SYLLABUS FOR THE POST OF SCIENTIFIC OFFICER
COMPUTER FORENSICS SECTION
FORENSIC SCIENCE LABORATORY-POLICE DEPARTMENT

1 Digital Forensic and Cyber Crime

Understanding Cyber Crime: Indian IT Act 2008 and amendments, categories of cyber crimes ie., unauthorized access and hacking, virus, worms & Trojan attacks, E-mail related crimes, Internet relay, chat relating crimes, sale of illegal articles, online gambling, phishing, Intellectual property crimes, web defacement, DOS attack, cyber stalking etc.,

2 Working with Windows and DOS Systems

Understanding File Systems, Exploring Microsoft File Structures, Examining NTFS Disks, Understanding Whole Disk Encryption, Understanding the Windows Registry, Understanding Microsoft Startup Tasks, Understanding MS-DOS Startup Tasks, and Understanding Virtual Machines. Macintosh and Linux Boot Processes and File Systems: Understanding the Macintosh File Structure and Boot Process, Examining UNIX and Linux Disk Structures and Boot Processes, Understanding Other Disk Structures. Free space Management Bit-Vector Linked List Grouping Counting Efficiency & Performance Recovery Physical Damage Physical Damage Recovery Logical Damage Logical, Damage Recovery.

3 Current Computer Forensics Tools:

Evaluating Computer Forensic Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating and Testing Forensics Software. Data Acquisition: Understanding Storage Formats for Digital Evidence, Determining the best Acquisition Method, Validating Data Acquisitions, Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisitions. Performing RAID Data Acquisitions, Using Remote Network Acquisition Tools, and Using Other Forensic Acquisition Tools. Recovering Graphics Files: Recognizing a Graphics File, Understanding Data Compression, Locating and Recovering Graphics Files, Identifying Unknown File Formats, Understanding Copyright Issues with Graphics.

4. Computer hardware/Software :

Hardware: Basic PC Components, Monitors, Keyboard, Storage devices: Hard Disk ; Storage related simple problems, CD, Mother-board, Printers its classification etc, OCR, OMR, BAR Code etc. Memory Hierarchies : Basics of Semiconductor Memories, ROM Cells & Circuits, Address Decoding, Access Time, Examples of Integrated Circuit ROMs, PROMs, EPROMs, EEPROM, Static Read/Write (RAM) Memory.CPU ;ALU, Components of CPU ; Register, Accumulator, IR, etc. Software System- application Software and their Examples in real life. Operating System and their usage. Multitasking –Multiprogramming- Multiprocessing Operating System.

5. NUMBER SYSTEMS AND CODES:

Basic Rules of Binary , Binary Number System, Octal Number System, Hexadecimal Number System, Bits and Bytes , 1's and 2's Complements, Decimal –to- Binary Conversion, Decimal-to- Octal Conversion, Decimal –to-Hexadecimal Conversion, Binary –octal and Octal – Binary Conversions , Hexadecimal – Binary and Binary – Hexadecimal Conversion, Hexadecimal –Octal and Octal –Hexadecimal Conversion.

6. TCP/IP

The Internet Protocol (IP), IP packet, IP addressing, subnet mask, classless interdomain routing (CIDR), address resolution, reverse address resolution, IP fragmentation and reassembly, ICMP, User Data gram Protocol (UDR), Transmission Control Protocol (TCP), TCP reliable stream services, TCP operation, TCP protocol, Dynamic Host Configuration Protocol (DHCP), mobile IP, IPv6, Internet routing protocols, routing information protocols, open shortest path first protocol, border gateway protocol, multicast routing, reverse path broadcasting, internet group management protocol, reverse path multicasting, distance vector multicast routing protocol. FILE SYSTEM, ACCESSING THE WORLD WIDE WEB-File systems, hypertext markup language, wireless application protocol, wireless data gram protocol, wireless transaction protocol, wsp/b over wtp, wsp/b as connectionless session service, wireless markup language, WTP class 0, WMLScript

7. NON LINEAR DATA STRUCTURES AND HASH TABLES

Introduction- Definition and Basic terminologies of trees and binary trees. Hash Tables: Introduction- Hash Tables- Hash Functions and its applications. HASH FUNCTIONS AND DIGITAL SIGNATURES-Authentication functions-Message authentication codes-Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm)-Digital signatures (Authentication protocols, Digital signature Standard).

8. NEXT GENERATION INTERNET PROTOCOL

Introduction to IPv6 – IPv6 Advanced Features –V4 and V6 header comparison – V6 Address types –Stateless auto configuration – IPv6 routing protocols – IPv4-V6 Tunnelingand Translation Techniques.

9. INITIAL RESPONSE AND FORENSIC DUPLICATION

Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive.

10. NETWORK FORENSICS

Performing Live Acquisitions, Developing Standard Procedures for Network Forensics, Using Network Tools. E-mail Investigations: Exploring the Role of E-mail in Investigations, Exploring the Roles of the Client and Server in E-mail, Investigating E-mail Crimes and Violations, Understanding E-mail Servers. Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud, SYSTEMS INVESTIGATION AND ETHICAL ISSUES-Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime, DATABASE AND WEB SPECIFIC INPUT ISSUES-Quoting the Input – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies.

11. RFID Security

Introduction, RFID Security and privacy, RFID chips Techniques and Protocols, RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography to Enhance Privacy in RFID Systems,

12. IMPLEMENTATION OF COVERT CHANNEL

Non self-reproducing Malware- Working principle of Trojan Horse- Implementation of Remote access and file transfer- Working principle of Logical Bomb, other worms. VIRUS AND WORM ANALYSYS-Klez Virus. Clone Virus- Doom Virus- Black wolf worm- Sassar worm- Happy worm 99. Virus components- Function of replicator, concealer and dispatcher- Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb

13. Ethical Hacking terminology

Five stages of hacking- Vulnerability Research- Legal implication of hacking- Impact of hacking. System Hacking-Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

14. Foot printing & Social engineering

Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks. Analysis of Deep web/ dark web and silk road analysis.

15. PUBLIC KEY CRYPTOGRAPHY

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman, Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography.