Course Name: Cyber Security

ABOUT THE COURSE

TOTAL DURATION:	45 Hrs
MODE OF DELIVERY	Virtual Instructor Led
TOTAL MARKS:	75

Course Learning Objectives	● Analyse the importance and application of cybersecurity in today's digital world. ● Identify various types of cyber threats, including malware, phishing, ransomware, and social engineering. ● Use range of cybersecurity tools and technologies used in the industry. ● Implement security features and best practices for operating systems (Windows, Linux) and network devices. ● Element of hands on – Kali Linux – for students to comprehend latest technical part for Cyber Security
Course Outcomes	Upon completion of the course, students will be able to: ● Use the features of Kali Linux. ● Analyse how attackers exploit vulnerabilities and compromise systems. ● Analyse the role of cryptography in securing data and communications.

TABLE 2: MODULE WISE COURSE CONTENT AND FINAL USECASE			
SL.NO	**MODULE NAME**	**MODULE CONTENT**	**FINAL USECASE**
1	**INTRODUCTION TO CYBERSECURITY**	Overview of the importance of cybersecurity in the digital landscape - Explanation of the role of cybersecurity in protecting information and systems - Basic networking concepts essential for	

		understanding cybersecurity - Overview of key terms and principles in networking - Practical simulation using CISCO Packet Tracer to understand network configurations - Hands-on experience with network setups to reinforce networking concepts.	**Phishing Attack Incident in Real Time or online financials scams:** Examine a real-world case where a phishing attack compromised sensitive information in an organization. Discuss preventative measures and employee training programs to ensure the risks of social engineering attacks.
2	**Explanation on Kali Linux**	Preparation for Kali Linux - Kali Linux Installation - Understanding the significance of Kali Linux in cybersecurity - Preparing the environment for subsequent modules by setting up Kali Linux	
3	**SOCIAL ENGINEERING ATTACKS**	Comprehensive understanding of phishing attacks and their mechanisms - Analysis of real-world examples to grasp the working flow of phishing attacks -Hands-on experience with setoolkit for creating phishing websites - Practical exercises to simulate and understand the phishing attack process - Explanation of keyloggers and their role in cybersecurity - Overview of different types of keyloggers and their functionalities - Strategies and countermeasures to enhance cybersecurity in the context of social engineering	

4	**BROWSER VULNERABILITY**	Configuration steps for the Beef tool in cybersecurity - Understanding the functionalities of the Beef tool in exploiting browser vulnerabilities - Practical exercises on using Beef tool commands for session hijacking - Understanding the impact and security implications of session hijacking	
5	**SYSTEM HACKING & SECURITY**	Overview of Nmap and its significance in system hacking - Understanding how Nmap is used for network discovery and security scanning - Practical application of Nmap commands to identify system vulnerabilities - Analyzing Nmap scan results for enhanced system security.	
6	**MAN IN THE MIDDLE**	Explanation of ARP spoofing and DNS spoofing techniques - Understanding their role in Man-In-The-Middle (MITM) attacks - In-depth analysis of Man-In-The-Middle attacks - Countermeasures and security practices to mitigate MITM vulnerabilities.	

7	**SECURE THE DATA TO PREVENT HACKERS**	Overview of steganography and its application in data security - Practical exercises using OpenStego tool and Python for hiding information - Understanding the significance of VeraCrypt in data encryption - Hands-on experience with VeraCrypt for securing sensitive data.	

Student Assessment Plan:

The final use case project will be divided into tasks by the training partner for each specific institution. Such tasks will be jointly evaluated by the college faculty and the training partner with following weightage to be followed,

- 75% weightage to the external practical assessment.
- 25% weightage to the internal assessment.

Assessment Rubric

Sl no	**Assessment Component**	**Evaluation Parameters**	**Maximum Marks**
1	Mentor Led Session Attendance	VIA LMS	30
2	Learning Plan (Self-Paced)	VIA IBM	25
3	Submission of Project Milestone Progress	VIA LMS	20
4	TOTAL		75

Employment Potential:

A student having completed this course will ready the learning for pursuing careers in the following job roles.

- **Security Analyst**: Analyzing and monitoring security threats, incidents, and vulnerabilities.
- **Network Security Analyst**: Focusing on securing an organization's network infrastructure and identifying and mitigating potential threats.
- **Security Operations Center (SOC) Analyst**: Monitoring and responding to security alerts and incidents in a SOC environment.
- **IT Security Administrator**: Implementing and managing security measures for IT systems, networks, and infrastructure.
- **Security Consultant**: Providing advisory services on cybersecurity best practices, conducting security assessments, and recommending improvements.