CYBER SECURITY

DURATION
90 Days

COURSE OVERVIEW

This course provides strong foundations in cyber security, privacy, ethical hacking, encryption, operating system security, threat modeling, and real-world attack & defense techniques. It blends theory + practical labs to prepare learners for industry and certification paths.

MODULE 1: COURSE INTRODUCTION & CYBER SECURITY FUNDAMENTALS

- Welcome and instructor introduction
- Course structure: theory vs hands-on learning
- Learning goals and objectives
- Target audience and career paths
- Cyber Security & Ethical Hacking career overview
- Why cyber security matters in today's digital world
- Protecting personal and organizational assets

MODULE 2: SECURITY CONCEPTS, PRIVACY & THREAT LANDSCAPE

- What is Cyber Security?
- Privacy, Anonymity, and Pseudonymity
- Security vs Privacy vs Anonymity
- Assets, vulnerabilities, threats, and adversaries
- Threat modeling and risk assessment
- Confidentiality, Integrity, and Availability (CIA Triad)

- Defense in Depth strategy
- Zero Trust Security Model

MODULE 3: CYBER THREATS & ATTACK VECTORS

- Value of a hack: why attackers attack
- Hackers vs crackers vs cyber criminals
- Malware types:
- Viruses, worms, trojans
- Rootkits and Remote Access Trojans (RATs)
- Spyware, adware, scareware, PUPs
- Browser hijacking
- Spamming, doxing, and identity abuse
- Social engineering:
- Phishing, scams, frauds, impersonation
- Crypto-mining malware & CPU hijackers
- Dark web, dark markets, exploit kits
- Governments, surveillance, censorship & backdoors

MODULE 4:CRYPTOGRAPHY & SECURE COMMUNICATION

- Basics of cryptography
- Symmetric encryption
- Asymmetric encryption
- Hash functions
- Digital signatures
- SSL & TLS fundamentals
- HTTPS and digital certificates
- Certificate Authorities (CA)
- End-to-End Encryption (E2EE)
- SSL stripping attacks
- Steganography
- Real-world encryption attacks and weaknesses

MODULE 5: CYBER THREAT INTELLIGENCE

- Understanding cyber threat intelligence (CTI)
- Staying informed about emerging threats
- Importance of proactive security awareness

MODULE 6: VIRTUALIZATION & LAB SETUP

- Importance of test environments
- Virtual machines overview
- VMware installation and usage
- VirtualBox installation and usage
- Kali Linux setup
- Safe lab environments for ethical hacking

MODULE 7: OPERATING SYSTEM SECURITY & PRIVACY

WINDOWS SECURITY

- Security features and vulnerabilities
- Windows privacy & tracking
- Disabling telemetry and tracking
- Cortana privacy concerns
- Wi-Fi Sense risks

MACOS SECURITY

- Privacy controls
- Tracking mechanisms

LINUX & UNIX SYSTEMS

- Linux security fundamentals
- Debian, Arch security overview

SECURITY-FOCUSED OS

- Qubes OS
- Subgraph OS
- Trisquel OS

ANONYMITY-FOCUSED OS

- Tails
- Whonix

PENETRATION TESTING OS

- Kali Linux and other ethical hacking distributions

MOBILE OS SECURITY

- LineageOS
- Sailfish OS

MODULE 8:PATCH MANAGEMENT & SYSTEM UPDATESI

- Importance of patching
- Windows update mechanisms
- Patch Tuesday and critical updates
- Automating patch management
- Linux patching
- MacOS patching
- Browser and extension updates
- Impact of auto-updates on privacy

MODULE 9: PRIVILEGE MANAGEMENT & ACCESS CONTROL

- Principle of least privilege
- Risks of admin/root access
- Using standard user accounts securely
- Privilege escalation risks

MODULE 10:SOCIAL MEDIA & IDENTITY SECURITY

- Information disclosure risks
- Identity verification and registration security
- Online behavior analysis
- Personal data exposure prevention

MODULE 11:SOCIAL ENGINEERING DEFENSE

BEHAVIORAL CONTROLS

- Identifying phishing attacks
- Recognizing spam and scam patterns
- Human-factor security awareness

TECHNICAL CONTROLS

- Email filtering
- Anti-phishing tools
- Browser and OS-level protection

MODULE 12: SECURITY DOMAINS & GOVERNANCE

- ISecurity domains overview
- Network security
- Application security
- Endpoint security
- Cloud security basics
- Governance, risk & compliance (GRC) overview

HANDS-ON LABS & PRACTICAL EXPOSURE

- IVirtual lab configuration
- Kali Linux tools usage
- OS hardening
- Privacy and tracking mitigation
- Secure browsing practices
- Encryption demonstrations

TOOLS & TECHNOLOGIES COVERED

- Kali Linux
- VirtualBox / VMware
- Windows, Linux, MacOS
- Encryption & security tools
- Browser privacy tools

CAREER OUTCOMES

- Cyber Security Analyst
- Ethical Hacker
- SOC Analyst
- Information Security Engineer
- Security Consultant