Post Graduate Certificate in Cyber Security

PROGRAMME CURRICULUM

Sem I

1. Cyber Security Fundamentals

1. Introduction to Cyber Security
2. Cyber Security Terminologies
3. Vulnerabilities, Threats, Threat Agents, Risks
4. Types of hackers
5. Types of Malicious Attacks
6. CIA / AIC Triad
7. Cyber kill chain methodology
8. Biometrics
9. Security Architecture and Design

2. Information Security Management Systems

1. Security Engineering
2. Cyber Security Architecture / Framework
3. Importance of Information Security in Business
4. Governance, Risk & Compliance
5. Risk Management
6. Cyber Security Policy, Standards, Procedures & Guidelines
7. Common International Compliance Frameworks (ISO 27001, NIST)
8. IT and National Acts
9. International Legal and Ethical Considerations
10. Cyber Crime and Cyber Law

3. Network Security

1. Overview of computer networks
2. Introduction to Network Security
3. Firewalls and Intrusion Detection/Prevention Systems
4. Demilitarized Zone (DMZ)
5. Proxy Servers and Application Layer Firewalls
6. Network Security Protocols (SSL/TLS, IPsec, VPNs and Remote Access Security)
7. Operating System security
8. System and Software Security
9. Remote Access Security

4. Cryptography and Applications

1. Principles of Cryptography
2. Symmetric and Asymmetric Cryptography
3. Encryption and Decryption Techniques
4. One-way Functions
5. Hash Functions
6. Digital Signatures
7. Public Key Infrastructure (PKI)
8. Key Management-Key Generation, Distribution, and Storage, Public Key Infrastructure (PKI)
9. Certificate Authorities (CA)
10. Encryption and Decryption Techniques

5. Assets Security, Identity and Access Management (IAM)

1. Asset Security
2. Data Security Principles
3. IAAA Principles of IAM
4. Mandatory Access Control (MAC)
5. Discrete Access Control (DAC),
6. Role-Based Access Control (RBAC)
7. Rule-Based Access Control (RB-BAC)
8. Defence in Depth
9. Zero Trust Architecture (ZTA)
10. Financial Assests

Sem II

1. Cyber Security Incident Management

1. Incident Management-Identification, Protection, Detection, Response, Recovery
2. Incident Response and Management
3. Business Continuity Management (BCM) and Principles-Business Impact Analysis (BIA) methodology
4. Business Continuity Planning (BCP), Disaster Recovery Planning (DRP)
5. Introduction to SIEM
6. SIEM Architecture
7. Anomaly Detection
8. Role of SIEM in Business Security Strategy
9. Properties of a Robust SIEM
10. Case study.

2. Web Security, Application Security and Mobile Security

1. Common web vulnerabilities
2. Web application firewalls
3. Web Application Security Risks
4. DevSecOps
5. Security challenges in mobile devices
6. Mobile App security
7. Unified Endpoint Management (UEM)
8. Mobile Device and Application Management.
9. Web Browser security
10. Android Malware

3. Forensics Investigation & Audit

1. Introduction to Digital Forensics and Audit
2. Role of Digital Forensics in Business Security
3. Email Investigation
4. Mobile device Forensics
5. Sans Investigative Forensics Toolkit (SIFT)
6. CAINE Forensic Environment
7. Database and Cloud Forensic
8. Ethics in Digital Forensics
9. Forensics Analysis Tools
10. Anti-Forensic Techniques.

4. Emerging Trends in Cyber Security

1. Threat Intelligence
2. Cloud Computing Fundamentals
3. Cloud Security
4. Automotive Industry
5. SCADA
6. IOT
7. AI and machine learning in cybersecurity
8. Blockchain and blockchain security
9. Current Threats and Mitigation
10. Targeted Ransomware

5. Project

Culminating project integrating concepts from the entire program