REVISED UG SYLLABUS UNDER CBCS
(Implemented from Academic Year 2020-21)

PROGRAMME: FOUR YEAR B.Sc. (Hons)

Domain Subject: **B. Sc - Cyber Forensics**
Skill Enhancement Courses (SECs) for Semester V, from 2022-23 (Syllabus/Curriculum)
Pair Options of SECs for Semester–V
(To choose one pair from the five alternate pairs of SECs)

Univ. Code	Courses 6&7	Name of Course	Th. Hrs. / Week	IE Marks	EE Marks	Credits	Prac. Hrs./ Wk	Marks	Credits
	6A	**Cyber Law**	3	25	75	3	3	50	2
	7A	**Advanced Cyber Forensics**	3	25	75	3	3	50	2
		OR							
	6B	**Machine Learning for Digital Forensics**	3	25	75	3	3	50	2
	7B	**Multimedia Forensics & Speaker Identification**	3	25	75	3	3	50	2
		OR							
	6C	**Social Media Forensics**	3	25	75	3	3	50	2
	7C	**Network Forensics**	3	25	75	3	3	50	2
		OR							
	6D	**Reverse Engineering & Malware Analysis**	3	25	75	3	3	50	2
	7D	**Vulnerability Assessment and Penetration Testing**	3	25	75	3	3	50	2

Note-1: For Semester–V, for the domain subject Botany, any one of the four pairs of SECs shall be chosen as courses 6 and 7, i.e., 6A & 7A or 6B & 7B or 6C & 7C or 6D & 7D. The pair shall not be broken (ABCD allotment is random, not on any priority basis).

Note-2: *One of the main objectives of Skill Enhancement Courses (SEC) is to inculcate field skills related to the domain subject in students. The syllabus of SEC will be partially skill oriented. Hence, teachers shall also impart practical training to students on the field skills embedded in the syllabus citing related real field situations.*

Semester-wise Revised Syllabus under CBCS, 2020-21
Four Year B.Sc. (Hons) - Semester – V (from 2022-23)
Subject: **B. Sc - Cyber Forensics**
Course-6A: **Cyber Law**
(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50 + 50

Learning Outcomes:

1. Overview of Indian Legal System
2. Overview of Cyber Space
3. Information Technology Act, 2000 and its Amendments (till date)
4. Outline of Electronic Governance
5. Copyright infringements
6. Incident Response Team Development
7. Identify, Interpret and Evaluate Laws, Government Regulations and International Legal Systems Pertinent to Ecommerce
8. Explain and Evaluate Emerging Legal and Ethical Issues in Ecommerce
9. Analyze Ethical Problems That Arise in The E-Commerce Context Through the Examination of Case Studies

Syllabus: *(Total Hours: 90 including Teaching, Lab, Field Training and unit tests etc.)*

UNIT - 1: Cyber crimes and related offences and penalties: Introduction to Cybercrimes, Classification of cybercrimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; Spamming, Phishing, Privacy and National Security in Cyberspace, Cyber Defamation and hate speech, computer vandalism etc.
Provisions in Indian Laws in dealing with Cyber Crimes and its critical analysis, Information Technology Act, 2000, Penalties under IT Act, Offences under IT Act, Offences and Analysis related with Digital Signature and Electronic Signature under IT Act, Statutory Provisions, Establishment of Authorities under IT Act and their functions, powers. Cyber crimes under IPC.

UNIT - 2: Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the IT Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the IT Act – Impact of the IT Act on other Laws .
Authentication of electronic records (Section-3, IT ACT), legal recognition of electronic records and digital signature (Section-4 and 5, IT Act), Certifying Authorities and Controller, Offences as per IT Act (Section-65 to Section-78), Special provision in Indian Evidence Act regarding admissibility of electronic records (Section-65B of IEA, 1872).

UNIT - 3: Cr.P.C and Indian Evidence Act - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases

UNIT - 4: Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases
Patents - Understanding Patents - European Law on Computer related Patents, Legal process on Computer related Patents - Indian process Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases

UNIT - 5: E-commerce and related laws: History, Overview of developments in Information Technology and Defining E-Commerce, Understanding Ethical, Social and Political issues in E-Commerce: A model for Organizing the issues, Basic Ethical Concepts, Analyzing Ethical Dilemmas, Candidate Ethical principles Privacy and Information Rights: Information collected at E-Commerce Websites, The Concept of Privacy, Legal protections Intellectual Property Rights: Types of Intellectual Property protection, Governance. UNCITRAL model law in electronic commerce.

