Cyber Security Techniques (MIT(CS)-102)

BLOCK-I

UNIT-I: INFORMATION SECURITY BASICS TO POLICIES

Introduction, Detailed description of it security policies, Security policy, why policies are important?, Ways to make policies more effective, Types of information security policies, Examples of information security policies, It security procedures, Differences between policies and procedures, Aspects of organizational security, Physical security, Examples of controls for physical security which you can easily see in your daily life, Financial security, Online security, Security token, Electronic mail security, Pretty good privacy (pgp), Multipurpose internet mail extensions (mime), Message authentication code, Firewall, Malicious software, Denial of service attack, Phishing, Application vulnerabilities

UNIT II:CYBER CRIME AND DIFFERNET MODES OF ATTACKS

Introduction, Types of attacks, Insider attack, Types of insider attack, How to prevent insider attack, Outsider attack, Types of outsider attack, How to prevent outsider attack, Cyber-crime, Overview of cyber-crime, Categories of cyber-crime, Challenges of cyber-crime, Complexities of cybercrime, Effects of cyber-crime, Solutions to cybercrime, How to report an incident.

UNIT III: INTRUSION DETECTION SYSTEM

Introduction, Components of ids, Characteristics of ids, Types of ids, Network intrusion detection system, Host based intrusion detection system, Misuse- detection ids (md-ids), Anomaly- detection ids (ad-ids), Role of ids in an organization, Steps to install an ids in an organization, Incident handling.

UNIT IV: IT ASSETS AND WIRELESS SECURITY

Introduction, Securing an asset, Steps of securing an asset, Hardware based security, Types of hsms, hsm functionality, How to implement hsm, Firewall, Types of firewalls, Software based firewalls, Hardware based firewalls, How to prevent your network from anonymous attack, Wireless security, Use of wi-fi, Types of wireless security, wpa.

BLOCK-II

UNIT I: CYBER SECURITY ASSURANCE FRAMEWORK

INTRODUCTION TO INFORMATION ASSURANCE: Dimensions of mccumber cube, Cyber security assurance framework – india, Strategic approach, Actions, Strategic objectives, Security policy, compliance and assurance, Security incident - early warning & response, Security training - security, digital evidence & forensics, Security r&d, Security best practices - compliance and assurance, Cyber security maturity and self-assessment, Cyber security capability maturity model (cmm), Selection of cyber capacity building factors, Guidelines for the use of cyber capability maturity model, Cyber security exercises for assessing the cyber defense preparedness, Types of cyber security exercises.

UNIT II: DESKTOP SECURITY AND MALWARE

Introduction, Virus, How computer virus works, Type of computer viruses, File virus, Boot sector virus, Macro virus, Electronic mail (email) virus, Multi-variant virus, Radio frequency identification (rfid) virus, Virus that wrecked havoc, Worm, Types of worm, Infamous worm examples, Trojan horse, Banking Trojan, Case study alureondns changer, Bots and botnets, Botnet families Ransomware, Rootkits, Mebroot and necurs, Some known rootkits, Exploit kits, Cyber weapons, Pos malware, Malware perpetrators and their motivations, Malware attacking techniques, Mobile malware transition, App based threats, OS based threats and vulnerabilities, Android security threats, Android app threats, What we can do?

UNIT III: E-COMMERCE AND WEB-APPLICATION SECURITY

Introduction, Web architecture, Hypertext markup language (html), Uniform resource identifier, Hypertext transfer protocol (http), Attaacks on applications, Demonstration of impact of xss vulnerability, The browser exploitation framework (beef), Vulnerablity study: malicious file upload and webshells, Application security, Security integration with sdlc, Input validation, Output encoding, Error handling, Sql statements, Least privilege model, Re-authentication for important transactions, Proper use of encryption, Manual security testing, Training and awareness, Security is a continuous process.

UNIT IV: SOCIAL ENGINEERING

Introduction: Social engineering, Social engineering attack cycle, Different types of social engineering, Physical social engineering, Remote social engineering, Computer-based social engineering, Social engineering by email,
Pop-up windows / browser interceptions, Social engineering by phone, Mumble attack, ivr or phone phishing (aka. vishing), Other methods, Boy who cries wolf attack, Road apples/ baiting, Diversion theft, Tools of the trade, Defending against social engineering, Continuous security awareness training for employees.

BLOCK-III

UNIT I: CYBER SECURITY RISK MANAGEMENT

Introduction, Risk management, Risk, Risk management, Risk assessment methodologies, iso/iec 27005:2011 (_information technology - security techniques - information security risk management‘), National institute of standards and technology (nist) sp 800-39 and sp 800-30, Octave allegro, isaca cobit, Cobra, Information risk assessment methodology 2 (iram2), Facilitated risk analysis process (frap), Threat agent risk assessment (tara), Tools for risk assessment, nist cybersecurity framework, Factor analysis of information risk, Threat.

UNIT II: COMPUTER FORENSICS FUNDAMENTALS AND COLLECTION OF DIGITAL EVIDENCE

Introduction, Computer forensics procedure, Data collection, Examination, Analysis, Reporting, Data collection and acquisition, Data collection, What is digital evidence, A word about write protection, examples commercial software: First responder toolkit, Seizure and acquisition, Cyber forensics acquisition tools, Evidence collection, Windows live response/ forensics, Capturing memory, Capturing the volatile data, Transferring data to the investigators machine, Introduction to disk image, Disk imaging, Acquiring disk image using ftk imager, Verifying the image created.

UNIT III: CYBER SECURITY INTIATIVES IN INDIA

Introduction, Cyber security initiatives, National cyber security policy, Critical information infrastructure protection, The types of threat to cii, the threat vectors and actors, National critical information infrastructure protection centre (nciipc), Functions of nciipc, Cyber crisis management plan and empanelment of information security auditing organizations, National cyber security exercise, National cyber coordination centre (nccc), Botnet cleaning center, e-mail policy of government of india, cert-in and other agencies, Indian computer emergency response team (cert-in), Ministry of communications & it, objectives, Cyber security, Institute for defense studies and analysis (idsa), Mission statement, National intelligence grid (natgrid), Structure and functions, National counter terrorism center, Structure and functions, Crime and criminal tracking network & systems (cctns), objectives, ministry of home affairs (mha), National crime records bureau (ncrb) Objectives, national critical information infrastructure protection centre (nciipc), Data security council of india (dsci).

UNIT IV: CYBER SECURITY STRATEGIES AND POLICIES

Introduction, Global cybersecurity index and cyberwellness profiles, National cyber security policy- india, vision, mission, objective and strategies mentioned in policy, National cyber security strategies and policies of various nations, The united states, International strategy for cyberspace, Cyberspace‘s future, Role of u.s. in cyberspace‘s future, Policy priorities, Moving forward, Canada, Specific initiatives for pillar 1- securing government systems, Specific initiatives for pillar 2- partnering to secure vital cyber systems outside the federal government, Specific initiatives for pillar 3- helping canadians to be secure online, Malaysia, Implementation approach, Establishment of the malaysia cyber security centre, New Zealand, Priority areas and key initiatives, Other initiatives, Estonia.