

CSC302:SECURING COMPUTING SYSTEMS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: discuss security concepts, compare threat types, and cryptographic solutions for robust security implementation.

CO2 :: utilize secure cryptographic protocols and techniques to ensure data confidentiality, integrity, and authenticity.

CO3 :: determine the secure cloud architectures, vulnerabilities, zero trust architecture, ensure resiliency, and manage assets and securities.

CO4 :: examine to enhance network, endpoint, and application security capabilities and protocols.

CO5 :: apply security assessments and incident response procedures to effectively detect, respond to, and recover from security incidents.

CO6 :: demonstrate risk management, data protection, and compliance through processes and policies

Unit I

Summarize Fundamental Security Concepts : Security Concepts, Security Controls

Compare Threat Types : Threat Actors, Attack Surfaces, Social Engineering

Explain Cryptographic Solutions : Cryptographic Algorithms, Public Key Infrastructure, Cryptographic Solutions

Unit II

Implement Identity and Access Management : Authentication, Authorization, Identity Management

Secure Enterprise Network Architecture : Enterprise Network Architecture, Network Security Appliances, Secure Communications

Unit III

Secure Cloud Network Architecture : Cloud Infrastructure, Embedded Systems and Zero Trust Architecture

Explain Resiliency and Site Security Concepts : Asset Management, Redundancy Strategies, Physical Security

Explain Vulnerability Management : Device and OS Vulnerabilities, Application and Cloud Vulnerabilities, Vulnerability Identification Methods, Vulnerability Analysis and Remediation

Unit IV

Evaluate Network Security Capabilities : Network Security Capability Enhancement, Network Security Baselines

Assess Endpoint Security Capabilities : Implement Endpoint Security, Mobile Device Hardening

Enhance Application Security Capabilities : Application Protocol Security Baselines, Cloud and Web Application Security Concepts

Unit V

Explain Incident Response and Monitoring Concepts : Incident Response, Digital Forensics, Data Sources, Alerting and Monitoring Tools

Analyze Indicators of Malicious Activity : Malware Attack Indicators, Physical and Network Attack Indicators, Application Attack Indicators

Summarize Security Governance Concepts : Policies Standards and Procedures, Change Management, Automation and Orchestration

Unit VI

Explain Risk Management Processes : Risk Management Processes and Concepts, Vendor Management Concepts, Audits and Assessments

Summarize Data Protection and Compliance Concepts : Data Classification and Compliance, Personnel Policies

List of Practicals / Experiments:

List of Practical's / Experiments

- Configuring Examples of Security Control Types
- Finding Open Service Ports
- Using Storage Encryption
- Using Hashing and Salting
- Managing Permissions
- Using IPSec Tunneling
- Using Virtualization
- Performing Drive Sanitization
- Exploiting and Detecting SQLi
- Understanding Security Baselines
- Using Group Policy
- Performing DNS Filtering
- Incident Response: Detection
- Using Network Sniffers
- Performing Root Cause Analysis
- Detecting and Responding to Malware
- Understanding On-Path Attacks
- Perform System Configuration Gap Analysis
- Using SET to Perform Social Engineering
- Managing Password Security
- Setting up Remote Access
- Using Containers
- Implement Backups
- Working with Threat Feeds
- Performing Vulnerability Scans
- Implementing a Firewall
- Hardening
- Configuring System Monitoring
- Performing Digital Forensics
- Using a Playbook
- Performing Reconnaissance
- Training and Awareness through Simulation
- Network Incident Investigation and Remediation
- Implementing Allow Lists and Deny Lists
- Use Cases of Automation and Scripting
- Performing Penetration Testing

References:

1. COMPTIA SECURITY+ STUDY GUIDE by JAMES PENGELLY, CompTIA
2. CYBERSECURITY: THE BEGINNER'S GUIDE by DR. ERDAL OZKAYA, PACKT PUBLISHING
3. COMPTIA SECURITY+SY0-701 CERTIFICATION STUDY GUIDE by JAMES PENGELLY, GARETH MARCHANT, CompTIA