References:

10. The Information Technology Act, 2000 Bare Act with Short Notes, Universal Law Publishing Co., New Delhi
11. Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi
12. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi
13. S.R.Myneni: Information Technology Law(Cyber Laws), Asia Law House, Hyderabad.
14. Chris Reed, Internet Law-Text and Materials, Cambridge University Press.
15. Pawan Duggal: Cyber Law- the Indian perspective Universal Law Publishing Co., New Delhi
16. Elias. M. Awad, " Electronic Commerce", Prentice-Hall of India Pvt Ltd.

Co-curricular Activities:

1. Court Visit
2. Cyber Cell Visit

Semester-wise Revised Syllabus under CBCS, 2020-21
Four Year B.Sc. (Hons) - Semester – V (from 2022-23)
Subject: **B. Sc - Cyber Forensics**
Course-7A: **Advanced Cyber Forensics**
(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Learning Outcomes:

1. Overview of Windows Forensics
2. File System Analysis
3. Overview of Cryptography
4. Encryption and Decryption
5. Overview of Memory Forensics
6. Anti-forensic Techniques
7. Hypervisor Files and Formats
8. Forensic Analysis of a Virtual Machine
9. Overview of Cloud Forensics
10. Analysis of Cloud Applications

UNIT 1: Windows Forensics - Volatile data collection, Non-volatile data collection, Registry Analysis, Browser Usage, Hibernate File Analysis, Crash Dump Analysis, File System Analysis, File Metadata and Timestamp Analysis, Event Viewer Log Analysis, MFT analysis, Timeline Creation, Evidence Collection in Linux and Mac Operating system.

UNIT 2: Cryptography - Cryptographic System, Classification of Cryptographic System, Secret Key, Cryptography, Cryptanalysis and Attacks, Encryption and their types, Encryption algorithms, brute force attack, Decryption and their types, HDD and Artifacts Encryption and Decryption Techniques.

UNIT 3: Memory Forensics - History of Memory Forensics, x86/x64 architecture, Data structures, Volatility Framework & plugins Memory acquisition, File Formats – PE/ELF/Mach-O, Processes and process injection, Command execution and User activity, Networking, sockets, DNS and Internet history, shellbags, paged memory and advanced registry artifacts, Related tools – Bulk Extractor and YARA, Timelining memory, Recovering and tracking user activity, Recovering attacker activity from memory, Introduction to Anti-forensics, tools and techniques.

UNIT 4: Virtual Machine Forensics - Types of Hypervisors, Hypervisor Files and Formats, Use and Implementation of Virtual Machines in Forensic Analysis, Use of VMware to establish working version of suspect's machine, Networking and virtual networks within Virtual Machine, Forensic Analysis of a Virtual Machine (Imaging of a VM, Identification and Extraction of supporting VM files in the host system, VM Snapshots, Mounting Image, Searching for evidence)

UNIT 5- Cloud Forensics - Introduction to Cloud Computing, Challenges faced by Law enforcement and government agencies, Cloud Storage Forensic Framework (Evidence Source Identification and preservation, Collection of Evidence, Examination and analysis of collected data) Cloud Storage Forensic Analysis.
Dropbox analysis: Data remnants on user machines, Evidence source identification and analysis, Collection of evidence from cloud storage services, Examination and analysis of collected data.

Google Drive: Forensic analysis of Cloud storage and data remnants, Evidence source identification and analysis - Collection of evidence from cloud storage services, Examination and analysis of collected data, Issues in cloud forensics.
Case Studies.

Reference:

1. Window Forensic Analysis (DVD Toolkit) by Harlan Carver
2. File System Forensic Analysis by Brain Carrier
3. Windows Registry Forensics
4. Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey
5. Cryptography and Network Security: United States Edition by William Stallings
6. Cryptography: An Introduction (3rd Edition) by Nigel Smart
7. An Introduction to Cryptography
8. Cryptography and Data Security by Dorothy Elizabeth Rob, ling Denning
9. The Art of Memory Forensics (Detecting Malware and Threats in Windows, Linux, and Mac Memory) Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters
10. Advances in Memory Forensics by Fabio Pagani
11. Virtualization and Forensics A Digital Forensic Investigator's Guide to Virtual Environments by Diane Barrett
12. http://atkison.cs.ua.edu/papers/ACMSE11_JF.pdf
13. https://stars.library.ucf.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2790&context=etd
14. https://odr.chalmers.se/bitstream/20.500.12380/300023/1/CSE%2019-10%20CPL%20Andersson.pdf
15. Cloud Forensics by Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie
16. Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data Paperback by Terrence V. Lillard
17. Data Collection Techniques for Forensic Investigation in Cloud by Thankaraja Raja Sree and Somasundaram Mary Saira Bhanu
18. https://www.researchgate.net/publication/235712413_Cloud_Forensics_A_MetaStudy_of_Challenges_Approaches_and_OpenProblems
19. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems by Vijay Prakash, Alex Williams, Lalit Garg, Claudio Savaglio and Seema Bawa. (Research Paper)

Semester-wise Revised Syllabus under CBCS, 2020-21
Four Year B.Sc. (Hons) - Semester – V (from 2022-23)
Subject: **B. Sc - Cyber Forensics**
Course-6B: **Machine Learning for Digital Forensics**
(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

LEARNING OUTCOMES:

- Understanding the important role of machine learning
- Analyzing large amounts of diverse datasets in order to reveal any criminal behavior
- Understanding various machine learning algorithms and techniques that can be useful in the process of extracting and analyzing digital evidence

UNIT 1: Introduction to Machine Learning
Brief Introduction to Machine Learning Well Posed Learning Problems, Motivation to Machine Learning, Applications of Machine Learning, Designing a Learning System, Perspective and Issues in Machine Learning, Concept Learning; Types of Machine Learning - Supervised Learning, Unsupervised Learning, Reinforcement Learning.
Applications of Machine Learning in Natural Language Processing, Image & Video Processing and Analysis, Computer Vision, Financial Data Processing and Social Network Analysis
Data analysis using machine learning for forensic expert, social media and machine learning, malware analysis using ML, HIDS, NIPS based analysis

UNIT 2: Dimensionality Reduction
Subset Selection, Shrinkage Methods, Principle Components Regression; Linear Classification, Logistic Regression, Linear Discriminant Analysis; Optimization, Classification-Separating Hyperplanes Classification.

UNIT 3: Supervised and Unsupervised Learning
Naïve Bayes Classification: Fitting Multivariate Bernoulli Distribution, Gaussian Distribution and Multinomial Distribution, K-Nearest Neighbors, Decision Trees.
Support Vector Machines: Hard Margin and Soft Margin, Kernels and Kernel Trick, Evaluation Measures for Classification, Ensemble Models, k-means and Hierarchical Agglomerative Clustering, Evaluation Measures for Clustering

UNIT 4: Artificial Neural Network
Artificial Neural Networks (Early models, Back Propagation, Initialization, Training & Validation), Parameter Estimation (Maximum Likelihood Estimation, Bayesian Parameter Estimation), Decision Trees, Evaluation Measures, Hypothesis Testing, Ensemble Methods, Graphical ModeL

UNIT 5- Clustering
Clustering, Gaussian Mixture Models, Spectral Clustering; Ensemble Methods; Learning Theory, Reinforcement Learning

Suggested Readings:

- Tom Mitchell, Machine Learning, TMH
- C. Bishop, Pattern Recognition and Machine Learning, Springer
- R. O. Duda, P. E. Hart and D. G. Stork, Pattern Classification and Scene Analysis, Wiley
- Kishan Mehrotra, Chilukuri Mohan and Sanjay Ranka, Elements of Artificial Neural Networks, Penram International
- Rajjan Shinghal, Pattern Recognition, Techniques and Applications, OXFORD
- Athem Ealpaydin, Introduction to Machine Learning, PHI
- Andries P. Engelbrecht, Computational Intelligence - An Introduction, Wiley Publication
- Prince , Computer Vision: Models, Learning, and Inference, Cambridge University Press, Theodoridis and Koutroumbas

Semester-wise Revised Syllabus under CBCS, 2020-21

Four Year B.Sc. (Hons) - Semester – V (from 2022-23)

Subject: **B. Sc - Cyber Forensics**

Course-7B: **Multimedia Forensic & Speaker Identification**

(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Learning Outcomes:

1. Overview of Multimedia Forensic
2. Image Enhancement Techniques
3. Video Frame Analysis
4. DVR Examination
5. Voice Production Process
6. Automatic Speaker Identification System

UNIT-1: Foundation to Multimedia Forensics

Introduction to digital signals: audio, image and video, Digitization process: sampling and quantization, Image Enhancement Techniques: Spatial and frequency domain, Image Compression Techniques: Introduction and techniques, Image description and representation techniques, Pattern clustering and classification.

