity, & availability
 - Nonrepudiation

Cyber security Roles:

- O Governance, risk management, & compliance
- What does a Cybersecurity professional do?
- Information Security roles
- Board of Directors
- o Executive management
- Senior Information security management
- o Cyber security practitioners

• Ethical Hacking:

- o Types of Hackers
- Phases of Ethical Hacking

• NMAP:

- Basics of Networking
- o TCP and UDP protocols
- o 3-Way TCP Handshake
- o Ping and Ping Scan
- Basics of NMAP
- Shortcuts to save time in nmap















✓ Hands-On /Demo:

- o How to spin up KALI Linux as virtual machine
- Dirbuster
- o 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
- o Host, nslookup and dig
- o 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

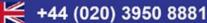
Common Attack Types & Vectors:

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

Policies & Procedures:

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















Cyber security Controls:

- Identity management
- Provisioning & de-provisioning
- Authorization
- Authentication
- o MBSA (Practical)
- o Tripwire (Practical)
- o Privileged user management
- o 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

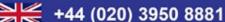
The OSI model:

o TCP/IP

Hands-On/Demo:

- o Identify the Network Routes in the System
- o DNS lookup and reverse lookup
- Network Path tracing
- Network Analysis
- Network scanning
- Enumeration















Defense in Depth:

• Firewalls:

- o Firewall general features
- Network firewall types
- Packet filtering firewalls
- Stateful inspection firewalls
- o Stateless vs. stateful
- o Examples of firewall implementations
- o Firewall issues
- o Firewall platforms
- Introduction to Honeypots

• Isolation & segmentation:

- o VLANs
- Security zones & DMZs

• Monitoring, Detection, and Logging:

- o Ingress, egress, & data loss prevention (DLP)
- O Antivirus & anti-malware
- Intrusion detection systems
- IDS limitations
- o IDS policy
- Intrusion prevention systems
- Malware and its propagation ways
- Malware components
- Types of malware
- Concept of sniffing
- Types of sniffing attacks
- o SQL injection
- o DoS attack
- o DDoS attack
- Common symptoms of DoS/DDoS attack
- Categories of DoS/DDoS Attack Vectors
- DoS/DDoS detection techniques
- Session hijacking
- o Application level session hijacking
- Network level session hijacking
- o Evading IDS











✓ Hands-On/Demo:

- o 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
- o DHCP attack using Yersinia
- o Bypass Authentication using SQL Injection
- o 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:

- o Symmetric (private) key encryption
- o Asymmetric (private) key encryption
- o Elliptical curve cryptography
- Quantum cryptography
- Advanced encryption standard
- Digital signature
- O Attacks on cryptosystems
- Virtual private network
- Wireless network protections
- Stored data
- o Public key infrastructure

Encryption Applications:

o Applications of cryptographic systems

✓ Hands-On/Demo:

- o Generating and identifying hashes
- Signing a file with digital signatures













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
- o Remediation
- o Reporting & metrics

✓ Hands-On/Demo:

- Find the vulnerabilities of the host/website using the Nessus tool
- o 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)
- o Ports & protocols
- o Port numbers
- Protocol numbers & assignment services
- Virtual private networks
- Remote access













Operating System Security:

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

• Application Security:

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

Data Security:

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

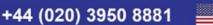
• Web server security:

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

✓ Hands-On/Demo:

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















Authentication:

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

✓ Hands-On/Demo:

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

Incident Response:

Event vs. Incident:

- o Events vs. incident
- Types of incidents

Security Incident Response:

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

Investigations, Legal Holds, & Preservation:

- o Investigations
- o Evidence preservation
- Legal requirements

Forensics:

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















Disaster recovery & business continuity plans

- What is a disaster?
- o Business continuity & disaster recovery
- o Business impact analysis
- o Recovery time objectives (RTO)
- o Recover point objective (RPO)
- o 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
- o APT characteristics
- APT targets
- Stages of an APT attack

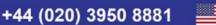
Mobile Technology – Vulnerabilities, Threats, & Risk:

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

Consumerization of IT & Mobile Devices:

- Consumerization of IT
- o BYOD















• Cloud & Digital Collaboration:

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















trainings@slearn.academy