Semester 5:

Cyber Forensics

Unit 1: Cyber Forensics Science: Forensics science, computer forensics, and digital forensics. **Computer Crime:** Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics -- 7L

Unit 2: Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation. -- 6L

Unit 3: Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause. -- 7L

Unit 4: Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, **Network Forensics:** open-source security tools for network forensic analysis, requirements for preservation of network data. --- 8L

Unit 5: Mobile Forensics: mobile forensics techniques, mobile forensics tools. **Legal Aspects of Cyber Forensics:** IT Act 2000, amendment of IT Act 2008.---- 5L

Unit 6: Recent trends in mobile forensic technique and methods to search and seizure electronic evidence ---- 3L

References:

1. John Sammons, The Basics of Digital Forensics, Elsevier Model Curriculum of Engineering & Technology PG Courses [Volume-I]

2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Cyber law and Ethics

Unit – 1: Introduction of Cybercrime: [4L]
What is cybercrime?, Forgery, Hacking, Software Piracy, Computer Network intrusion

Unit – 2: Category of Cybercrime: **[4L]**
how criminals plan attacks, passive attack, Active attacks, cybers talking.

Unit – 3: Cybercrime Mobile & Wireless devices: [8L]
Security challenges posted by mobile devices, cryptographic security for mobile devices, Attacks on mobile/cellphones, Theft, Virus, Hacking. Bluetooth; Different viruses on laptop.

Unit -4: Tools and Methods used in Cyber crime: [8L]
Proxy servers, panword checking, Random checking, Trojan Horses and Backdoors; DOS & DDOS attacks; SQL injection: buffer over flow.

Unit– 5: Phishing & Identity Theft: [4L]
Phising methods, ID Theft; Online identity method.

Unit --6: Cybercrime & Cybersecurity: [4L]
Legal aspects, indian laws, IT act, Public key certificate

Unit—7: Ethics [4L]: Legal Developments, Cyber security in Society, Security in cyber laws case studies, General lawand Cyber Law-a Swift Analysis.

Text: 1. Cyber security by Nina Gobole & Sunit Belapune; Pub: Wiley India.

1. Mark F Grady, Fransesco Parisi, “The Law and Economics of Cyber Security”, Cambridge University Press, 2006

Malware Analysis and Reverse Engineering

Unit 1: Fundamentals of Malware Analysis (MA): Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools --- 11 L

Unit 2: Malware Forensics: Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates. ---6L

Unit 3: Malware and Kernel Debugging: Opening and Attaching to Processes, Configuration of JIT Debugger for Shell code Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands**,** DLL Export Enumeration, Execution, and Debugging**,** Debugging a VMware Workstation Guest (on Windows)**,** Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts**,** Kernel Debugging with IDA Pro. ---8L

Unit 4:Memory Forensics and Volatility: Memory Dumping with MoonSols Windows Memory Toolkit**,** Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artifacts in Process Memory**,** Identifying Injected Code with Malfind and YARA. ---6L

Unit 5: Researching and Mapping Source Domains/IPs: Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps.---6L

Unit 6: Case Study: Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA --3L

Book:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollo

Intrusion Detection and Prevention Systems-(Elective-1)

Unit1: History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources. The state of threats against computers, and networked systems, Overview of computer security solutions and failure causes, Vulnerability assessment, firewalls—6L

Unit2: Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS, Evaluation of IDS, Cost sensitive IDS, Anomaly Detection Systems and Algorithms, Network Behavior Based Anomaly Detectors (rate based), Host-based Anomaly Detectors—6L

Unit3: Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques, Classes of attacks, Network layer attack (scans, denial of service, penetration), Application layer attack(software exploits, code injection), Human layer attack (identity theft, root access), Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis, Automated: Drones, Worms, Viruses—8L

Unit4: A General IDS model and taxonomy, Signature-based Solutions, Introduction to Snort, Snort rules, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes, State transition, Immunology, Payload Anomaly Detection, Attack trees and Correlation of alerts, Autopsy of Worms and Botnets, Malware detection—8L

Unit5: Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL, Email/IM security issues, Viruses/Spam, From signatures to thumbprints to zero-day detection, Insider Threat issues , Masquerade and Impersonation, Traitors, Decoys and Deception Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs—8L

Books:

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," Prentice Hall
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "Intrusion Detection and Correlation Challenges and Solutions",
3. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention", Tata McGraw-Hill
4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", New Riders Publishing
5. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". Khanna Publihsers

Enterprise Security Architecture and Design (CYS(PE) – 504A)

Module1:

IT Security Governance and Risk Management: Four types of policies Develop and manage security policies Perform risk management for IT security Threat identification and classification Incident Management.

