IntelliQ IT
Trainings



Cyber Security & Ethical Hacking

Course Content · 16 Modules · 9 Hands-On Labs

Date: **Timings:**

Duration: **Fee:**

Faculty:

Cyber Security & Ethical Hacking

✓ Cyber Security Fundamentals	Module 01
✓ Ethical Hacking & Penetration Testing	Module 02
✓ Networking & Packet Analysis	Module 03
✓ Reconnaissance & Footprinting (OSINT)	Module 04
✓ Network Scanning & Enumeration	Module 05
✓ Gaining & Maintaining Access	Module 06
✓ Web Application Hacking	Module 07
✓ Malware & Exploit Analysis	Module 08
✓ Defensive Security	Module 09
✓ SOC Overview	Module 10
✓ SOC Functions	Module 11
✓ Threat Intelligence & Incident Response	Module 12
✓ AI in Cyber Security	Module 13
✓ Cloud Security Basics (AWS / Azure / GCP)	Module 14
✓ Capture the Flag (CTF)	Module 15
✓ Bug Bounty & Kali Linux	Module 16

01 Cyber Security Fundamentals

Learn how to protect computers, networks and data.

- ✓ **CIA Triad**: Confidentiality, Integrity, Availability
- ✓ **Threats, Vulnerabilities & Risks**: what can go wrong and why
- ✓ **Attack Surface**: all possible ways a system can be attacked
- ✓ **Security Controls**: methods used to protect systems
- ✓ **Cyber Kill Chain & MITRE ATT&CK**: attack frameworks
- ✓ **Common Attack Methods**: how attackers target systems

02 Ethical Hacking & Penetration Testing

Understand hacking and how to do it legally.

- ✓ **Types of Hackers**: White, Black and Grey Hat
- ✓ **Rules and principles of ethical hacking**
- ✓ **Cyber security laws and regulations**
- ✓ **Steps involved in penetration testing**
- ✓ **Bug bounty programs and responsible reporting**

LAB 1 **Setting Up Your Practice Environment**

- ✓ **Install VMware or VirtualBox**
- ✓ **Install Kali Linux**
- ✓ **Basics of Nmap, Metasploit, Burp Suite**
- ✓ **Set up a vulnerable practice machine**

03 Networking & Packet Analysis

Understand how computers communicate.

- ✓ **OSI & TCP/IP**: network models
- ✓ **IPv4 & IPv6**: IP address types
- ✓ **Ports & Protocols**
- ✓ **DNS & DHCP**: names and automatic addressing
- ✓ **Routing & Switching**
- ✓ **VPN**: protected connections
- ✓ **Packet Analysis**: inspect network traffic

LAB 2 **Network Setup & Packet Analysis**

- ✓ **Connect virtual computers in a practice network**
- ✓ **Test connectivity with Ping**
- ✓ **Trace data paths with Traceroute**
- ✓ **Capture and study traffic in Wireshark**

04 Reconnaissance & Footprinting (OSINT)

Collect information about a target before testing its security.

- ✓ **Passive Reconnaissance**: no direct interaction
- ✓ **Active Reconnaissance**: interacting with the target
- ✓ **WHOIS, nslookup and Shodan**
- ✓ **OSINT**: publicly available intelligence
- ✓ **Social Engineering**: manipulating people into revealing information

LAB 3 **Reconnaissance & OSINT (authorized environment)**

- ✓ **Discover devices and services with Nmap**
- ✓ **Check domain registration and DNS records**
- ✓ **Find subdomains**
- ✓ **Google Dorking and Maltego**
- ✓ **Study simulated phishing attacks**

05 Network Scanning & Enumeration

Find open ports, running services and possible weaknesses.

- ✓ **Port Scanning**: find open ports
- ✓ **Banner Grabbing**: identify running services
- ✓ **Version Detection**: find software versions
- ✓ **Vulnerability Identification**
- ✓ **SMB, SNMP & NetBIOS**: network service information

LAB 4 **Network Scanning**

- ✓ **Scan ports using Nmap**
- ✓ **Identify services on a target machine**
- ✓ **Check vulnerabilities with Nessus**
- ✓ **Practice SMB and SNMP enumeration**

06 Gaining & Maintaining Access

How attackers exploit weaknesses and how defenders prevent it.

