CCCS-1-03T Cyber Attacks and Counter Measures

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits:4
Pass Percentage: 40%

Objective
Objective of this paper is to explain the basic Cyber Attacks and Counter Measures.

Section-A

Unit I: Cyber Attacks: Introduction, Types. Assets: Identification, Accountability. Vulnerability and Threats, Risk Management, Qualitative Risk Assessment, Information Security Framework: Introduction, Policies, Standards, Baselines, Guidelines and Procedures.

Unit II: Security: Basics, User Access Controls, Authentication, Access Control: Framework, Techniques and Technologies, Training and Awareness and Its types, Technical Security Controls: Preventive, Detective, Corrective. Protection form malicious attacks

Unit III: Networks and Communication: Data Communication, Characteristics and components, Data flow. Computer Network, Categories, Protocol, External Services, Cloud Computing: Introduction, Models, Benefits, Challenges, Private, Public Clouds,

Unit IV: Software Engineering Life Cycle: Stages, Models: Waterfall, Iterative, Spiral, V-Model, Big Bang, Agile, RAD, Prototype,

Section-B

Unit V: Authentication: Authentication Vs Authorization, Methods and Protocols: Kerberos, SSL, Protocol, Password Authentication, Challenge-Handshake Authentication (CHAP), MS-CHAP, Extensible Authentication, Remote Authentication.

Unit VI: Service Set Identification (SSID), Encryption Methods: Wire Equivalent Privacy, WPA, WPA2, MAC Filtering, Wireless Routers, Creating Wireless Network, WLAN

Unit VII: Investigation Techniques and Cyber Forensics, Types of Investigation, Evidence and Analysis, Steps for Forensics Investigation, Forensics Tools, Investigation, Common Types of Email Abuse, Tracking Location of Email Sender, Scam or Hiex Emails and Websites, Fake Social Media Profile,

Unit VIII: Cryptography: Objectives, Type, OS Encryption, Public key Cryptography,