Information System (MIT(CS)-104)

BLOCK-I

UNIT I: NETWORKING AND COMMUNICATION

INTRODUCTION TO OSI MODEL, SENDING DATA VIA OSI MODEL, DIFFERENT TYPES OF PROTOCOLS, TCP/IP, IPX/SPX, DECnet, AppleTalk, NetBIOS, NetBEUI, Server Message Block (SMB), TCP/IP ARCHITECTURE, Layered Protocols, IP Routing, ADDRESSING, The IP Address, Subnets, Types of Subnetting, Static Subnetting, Variable Length Subnetting, Mixing Static and Variable Length Subnetting, A Static Subnetting Example, PRIVATE INTERNETS, CLASSLESS INTER-DOMAIN ROUTING (CIDR), DOMAIN NAME SYSTEM, THE HIERARCHICAL NAMESPACE, FULLY QUALIFIED DOMAIN NAMES (FQDNs), COUNTRY DOMAINS, MAPPING DOMAIN NAMES TO IP ADDRESS, INTERNET PROTOCOL (IP), IP Datagram, Direct and Indirect Destinations, IP Routing Table, INTERNET CONTROL MESSAGE PROTOCOL (ICMP), TRANSMISSION CONTROL PROTOCOL, Three-Way Handshakes, USER DATAGRAM PROTOCOL, PORTS AND SOCKETS, INTERNET PROTOCOLS , The Simple Mail Transfer Protocol, The Mail Transaction, Post Office Protocol, version 3 (POP3), Internet Message Access Protocol (IMAP), HOW INTERNET EMAIL WORKS, Two Flavors of HELO, The Sender, The recipient, The Message, FTP, Basic Commands, Initiating a Session, Getting What You Want, SSH (SECURE SHELL), SSL, How SSL Works.

UNIT II: CRYPTOGRAPHY

WHAT IS CRYPTOGRAPHY?, CRYPTOGRAPHY AND SECURITY, CRYTOGRAPHIC ALGORITHMS, Hash Algorithm, Message Digest (MD), Message Digest 4, Message Digest 5 (MD5), Secure Hash algorithm (SHA), Whirlpool, RACE Integrity Primitives Evaluation Message Digest (RIPEMD), PASSWORD HASHES, SYMMETIC CRYPTOGRAPHIC ALGORITHMS, Understanding Symmetric Algorithms, Block Cipher, Data Encryption System (DES), Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES), Other Algorithms, ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS, RSA, Elliptic curve Cryptography (ECC), Quantum Cryptography, NTRUEncrypt, USING CRYPTOGRAPHY, Encryption through Software, File and File System Cryptography, Pretty Good Privacy (PGP/GPG), Microsoft Windows Encrypting File System (EFS), Whole Disk Encryption, HARDWARE ENCRYPTION, USB Device Encryption, Hard Disk Drive Encryption, Trusted Platform Module (TPM), Hardware Security Module (HSM), DIGITAL CERTIFICATES, Defining Digital Certificates, Managing Digital Certificates, Certificate Authority (CA), Registering Authority(RA), Certificate Revocation List (CRL), Certificate Repository (CR), Certificate Repository (CR), Web Browser Management, Types of digital certificates, Class 1: Personal Digital certificates, Class 2: Server Digital Certificates, Class 3: Software Publishers Digital Certificates, Dual-Key and Dual-sided Digital Certificates, X.509 Digital Certificates, PUBLIC KEY INFRASTRUCTURE (PKI), Public-Key Cryptographic Standards (PKCS),Trust Models, Hierarchical Trust Model, Distributed Trust Model, Bridge Trust Model, MANAGINGPKI, Certificate Policy, Certificate Practice Statement (CPS), Certificate Life Cycle, KEY MANAGEMENT, Key Storage, Key Usage, Key-Handling Procedures, Escrow, Expiration, Renewal, Revocation, Recovery, TRANSPORTATION ENCRYPTION ALGORITHMS, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), Hypertext Transport Protocol over Secure Sockets Layer (HTTPS), IP SECURITY (IPSEC), IP security (IPsec).

UNIT III: VULNERABILITY ANALYSIS/PENETRATION TESTING BASICS

INTRODUCTION, TYPES OF PENTESTING, Black Box, Gray Box, White Box, CIA triad, VULNERABILITY RESEARCH AND TOOLS, ETHICS AND THE LAW, HACKING, Culture of hacking, Types of hackers, PHASES OF PENETRATION TESTING, Footprinting, Why Perform Footprinting? Goals of the Footprinting Process, Types of Reconnaissance, Scanning, Enumeration, Gaining Access, Password Cracking Techniques, Dictionary Attacks, Brute-force Attacks, Hybrid Attack, Syllable Attack, Rule-based Attack, Passive Online Attacks, Active Online Attacks, Offline Attacks, Nontechnical Attacks, Privilege Escalation, Pilfering, Creating backdoors, Covering tracks, Disabling Auditing, DataHiding, Alternate Data Streams (ADS), Denial of Service (DoS), HACKING TOOLS AND TECHNIQUES.

