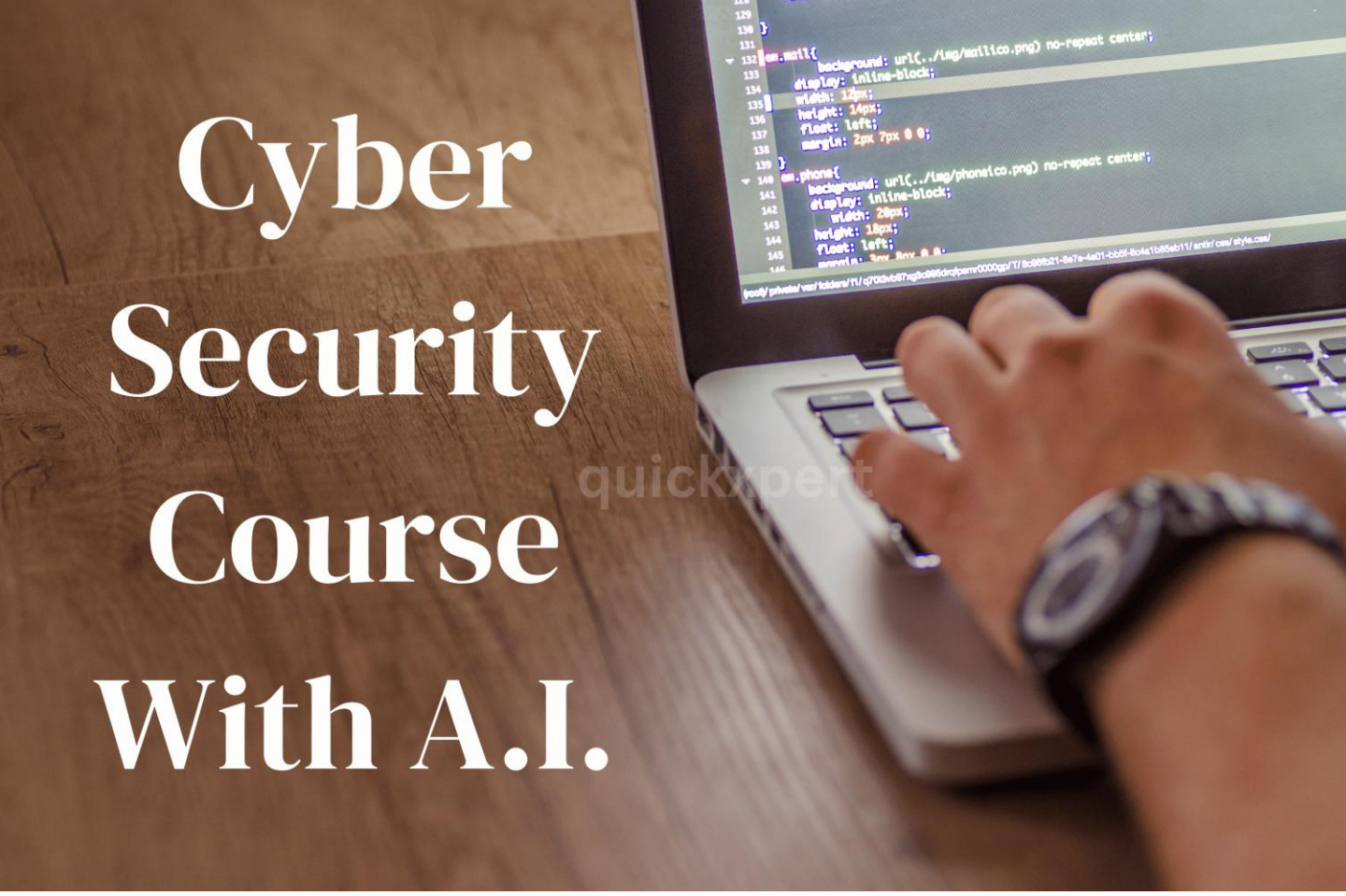

About QuickXpert Infotech

Best institute for IT training and placements for classroom and online training for students and corporates. We are an ISO certified institute and in the industry since 2014. Our strong training and placement team have helped thousands of students build their career.

Courses - JAVA, Dot Net, Software Testing, Web Development, Full Stack Development, MERN, MEAN, Oracle, Digital Marketing, Python, Data Analytics, Data Science & A.I., Cyber Security, Salesforce, Service Now, Tableau, Power BI, Excel, React, Angular etc.

Live Projects - MarriageKing, theVibrantBirdie, CRM etc

Corporate Trainings - GeBBS Healthcare, NVest Solutions, Infogix, PDG Software, GMV India etc.

Syllabus mentioned below.

