CURRICULUM & SYLLABUS

For

B.E.,(Hons.) Computer Science and Engineering with Specialization in Cyber Security

(Choice Based Credit System)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Sri Chandrasekharendra Saraswathi ViswaMahavidyalaya
SCSVMV
(Deemed to be University U/S 3 of UGC Act 1956)
Accredited with "A" Grade by NAAC
Enathur, Kanchipuram – 631 561

B.E(Hons.) Computer Science and Engineering with Specialization in Cyber Security

Professional Specialized Courses (PSC)								
SL. No	Semester	Course Category	Course Code	Name of the Course	Hours per week			Credit
					L	T	P	
1.	3	PSC		Introduction to Cyberspace Operations and Design	3	0	0	3
2.	4	PSC		Security Audit and Risk Assessment	3	0	0	3
3.	5	PSC		Database security	3	0	0	3
4.	5	PSC		Database & Network Security Lab	0	0	2	2
5.	6	PSC		Ethical hacking & Digital Forensics	3	0	0	3
6.	6	PSC		Forensics & Investigation Lab	0	0	2	2
7.	7	PSC		Vulnerability Discovery & Exploit Development	3	0	0	3
Total Credits								19

SEMESTER-III

Course Code :	INTRODUCTION TO CYBERSPACE OPERATIONS AND DESIGN	L	T	P	C
		3	0	0	3

PRE-REQUISITE:

Knowledge of Computer Networks .

OBJECTIVES:

- Learn the foundations of Cyber security and cyber crime.
- Educate students to understand impact of cybercrime in society.
- To develop skills in cyber security mechanisms to ensure the protection of information technology assets.
- To expose students about the Mobile and wireless device security.
- To expose students about digital forensics .

COURSE OUTCOME:

The end of course the students can able to

1. Understand the concept of Cyber security and issues and challenges associated with it.
2. Understand the cybercrimes and its categories.
3. Understand the mobile devices and its securities and digital forensics.
4. Understand the basic concepts of cyber crime and its methods against digital payment frauds.
5. Understand about the digital forensics.

MAPPING WITH PROGRAMME OUTCOMES:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	M				S							M
CO2				S				L				
CO3		M					L			M		
C04			S			M						
CO5				M							M	

S - STRONG M – MEDIUM L – LOW

UNIT- I INTRODUCTION

Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Concept of cyber security, Design principles, Issues and challenges of cyber security.

UNIT –II CYBERCRIME

Cybercrime- Definition and Origins of the Word Cybercrime and Information Security, Cybercriminals, Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cyber offenses, Cyber Attacks, Social Engineering, Cyber stalking, Cyber cafe and Cybercrimes.

UNIT –III Mobile and Wireless Devices

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile Phones ,Security Implications for organizations, Organizational Measures for Handling Mobile.

UNIT –IV METHODS USED IN CYBERCRIME

Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Attacks on Wireless Networks. Introduction to Phishing, Identity Theft (ID Theft).

UNIT –V UNDERSTANDING COMPUTER FORENSICS

Introduction, Digital Forensics Science, Need Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Network Forensics, Approaching a Computer Forensics Investigation.

TEXTBOOKS:

1. SunitBelapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, Publish Date 2013.

2. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Press. ISBN: 9789351194736, 2015.

REFERENCE BOOKS:

1. Thomas J. Mowbray, “Cyber security: Managing Systems, Conducting Testing, and

2. Investigating Intrusions”, Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 - 84965 -1.

3. James Graham, Ryan Olson, Rick Howard, “Cyber Security Essentials”, CRC Press, 15-Dec 2010.

4. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.

SEMESTER -IV

Course Code :	SECURITY AUDIT AND RISK ASSESSMENT	L	T	P	C
		3	0	0	3

PRE_REQUISTICS: NIL

COURSE OBJECTIVES:

6. Understand the security audit planning strategies
7. Gain knowledge about information risk
8. Discover knowledge in collecting data about organization
9. Acquire knowledge in various analyses on information risk assessment
10. Introduce the system risk analysis and system specific risk

COURSE OUTCOMES

Co1. Acquire the knowledge on various secure auditing techniques and to identify knowledge in information risk

Co2. Understand the basic ideas about data collection

Co3. Appreciate the concepts of vulnerability catalogs and impact analysis scheme

Co4. Identify the knowledge in risk classification techniques

Co5. Acquire the knowledge on system specific risk

S - STRONG, M- MEDIUM, L- LOW

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S											L
CO2	S										M	
CO3		S								M		
CO4	S										M	
CO5		S										L
CO6												

UNIT – I INTRODUCTION

What is Risk? –Information Security Risk Assessment Overview- Drivers, Laws and Regulations- Risk Assessment Frame work – Practical Approach.

UNIT- II DATA COLLECTION

The Sponsors- The Project Team- Data Collection Mechanisms- Executive Interviews- Document Requests- IT Assets Inventories- Profile & Control Survey Consolidation.

