CYBER SECURITY

Become a Cyber Security Expert in three months

COURSE OUTLINE

Module01: Introduction to Cybersecurity

Module02: Linux Administration

Module03: Ethical Hacking Basics & OSINT

Module04: Vulnerability Assessment and Exploitation

Module05: Web Application Security

Module06: Wireless and Mobile Security

Module07: Sniffing, DDoS, & Social Engineering

Module08: Firewalls, IDS/IPS & Cryptography

Module09: Digital Forensics Fundamentals

Module10: OS, Network, Web, Email, DarkWeb Forensics

Module11: Security Information and Event Management (SIEM)

Module12: Advanced SIEM and Threat Hunting

Module01

Introduction to Cybersecurity

- Overview of cybersecurity concepts and importance
- Introduction to Linux operating system
- Overview of Kali Linux as a cybersecurity
- focused distribution
- Installation of Kali Linux (virtual machine or du al-boot setup)

- Basic Linux commands and navigation

Module02

Linux Administration

- Networking Commands
- User and group management
- Files & Folders Permissions
- Services & Process Management
- Aliases & Password Recovery

Module03

Ethical Hacking Basics & OSINT

- Understanding ethical hacking
- Legal and ethical considerations
- Different hacking phases and methodologies
- Information Gathering and Reconnaissance
- OSINT (Open Source Intelligence) techniques
- Reconnaissance tools (e.g., Nmap, Recon-ng)
- Footprinting and scanning

Module04

Vulnerability Assessment and Exploitation

- Identifying vulnerabilities and weaknesses
- Scanning and enumeration (e.g., Nmap, Nessus, Ope nVas)
- Vulnerability Assessment (e.g., CVE, CWE, CVSS)
- Exploiting vulnerabilities safely
- Gaining access and maintaining control (Metasploi t)

- Privilege escalation and lateral movement

Monthly Practical Task 01

At the end of Month 1, students will be given a practical task to perform a basic security assessment of a simulated network using the skills they have learned, including setting up a basic Linux firewall, user management, and vulnerability scanning.

Module05

Web Application Security

- OWASP Top Ten vulnerabilities
- Web application penetration testing techniques
- Different scanning tools(ZAP, Burpsuite)

Module06

Wireless and Mobile Security

- Wireless network vulnerabilities (e.g., WEP, WPA)
- Mobile application security testing
- Bluetooth and IoT security

Module07

Sniffing, DDoS, & Social Engineering

- Packet sniffing techniques and tools (e.g., Wiresh ark)

- Social engineering attacks and methods
- Prevention and mitigation strategies
- Understanding DDoS attacks (types and vectors)
- DDoS attack tools and techniques
- DDoS mitigation strategies and practices

Module08

Firewalls, IDS/IPS & Cryptography

- Introduction to firewalls and firewall types
- Configuring and managing firewalls
- Intrusion Detection and Prevention Systems (IDS/I PS)
- Introduction to cryptography and encryption
- Cryptographic algorithms and protocols
- Securing communications and data encryption

Monthly Practical Task 02

At the end of Month 2, students will be
tasked with designing and implementing
a basic network security setup that
includes a firewall, IDS/IPS, and
encryption for secure communication.

Module09

Digital Forensics Fundamentals

- Introduction to digital forensics
- Evidence preservation and chain of custody

- File system analysis (e.g., Autopsy, FTK)

- OS Forensics

Module10

OS, Network, Web, Email, DarkWeb Forensics

- Capturing and analyzing network packets

- Wireshark and tcpdump

- Analyzing logs

- Identifying network-based attacks

- Types of malware

- Static and dynamic malware analysis

- Identifying malware indicators

- Reverse engineering techniques

- Email client forensics

- Recovering deleted emails

- Identifying illegal activities and threats

- Evidence collection and preservation

Module11

Security Information and Event Management (SIEM)

- Understanding SIEM concepts

- Popular SIEM systems (e.g., Wazuh, Graylog)

- Configuration of Wazuh Indexer, Wazuh Dashboard, G raylog

- Log collection methods (syslog, agents, APIs)

- Parsing and normalizing logs

- Real-time log analysis

Module12

Advanced SIEM and Threat Hunting

- Creating SIEM use cases for threat detection
- Custom correlation rules
- Incident detection and response workflows
- Threat hunting techniques using SIEM
- Security analytics and anomaly detection
- Identifying advanced threats and persistent adversaries

Monthly Practical Task 03

At the end of Month 3, students will be
given a comprehensive digital forensics
and incident response scenario. They will
have to collect evidence, analyze logs,
and use SIEM tools to investigate and
report on a simulated cyber incident.

Mail: info@itsolera.com

Phone: +923334471066

Website: itsolera.com