PRINCIPLES OF INFORMATION SECURITY

Credits:2 **Semester:III**
Course Code:G22CSCS1T **No. of Lecture hours:30**
Objectives:

- To compile, analyse, and assess the applicability of best practices in addressing information.
- To address the issues relevant to the cyber security community

Course Outcomes:

CO1: **Explain** concepts of confidentiality, availability and integrity (CIA) in context of Information security
CO2: **Identify** the risk, assess and risk control strategies.
CO3: **Demonstrate** expertise in configuring host and network level technical security controls to include host firewalls
CO4: **Analyse** systems, tools, methods, and techniques for securing digital information within an organisation
CO5: **Develop** encryption and decryption techniques.

UNIT –I	**6Hrs**
INTRODUCTION OF INFORMATION SECURITY	
1. Introduction to Security, Critical Characteristics of Information	2
2. NSTISSC Security Model, Components of Information Security, Balancing Information Security and Access	2
3. Security System Development Life Cycle	2
UNIT –II	**6 Hrs**
THE NEED FOR SECURITY	
1. Important functions of Information Security	2
2. Threats and category of Threats	2
3. Attacks and Types of Attacks	2
UNIT –III	**6Hrs**
1. Firewalls: Processing modes, categorizations	2
2. Firewall Architecture, Choosing a Firewall	2
4. Firewall Rules	1
5. VPN: Transport and Tunnel Mode	1
UNIT-IV	**6 Hrs**
1. IDPS :terminology, types of IDPS	1
2. IDPS Detection Methods, IDPS Response Behaviour	2
3. Strengths and Limitations of IDPS	1
4. Honeypots, Honeynets and Padded Cell Systems	1
5. Port Scanners	1
UNIT-V	**6 Hrs**
1. Terminology	1
2. Steganography	1
3. Protocol for Secure Communication: Securing Internet with SSL	1
4. Securing web Transactions SET	2
5. Securing wireless Network with WEP and WPA	1

ESSENTIAL READING

1. Whitman Michael, E. and Mattord Herbert, J. 2011. **Principles and practices of Information Security**. 4th Edition. USA: Course Technology

Principles of Information Security Lab

Credits:1 **Semester:III**

Course Code: GE22CSCS1P **No. of Practical hours:30**

Objective: To get hands on experience with popular hacking tools and understand various hacking techniques in brief.

Outcome: Students will be able to learn some of the skills that you would require to become an expert in Ethical Hacking.

Topics to be covered

1. Installation of Operating System Using VMware.
2. Exploring Internet Options for a Browser, Examination and configuring the Contents of Security and Privacy Tabs.
3. Setting up a Simple network using Simulation Tools(Packet tracer)
4. Perform an experiment to Grab a Banner with Telnet
5. Using Nmap
   - Find open ports on a System
   - Find the machines which are active
   - Find the version of Remote OS on other systems
   - Find the version of Software installed on another system.
6. Program to implement Virus.
7. Demonstrate Intrusion Detection System
8. Implementation of Stenography–Hiding a Text File within a Image File using WinRar
9. Digital Signing a word document, PDF document and Email