MIT(CS)-203

Advanced cyber security techniques

BLOCK I

UNIT I: NETWORK SEURITY - THREATS

INTRODUCTION, NETWORK ATTACKS, Man-in-the-Middle (MITM) Attack, Replay Attack, Denial of Service (DoS) and Distributed Denial of Service (DDoS), Password Based Attacks, Spoofing, Eavesdropping, Installation of malicious programs - Backdoor or rooting, THREAT LANDSCAPE - NETWORK SECURITY, Threats to watch, Hactivist attacks, DDoS Attacks, TOR- Onion Routing, Web application attacks, Malware propagation through Web, Targeted Attacks, Exploit Pack Toolkit, Ransomware, Attacks targeting Industrial Control Systems Networks, Social Network Sites (SNS) Threats, Threats to Mobile Devices and Mobile Communication, Threats to Client System, Attacks on Certifying Authorities - Trust Infrastructure, Emerging Threats, Emerging threats targeting Industrial Control Systems (ICS), Emerging Threats to cloud computing environment, Emerging threats in Big Data, Emerging threats in Internet of Things.

UNIT II: NETWORK SEURITY TECHNOLOGIES

INTRODUCTION, FIREWALL, Network Firewalls, Host-Based Firewalls, INTRUSION DETECTION AND PREVENTION SYSTEM, IDPS - Detection Technologies, Anomaly-Based Detection, Stateful Protocol Analysis, Types of Intrusion Detection and Prevention system (IDPS), Network Based Intrusion Detection and Prevention Systems (NBIDPS), Host Based Intrusion Detection and Prevention System (HBIDPS), Wireless Intrusion Detection and Prevention Systems (WIDPS), Network Behavior Analysis (NBA), SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM), HONEYPOT.

UNIT III: NETWORK SEURITY - CONTROLS AND BEST PRACTICES

INTRODUCTION, NETWORK INFRASTRUCTURE SECURITY BEST PRACTICES, Threats to the organization network Infrastructure, Best practices for network infrastructure security, Secure the Network Infrastructure Edge, Protect Infrastructure Device Access, Routing infrastructure Security, Monitoring, Analysis and Correlation, Network Policy Enforcement, Switching Infrastructure Security, Threat Control and Containment, Endpoints Security, Secure Third-Party Connectivity, CRITICAL SECURITY CONTROLS, SANS 20 critical controls for cyber defense, Brief description of Critical Controls- Need of Critical Control.

UNIT IV: NETWORK SECURITY (PHYSICAL AND ENVIRONMENT SECURITY)

INTRODUCTION, PHYSICAL SECURITY- INFORMATION AND COMMUNICATIONS TECHNOLOGY, Strategy for Physical Security, Physical Security - Best Practices, Physical Security – Guidelines, Physical security of Information and Communications Technology (ICT) Equipment, Physical security of Information and communications Technology (ICT) system equipment, Physical security of ICT facilities, DATA CENTER SECURITY – GUIDELINES, Securing the Data Centre, Best Practices in the Data Centre, ENVIRONMENT

SECURITY - INFORMATION AND COMMUNICATIONS TECHNOLOGY, Strategy for Environmental Security, Environmental Security - Best Practices, Environmental Security - Guidelines

BLOCK II

UNIT I: SERVER SIDE THREATS AND VULNERABILITIES- COUNTERMEASURES AND BEST PRACTICES

INTRODUCTION, ADDRESSING THREATS, BAISC DEPLOYMENT QUESTIONS, Identification of Server role, Identification of network services, Methods of authentication, Security plan, Physical security, INSTALLATION & CONFIGURATION, OS Hardening, Patches, Disabling unwanted services and protocols, OS authentication, Protecting server against unauthorized network access, Encryption, Intelligent usage of ACL‘s, Access Control and Permissions, Tools, SECURING THE SERVER PLATFORM, Access / resource Restrictions, ENFORCING AND MAINTAING SECURITY BEST PRACTICES, Account Policy, User privileges & rights, Audit & logs Management, OPERATIONS & MAINTENANCE, Patches, Anti-virus, System monitoring, Performance, Incident detection tools, Backups, Recovery, INCIDENT HANDLING, Define incident, Incident detection.

UNIT II: SECURING IT INFRASTRUCTURE SERVICES

INTRODUCTION, WEB SERVERS SECURITY, Defense in depth, Third party hosting, CERT-In Guidelines, security auditing: Third party hosting service provider, EMAIL SECURITY, Security Threats to Email Service, Security Guidelines-email server, DATABASE SERVER SECURITY, Database Vulnerabilities, Database Security, Planning, Installation & Configuration, Operations & Maintenance, Backup & Recovery, Web Based Databases, Security Checklist for a Database Administrator, DNS SERVERS SECURITY, Threats to DNS Server, DNS Security.