UNIT-2: Introduction to Multimedia Forensics

Introduction and scope of Multimedia Forensics, Basics of Multimedia Devices for capturing image and video, audio, Standard and best practices in Multimedia Forensics, Admissibility of multimedia evidence to the court of law along with various acts.

UNIT-3: Image and Video Forensics

Introduction and scope, Standards for video transmission, Active and passive image/video forensics, Blind and non-blind image/video forensics, Methods of source camera identification, Methods for tampering of digital image/video, Forensic authentication of digital image/video, Enhancement of digital image/video, Specific Frame Analysis, Scope & it's Forensic Application in the Field of Security, DVR Examination.

UNIT-4: Audio Forensics

Introduction and scope, Analog to Digital Conversion- Sampling and Quantization, Acoustic Parameters of Sound, Fourier Analysis, Frequency and Time Domain Representation of Speech Signal, Fast Fourier Transform, Methods of tampering for digital audio, Forensic authentication of digital audio, Microphone Forensics, Enhancement of digital audio.

UNIT-5: Speaker Identification

Introduction and scope of speaker identification, Human vocal tract and production and description of speech sound, Voice Production Theory, Speech Signal Processing and Pattern Recognition, Forensic phonetics and phonetic transcription, Methods of speaker identification: auditory and spectrographic analysis, Spectrographic cues for Vowels and Consonants, Automatic Speaker Identification System, Collection of voice samples: methods and challenges.

REFERENCES

- Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T S Ho, Shujun Li
- Multimedia Forensics and Security Foundations, Innovations, and Applications by Aboul Ella Hassanien, Mohamed Mostafa Fouad
- Fundamentals of Speaker Recognition by Homayoon Beigi
- Fundamentals of Speaker Recognition Law Enforcement and Counter- Terrorism by Amy Neistein, Hemant A. Patil
- Forensic Comparison of Voice, Speech and Speakers by Jonas Lindh

Semester-wise Revised Syllabus under CBCS, 2020-21

Four Year B.Sc. (Hons) - Semester – V (from 2022-23)

Subject: **B. Sc - Cyber Forensics**

Course-6C: **Social Media Forensics**

(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Learning Outcomes:

1. Overview of Social Media Forensics
2. Cyber Crimes related to social media
3. Open Street Map
4. Open-Source tools for social media analytics

UNIT 1: What is Online Social Networks, data collection from social networks, challenges, opportunities, and drawbacks in online social network, Cybercrimes related to social media and its awareness, scrapping of data from social media API's.

UNIT 2: Information privacy disclosure, revelation and its effects in OSM and online social networks, Privacy issues related to location-based services on OSM.

UNIT 3: Tracking social footprint / identities across different social network, Identifying fraudulent entities in online social networks, Effective and usable privacy setting and policies on OSM, Policing & OSM.

UNIT 4: Detection and characterization of spam, phishing, frauds, hate crime, abuse and extremism via online social media, Data Collection & Analysis, Fake News & content on social media.

UNIT 5: Social Media Forensics: Case Studies Open-Source tools or social media analytics, Safety on social media. Legal Issues in world social media, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

References:

- Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
- Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.
- Understanding Social Networks: Theories, Concepts by Charles Kadushin
- Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

Semester-wise Revised Syllabus under CBCS, 2020-21

Four Year B.Sc. (Hons) - Semester – V (from 2022-23)

Subject: **B. Sc - Cyber Forensics**

Course-7C: **Network Forensics**

(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Learning Outcomes:

1. Overview of networks
2. Overview of Wireless Network Forensics
3. Packet Analysis
4. Different Malware Analysis techniques and their behaviour.
5. Ransomware Analysis

