

CSH302: PRINCIPLES OF CYBER SECURITY

Hours/Week: 4

I.A. Marks: 30

Credits: 4

Exam. Marks: 70

Course Learning Objectives: Students will try to learn

1. Basics of cyber security and cyber security framework.
 2. The concept of System Access, Threat and incident management and cyber-attack protection.
 3. Various techniques to solve cyber security threats and concepts of phishing.
 4. Cybercrime concepts and security in real time applications.
-

Course Outcomes: After completing the course, the students will be able to,

- CO1: Define and illustrate cyber security concepts and principles
 - CO2: Analyze the working of cyber security principles to system design
 - CO3: Apply appropriate techniques to solve cyber security threats
 - CO4: Evaluate cyber security through network defense controls
 - CO5: Realize the importance of security in real time applications
 - CO6: Understand the tools and methods used in cyber security.
 - CO7: Knows the concept of cybercrime and firewall protection
-

UNIT-I

12 Hrs

Introduction to Cyber Security, Defining Cyberspace and Cyber security, Standards of Good Practice for Information Security, **ISO Suite** of Information Security Standards, **NIST Cyber security** Framework and Security Documents, CIS Critical Security Controls for Effective Cyber Defense, **COBIT 5 for Information Security**, Payment Card Industry Data Security Standard.

UNIT-II

12Hrs.

System Access System Access Concepts, User Authentication, Password-Based Authentication, Possession-Based Authentication, **Biometric Authentication**, Risk Assessment for User Authentication, Access Control, Customer Access. Threat and Incident Management Technical Vulnerability Management, Security Event Logging, Security Event Management, Threat Intelligence, **Cyber Attack Protection**.

UNIT-III

12Hrs.

Phishing and Identity Theft Introduction, Phishing - Methods of Phishing, Phishing Techniques, Phishing Toolkits and Spy Phishing. Identity Theft – PII, Types of Identity Theft, Techniques of ID Theft. **Digital Forensics Science**, Need for Computer Cyber forensics and Digital Evidence, Digital Forensics Life Cycle

UNIT-IV

12Hrs.

Tools and Methods used in Cybercrime Introduction, Proxy Server and Anonymizers, Password Cracking, Key loggers and Spyware, **Virus and Worms**, **Trojan and backdoors**, Steganography, DOS and **DDOS attack**, **SQLinjection**, Buffer Overflow Network Defense tools Firewalls and Packet Filters: Firewall Basics, **Packet Filter Vs Firewall**, How a Firewall Protects a Network, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls

REFERENCE BOOKS:

1. William Stallings, Effective Cyber Security: A Guide to Using Best Practices and Standards, Addison-Wesley Professional, ISBN-13: 978-0134772806.
 2. Nina Godbole&SunitBelapure, Cyber Security, Wiley India, 2012, ISBN: 9788126521791.
-

3. Mike Shema, Anti-Hacker Tool Kit (Indian Edition), 4th Edition, Publication McGraw Hill, ISBN: 9789339212155.
4. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley Publication, ISBN 9788126521791.