UNIT IV: NETWORK, EMAIL, INFRASTRUCTURE & WEB APPLICATION SECURITY

INTRODUCTION, NETWORK SECURITY CONCEPTS, SECURITY MANAGEMENT, Passive attacks, Wiretapping, Port scanner, Idle scan, Active attacks, Denial-of-service attack, DNS spoofing, Man in the middle, ARP poisoning, VLAN hopping, Switch spoofing, Double tagging, Smurf attack, Buffer overflow, Heap overflow, Format string attack, SQL injection, Phishing, Cross-site scripting, CSRF, Cyber-attack, E-MAIL SECURITY, Filtering, Web email, Reaper exploit, Encryption, WEB APPLICATION SECURITY, Security threats, Best Practices Recommendation, Security standards, Security technology, INFRASTRUCTURE SECURITY, Potential causes of infrastructure failure, Security challenges for the electricity infrastructure, Remedies.

BLOCK-II

UNIT I: CRYPTOGRAPHY BASICS

INTRODUCTION, THE PURPOSE OF CRYPTOGRAPHY, HISTORY OF CRYPTOGRAPHY, Classical cryptography, Medieval cryptography, Cryptography from 1800 to World War II, World War II cryptography, Modern cryptography, CIPHER, Simple substitution, Transposition cipher, Rail Fence cipher, Route cipher, Columnar transposition, Double transposition, Myszkowski transposition, Disrupted transposition, DETECTION AND CRYPTANALYSIS, Combinations, Fractionation, MORDERN ENCRYPTION METHODS, KEY SIZE AND VULNERABILITY, KEY MANAGEMENT, Types of keys, Key exchange, Key storage, Key use, Public Key Infrastructure (PKI), Enterprise Key and Certificate Management (EKCM), Multicast Group Key Management, Challenges, Key management solution.

UNIT II: CRYPTOGRAPHIC ALGORITHM

INTRODUCTION, TYPES OF CRYPTOGRAPHIC ALGORITHMS, Secret Key Cryptography, Stream ciphers, Block Cipher, Data Encryption Standard (DES), Advanced Encryption Standard (AES), FUNER DETAILS OF DES, BREAKING DES, AND DES VARIANTS, DES Operational Overview, Breaking DES, DES Variants, Closing Comments on DES, The Advanced Encryption Standard (AES) and Rijndael, AES (Rijndael) Overview, The SubBytes transformation, The ShiftRows transformation, The MixColumns transformation Round Key generation and the AddRoundKey transformation, Summary AES, Cisco's Stream Cipher, PUBLIC-KEY CRYPTOGRAPHY, Some of the Finer Details of Diffie-Hellman, A short digression on modulo arithmetic,

Some of the Finer Details of RSA Public-Key Cryptography, DATA INTEGRITY ALGORITHMS, Checksum, Checksum algorithms, Parity byte or parity word, Modular sum, Position-dependent checksums, General considerations, Hash Functions, WHY THREEENCRYPTION TECHNIQUES?, THE SIGNIFICANCE OF KEY LENGTH.

UNIT III: KEY DISTRIBUTION AND MANAGEMENT

INTRODUCTION, KEY GENERATION, KEY DISTRIBUTION, Key distribution methods, Key Distribution Using Symmetric Key Protocols, Mouth Frog Protocol, Needham-Schroeder Secret-Key Protocol, Otway-Rees Protocol, Kerberos Protocol, Implementation of Kerberos, SYMMETRIC KEY DISTRIBUTION USING ASYMMETRIC ENCRYPTION, ENTERPRISE KEY AND CERTIFICATE MANAEMENT (EKCM), Public Key Certificates and Certificate Authorities, Multicast Group Key Management, Challenges, Key management solution, Key installation, Key storage, Key change, Key exchange, Key use, Key control, Key disposal.

UNIT IV: CRYPTOGRAPHY FOR INTERNET SECURITY

INTRODUCTION, METHODS OF ATTACK ON CRYPTOGRAPHIC SYSTEMS, The Birthday Attack, Digital signature susceptibility, Ciphertext Only Attack (COA), Chosen Text Attack (CTA), Known Plaintext Attack (KPA), Man-in-the-middle attack, Defenses against the attack, See key-agreement protocol for a classification of protocols that use various forms of keys and passwords to prevent man-in-the-middle attacks, Meet-in-the-Middle, Replay Attack, Countermeasures, INTERNET SECURITY APPLICATIONS, Secure Electronic Transaction (SET), How it Works, Dual signature, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Description, Secure Hypertext Transfer Protocol (S-HTTP), Overview, Usage in websites, Browser integration, Security, TechnicalDifference from HTTP, Network layers, Server setup, Acquiring certificates, Use as access control, In case of compromised secret (private) key, Limitations, IPSEC, E-MAIL SECURITY APPLICATIONS, Secure Multipurpose Internet Mail Extensions (S/MIME), Function, S/MIME certificates, Obstacles to deploying S/MIME in practice, MIME Object Security Services (MOSS), Privacy Enhanced Mail (PEM), PRETTY GOOD PROVACY (PGP).

