CCCS-1-04T Cyber Security Techniques

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 Security Techniques.

Section-A

Unit I: IT Security Policies, Types of Information Security Policies, IT SECURITY PROCEDURES, ORGANIZATIONAL SECURITY: Physical Security, Financial Security, Online Security, Security Token, Electronic Mail Security, Pretty Good Privacy, Multipurpose Internet Mail Extensions, Message Authentication Code, Firewall, Malicious Software, Denial of Service Attack, Phishing,

Unit II: ATTACKS: Insider Attack and its Prevention, Outsider Attack and its Prevention, CYBER CRIME: Overview, Categories, Challenges, Complexities and effects, Intrusion Detection System (IDS): Introduction, Components, CHARACTERSTICS, Types of IDS: Network IDS, Host Based IDS, Misuse-Detection IDS, Anomaly- Detection IDS, STEPS TO INSTALL AN IDS IN AN ORGANIZATION, INCIDENT HANDLING,

Unit III: Assets: Introduction, SECURING AN ASSET, HARDWARE BASED SECURITY: Types, Functionality, Implementation, FIREWALL: Types, Hardware Based, Software Based, WIRELESS SECURITY, NFORMATION ASSURANCE: Introduction, Dimensions of McCumber Cube, CYBER SECURITY ASSURANCE FRAMEWORK – INDIA: Strategic Approach, Actions, Strategic Objectives,

Unit IV: CYBER SECURITY MATURITY AND SELF ASSESMENT: Cyber Security Capability Maturity Model (CMM), Selection of Cyber Capacity Building Factors, Guidelines for the use of Cyber CMM, Virus and its Types, Worm and its tyoes, Trojan Horse, Bot and Botnets, RANSOMWARE, ROOTKITS, EXPLOIT KITS, CYBER WEAPONS, POS MALWARE , MALWARE PERPETRATORS, MALWARE ATTACKING TECHNIQUES, MOBILE MALWARE TRANSITION: App Based Threats, OS based Threats, Android Security Threats, Android Security Threats,

Section-B

Unit V: Web Architecture: Hyper Text Markup Language (HTML), Uniform Resource Identifier, Hyper Text Transfer Protocol (HTTP), ATTAACKS ON APPLICATIONS, DEMONSTRATION OF IMPACT OF XSS VULNERABILITY, APPLICATION SECURITY, SOCIAL ENGINEERING: Life Cycle, TYPES: Physical, Remote, Computer-based, Phone Based,

Unit VI: COMPUTER FORENSICS PROCEDURE: Data Collection, Examination, Analysis, Reporting, DATA COLLECTION AND ACQUISITION, WINDOWS LIVE RESPONSE/ FORENSICS, Capturing Memory, Capturing the volatile data, Transferring data to the investigators machine, Introduction to Disk Image.

Unit VII: CYBER SECURITY INITIATIVES: National Cyber Security Policy, Critical Information Infrastructure Protection, Cyber Crisis Management Plan, CERT-IN AND OTHER AGENCIES: Indian Computer Emergency Response Team (CERT-In), Ministry of Communications & IT, Institute for Defense Studies and Analysis (IDSA) , National Intelligence Grid (NATGRID), National Counter Terrorism Centre, Crime and Criminal Tracking Network & Systems (CCTNS), Data Security Council of India (DSCI)

Unit VIII: RISK MANAGEMENT, RISK ASSESSMENT METHODOLOGIES, GLOBAL CYBERSECURITY INDEX AND CYBERWELLNESS PROFILES, NATIONAL CYBER SECURITY POLICY- INDIA,