Cyber Security and Ethical Hacking

Department : Computer Science

Title of the Course: Cyber Security and Ethical Hacking

Course Director : Prof. Selwyn Paul e mail: selwynpaul438@gmail.com

Duration of Hours: 90 Hrs. Credits: 3

Course Fee : 3,500/-

Objectives of the course:

1. The learner will gain knowledge about securing both clean and corrupted systems, protect personal data, and secure computer networks.

2. The learner will understand key terms and concepts in cyber law, intellectual property and cyber-crimes, trademarks and domain theft.

3. The learner will be able to examine secure software development practices.

4. The learner will understand principles of web security.

5. The learner will be able to incorporate approaches for incident analysis and response.

6. The learner will be able to incorporate approaches for risk management and best practices.

7. The learner will gain an understanding of cryptography, how it has evolved, and some key encryption techniques used today.

8. The learner will develop an understanding of security policies (such as confidentiality, integrity, and availability), as well as protocols to implement such policies.

Syllabus:

Cyber Security and Cyber Laws 10 hours

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats: - Cyber Warfare-Cyber Crime-Cyber Terrorism-Cyber Espionage, need for a Comprehensive Cyber Security Policy, need for a Nodal Authority, Need for an International convention on Cyberspace. Introduction, Cyber Security Regulations, Roles of International

Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013.

Network Security **10 hours**

Introduction To The Concepts Of Security, Security Approaches, Principles Of Security, Types Of Attacks, Intruders, (IDS and IPS)Intrusion Detection And Prevention System, Password Management, Viruses And Related Threats, MFA (Multifactor Authentication) DOS (Denial Of Service) And DDOS Distributed Denial Of Service Attack, Firewall, Design Principles, Virtual Private Network (VPN).

Cryptography **15 hours**

Convention Encryption Model, Steganography, Classical Encryption Techniques, Simplified DES, Block Cipher Principles, The Data Encryption Standard, The Strength Of DES, Differential And Linear Cryptanalysis Block Cipher, Design Principles, Block Cipher Modes Of Operations, Conventional Encryption Algorithms, Public Key Encryption.

Ethical hacking **15 hours**

Introduction to Ethical Hacking - Classes of hacker, hacking methodology, Penetration testing, **Scanning and Enumeration** – Types of scanning, OS finger printing, vulnerability management, **Sniffing and Social Engineering** – MAC flooding, DHCP attack, ARP poisoning, MCA spoofing, impact of social engineering, **Dos and Session Hijacking** – DDoS attack methodology, spoofing vs hijacking at the application level, session hijacking defensive strategies, **Web Server and applications** – client server relationship, vulnerabilities of web server and applications, session management issues.

Cyber Forensics **15 hours**

Overview of Cyber Forensics – Preparing digital investigation, private sector investigation, **Data Acquisition and Incident Scenes** – Understanding storage format for digital investigation, Examining NTFS disk, **Network and Cloud Forensics** – Developing procedure for network forensics, challenges in cloud forensics, acquisition in cloud forensics, **Email and Social Media Forensics** – exploring the role of email and server investigation, **Forensics Report Writing and Ethics for Expert Witness** - Understanding the importance of reports, guidelines for writing reports and generating report using forensic software.

Virtual Lab Sessions **15 hours**

1. **Ethical Hacking Lab**
   AIM: 1. Program to scan vulnerability ports.
   2. External Network scanning using Supers can tool.

3. SQL injection attack

2.**Network Security Lab**

AIM: 1. Network Sniffing and Collection of Information in the Network.

2. To degrade the performance of the system using DOS attacks.
3. Manipulate the database using SQL Map.
4. Monitor malicious activity on your system.
5. Performance monitor.

3.**Cyber Forensics Lab**

AIM: 1. recovering of deleted data from the storage medium.

2. Image creation from seized storage medium.
3. FAW – Forensic acquisition of website.
4. Autopsy – storage media analysis.

Email header using Email header pro.

Methodology:

- **Group Discussions.**
- **Presentations Submission and Assignment Evaluation**
- **Practical Sessions.**
- **Tools installation.**