BLOCK-III

UNIT I: FOOTPRINTING AND RECONNAISSANCE

INTRODUCTION, INFORMATION GATHERING TECHNIQUES, ActiveInformationGathering, PassiveInformationGathering, SOURCES OF INFORMATION GATHERING, ACTIVE INFORMATION GATHERRING, CopyingWebsitesLocally, InformationGatheringwithWhois, FindingOtherWebsitesHostedontheSameServer, Yougetsignal.com, TracingtheLocation, Network Orientation using Traceroute, Network Mapping, NeoTrace, Cheops-ng, EnumeratingandFingerprintingtheWebservers, Intercepting aResponse, Acunetix VulnerabilityScanner, WhatWeb, PASSIVE INFORMATION GATHERING, Netcraft, GoogleHacking, SomeBasicParameters, Google Hacking Database, Hackersforcharity.org/ghdb, Xcode Exploit Scanner, File Analysis, Foca, Harvesting E-Mail Lists, Gathering Wordlist from a Target Website, Scanning for Subdomains, TheHarvester, Fierce in BackTrack, Knock.py, Wolframaplha, Scanning for SSL Version, DNS Enumeration, Interacting with DNS Servers, Automating Zone Transfers, DNS Cache Snooping, ATTACK

SCENARIO, Automating DNS Cache Snooping Attacks, ENUMERATING SNMP, Problem with SNMP, Sniffing SNMP Passwords, OneSixtyOne, Snmpenum, SMTP Enumeration, DETECTING LOAD BALANCERS, Load Balancer Detector, Determining Real IP behind Load Balancers, BYPASSING CLOUDFLARE PROTECTION, INTELLIGENCE GATHERING USING SHODAN.

UNIT II: SCANNING AND ENUMERATION

INTRODUCTION, HOST DISCOVERY, SCANNING FOR OPEN PORTS AND SERVICES, Types of Port Scanning, Understanding the TCP Three-Way Handshake, TCP Flags, Port Status Types, TCP SYN Scan, TCPConnectScan, NULL, FIN, and XMAS Scans, NULL Scan, FIN Scan, XMAS Scan, TCP ACK Scan, UDP Port Scan, ANONYMOUS SCAN TYPES, IDLE Scan, ScanningforaVulnerableHost, Performing an IDLE Scan with NMAP, TCP FTP BOUNCE SCAN, SERVICE VERSION DETECTION, OS FINGERPRINTING, POF, Output, Normal Format, Grepable Format, XML Format, ADVANCED FIREWALL/IDS EVADING TECHNIQUES, TIMING TECHNIQUE, SOURCE PORT SCAN, SPECIFYING AN MTU, SENDING BAD CHECKSUMS, DECOYS, ZENMAP.

UNIT III: Gaining Access and Exploitation

INTRODUCTION, SYSTEM HACKING, Password Cracking, Password Cracking Techniques, Dictionary Attacks, Brute-force Attacks, HybridAttack, Syllable Attack, Rule-based Attack, PassiveOnlineAttacks, Active Online Attacks, Offline Attacks, Non-technical Attacks, PASSIVE ONLINE ATTACKS, Packet Sniffing, Man-in-the-middle, Replay Attack, ACTIVE ONLINE ATTACKS, Password Guessing, Trojans, Spyware, and Keyloggers, Hash I.njection, PASSWORD HASHING, OFFLINE ATTACKS, Extracting Hashes from a System, Pre computed Hashes or Rainbow Tables, Generating Rainbow Tables, Creating Rainbow Tables, Working with Rainbow Crack, DISTRIBUTED NETWORK ATTACKS, SeekingOutNew Life, OTHER OPTIONS FOR OBTAINING PASSWORDS, Default Passwords, Guessing, USB Password Theft, Using Password Cracking, AUTHERNTICATION ON MICROSOFT PLATFORM, Security Accounts Manager (SAM), How Passwords Are Stored within the SAM, NTLM Authentication, Kerberos, PRIVILEGE ESCALATION, Trinity Rescue Kit (TRK), Executing Applications, PLANTING A BACKDOOR, COVERING YOUR TRACKS, Disabling Auditing, Data Hiding, Alternate Data Streams (ADS).

UNIT IV: POST EXPLOITATION ACTIVITIES

INTRODUCTION, ACQUIRING SITUATION AWARENESS, Enumerating a Windows Machine, EnumeratingLocal Groups and Users, Enumerating Linux Machine, Enumerating with Meterpreter, Identifying Processes, Interacting with the System, UserInterfaceCommand, Privilege Escalation, Maintaining Stability, Escalating Privileges, Bypassing User Access Control, Impersonating the Token, MAINTAINING ACCESS, Installing a Backdoor, Cracking the Hashes to Gain Access to Other Services, Backdoors, Disabling the Firewall, Killing the Antivirus, Netcat, MSFPayload/MSFEncode, Generating a Backdoor with MSFPayload, MSFEncode, MSFVenom, Persistence, DEEP DIVE (MAINTAINING ACCESS), What Is a Hash?, Hashing Algorithms, LAN Manager (LM), NTLM/NTLM2, Kerberos.