UNIT III: WEB APPLICATION SEURITY

INTRODUCTION, WEB-APPLICATION SECURITY VERSUS PERIMETER SECURITY, ATTACK SURFACE, Web application Attacks, Cross-Site Scripting (XSS or CSS), SQL Injection (SQL-i), Remote File Inclusion (RFI), Cross Site Request Forgery (CSRF), HTTPS Cookie Hijacking, File Upload Vulnerabilities, Insecure Data Transfer and Storage, SECURE WEB APPLICATION DEVELOPMENT- BEST PRACTICES, 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, WEB APPLICATION SECURITY TESTING, The OWASP Testing Framework OWASP Testing Guide, WHAT DO WE NEED TO SECURE?, Authentication, Integrity, Confidentiality, Non-repudiation, SECURITY PROTOCOLS, Secure HTTP, S/MIME, How S/MIME work?, PRETTY GOOD PRIVACY (PGP), How PGP works?, PGP Web of trust, Secure Electronic Transaction, SECURE SOCKETS LAYER (SSL) /TRANSPORT LAYER SECURITY, How SSL works?, The main objectives of SSL are Specific Protocol, SSL SESSION AND CONNECTION, The Handshake Protocol, SSL Record Protocol, The Alert Protocol, The Change Cipher Specification Protocol, IPSec, THE IP DATAGRAM, IPSec:AH: AUTHENTICATION HEADER - AUTHENTICATION ONLY, ESP-ENCAPSULATING SECURITY PAYLOAD, DNSSEC, SECURE SHELL (SSH), Mailing protocols.

BLOCK III

UNIT I: DESKTOP HARDENING- A WINDOWS CLIENT PERSPECTIVE

INTRODUCTION, WINDOWS SECURITY CONTROLS ESSENTIAL FOR HOME USER, Passwords, Windows Updates, PRINCIPLE OF LEAST PRIVILEGE(PLP), EMET(Enhanced Mitigation Experience Toolkit) anti exploitation tool- silver bullet from Microsoft, AUTORUN /AUTOPLAY, Disabling Auto Run/ AutoPlay in Windows Operating Systems, Disable Autorun in Windows 7/ Vista with Group policy Settings, Disable AutoPlay in Windows 7 /Vista, SOFTWARE RESTRICTOIN POLICY, BROWSERS AND SECURITY, IE security settings, Mozilla Firefox, Low Integrity Firefox, Chrome, Sandboxing your Browser, MBSA (MICROSOFT BASELINE SECURITY ANALYSER), SET UP AND CONFIGURE WINDOWS FIREWALL, Advanced Settings for Firewall, Example for setting windows update service outbound allow, PHYSICAL SECURITY, BitLocker Drive Encryption, Enabling SysKey functionality to Enhace Desktop Security, Set restore points, Do an Image Backup of the Hard Drive take regular backup, BASIC GUIDELINES FOR ENABLING SECURITY IN YOUR DESKTOP, Basic Desktop Hardening, Basic Network Hardening, ENABLING SECURITY FEATURES IN MS OFFICE.

UNIT II: WIRELESS SECURITY AND MOBILE DEVICE THREATS- USER PERSPECTIVE

INTRODUCTION, WIRELESS NETWORK SECURITY: VULNERABILITIES, THREATS AND COUNTERMEASURES, What is WLAN, WLAN components, WLAN 802.11 security, WAP Version 1, WPA1 addendum, Wi-Fi Protected Access II (WPA2), Issues with WAP, WLAN THREATS, WLAN Attacks causing Loss of confidentiality, Traffic Analysis, Eavesdropping, Man-in-the-Middle Attack, Evil Twin AP, ATTACKS CAUSE LOSS OF INTEGRITY, Session Hijacking, Replay Attack, 802.11 Frame Injection Attack, 802.11 Data deletion, ATTACKS CAUSING LOSS OF AVAILABILITY, Denial-of-Service Attack, Radio frequency (RF) Jamming, 802.11 Beacon Flood, 802.11 Associate/Authentication Flood, Queensland DoS / Virtual carrier-sense attack, Fake SSID flooding, EAPOL flood, GreenField Mode, AUTHENTICATION ATTACKS, Dictionary & Brute force attack, Attacks targeting Access Controls, MAC spoofing, War Driving/ access point mapping, Rogue Access Point, ATTACKS ON ENCRYPTION STANDARDS, WEP attacks, FMS (Fluhrer, Mantin and Shamir) attack, Korek CHOPCHOP Attack, Coolface attack, HOME WIRELESS THREATS, PUBLIC WIRELESS THREATS, Unauthorized Computer Access, Safe Wireless Networking in Public Spaces, Wireless Client Device Security and best practices, Mobile devices threats, Mobile malware prevention steps.

UNIT III: FUNDAMENTAL ARTEFACT & MALWARE ANALYSIS

INTRODUCTION, MALWARE ANALYSIS FUNDAMENTALS, Various approaches to malware analysis, Basic static analysis, Behavioral analysis, Automatic Analysis, Volatile Memory Analysis, Advanced dynamic analysis, Advanced static analysis, SETTING UP MALWARE ANALYSIS FACILITY, Creating sandboxed / virtual environments, STATIC ANALYSIS, Detecting Packers and Cryptors, Notable strings, PE structure Analysis, DYNAMIC ANALYSIS, Dynamic Analysis Tools, Baseline the guest machine with Capture Bat, AUTOMATIC ANALYSIS, MALWARE COLLECTION PROCESS WOTH MALWARE HONEYPOTS, Installing

Nepenthes, Installing Nepenthes, Dionaea Honeypot installation, Installing Dionaea, Installing Thug for web based malware, MEMORY ANALYSIS, Capturing Memory, Memory Analysis using Volatility.

UNIT IV: ADVANCED PERSISTENT THREATS

INTRODUCTION, APT LIFE CYCLE, CASE STUDY, Information gathering, Delivery, Initial Compromise, Exploit detected inside crafted/malicious document, Command and Control mechanisms, Lateral movement, Data Exfiltration.