ANNEXURE I

Course Name: Certificate Course in Cyber Security and Malware Analytics

Course Objective: The objective of this course is to provide the students a detailed knowledge in the field of Cyber security & Malware Analysis. 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, web application, overview of cryptography and Malware Analysis that will help the students to make carrier in Network Management and Cyber Security.

Teaching Schema:

Module	Title	Hours
1	Windows & Linux Environment	12
2	TCP/IP Cyber Security Perspective	12
3	Security Threats and Vulnerabilities	15
4	Overview of Network Defence	15
5	Web Application Security	15
6	Cryptography and Network Security	15
7	OS Hardening	10
8	Introduction to Digital Forensics	06
9	Malware Analysis	20
	Total	**120**

Course Content:

Module 1 - Windows & 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

Module 2: TCP/ IP Cyber Security Perspective

- Basics and Fundamentals
- CIA Triad
- Security principles
- Describe OSI Layers and TCP/IP suite of layers
- Describe the need of layers
- Describe the difference between layers
- Describe the layers wise protocols with practical

Module 3: 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

Module 4: Overview of Network Defence

- Network Components (Firewall, IDS, Router)
- Defensible Network Architecture
- Introduction to Perimeter Security
- OWASP Concept
- 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

Module 5: Web Application Security

- HTTP Request and Response Headers

- Introduction to Web Application Security & its importance
- Information Gathering
- Burp suite Using Proxy Server
- Insecure Direct Object Reference
- Tools: Burp suite, Nmap, Wireshark, Metasploit, Ettercap etc.

Module 6: Cryptography and Network Security

- Cryptography and its Applications
- Network Security
- Digital signature concept
- Apache SSL concept

Module 7: OS Hardening

- Process of securely configuring the system
- Correcting misconfiguration
- Disabling unnecessary & vulnerable services
- Make system more reliable
- Protect system from exploits and attacks
- Tools: Nessus Professional, Burp Suite etc

Module 8: Introduction to Cyber Forensics

- Cyber Crimes
- Cyber Laws
- Digital Forensic
- Disk Forensics
- Memory Forensics
- Tools: FTK, AUTOPSY ETC

Module 9: Malware Analysis

- Malware Types
- Malware Analysis Methodology
- Static Malware Analysis
- Dynamics of Malware Analysis
- Malware detection techniques
- Basic features of OllyDbg
- Introduction to file format
- Data encoding & Polymorphism
- Keyloggers and Information stealers
- Malware Analysis using OllyDbg, IDA pro and WINDBG
- Case Study