- ✓ **Exploitation**: using a vulnerability to gain access
- ✓ **Password Attacks**: testing and cracking weak credentials
- ✓ **Privilege Escalation**: gaining higher permissions
- ✓ **Maintaining Access**: how attackers keep a foothold
- ✓ **Clearing Tracks**: hiding activity and how defenders detect it

LAB 5 **Exploitation & Metasploit (controlled lab)**

- ✓ **Test known vulnerabilities with Metasploit**
- ✓ **Understand how exploits work**
- ✓ **Create and test basic exploits, authorized only**

07 Web Application Hacking

Learn how websites become vulnerable to attacks.

- ✓ **OWASP Top 10**: key web security risks
- ✓ **Burp Suite**: website security testing
- ✓ **SQL Injection**: unsafe database queries
- ✓ **XSS**: harmful scripts in web pages
- ✓ **CSRF**: unwanted browser requests
- ✓ **SSRF**: unintended server requests
- ✓ **Input Validation**
- ✓ **Authentication Flaws**

LAB 6 **Web Application Penetration Testing**

- ✓ **Inspect HTTP requests with Burp Suite**
- ✓ **Test for SQL injection and XSS**
- ✓ **See how session hijacking works**
- ✓ **Learn to fix and prevent each issue**

08 Malware & Exploit Analysis

How security professionals examine malicious software.

- ✓ **Virus**: attaches to files or programs
- ✓ **Worm**: spreads between systems
- ✓ **Trojan**: disguised as legitimate software
- ✓ **RAT**: remote access trojan
- ✓ **Static Analysis**: examine without running
- ✓ **Dynamic Analysis**: observe in a safe environment
- ✓ **Basic exploit development and antivirus evasion concepts**

09 Defensive Security

Protect systems against cyberattacks.

- ✓ **Blue, Red & Purple Teams**: defend, attack, collaborate
- ✓ **Preventive, Detective & Corrective Controls**
- ✓ **Firewall**: controls network traffic
- ✓ **IDS/IPS**: detect or block suspicious activity
- ✓ **SIEM**: collect and analyze security logs
- ✓ **Antivirus & EDR**: detect and respond on computers

LAB 7 Defensive Security

- ✓ **Configure and test Snort IDS**
- ✓ **Create and test firewall rules**
- ✓ **Detect and block suspicious activity**

10 SOC Overview

How a Security Operations Centre works.

- ✓ **Tier 1**: monitors alerts
- ✓ **Tier 2**: investigates suspicious activity
- ✓ **Tier 3**: advanced analysis and threat hunting
- ✓ **How SIEM tools detect incidents**
- ✓ **Splunk, ELK Stack and AlienVault**
- ✓ **Logs from firewalls, computers, proxies and logins**

11 SOC Functions

Main responsibilities of a SOC team.

- ✓ **Monitor systems and detect threats**
- ✓ **Triage alerts and prioritize**
- ✓ **Escalate serious incidents**
- ✓ **Respond and limit damage**
- ✓ **Investigate and find the root cause**
- ✓ **Prepare reports and follow requirements**

12 Threat Intelligence & Incident Response

Understand threats and handle security incidents.

- ✓ **Threat Intelligence**: information about attackers
- ✓ **IOC**: e.g. suspicious file hash or malicious IP
- ✓ **IOA**: behavior suggesting an attack
- ✓ **Kill Chain and MITRE ATT&CK in practice**
- ✓ **IR lifecycle**: preparation, detection, containment, eradication, recovery
- ✓ **FTK Imager and Autopsy**: digital evidence

LAB 8 Incident Response

- ✓ **Investigate a simulated breach**
- ✓ **Collect digital evidence**
- ✓ **Identify what happened**
- ✓ **Contain the incident and support recovery**

13 AI in Cyber Security

How AI can help improve security.

- ✓ What Artificial Intelligence means
- ✓ AI for detecting threats and suspicious activity
- ✓ Security risks associated with AI
- ✓ AI security controls and best practices

14 Cloud Security Basics (AWS / Azure / GCP)

Protect data and systems in the cloud.

- ✓ Shared responsibility model
- ✓ Secure cloud data, applications, infrastructure
- ✓ Common cloud security threats
- ✓ Methods for reducing cloud risk

15 Capture the Flag (CTF)

Learn by solving practical challenges.

- ✓ How CTF competitions work
- ✓ Hack The Box and TryHackMe
- ✓ Puzzles in simulated environments
- ✓ Apply ethical hacking and defense skills

LAB 9 Capture the Flag

- ✓ Participate in CTF challenges
- ✓ Solve security-related puzzles
- ✓ Apply pentesting and defense techniques

16 Bug Bounty & Kali Linux

Turn skills into real-world practice.

- ✓ Kali Linux for security testing
- ✓ How bug bounty programs work
- ✓ Find, document and responsibly report vulnerabilities