Course Content

- Cyber Security
- Intrusion Detection System
- Footprinting and SQL Injection
- Public Key Infrastructure
- Forensics Steps: Overview
- Information Life Cycle
- Cryptography: Overview
- NIST RMF: Overview
- Physical Security
- IAM(Identiity and Access Management)
- Penetration Testing: Overview
- Web Application Testing: Overview
- OWASP Top 10: Overview
- Cross Site Scripting and Reconnaissance
- Password Cracking and Social Engineering
- Shell Scripting(Linux): Introduction only
- Incident Response Steps: Overview
- Network Defense: Best Practices
- SDLC(Systems Development Life Cycle)
- Malware and Sniffing
- DOS(Denial of Service)
- Introduction to Ethical Hacking & Phases of Hacking
- Introduction to Penetration Testing & Phases of Pen-Testing
- Information Gathering
- Target Enumeration and Port Scanning Techniques
- Finding Vulnerabilities and Metasploit Framework
- OWASP Top 10 Web Application Security Risks
- Cryptography
- Penetration Testing for Sniffing Attacks
- Penetration Testing for Social Engineering
- Penetration Testing for Web Application
- Penetration Testing for Database
- Penetration Testing for Network Infrastructure
- Firewalls and Intrusion Prevention System
- Cloud Computing threats & attacks
- Internet of Things threats & attacks

- Malware Threats
- Wireless Attacks & Countermeasures
- Hacking for Managers