ANNEXURE I

Course Name: Certificate Course in Fundamentals of Cyber Security & Cyber Forensics

Course Objective: The objective of this course is to provide the students a detailed knowledge in the field of Cyber security. The students will learn the fundamental ideas behind cyber security, the evolution of the paradigm, its applicability, benefits, as well as current and future challenges.

Prerequisite: Candidates should be proficient in Computer Fundamentals, Networking concept and experience in IT Domain.

Course Outcome: The students will be provided an overview of networking and its maintenance, TCP/IP cyber security, network defence and web application and overview of cryptography and will help the students to make carrier in Network management and cyber security.

Course Duration: 80 Hrs (8 hours/ day for 2 Weeks)

Teaching Schema

S. No.	Modules	Hours
1	Windows & Linux Environment	10
2	TCP/IP Cyber Security Perspective	10
3	Security Threats and Vulnerabilities	12
4	Overview of Network Defence & web applications	14
5	Cryptography and Network Security	12
6	Introduction to Cyber Forensics & cybercrime investigation	10
7	Digital Forensics Tools and Techniques	12
	Total	**80**

Detailed Course Content

1. **Windows Environment**
   - User account
   - Basic commands
   - File management etc.
2. **Linux Environment**
   - Introducing Linux,
   - Installing Linux
   - Distributions
   - Devices and drives in Linux
   - File system Hierarchy
   - How user preferences are stored in your home directory
   - Updating your system with up2date / yum.
   - The command-line (shells, tab completion, cd, ls)
   - file management: cd, df, find, locate
   - Adding users, groups
   - su - the obsoleted way to become the root user.
   - All basic commands and etc.
3. **TCP/IP Cyber Security Perspective**
   - Describe OSI Layers and TCP/IP suite of layers
   - Describe the need of layers
   - Describe the difference between layers
   - Describe the layers wise protocols
4. **Security Threats and Vulnerabilities**
   - Understand the vulnerabilities and security threats

- Understand stages of attack
    - Information Gathering
    - Scanning
    - Vulnerability Analysis
    - Exploit systems
    - Covering Tracks
- Tools used at attack stages

5. Overview of Network Defence & Web Application Security

- Network Components (Firewall, IDS, Router)
- Defensible Network Architecture
- Introduction to Perimeter Security
- What is a Firewall?
    - Why do you need firewall?
    - Types of firewalls
    - What can a firewall do?
    - Is a firewall sufficient to secure network?
    - What can a firewall not do
    - Describe what is a Perimeter Security?
    - Describe what are Perimeter Security devices?
    - Describe why we use so many devices?
    - Describe about the purpose and limitations of
    - Perimeter Defenses
    - Describe the challenges and Perimeter Design
    - Describe defense in depth
- Burp suite Using Proxy Server
- Http request & response
- Tools: Burp suite, Nmap, Wireshark, Metasploit, Ettercap etc

5. Cryptography and Network Security

- Cryptography and its Applications
- Network Security and Protocols for Secure Communication
- Digital signature concept
- Apache SSL concept

6. Introduction to Cyber Forensics & cybercrime investigation

- Overview of cybercrime and its impact on society
- Types of cybercrime and their characteristics
- Importance of cybercrime investigation
- Legal and ethical considerations in cybercrime investigation
- Digital evidence collection and preservation
- Computer forensics and analysis
- Network forensics and analysis
- Mobile device forensics and analysis

7. Digital Forensics Tools and Techniques

- Introduction to digital forensics and its role in cybercrime investigations
- Basic principles of computer and mobile device forensics, including the collection, preservation, and analysis of digital evidence
- Common digital forensics tools and software used in cybercrime investigations, including EnCase, FTK, and Autopsy
- Techniques for conducting a forensic examination, including imaging and analyzing hard drives, memory dumps, and mobile devices
- Understanding the types of digital evidence, including email, instant messages, social media, and web browsing history
- Techniques for collecting digital evidence, including search and seizure, subpoenas, and warrants
- Procedures for handling digital evidence, including maintaining chain of custody, ensuring integrity, and preventing contamination.