Module2:

Business Continuity Planning and Disaster Recovery Planning: IT security business continuity planning IT security disaster recovery planning.

Module3:

Software Development Security: Software development lifecycle Security design reviews Best practices in software engineering.

Module4:

IT Security Enterprise Solutions: Network security in context Protecting TCP/IP networks Virtual Private Networks IPSec Overview of Cloud Security.

Module5:

Network Security architecture and design: Defining the trusted computing base System security assurance concepts Confidentiality and Integrity models.

Reference books:

1. Nicholas A Sherwood; "Enterprise Security Architecture: A Business-Driven Approach"; 1st Edition; CRC Press.
2. Ross;" Enterprise Architecture as Strategy: Creating a Foundation for Business Execution"; 1 August 2006; Harvard Business Review Press.
3. Nitesh Garg, Atul Sharma; "Enterprise Solution Architecture - Strategy Guide"; 29 July 2021; BPB Publications.
4. Norbert Pohlmann, Tim Crothers; "Firewall Architecture for the Enterprise" 2005 Edition; Laxmi Publications.

Data Science, Algorithms and Complexity in Cyber Context (CYS(PE) – 505C)

Module1:

Basic analysis of Cyber context.

Module2:

Algorithmic strategies.

Module3:

Fundamental data structures and algorithms.

Module4:

Basic automata, computability and complexity.

Module5:

Topics in data science and machine learning.

Reference Book:

2. Allen B.Downey; "Think Complexity: Complexity Science And Computational Modeling"; Second Edition; O'Reilly.
3. "G Venkatesh, Madhavan Mukund"; Computational Thinking: A Primer for Programmers and Data Scientists" 31 August 2021.
4. Steele Brian; "Algorithms for Data Science"; Springer International Publishing AG.
5. Ingo Wegener; "Complexity Theory" 2005; Springer.

Biometric Security (Elective-2)

Unit 1: Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies.--- 5L

Unit 2: Bio-metric technologies: Fingerprint, Face, Iris, Hand Geometry, Gait Recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face Recognition, Dental Identification and DNA.---8L

Unit 3: The Law and the use of multi bio-metrics systems. ---4L

Unit 4: Statistical measurement of Bio-metric. Bio-metrics in Government Sector and Commercial Sector. –8L

Unit 5: Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities.---7L

Unit 6:
Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D face recognition and DNA matching.---4L

Books:

1. Paul Reid, Biometrics for network security, Hand book of Pearson, 2004.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, 2003
3. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.
5. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer, 2011.
6. Biometric Systems: Technology, Design and Performance Evaluation, J. Wayman, A.K. Jain, D. Maltoni, and D. Maio
7. Gonzalez, R.C. and Woods, R.E., Digital Image Processing. 2nd ed. India: Person Education, 2009

Cyber Forensics Lab

1. Data acquisition using tools like FTK Imager, DumpIt etc.
2. Volatile Memory Analysis using Hex Editor and Volatility.
3. Defeating Anti Forensic Technique using tools like EaseUS Data recovery, Recuva, Steller Data recovery, Passware password recovery tools, Stegspy, Open Stego and crypt analysis etc.
4. Metadata extraction Using Exif tools
5. Network Forensic Using Wireshark.
6. Operating System Forensic using OSForensic, Autopsy.
7. Malware Analysys using tools like **ProcessMonitor, ProcessExplorer, RegShot / TotalCommander, PeStudio, Resource Hacker etc.**
8. Mobile Forensic using tools Mobileedit, Oxygen etc.
9. Cloud Forensic Lab

Malware Analysis Lab

1. Windows PE Format Analysis
2. Application Cracking
3. Basic Static Malware Analysis
4. Basic Dynamic Malware Analysis
5. Advanced Malware Analysis
6. Tool Used: Ollydbg, Immunity Debugger, Hex Editor, etc.