MIT(CS)-103

Cyber Attacks and Counter Measures: User Perspective

BLOCK-I

UNIT I: CYBER ATTACKS, TYPES OF ATTACKS MOTIVATION

Introduction, Cyber-attack, Types of cyber-attack or threats.

UNIT II: ASSET, THREAT AND RISK MANAGMENT

Introduction to asset, Identification of assets, Information assets, Software assets, Physical assets, Services, Accountability of assets, Assets valuation, Preparing a schema for classification, Implementation of the classification schema, vulnerability and threats, Types of threat, Risk management, Quantitative risk assessment, Advantages of quantitative risk assessments, Disadvantages of quantitative risk assessments, Qualitative risk assessment, Advantages of qualitative risk assessments, Disadvantages of qualitative risk assessments.

UNIT III: ORAGANIZATION SECURITY & FRAMEWORKS

Introduction to information security framework, Advantage of Information Security framework, Standards, Best Practices and Frameworks, ISO, COSO, COBIT (IT Governance Framework), POLICIES, STANDARDS, BASELINES, GUIDELINES AND PROCEDURES, Security Policy.

UNIT IV: INFORMATION SECURITY GOVERNANCE

Introduction to information security governance, Desired Outcome, Benefits of Information Security Governance, Importance of information security and information security governance, legal frameworks, Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Security standards and procedure, Why do we need security standards?.

BLOCK-II

UNIT I: SECURITY CONTROLS

SECURITY BASICS, Physical Controls, Technical Controls, Administrative Controls, Physical security, protection on the inside, Partitioning and protecting network boundaries with firewalls, USER ACCESS CONTROLS, Why Access Controls are required, What are Access Control Models, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC), Authentication, User password Authentication, Windows user based authentication, Directory based authentication, Certificate based authentication, Smart card based authentication, Biometrics, Grid based Authentication, Knowledge-based authentication, Machine Authentication, One time Password (OTP), Access Control Framework (ACF), Access Control Techniques and Technologies, Rule Based Access

control, Menu Based Access Control, Access Control List, Content Based Access Control, Access control Markup Language (XACML), Security Assertion Markup Language (SAML), TRAINING AND AWARENESS, Types of Training, Classroom-Style Training, Security Awareness Website, Helpful Hints, Visual Aids, Promotions, Training Topics, Physical Security, Desktop Security, Wireless Networks and Security, Password Security, Phishing, Hoaxes, Malware, Viruses, Worms, Trojans, Spyware and Adware.

UNIT II: SECURITY CONTROL DESIGN

Introduction, Technical security controls, Preventive Technical Controls, Access Control Software, Antivirus Software, Library Control Systems, Passwords Smart Cards, Encryption, Dial-Up Access Control and Callback Systems, Detective Technical Controls, Audit Trails, Intrusion Detection Systems, Corrective Technical Controls, OS Upgrade, Backup Data restoral, Vulnerability Mitigation, PROTECTION FROM MALICIOUS ATTACKS, NETWORKS AND COMMUNICAITON, Data Communication, Characteristics of Data Communication, Components of Data Communication, Data Representation, Data Flow, Simplex, Half Duplex, Full Duplex, COMPUTER NETWORK, Categories of Network, Protocol, Elements of a Protocol, External Services, Policy on Use of External Services, CLOUD COMPUTING, Cloud Computing Models, Understanding Public and Private Clouds, Public Cloud, Private Cloud, Hybrid Cloud, Cloud Computing Benefits, Cloud Computing Challenges, IT Infrastructure.

