Pimpri Chinchwad Education Trust's

PIMPRI CHINCHWAD COLLEGE OF ENGINEERING

SECTOR NO. 26, PRADHIKARAN, NIGDI, PUNE 411044

An Autonomous Institute Approved by AICTE and Affiliated to SPPU, Pune

DEPARTMENT OF COMPUTER ENGINEERING

Curriculum Structure and Syllabus

of

Honors in Cyber Security

(Course 2020)

Effective from Academic Year 2023-24

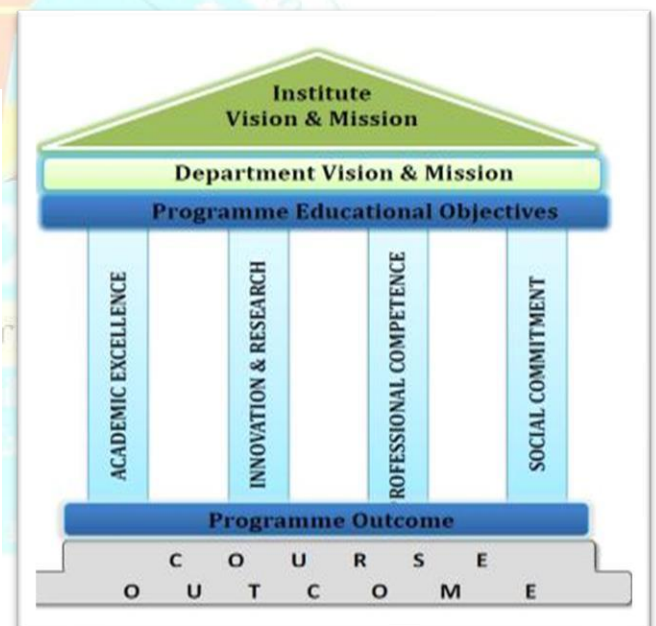## (Updated with minor changes)

Institute Vision

To be one of the top 100 Engineering Institutes of India in coming five years by offering exemplarily Ethical, Sustainable and Value Added Quality Education through a matching ecosystem for building successful careers.

Institute Mission

1. Serving the needs of the society at large through establishment of a state-of-art Engineering Institute

2. Imparting right Attitude, Skills, Knowledge for self-sustenance through Quality Education

3. Creating globally competent and Sensible engineers, researchers and entrepreneurs with an ability to think and act independently in demanding situations

Quality Policy

We at PCCOE are committed to impart Value Added Quality Education to satisfy the applicable requirements, needs and expectations of the Students and Stakeholders. We shall strive for academic excellence, professional competence and social commitment in fine blend with innovation and research. We shall achieve this by establishing and strengthening state-of- the-art Engineering and Management Institute through continual improvement in effective implementation of Quality Management System.

	Pimpri Chinchwad Education Trust's **Pimpri Chinchwad College of Engineering**	
	Course Approval Summary	

A) Board of study - Department of Computer Engineering

Sr. No.	Name of the Course	Course Code	Page number	Signature and stamp of BoS
1	Cyber Law andCryptography	HCE5983	5	
2	Cryptography Laboratory	HCE5984	8	
3	Advance Security andDigital Forensics	HCE6983	11	
4	Cyber Forensics Laboratory	HCE6984	13	
5	Block chain ArchitectureDesign	HCE7982	16	
6	Ethical Hacking	HCE7983	18	
7	Project	HCE8982	21	

Approved by Academic Council:

Chairman, Academic Council
Pimpri Chinchwad College of Engineering

Approved by Board of Governors:

Chairman, Board of Governors
Pimpri Chinchwad College of Engineering

Preface

Looking at Global Scenario to enhance the employability skills and impart deep knowledge in emerging/ multidisciplinary areas, an additional avenue is provided to passionate learners through the Minors and Honors Degree Scheme in academic structure.

For **Honors degree** program, student has to earn additional 20 credits in emerging area of one's own domain.

