FUTURE PROOF LEARNING - NEP ALIGNED
www.mycreditcourses.com

CERTIFICATE IN CYBER SECURITY & ETHICAL HACKING

Duration: 120 Hours
Total Credits: 4

COURSE SYLLABUS

Objective

This course provides comprehensive training in cyber security principles and ethical hacking techniques. It equips learners with the skills to identify, analyze, and mitigate cyber threats, ensuring the security of digital systems and networks. The curriculum covers core concepts such as security mechanisms, network protection, system and application security, and ethical hacking tools. By the end of the course, participants will be able to assess vulnerabilities, prevent unauthorized access, and ethically test systems to strengthen cybersecurity measures, preparing them for careers in cybersecurity and ethical hacking.

Exit Profile

- Network Security and Protection
- Ethical Hacking Techniques
- Cybersecurity Incident Response
- Ethical Hacking and Penetration Testing
- Legal and Ethical Responsibilities in Cyber Security

Career Path

- Application security engineer
- Cybersecurity engineer
- Data security engineer
- IT security engineer
- Web applications security engineer

Course Outline

Course Name:	CERTIFICATE IN CYBER SECURITY & ETHICAL HACKING	Duration:	
Module	Topic	Duration	Total Duration
Module - I	Security Concepts and Mechanisms	30H	60 H
	Security Management	30H	
Module - II	Network Security	30H	60 H
	System and Application Security	30H	

Course in Detail

MODULE - 1

SECURITY CONCEPTS AND MECHANISMS:

Networking Concepts Overview:

- Basics of Communication Systems
- Transmission Media
- ISO/OSI and TCP/IP Protocol Stacks
- Local Area Networks
- Wide Area Networks
- Internetworking
- Packet Formats
- Wireless Networks
- The Internet

Information Security Concepts:

- Information Security Overview
- Information Security Services
- Types of Attacks
- Goals for Security
- E-commerce Security
- Computer Forensics
- Steganography
- Security Engineering

Security Threats and vulnerabilities:

- Overview of Security threats
- Hacking Techniques
- Password Cracking
- Insecure Network connections
- Malicious Code
- Programming Bugs
- Cyber-crime and Cyber terrorism
- Information Warfare and Surveillance

Cryptography:

- Introduction to Cryptography

- Symmetric key Cryptography
- Asymmetric key Cryptography
- Message Authentication and Hash functions
- Digital Signatures
- Public Key infrastructure
- Diffie-Hellman key exchange protocol
- Applications of Cryptography

SECURITY MANAGEMENT:

Security Management Practices:

- Overview of Security Management
- Information Classification Process
- Security Policy
- Risk Management
- Security Procedures and Guidelines
- Business Continuity and Disaster Recovery

Security Laws and Standards:

- Security Assurance
- Security Laws
- International Standards
- Security Audit
- OCTAVE approach
- SSE-CMM

MODULE - 2

NETWORK SECURITY:

Access Control and Intrusion Detection:

- Overview of Identification and Authorization
- I & A Techniques
- Overview of IDS
- Intrusion Detection Systems and Intrusion Prevention Systems

Server Management and Firewalls:

- User Management
- DNS Routing and Load Balancing
- Overview of Firewalls

- Types of Firewalls
- DMZ and firewall features

Security for VPN and Next Generation Networks:

- VPN Security
- Security in Multimedia Networks
- Fax Security
- Link Encryption Devices

SYSTEM AND APPLICATION SECURITY:

Security Architectures and Models

- Designing Secure Operating Systems
- Controls to enforce security services
- Information flow model and Biba model

System Security

- Desktop Security
- email security: PGP and SMIME
- Web Security: web authentication, SSL and SET

OS Security

- OS Security Vulnerabilities, updates and patches
- OS integrity checks
- Anti-virus software
- Design of secure OS and OS hardening
- Configuring the OS for security
- Trusted OS