COURSE HANDOUT (COURSE CURRICULUM)

Course Title : **CYBER SECURITY**

Credits -4

1. Course Description:

This Course was designed to help learners develop a deeper understanding of modern information and system protection technology and methods. The learning outcome is simple: We hope learners will develop a lifelong passion and appreciation for cyber security, which we are certain will help in future endeavors. Students, developers, managers, engineers, and even private citizens will benefit from this learning experience. Special customized interviews with industry partners were included to help connect the cyber security concepts to live business experiences.

2. Skills You Will Gain

- Cryptography
- Cybersecurity
- Risk Assessment
- Cyber Defense
- Cyber Attacks
- Information Security (INFOSEC)
- Denial-Of-Service Attack (DOS)
- Ethical Hacker

3. The course content enables students to:

1. Summarize the main purpose of cyber security as a discipline
2. Summarize the basics of identification and authentication in cyber security
3. Explain the pros and cons of security through obscurity
4. Develop a lifelong learning plan for potential careers in cyber security

5. How the Specialization Courses Works: -

- Take Courses
- Hands-on Project
- End Assessment
- Earn Credit Based Certificate

6. Course Outcomes: -

1. To understand various types of cyber-attacks and cyber-crimes
2. To learn threats and risks within context of the cyber security
3. To have an overview of the cyber laws & concepts of cyber forensics
4. To study the defensive techniques against these attacks

SYLLABUS:

Module-1
Introduction to Cyber Security
- What is Cyber Security?
- Importance of Cyber Security
- Cyber Security Domains
- CIA Triad
- Vulnerability, Threat and Risk

Module-2
Linux Essentials
-History and Features of Linux
-Architecture of Linux OS
-Linux Distributions
-Linux Command Line
-Software Package Management

Module-3
Linux Administration
-File System
-Users and Groups
-File/Folder Permissions
-Special Permissions
-Disk Management
-Service and Process Management

Module-4
Networking Fundamentals
- Computer Networks and Types of Networks
- Network Devices
- IP and MAC Address
- IPv4 and IPV6 Packet Structure
- Addressing and Subnetting
- OSI Model and TCP/IP Model
- Network Protocols (TCP, UDP, ICMP, ARP)

- Network Services (DNS, DHCP, SNMP, FTP)
- Packet Analysis using Wireshark

Module-5

Vulnerability Management
- Fundamentals of Vulnerability Assessment and Management
- Vulnerability Assessment tool Deployment Strategy
- Scanning Methodologies
- Authenticated vs Non-Authenticated Scanning
- Planning and Performing Infrastructure Security Assessment
- Interpreting and Calculating CVSS Score
- Risk Identification and Categorization
- Reporting
- Patches and Updates

Module-6

Network Penetration Testing
- Introduction to Penetration Testing
- Types of Penetration Testing
- Pentesting Services
- Penetration Testing Phases
- Pre-Engagement Actions
- OSINT
- Exploitation (Automated)
- Password Cracking
- Red Team Vs Blue Team Operations

Module-7

Advanced Network Pentesting
- Manual Exploitation of System Vulnerabilities
- Post-Exploitation
- Privilege Escalation (Linux and Windows)
- Pivoting and Double Pivoting
- Cyber Kill Chain, MITRE ATT&CK

Module-8

Cryptography
- Introduction to Cryptography
- Symmetric Ciphers
- Asymmetric Ciphers
- Pseudo-Random Number Generator
- Building SSL certificates
- Digital Certificates and Digital Signatures

- Disk Encryption
- Hashing
- Encoding
- Steganography

Module-9

Web Fundamentals

- Web application Technologies
- Web Application offence and defence
- Web Reconnaissance
- Web Application Vulnerability Assessment
- CMS Enumeration and Exploitation
- Tools - Nikto, OWASP-Zap, gobuster, wpscan

Module-10

Web Application Pentesting

- OWASP Top 10 Web Risks
- Web Application Pentesting Checklist
- Authentication & Authorization
- Session Management
- File Security
- Web Application Firewalls
- Tools - BurpSuite, Sqlmap, wafw00f
- Practical Assignment - III & Capture The Flag (CTF) - II

Module-11

Bug Bounty Secrets

- Introduction to bug bounty
- Bug Bounty Hunting vs Penetration Testing
- Bug bounty essentials and platforms
- Mind Maps and Recon
- Bug bounty report writing

Capstone Project

- **Real-World Application:**
  - Participants will develop a comprehensive cybersecurity plan, conduct a penetration test, or analyze a major breach.
- **Presentation and Review:**
  - Showcase project outcomes to industry experts.

Tools and Technologies Covered:

- Wireshark, Nessus, Metasploit, Burp Suite, OWASP ZAP, Splunk, QRadar, AWS Security Tools

Cybersecurity Course Outcomes

1. **Foundational Knowledge**:
    - Demonstrate a strong understanding of core cybersecurity principles, including confidentiality, integrity, and availability (CIA triad).
2. **Risk Assessment and Management**:
    - Conduct risk assessments to identify vulnerabilities and implement effective system mitigation strategies.
3. **Cryptography Skills**:
    - Apply cryptographic techniques to secure data transmission and storage, understanding the use of encryption, decryption, and key management.
4. **Network Security**:
    - Configure and manage firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to secure organizational networks.

- Hands-on Project – 4 Hrs
- End Assessment – 1 Hr (50 Questions)
- **Earn Credit Based Certificate**
- **Internship Certificate**
- **Live Class through Industry Experts**