Objectives of Honors Degree

- To enable students to pursue allied academic interest in contemporary areas.
- To provide effective yet flexible options for students to achieve basic to intermediate level competence in the contemporary area.
- To enhance the employability skills with different combinations of competencies and flavors.
- To provide an academic mechanism for fulfilling demand of specialized areas from industries for higher order skill jobs.
- To provide a strong foundation to students aiming to pursue research/ higher studies in the contemporary field of study.
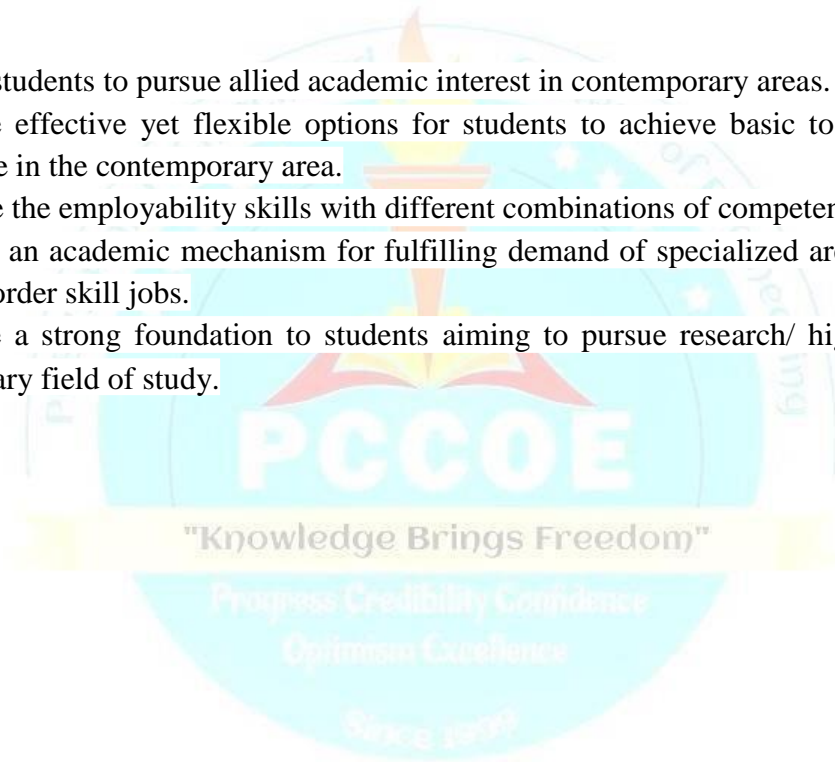
Preface of Honors in Cyber Security

Today's digital world increases the sophistication of threats to the cyber landscape coupled with the rapid increase in attempts to disrupt our critical systems and gain commercial and personal data. There is an ever-increasing demand for highly skilled cyber security graduates to defend individuals and organizations from various cybercrimes. The Cyber Security Honors Program is created to train the next generations of cyber security experts to develop reliable and lawful networks. Security, cryptography, cyber law, incident response, and digital forensics are just some of the topics that will be covered in this comprehensive program.

With a carefully designed curriculum that emphasizes practical experience, students working toward an honors degree in cyber security can acquire the analytical and investigative skills necessary to keep up with the ever-changing nature of cybersecurity threats. Department of Computer Engineering Cyber Security Honors Program teaches students to think critically about security in order to address complex problems, identify and counteract cyber threats, evaluate risks, and implement state-of-the-art security measures. Courses in Advanced Security and Digital Forensics, as well as Blockchain Architecture Design, are among those available through the Honors program. Through the course of study, students will acquire the broad range of knowledge, skills, abilities, and dispositions necessary for success as cybersecurity professionals in a variety of public and private sectors.

Objectives

This program aims to
1. Prepare responsible Cyber Security professionals by training them about cyber laws, Information security compliances, and ethical disclosures.
2. Apply security best practices to keep the system running as usual despite the existence of inherent risks.
3. Design, deploy, and assess a computational solution to the issue of securing software and systems.

Learning Outcomes

Students, after completing this Honors course successfully, will be able to
1. Reflect critically on existing theoretical knowledge, ideas, and practice within computing and cyber security to address the research topic.
2. Realize legal and ethical principles to be adopted in the domain of security practices
3. Demonstrate an understanding of specialized knowledge in computing and cyber security, tools and techniques, and digital forensic lifecycle for proactive security.

Department of Computer Engineering

INDEX

LIST OF ABBREVIATIONS IN CURRICULUM STRUCTURE

Sr. No.	Abbreviation	Expansion
1.	L	Lecture
2.	P	Practical
3.	T	Tutorial
4.	H	Hours
5.	CR	Credits
6.	IE1	Internal Evaluation 1
7.	IE2	Internal Evaluation 2
8.	ETE	End Term Evaluation
9.	TW	Term Work
10.	OR	Oral
11.	PR	Practical
12.	PROJ	Project

Curriculum Structure

Honors in Cyber Security

CURRICULUM STRUCTURE

Structure for Honors in Cyber Security (Computer Engineering)

Semester	Course code	Course Name	Teaching Scheme				CR	Evaluation Scheme						
			L	P	T	H		IE1	IE2	ETE	TW	PR	OR	Total
V	HCE5983	Cyber Law and Cryptography	3	-	-	3	3	20	30	50	-	-	-	100
V	HCE5984	Cryptography Laboratory		4	-	4	2				50			50
VI	HCE6983	Advance Security and Digital Forensics	3		-	3	3	20	30	50	-	-	-	100
VI	HCE6984	Cyber Forensics Laboratory	-	4	-	4	2	-		-	50	-	-	50
VII	HCE7982	Block chain Architecture Design	3	-	-	3	3	20	30	50	-	-	-	100
VII	HCE7983	Ethical Hacking	-	4	-		2	-		-	50	-	-	50
VIII	HCE8982	Project	-	10	-	10	5			-	100		50	150
	Total		**9**	**22**	**0**	**31**	**20**							**600**