UNIT- III DATA ANALYSIS

Compiling Observations- Preparation of catalogs- System Risk Computation Impact Analysis Scheme- Final Risk Score.

UNIT – IV RISK ASSESSMENT

System Risk Analysis- Risk Prioritization- System Specific Risk Treatment- Issue Registers- Methodology- Result- Risk Registers- Post Mortem.

UNIT – V SECURITY AUDIT PROCESS

Pre-planning audit- Audit Risk Assessment- Performing Audit- Internal Controls Audit Evidence- Audit Testing- Audit Finding- Follow-up activities.

REFERENCES

1. Mark Talabis, “Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis”, Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.
2. David L. Cannon, “CISA Certified Information Systems Auditor Study Guide”, John Wiley & Sons, ISBN: 978-0-470-23152-4, 2009.

SEMESTER-V

Course Code :	DATABASE SECURITY	L	T	P	C
		3	0	0	3

PRE-REQUISITES

Students should have an understanding of basic database concepts and mathematics.

COURSE OBJECTIVES

- To learn the security of databases
- To learn the design techniques of database security
- To learn the secure software design.

COURSE OUTCOMES

Co1. Avoid unauthorized data observation.
Co2. Avoid unauthorized data modification.
Co3. Ensure the data confidentiality.
Co4. Prove that the data integrity is preserved.
Co5. Prove that, only authorized user has access to the data.
Co6. Identify security threats in database systems.
Co7. Design and Implement secure database systems.
Co8. Solve Complex Problems in a Team of database works

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S	M	L	-	-	-	-	M	M	L	-	L
CO2	S	S	M	M	L	-	-	M	M	L	-	M
CO3	S	S	S	L	L	-	-	M	M	L	-	M
CO4	S	S	M	M	L	-	-	S	S	L	-	M
CO5	S	s	M	M	L	-	-	M	M	L	-	M
CO6	M	M	L	L	L	-	-	L	L	L	-	L
CO7	M	M	L	L	M	-	-	L	L	L	-	L
CO8	M	M	L	L	M	-	-	M	M	L	-	L

S STRONG, M MEDIUM, L LOW

UNIT- I

Introduction: Introduction to Databases Security Problems in Databases Security Controls Conclusions. Security Models - Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases.

UNIT – II

Security Mechanisms : Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria

UNIT - III

Database Security: Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

UNIT - IV

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities.

UNIT – V

Future Trends Privacy in Database Publishing: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

TEXTBOOKS:

1. Database Security by Castano Pearson Edition (lie) Database Security and Auditing: Protecting Data Integrity and Accessibility, 1st Edition, Hassan Afyouni, THOMSON Edition.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia.

REFERENCE BOOK

1. Database security by Alfred Basta, Melissa Zgola, CENGAGE learning.

Course Code :	DATABASE & NETWORK SECURITY LAB	L	T	P	C
		0	0	2	2

COURSE OBJECTIVES:

- To engage themselves in lifelong learning of Database management systems theories and technologies this enables them to purse higher studies
- Learn to implement the algorithms DES, RSA,MD5,SHA-1
- Learn to use network security tools like GnuPG, KF sensor, Net Strumbler

SOFTWARE REQUIREMENTS

- DBMS: DDL, DML, DCL
- C & C++
- Java or equivalent compiler GnuPG
- KF Sensor or Equivalent.

COURSE OUTCOMES:

Co1.Students will learn to draw ER, EER, and UML Diagrams.

Co2. In analyzing the business requirements and producing a viable model for the implementation of the database.

Co3. Students will learn to convert the entity-relationship diagrams into relational tables.

Co4. To develop appropriate Databases to a given problem that integrates ethical, social, legal, and economic concerns.

Co5. Implement the cipher techniques, develop the various security algorithms

Co6. Use different open source tools for network security and analysis

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	M	L	S	-	-	-	-	-	M	L	-	L
CO2	M	S	L	M	L	-	-	-	M	L	-	L
CO3	M	M	S	L	L	-	-	-	M	L	-	M
CO4	L	M	M	M	L	-	-	-	S	L	-	L
CO5	M	S	M	M	S	-	-	-	M	L	-	L
CO6	S	M	L	L	S	-	-	-	L	L	-	L

S-STRONG ,M-MEDIUM, L-LOW

LIST OF EXERCISES

1. Draw E-R diagram and convert entities and relationships to relation table for a given scenario. a. Two assignments shall be carried out i.e. consider two different scenarios (eg. bank, college)
2. Write relational algebra queries for a given set of relations.
3. Perform the following: a. Viewing all databases, Creating a Database, Viewing all Tables in a Database, Creating Tables (With and Without Constraints), Inserting/Updating/Deleting Records in a Table, Saving (Commit) and Undoing (rollback)