Tools You Learn

Computer Networks & Network Security

OSI & TCP/IP Models

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

Network protocol

- Network Protocol, Types of Network – TCP , IP, UDP, POP3, SMTP
- HTTP , HTTPS, Telnet, SNMP, DNS, DHCP, TFTP, ARP, IMAP
- Assignment of Network Protocol

Network Devices

- Types of network Device- NIC Card , Repeater
- HUB Switch and Bridge
- Gateway Router Modern

IP Addressing

- IP Address
- IP Address Class
- Subnetting

Next Generation Firewalls

Basic Routing Technologies

- Static Routing
- Default Routing
- Dynamic Routing

Wireshark Packet Analysis

Tools: Wireshark , Net-cat , TCP dump and More…

CEH (Certified Ethical Hacker v13)

CEHv-13 Modules:

Module 1 - Introduction to Ethical Hacking

- Information Security Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Hacking Methodologies and Frameworks
- Information Security Controls

Module 2 - Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through internet Research Service
- Whois Footprinting
- DNS Footprinting
- Network and Email Footprinting
- Using advance tool and AI

Module 3 - Scanning Networks

- Network Scanning Concepts
- Host discovery
- Ports and Service Discovery
- Scanning Beyond IDS and Firewall
- Network Scanning Countermeasures

Module 4 Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- FTP Enumeration
- NTP and NFS Enumeration
- Other Enumeration Techniques

Module 5 Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Assessment Tools

Module 6 - System Hacking

- Gaining Access
- Maintaining Access
- Clearing Logs

Module 7 - Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Countermeasures

Module 8 - Sniffing

- Sniffing Technique : MAC Attacks
- Sniffing Technique : DHCP Attacks
- Sniffing Technique : ARP Poisoning
- Sniffing Technique : Spoofing Attacks
- Sniffing Tools

Module 9 - Social Engineering

- Social Engineering Concepts
- Human-based Social Engineering Concepts
- Computer-based Social Engineering Concepts
- Mobile-based Social Engineering Concepts

Module 10 - Denial-of-Service

- DoS/Ddos Concepts
- Botnets
- DDos Case Study
- DoS/DDoS Attack Techniques

Module 11 - Session Hijacking

- Session Hijacking Concepts
- Application-Level Session Hijacking
- Network -Level Session Hijacking
- Session Hijacking Tools

Module 12 - Evading IDS, Firewalls & Honeypots

- IDS, IPS, and Firewall Concepts
- IDS, IPS, and Firewall Solutions
- Evading IDS/Firewall
- IDS/Firewall Evading Tools
- Honeypot Concepts

Module 13 - Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Countermeasure

Module 14 - Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web Application Security

Module 15 - SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SOL Injection Methodology
- Evasion Techniques

Module 16 - Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Attack Countermeasure

Module 17 - Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking iOS
- Mobile Security Guidelines and Tools

Module 18 - IoT Hacking

- IoT Hacking
- OT Hacking

Module 19 - Cloud Computing

- Cloud Computing Concepts
- Container Technology
- Serverless Computing
- Cloud Hacking
- Cloud Security

Module 20 - Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Application of Cryptography
- Cryptanalysis
- Cryptography Attack Countermeasures

Tools: Nmap, Netcat, Metasploit, Wireshark, Cain & Abel, Maltego, Aircrack-ng, John the Ripper, gophish, sqlmap, Metasploit-framework, macchanger, crunch, hydra, medusa, Amaas, mdk3 and more ..

Web Application Penetration Testing

- Topics Covered (OWASP Top 10 – 2021):
- A01: Broken Access Control
- A02: Cryptographic Failures
- A03: Injection (SQLi, Command)
- A04: Insecure Design
- A05: Security Misconfiguration
- A06: Vulnerable & Outdated Components
- A07: Identification & Authentication Failures
- A08: Software and Data Integrity Failures
- A09: Security Logging and Monitoring Failures
- A10: Server-Side Request Forgery (SSRF)
- **Tools:** Burp Suite Pro, OWASP ZAP, Nuclei, FFUF, Dirb, SQLMap, Nikto, Postman and more

API Security & Penetration Testing

- OWASP API Security Top 10 (2023)
- BOLA (Broken Object Level Authorization)
- BFLA (Broken Function Level Authorization)
- Mass Assignment, Rate Limit Bypass
- JWT Token Attacks, Information Disclosure
- Fuzzing Parameters & HTTP Methods
- **Tools:** Postman, Burp Suite, Insomnia, Restler, OWASP Amass and more..

Mobile Application Penetration Testing

- Static Analysis with MobsF
- Runtime Analysis using frida and objection
- SSL pinning Bypass, Insecure data storage
- Root Detection Bypass, Activity Hijacking
- **Tools:** MobSF, APKTool, jadx Frida, Objection , Burp suite More…..

Network Penetration Testing

Network Penetration Testing

White, Black or Gray -box Network Penetration Testing

- Port Scanning
- Discover Live Hosts
- ICMP Scanning
- Identify Default Open Ports
- Use illegal Flag
- List Open and closed Ports

OS and Service Fingerprinting

- Fingerprint the OS
- Examine the Patches Applied to the OS
- Fingerprint Services

Vulnerability Research

- External Vulnerability Assessment
- Associated Security Vulnerabilities
- Find Out Security Vulnerability Exploites

Exploit Verification

Note - Tools mentioned may get changed, removed, added (similar tools will be taken)

Duration

- Weekdays (MTTF, Wed is off/practice break)
  - Option 1 – 6 to 7 months - 1.5 to 2 hrs/day
  - Option 2 – 4.5 months – 2.5 hrs/day
- Weekends (S S)
  - Option 1 – 8 months - 2 to 2.5 hrs/day
  - Option 2 – 6 months - 2.5 to 3 hrs/day

more info - https://quickxpertinfotech.com/cyber-security-course

Our Recruiters (1000+ Companies)

etc.

Our 5 Steps Process for Success

Contact Us

Call us - +91-7276681665, 7506252588

Address - Office 101 & 102, Pahlaj Kunj, Lohar Ali road, besides Karnavat Classes, near Jagdish Book Depot, 3 mins walk from Thane west rly stn.

Website - https://quickxpertinfotech.com

Message

Join us today !!