UNIT III: SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

Introduction, SOFTWARE DEVELOPMENT LIFECYCLE (SDLC), Definition Stages in SDLC, SDLC MODELS, WATERFALL MODEL, Waterfall Model Design, Stages of the Waterfall model, Application, Advantages and Disadvantages of Waterfall Model, Advantages, Disadvantages, ITERATIVE MODEL, Iterative Model design, Application, Advantages and Disadvantages of Iterative Model, Advantages, Disadvantages, SPIRAL MODEL, Spiral Model design, Application, Advantages and Disadvantages of Spiral Model, Advantages, Disadvantages, V – MODEL, V- Model design, Verification Phases, Coding Phase, Validation Phases, Application, Advantages and Disadvantages of Software Prototyping V-Model, Advantage, Disadvantage, BIG BANG MODEL, Big Bang Model design and Application, Advantages and Disadvantages of Waterfall Model, Disadvantage, AGILE MODEL, Concept of Agility, RAPID APPLICATION DEVELOPMENT MODEL, RAD Concept, RAD Model Design, RAD Model Applications, Advantages and Disadvantages of RAD Model, Advantage, Disadvantage, SOFTWARE PROTOTYPING MODEL, Software Prototyping Concept, Steps involved in Software Prototyping, Software Prototyping Types, Software Prototyping Application.

BLOCK III

UNIT I: AUTHENTICATION AND PASSWORD SECURITY

INTRODUCTION, AUTHENTICATION, Definition of Authentication, Definition of Electronic Authentication, Authentication vs. Authorization, Types of Authentication Factors, Multi Factor and Two Factor Authentication, AUTHENTICATOIN METHODS AND PROTOCOLS, Kerberos, Secure Sockets Layer(SSL), Microsoft NTLM, Password Authentication Protocol, Challenge-Handshake Authentication Protocol(CHAP), Microsoft Challenge Handshake Authentication Protocol(MS-CHAP), Extensible

Authentication Protocol, Remote Authentication Dial-In User Service (RADIUS), Certificates, Security Tokens, Selecting a Strong Password, Bad Password Combinations, Tips for a Strong Password.

UNIT II: WIRELESS SECURITY

Introduction, SERVICE SET IDENTIFICATION (SSID), Security of SSID hiding, ENCRYPTION METHODS, WEP (Wire Equivalent Privacy), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2), MAC Filtering, Configuration of Wireless MAC address filter on wireless router, WIRELESS ROUTER, HOW TO CREATE A WIRELESS NETWORK, CONFIGURATION OF WIRELESS ROUTER, WLAN, Major issues with WLAN.

UNIT III: INVESTIGATION AND DIGITAL FORENSIC

Introduction, Drivers behind this new cyber reality?, Cyber Crime and Challenges Ahead, INVESTIGATION TECHNIQUES & COMPUTER FORENSICS, Digital Forensics System, Computer based crime, Computer facilitated crime, TYPES OF INVESTIGATION, Criminal forensics, Intelligence gathering, Electronic discovery (eDiscovery), Intrusion investigation, EVIDENCE AND ANALYSIS, Attribution, Alibis and statements, Intent, Evaluation of source, Document authentication, STEPS IN FORENSICS INVESTIGATION, FORENSICS TOOLS, General forensic tools, Specialist forensic tools, Case management, Useful software, INVESTIGATION, Some important terminologies, HOW EMAIL WORKS, COMMON TYPES OF E-MAIL ABUSE WHERE THE SENDER ADDRESS IS FORGED4, Sender Addresses in E-Mails, Parts of an email, How to Identify Fake EMail And Trace Sender's Location, Fake Emails, HOW TO TRACE LOCATION OF EMAIL SENDER, What to do if IP is not there or Email is sent from Gmail, RECOGNISE SCAM OR HIAX EMAIL AND WEBSITES, Scams, Steps to avoid online scams and hoaxes, Points to Remember, FAKE SOCIAL MEDIA PROFILE INVESTIGATION, How to spot fake facebook account.

UNIT IV: INTRODUCTION TO CRYPTOGRAPHY

Introduction, Cryptography Objectives, Cryptography Glossary, TYPES OF CRYPTOGRAPHY, WHY OS ENCRYPTION IMPORTANT?, Why should Encryption be used?, How does it work?, PUBLIC KEY CRYPTOGRAPHY, Public keys and private keys, Combining public key and secret key cryptography, How public key cryptography works, APPLICATIONS OF PUBLIC KEY CRYPTOGRAPHY, Secure Web communication, Secure content distribution, SECRET KEY CRYPTOGRAPHY, Encryption and decryption using a secret key, How to get the key to the recipient, How secret key cryptography works, APPLICATIONS OF SECRET KEY CRYPTOGRAPHY, Hiding spoilers, Encrypting the contents of hard disks, Protecting pay TV transmissions.