UNIT - 1: BASICS OF NETWORK ARCHITECTURE & INTERNET - Part 1

Network Forensics: Overview, Securing a Network, Scope, Standard Operating Procedure of Network Data, Introduction to Networks: ARPANET Protocols, Network, Need of Networks.
Classification by Network Geography: Types of Topologies- RING, STAR, BUS, MESH (features, advantages, disadvantages). Classification by Component: Peer to Peer, Client/ Server
Types of Networks: LAN, MAN, WA (with applications). Wireless Network: Wireless LAN, MAN, WAN

UNIT - 2: BASICS OF NETWORK ARCHITECTURE & INTERNET Part 2

Network Communication: Introduction, Types of network communication
Network Components: Twisted Pair Cable, Shielded Twisted Pair, Unshielded Twisted Pair, Unshielded Twisted Pair, Coaxial cable, Fiber Optic Cables Standard categories of cables. Network Interface Card- HUB, Switch, Router. Router: Working of Router, Router Logs, Routing, Routing Table.

UNIT - 3: PACKET SWITCHING

Basic Terms: MAC Address, ARP, NAT, Gateway, Wireless Access Point, Lifi
ISO/OSI Model in Communication Networks: Features of OSI Model, Functions of layers- Physical, Data Link, Network, Transport, Session, Presentation, Application. Merits of OSI
TCP/IP Reference Model: Overview, Different TCP/IP Protocols, Merits/ Demerits
Packet Routing: Packet in Internet, Processing packet at source machine, router

UNIT - 4 NETWORK TRAFFIC- CAPTURING & ANALYSIS

Basics: NeSA (features, Creating a dump file, Preliminary Settings, Loading a dump file, Session Filtering) Wireshark: Overview, features, Running the application, FTP Analysis, SMTP Analysis, SSL Decryption. Extraction of Media Files from Network Traffic: NetworkMiner, Xplico.

UNIT - 5: MALWARE ANALYSIS AND RANSOMWARE ANALYSIS

Introductory Malware Analysis: Malware, viruses, and worms, Importance of Malware Analysis, Essential Skills and Tools for Malware Analysis, Dependency walker, PEview, W32dasm, OllyDbg, Wireshark, Convertshell Code. Trends in Malware Evolution: Botnets, Encryption and Obfuscation, Automatic Self Updates, Metamorphic network behaviour, Blending Network Activity. Ransomware Analysis: Patterns of Ransomeware, Cruptolocker, Moscellaneous Ransomeware, RSO Cryptosystem, AES Cryptosystem, Cryptographich Techniqyes as Hacking tools, Tor Network, Digital Cash and Bitcoin.

References:

1. Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensics analysis using Wireshark. *International Journal of Security and Networks*, *10*(2), 91-106.
2. Meghanathan, N., Allam, S. R., & Moore, L. A. (2010). Tools and techniques for network forensics. *arXiv preprint arXiv:1004.0570*.
3. Davidoff, S., & Ham, J. (2012). *Network forensics: tracking hackers through cyberspace* (Vol. 2014). Upper Saddle River: Prentice Hall.
4. Social Media & Network Forensics, CDAC
5. Monnappa, K. A. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing Ltd.
6. Mohanta, A., Velmurugan, K., & Hahad, M. (2018). *Preventing Ransomware: Understand, prevent, and remediate ransomware attacks*. Packt Publishing Ltd.

Semester-wise Revised Syllabus under CBCS, 2020-21

Four Year B.Sc. (Hons) - Semester – V (from 2022-23)

Subject: **B. Sc - Cyber Forensics**

Course-6D: **Reverse Engineering and Malware Analysis**

(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Aim and Objectives of Course: Understanding Reverse Engineering, Typical Malware Behaviour, Working with the Payload. Also covering the Low-Level Language, Binary Obfuscation Techniques, Anti-emulation tricks, and Anti-dumping tricks.

Learning Outcomes

1. Overview of Tools like Autoruns and The Process Explorer
2. Design a payload
3. Working with Assemblers
4. Binary Obfuscation Techniques
5. Passing code execution via SHE
6. Reversing Various File Types

Unit I- Preparing to Reverse Engineer

What is Reverse engineering, Reverse engineering as a process, Tools, The operating system environment, Typical malware behaviour: Persistence, Malware delivery, Software piracy, Payload – the evil within, Tools: Autoruns, The Process explorer.

Unit II- The Low-Level Language

Binary numbers, x86: Registers, Memory addressing: Endianness. Basic instructions, Bitwise algebra, Control flow, Stack manipulation, Tools – builder and debugger: Popular assemblers: MASM, NASM, FASM, x86: Debuggers, WinDbg, Ollydebug, x64dbg.
Hello World: Installation of FASM, Dealing with common errors when building, Dissecting the program. After Hello: Calling APIs, Common Windows API libraries, Short list of common, API functions, Debugging

Unit III- Static and Dynamic Reversing

Assessment and static analysis: Static analysis, File types and header analysis: Extracting useful information from file, Other information: PE executables. Deadlisting: IDA (Interactive Disassembler), Decompilers: ILSpy – C# Decompiler. Dynamic analysis, Analysis environments, Information gathering tools, Disassemblers, Debuggers, Decompilers, Network tools, Editing tools, Attack tools, Automation tools, Software forensic tools, Automated dynamic analysis, Online service sites.

Unit IV- Sandboxing and Binary Obfuscation Techniques

Emulation of Windows and Linux under an x86 host, Analysis in unfamiliar environments: Linux ARM guest in QEMU, MBR debugging with Bochs. Binary Obfuscation Techniques: Data assembly on the stack, Encrypted data identification, Assembly of data in other memory regions,

Decrypting with x86dbg, Other obfuscation techniques, Packing and Encryption: A quick review on how native executables are loaded by the OS, Packers, crypters, obfuscators, protectors and SFX, Unpacking, Dumping processes from memory, How about an executable in its unpacked state? Other file-types.

Unit V- Anti-analysis Tricks

Anti-debugging tricks, Debugger information from NtQueryInformationProcess, Timing tricks. Passing code execution via SHE, Anti-VM tricks, Anti-emulation tricks, Anti-dumping tricks. Practical Reverse Engineering of a Windows Executable, Initial static analysis, Debugging, Reversing Various File Types: Analysis of HTML scripts, MS Office macro analysis, PDF file analysis, SWF file analysis: SWFTools, FLASM, Flare, XXXSWF, JPEXS SWF decompiler.

Suggested Reading:

1. Mastering Reverse Engineering, Reginald Wong
2. Practical Reverse Engineering by Bruce Dang, Alexandre Gazet, Elias Bachaalany
3. Reversing: Secrets of Reverse Engineering by Eldad Eilam
4. Implementing Reverse Engineering: The Real Practice of X86 Internals by Jitender Narula
5. Ghidra Software Reverse Engineering for Beginners: Analyze, identify, and avoid malicious code and potential threats in your networks and systems by A. P. David

Semester-wise Revised Syllabus under CBCS, 2020-21

Four Year B.Sc. (Hons) - Semester – V (from 2022-23)

Subject: **B. Sc - Cyber Forensics**

Course-7D: **Vulnerability Assessment of Application Security**

(Skill Enhancement Course (Elective), 5 credits, Max Marks: 100+50

Aim and Objectives of Course: Understanding Vulnerability Assessment, Differences between a bug bounty and a client-initiated pentest, Detecting SQL Injection flaws. Also covering the Extracting data using Insecure Direct Object Reference (IDOR) Flaws, Discovering Authentication methods.

Learning Outcomes

1. Working with Proxies and non-proxy-aware clients
2. Setting up Vulnerable web applications
3. Identifying XSS, XML, SSTI, SSRF, and CSRF vulnerabilities
4. Executing an out-of-band command injection
5. Exploiting crypto vulnerabilities
6. Discovering Blind SQL injection

Unit I- Configuring Burp Suite

Setting up proxy listeners, Working with non-proxy-aware clients, Creating target scopes in Burp Suite, Working with target, Additional browser add-ons that can be used to manage proxy Settings, Setting system-wide proxy for non-proxy-aware clients, Setting up Android and iOS to work with Burp Suite, Differences between a bug bounty and a client-initiated pentest, Why Burp Suite?: Types and features, Crawling. Why Burp Suite Scanner?: Auditor/Scanner, Understanding the insertion points. Detailed Stages of an application pentest, Features of Burp Suite.

Unit II- Preparing for an Application Penetration Test and Identifying Vulnerabilities

Setup of vulnerable web applications, Reconnaissance, and file discovery: Using Burp for content and file discovery. Testing for authentication via Burp, Detecting SQL injection flaws, Detecting OS command injection, Detecting XSS vulnerabilities, Detecting XML-related issues such as XXE, Detecting SSTI, Detecting SSRF, Detecting CSRF, Detecting Insecure Direct Object References, Detecting security misconfigurations, Detecting insecure deserialization, Detecting OAuth-related issues, Detecting broken authentication.

