Cyber Security Expert – Course Modules

Module 1 – Introduction to Cyber Security

- *Understanding cyber threats, attacks, and vulnerabilities*
- *Importance of cyber security in the modern world*
- *Key concepts: CIA triad (Confidentiality, Integrity, Availability)*
- *Types of cyber attackers (black hat, white hat, grey hat)*

Module 2 – Networking Fundamentals for Security

- *OSI & TCP/IP models*
- *IP addressing, subnets, and protocols*
- *Network devices: routers, switches, firewalls*
- *Common network attacks and defense strategies*

Module 3 – Operating Systems & Security

- *Windows security basics (User accounts, policies, permissions)*
- *Linux security fundamentals (File permissions, user management)*
- *Secure configuration and hardening techniques*

Module 4 – Ethical Hacking Fundamentals

- *Reconnaissance techniques (Passive & Active)*
- *Scanning & enumeration*
- *Vulnerability assessment basics*
- *Common hacking tools (Nmap, Wireshark, Metasploit)*

Module 5 – Web Application Security

- *OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF, etc.)*
- *Secure coding practices*
- *Web application penetration testing*
- *Tools: Burp Suite, OWASP ZAP*

Module 6 – Malware Analysis & Prevention

- *Types of malware (viruses, worms, ransomware, trojans, spyware)*
- *Malware infection vectors*
- *Static and dynamic malware analysis techniques*
- *Antivirus and EDR solutions*

Module 7 – Cryptography & Data Security

- *Symmetric vs asymmetric encryption*
- *Hashing & digital signatures*
- *SSL/TLS and HTTPS*
- *Public Key Infrastructure (PKI)*

Module 8 – Incident Response & Digital Forensics

- *Incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery)*
- *Evidence collection and preservation*
- *Disk and memory forensics tools*
- *Case study of a cyber breach*

Module 9 – Cloud & IoT Security

- *Cloud security challenges (AWS, Azure, GCP)*
- *Shared responsibility model*
- *IoT vulnerabilities and security best practices*

Module 10 – Cyber Security Tools & Automation

- *SIEM tools (Splunk, ELK)*
- *Scripting for automation (Python, Bash)*
- *Security monitoring and log analysis*

Module 11 – Compliance & Risk Management

- *GDPR, HIPAA, ISO 27001, PCI-DSS basics*
- *Risk assessment and mitigation strategies*
- *Security policies and documentation*

Module 12 – Final Project & Certification Prep

- *Simulated penetration testing of a network*
- *Incident report creation*
- *Preparation for certifications (CEH, CompTIA Security+, CISSP)*