SEMESTER-V

COURSE 14: CYBER SECURITY

Theory Credits: 3 3 hrs/week

Course Objectives:

The aim of this course is to help the learner to understand key terms and concepts in cyber security. The Learner will learn to secure clean and corrupted systems, protect personal data, and secure computer networks. The Learner will be able to examine secure software development practices and gain an understanding of cryptography, how it has evolved, and some key encryption techniques used today.

Learning Outcomes:

The students will be able to:

Analyze and evaluate the cyber security needs of an organization. Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation. Measure the performance and troubleshoot cyber security systems. Implement cyber security solutions and use of cyber security, information assurance, and cyber / computer forensics software/tools. The Learner will develop an understanding of security policies (such as confidentiality, integrity, and availability) and protocols to implement such policies and will gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.

Unit 1: Cyber Security Fundamentals: Network Security Concepts: Information Assurance Fundamentals, Basics of Cryptography: Symmetric and Asymmetric, DNS, Firewalls, Virtualization, Radio-Frequency Identification Microsoft Windows Security Principles: Windows Tokens, Window Messaging, Windows Program Execution, Windows Firewall

Case Study: Install any Virtualization Software and perform various tasks

Unit 2: Attacker techniques and motivations: Anti forensics, Tunneling Techniques, Fraud Techniques, and Threat Infrastructure

Case Study: Working with Free and commercial proxies available from web-hack.ru.

Unit 3: Exploitation: Techniques to gain a Foothold, Misdirection, Reconnaissanse, and Disruption Methods

Case Study: Working with SQL Injection attacks and DDoS attacks

ADIKAVI NANNAYA UNIVERSITY: RAJMAHENDRAVARAM
Single Major B.Com. Computer Applications (w.e.f:2023-24A.B)

Unit 4: Malicious Code: Self-Replicating Malicious Code, Evading Detection and Elevating Privileges, Stealing Information and Exploitation.

Case Study: Identify latest Malwares and differentiate different types of malwares

Unit 5: Defense and Analysis Techniques: Memory Forensics, Honeypots, Malicious Code Naming, Automated Malicious Code Analysis Systems, Intrusion Detection Systems

Case Study: Identify latest Anti-Virus Softwares in the market and compare the functionality of each Anti-Virus

Text Books:

1. Cyber Security Essentials by James Graham, Richard Howard, Ryan Olson, CRC Press
2. Introduction to Cyber Security by Jeetendra Pandey
3. Cryptography and Network Security by William Stallings

References:

Cyber Security for Beginners by Heimdal® Security - Proactive Cyber Security Software (heimdalsecurity.com)