Unit III- Detecting and Exploiting Vulnerabilities - 1

Data exfiltration via a blind Boolean-based SQL injection, Executing OS commands using an SQL injection, Executing an out-of-band command injection, Stealing session credentials using XSS, Taking control of the user's browser using XSS, Extracting server files using XXE vulnerabilities, Performing out-of-data extraction using XXE and Burp Suite collaborator, Exploiting SSTI vulnerabilities to execute server commands.

Unit IV- Exploiting Vulnerabilities Using Burp Suite - 2

Using SSRF/XSPA to perform internal port scans. Using SSRF/XSPA to extract data from internal machines, Extracting data using Insecure Direct Object Reference (IDOR) Flaws. Exploiting security misconfigurations, Directory listings, Default credentials, Untrusted HTTP methods. Using insecure deserialization to execute OS commands, Exploiting crypto vulnerabilities, Brute forcing HTTP basic authentication, Brute forcing forms, Bypassing file upload restrictions.

Unit V- Writing Burp Suite Extensions and Breaking the Authentication

Setting up the development environment, Writing a Burp Suite extension: Burp Suite's API, Modifying the user-agent using an extension. Executing the extension, Performing information gathering, Port scanning, Discovering Authentication method. Exploiting and Exfiltrating Data from a Large Shipping Corporation: Discovering Blind SQL injection: Automatic scan, SQLMap detection, Intruder detection.

Suggested Reading:

1. Hands-on Penetration Testing for Web Applications: Run Web Security Testing on Modern Applications Using Nmap, Burp Suite and Wireshark by Richa Gupta
2. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more by Gus Khawaja
3. Hands-On Application Penetration Testing with Burp Suite: Use Burp Suite and its features by Carlos A. Lozano, Dhruv Shah, et al.

MODEL QUESTION PAPER (Sem-end. Exam)
B. Sc DEGREE EXAMINATION
SEMESTER –V

Time:3Hrs **Max.marks:75**

Suggested Theory Question Paper Pattern
SECTION A

Very Short Answer Questions 5 x2 10 Marks

1. What are the necessary components of search warrant?
2. What are the three rules of forensic hash?
3. List three sub-function of the extraction function.
4. What are different data hiding techniques?
5. What is the role of client and server in E-mail?

SECTION B

(Answer any four questions. Each answer carries 5 marks

(At least 1 question should be given from each 5x5=25 Marks

1. Define Digital Investigation Process.
2. Determine the best acquisition method, Discuss in brief.
3. Write about different Digital Forensic Lab certification requirements.
4. Define the term: A. Innocent Information B. The Plain View of Doctrine C. HAZMAT D. Commingled Contraband E. Hash Functions
5. Describe different storage formats of Digital Evidence along with advantages and disadvantages.
6. How can you validate forensic data?
7. What is Steganography and discuss different Steganalysis methods.
8. What is Honeynet Project and how to examine it?

SECTION C (4x10 = 40 Marks)

(Answer any four questions. Each answer carries 10 marks)

(At least 1 question should be given from each Unit)

1. What are different data hiding techniques. Explain in detail.
2. What is RAID, different types of RAIDS and how can you perform RAID data acquisition.
3. Discuss in detail various Corporate High-Tech Investigation.
4. What are the functions of Digital Forensic tools and define sub-functions of each.
5. Write about different Mobile Phone acquisition which one is the best method justify.
6. How to validate disk image using various Digital Forensic Tools.

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6

Time: 3 hrs Max. Marks: 50

1. Perform Acquisition of RAM using Magnet Forensics Tool. 08 M

2. Recover an E-mail using Magnet AXIOM. 08 M

3. Extract Data of "Forensic Image" created using FTK Imager and observe its properties. 12 M

4. Image Acquisition using "dd commands" in Kali Linux. 4 x 3 = 12 M

   A. Generate hash values of original evidence (sda2/sda5)

   B. Generate hash values of Forensic Images.

   C. Comparison of values with hashdeep command.

   D. Give the same name to both the forensic images and the calculate and compare the hash values.

5. Record + Viva-voce 6+4 = 10 M