Course Name: Certificate Course in Cybersecurity & Malware Analytics

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	Operating System Environment	10
2	TCP/IP Cyber Security Perspective	10
3	Security Threats and Vulnerabilities	12
4	Overview of Network Defense	14
5	Web Application Security	12
6	Cryptography and Network Security	10
7	Malware Analytics	12
	Total	**80**

Detailed Course Content

1. **Operating System Environment**
   - Introducing Windows
   - Windows Tools
   - Introduction to 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

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

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

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?
- 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

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

6. Cryptography and Network Security

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

7 Fundamentals of Malware Analytics

- Malware Types
- Malware Analytics methodology
- Static Malware Analytics
- Dynamis Malware Analytics
- Malware detection techniques
- Advanced Malware analytics
- Basic features of OllyDbg
- Introduction to file format
- Data encoding & Polymorphism
- Keyloggers and Information stealers
- Malware Analytics using OllyDbg, IDA pro and WINDBG
- SNORT

Case study