4. Perform the following: a. Altering a Table, Dropping/Truncating/Renaming Tables, Backing up / Restoring a Database.
5. For a given set of relation schemes, create tables and perform the following Simple Queries, Simple Queries with Aggregate functions, Queries with Aggregate functions (group by and having clause), Queries involving- Date Functions, String Functions , Math Functions Join Queries- Inner Join, Outer Join
6. Implement the following Substitution & Transposition Techniques concepts:
   a) Caesar Cipher
   b) Playfair Cipher
   c) Hill Cipher
   d) Vigenere Cipher
   e) Rail fence – row & Column Transformation.
7. Implement the following algorithms
   a) DES
   b) RSA Algorithm
   c) Diffiee-Hellman
   d) MD5
   e) SHA-1
8. Implement the Signature Scheme - Digital Signature Standard
9. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)
10. Setup a honey pot and monitor the honeypot on network (KF Sensor)

SEMESTER-VI

Course Code :	ETHICAL HACKING & DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

PRE_REQUISTICS: Computer Networking and Cryptgraphy skills

COURSE OBJECTIVES

1. To learn various hacking techniques and attacks.
2. To know how to protect data assets against attacks from the Internet.
3. To evaluate where information networks are most vulnerable.
4. To perform penetration tests into secure networks for evaluation purposes.
5. To enable students to understand issues associated with the nature of forensics

COURSE OUTCOMES

Co1. To known about hacking concepts system maintenance.

Co2. Apply the Architecture strategies for computer fraud Prevention.

Co3. Awareness of Key frauds and system security

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S										M	L
CO2		S										M
CO3		S									L	

UNIT- I HACKING WINDOWS

Hacking windows – Network hacking – Web hacking – Password hacking - A study on various attacks – Input validation attacks – SQL injection attacks – Buffer overflow attacks - Privacy attacks.

UNIT- II TCP / IP AND FIREWALLS

TCP / IP – Checksums – IP Spoofing port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls - Packet Inspection firewalls – Application Proxy Firewalls - Batch File Programming.

UNIT- III COMPUTER FRAUD

Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks – Managing the threat – Strategic Planning Process.

UNIT- IV ARCHITECTURE STRATEGIE

Architecture strategies for computer fraud prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks.

UNIT- V FORENSIC

Accounting Forensics – Computer Forensics – Journaling and it requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

TEXT / REFERENCE BOOKS

1. Kenneth C.Brancik, "Insider Computer Fraud", Auerbach Publications Taylor & Francis, Group 2008.
2. Ankit Fadia, "Ethical Hacking", Second Edition Macmillan India Ltd, 2006

Course Code :	FORENSICS & INVESTIGATION LAB	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

Co1. To Understand the concepts of open source tools
Co2. To identify and report the forensic on disk level
Co3. To Implement forensic concepts in network level
Co4. To Analyze Virtual machine forensic
Co5. To Analyze various cloud forensic

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S									M		L
CO2		S										M
CO3		S								M		
CO4	S											L
CO5		S										L

List of Exercise

1. Study of Computer Forensics and different tools used for forensic investigation
2. How to Recover Deleted Files using Forensics Tools
3. Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.
4. How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software
5. How to make the forensic image of the hard drive using EnCase Forensics.
6. How to Restoring the Evidence Image using EnCase Forensics
7. How to Collect Email Evidence in Victim PC
8. How to Extracting Browser Artifacts
9. How to View Last Activity of Your PC
10. Find Last Connected USB on your system (USB Forensics)
11. Comparison of two Files for forensics investigation by Compare IT software
12. Live Forensics Case Investigation using Autopsy
13. Forensic analysis of a Virtual Machine and Cloud storage

SEMESTER-VII

Course Code :	VULNERABILITY DISCOVERY & EXPLOIT DEVELOPMENT	L	T	P	C
		3	0	0	3

PRE_REQUISTICS: Good knowledge and practical experience in penetration testing.

COURSE OBJECTIVES:

1. To focus on a comprehensive coverage of software exploitation.
2. To present different domains of code exploitation and how they can be used together to test the security of an application.

COURSE OUTCOMES:

Co1. Understand how to exploit a program and different types of software exploitation techniques

Co2. Understand the exploit development process

Co3. Search for vulnerabilities in closed-source applications

Co4. Write their own exploits for vulnerable applications

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S					M					L	
CO2		S									S	M
CO3			M									L
CO4		S								L		
CO5			S									

S - STRONG, M- MEDIUM, L- LOW

UNIT - I

Background- Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing

UNIT-II

Targets and Automation- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation

UNIT- III

Advanced Fuzzy Technologies- Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection. Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, Visualizing code changes and identifying fixes, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls.

UNIT- IV

Windows Kernel Debugging and Exploitation - Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques.

Windows Heap Overflows and Client -Side Exploitation- Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls

UNIT-V

Android Exploitation - Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis.

iOS exploitation -Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation.

TEXT BOOKS AND REFERENCES:

1. Hack I.T. - Security through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni.
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm.