IT KART ACADEMY

Cyber Security Course Content

Module	Duration (Weeks)
Bootcamp Phase	
Communication Skills	1
Security Fundamentals	1
Networking Concepts	1
Ethical Hacking	4
Specialization Phase	
Security Solutions	3
SOC & Monitoring	3
Threat Hunting	2
Security Testing	3
Security Frameworks	2
Total Duration	20

Bootcamp Phase

Communication

Training

Security Fundamentals

Windows

- Overview & Architecture
- Various Security features
- Partitioning & Formatting techniques
- Filesystems understanding
- Applying Basic Security Policies

Linux

- Architecture
- Security features
- How it differ from Windows in terms of Security, Consistency
- Applying Basic Security Policies

Networking Concepts

- Networking overview
- Network Devices
- Topology
- OSI Model
- TCP/IP Model
- Networking Protocols
- IP V4 Overview, Classification, Subnetting, Examples
- IPV6 Overview
- Configuring IPv6
- DHCP
- Secure Architecture Overview
- Net BIOS and DNS namespace
- Understanding DNS
- Remote Access Service
- VPN
- Networking Media

Ethical Hacking

Module 1: Introduction to Ethical Hacking

- Definition and scope of ethical hacking
- Importance of ethical hacking in cybersecurity
- Legal and ethical considerations

Module 2: Footprinting and Reconnaissance

- Gathering information about target systems and networks
- Techniques for footprinting and reconnaissance
- Tools for reconnaissance

Module 3: Scanning and Enumeration

- Port scanning techniques
- Service enumeration
- Vulnerability scanning

Module 4: System Hacking

- Password cracking techniques
- Privilege escalation
- Exploiting system vulnerabilities

Module 5: Network Hacking

- Sniffing and spoofing attacks
- Man-in-the-middle attacks
- Wireless network hacking

Module 6: Web Application Hacking

- Common web application vulnerabilities
- SQL injection attacks
- Cross-site scripting (XSS) attacks

Module 7: Social Engineering

- Psychological principles behind social engineering
- Techniques for social engineering attacks
- Mitigating social engineering risks

Module 8: Evading IDS, Firewalls, and Honeypots

- Intrusion Detection Systems (IDS)
- Firewall evasion techniques
- Honeypot detection and evasion

Module 9: Penetration Testing

- Planning and preparation for penetration testing
- Conducting penetration tests
- Reporting and remediation

Module 10: Case Studies and Practical Applications

- Analyzing real-world hacking incidents
- Ethical hacking in different industries
- Hands-on exercises and simulations

Mock Client Interview + Assessment

Specialization Phase

Security Solutions

Firewall

- Firewall introduction
- Firewall types
- Packet filtering firewalls
- Stateful packet filtering
- Proxy firewalls
- Personal firewalls
- Firewall architectures
- Configuration checklist, monitoring firewalls, logging, syslog
- Understanding of VPN technologies

IDS/ IPS

- Introduction to Intrusion Detection and Prevention
- IDS/IPS characteristics
- IDS/IPS types
- Network-based and host-based IDS/IPS
- Industry best practices
- Adapting Traffic Analysis and Response to the Environment
- Managing and Analyzing Events

DAM

- Introduction to Database Activity Monitoring
- What is DAM and need for DAM
- Various Types of DAM and it's use

PAM

- Introduction to Privileged Access Management
- What is PAM and need for PAM
- Password Vault concepts
- Integration with various devices and its uses and concepts
- Various Types of PAM software
- PAM deployment and configuration
- What is PIM
- Various modules in PIM and PAM
- Asset Management Introduction

Proxy

- Introduction to Proxy
- Types of proxy
- Basic Policy Control
- Introduction to Content/URL Filtering

DLP

- Data Loss Prevention Solution Overview
- Data Loss Prevention Endpoint Fundamentals
- Privileged Users and End-User Group Definitions
- Monitoring and Reporting
- Basic Troubleshooting

WAF

- Introduction to Web Application Firewalls
- What is WAF and need for WAF
- Various Types of WAF
- Strategy for WAF deployment and configuration
- Introduction to OWASP TOP 10 Attacks

EndPoint Security

- Endpoint Security Overview
- Introduction to Antivirus
- Introduction to Endpoint DLP
- Introduction to Disk Encryption
- Introduction to HIPS
- Introduction to Best Industry Practices

IDM

- Introduction to Identity Manager Terminologies like User, Enterprise Role, Resource Object, IT Resource, attributes, roles, groups and mapping of attributes.
- Introduction to Identity Manager Architecture and design concepts.
- Introduction to Identity Manager concepts like Identity Reconciliation, Account Management, Provisioning, Access Request, Approvals, certifications and Lifecycle Management(LCM),JML process.
- Introduction to Connectors, Type of connectors, customization and Mainframe

IAM

- Introduction to Access Management concepts
- Introduction to access provisioning and deprovisioning
- Introduction to SAML, ADFS, oAuth, Social authentication, federation
- Introduction to OpenID, UMA and SCIM concepts
- Introduction to connector development and OpenID coding using JAVA,perl, python and jscript.
- Introduction to various tools
- Introduction to IdaaS

SOC & Monitoring

- Introduction to SIEM tool
- SIEM tool Architecture
- Log Monitoring (Windows, Linux etc.)
- Alert Analysis
- Incident Handling
- Threat Intelligence
- Log source Integration
- Content Development
- Incident Life Cycle
- Ticketing tool Overview
- Key processes overview

Advance Security Testing

- Security Testing Requirements
- Overview of Testing
- Overview of VA
- Overview of PT
- Overview of Appsec
- Assessment Report Preparation

Threat Hunting

- Threat Hunting Overview
- Cyber Analytics using ELK

Security Frameworks

- Overview of ISO 27001
- Overview of PCI DSS
- Overview of BCP / DR
- Overview of Data Privacy & GDPR
- Guidelines
- Principles
- Standards
- Frameworks/breakdowns/structures
- Checklists
- Audit guidelines/outlines
- Reporting standards
- Product evaluation

Assessment