L-Lecture, **P**-Practical, **T**-Tutorial, **H**-Hours, **Cr**-Credits, **IE** Internal Evaluation, **ETE**-End Term Evaluation, **TW**-Term Work, **OR**-Oral, **PR**-Practical

<div style="text-align: center">

Course Syllabus

Semester – V

Honors in Cyber Security

</div>

Department of Computer Engineering

Program:	**B. Tech. (Computer) - Honors in Cyber Security**			Semester: V			
Course:	**Cyber Law and Cryptography**			Code: HCE5983			
Teaching Scheme				**Evaluation Scheme**			
Lecture	**Tutorial**	**Credit**	**Hours**	**IE1**	**IE2**	**ETE**	**Total**
03	-	03	03	20	30	50	100

Prior Knowledge of:
1. Basic algorithm analysis
2. Complexity theory,
3. Elementary notions of logic
4. Set theory.
is essential.

Course Objectives:

1. To provide a detailed understanding of Cyber Crimes, Countermeasures and Cyber Laws, and Information SecurityStandard.
2. Analyze the legal perspectives and laws related to cybercrimes in the Indian context.
3. To provide the fundamental mathematical base for cryptographic algorithms
4. To provide in-depth knowledge of cryptography theories, algorithms, and systems.

Course Outcomes:

After learning the course, the students will be able to:

1. Comprehend how various cybercrime take place and evaluate the effect of cybercrime
2. Comprehend how cyber laws are effective against cybercrimes and design a system compliant with Information SecurityStandard
3. Apply the knowledge of Finite Fields for various algorithms of cryptography
4. Apply the knowledge of various identification schemes.
5. Evaluate the performance of different message digest and hash algorithms.
6. Analyze and model modern cryptography including problem statements and mathematical approaches.

Detailed Syllabus:		
Unit	**Description**	**Duration (H)**
I	**Fundamentals of Cyber Crime:** Overview, nature, scope, and types of Cyber Crime;Comparison between traditional criminal techniques and cybercrime; Impact ofcybercrime on E-Governance and E-commerce; Best Practices of cybercrime investigation Procedure for search and seizure for digital evidence. Tools and Methods of Cyber Crime: Phishing, Password Cracking, Keyloggers, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Identity Theft Case Study: Challenges in handling cybercrime from the perspective of Individuals and enterprises	**08**

II	**Cyber Security Laws and Regulations:** Indian Law Perspective - IT Act (2000) and Personal Data Protection Bill (2019); Global-Regulation Perspective - GDPR, GLBA, HIPAA; **Cyber Laws and Compliance:** Different Aspects of Cyber Laws - Contractual aspects, Intellectual property aspect, Criminal Aspects; Legal framework for managing cyber security; Information Security Standards - SOX, NIST, ISO Case Study: Legal Procedure for GDPR violation	07	
III	**Finite Fields:** Modular Arithmetic, congruence theorem, Algebraic structure, GF (2n) fields Euclidean theorem, Extended Euclidean theorem, Factorization, Fermat's theorem, Euler's theorem, Chinese remainder theorem, Discrete logarithms, Lagrange's method.	08	
IV	**Advance Cryptosystems** **Asymmetric key Cryptosystems:** Rabin, El-Gamal, Knapsack**,** Elliptic Curve cryptosystem, Pairing-based Cryptography**,** Identity-Based and Attribute-Based cryptosystem**.** **Symmetric key Cryptosystems:** IDEA, Blowfish, CAST-128**.**	07	
V	**Introduction to Cryptographic Hash Functions**: Fundamentals of MAC Protocols, HMAC, CMAC, CBC-MAC and PMAC, Design of Collision-Resistant Hash Functions, Popular Uses of Collision-Resistant Hash Functions, MD5, SHA-I, SHA-256. **Digital Signature schemes:** Elgamal, Schnorr signature schemes, ECDSA, CCA security for symmetric encryption. Case study: Multi-collision resistant hash function.	08	
VI	**Cryptography in the age of quantum computers:** Grover's algorithm and symmetric cryptography, Shor's algorithm and public-key cryptography, Quantum key distribution, Quantum secret sharing, and multiparty computation, post-quantum cryptography. Case study: The DARPA Quantum Cryptography Network.	07	
	Total	45	

Text Books:

1. William Stallings**, "**Cryptography and Network Security: Principles and Practice", 6th Edition, Pearson Education, ISBN 13: 9781292158587
2. Forouzan, B.A., **"**Cryptography & Network Security" Tata McGraw-Hill Education, ISBN-13: 978-0070702080
3. Kahate, A.,"Cryptography, and Network Security". McGraw-Hill Higher Ed., ISBN-13: 9789353163303
4. Godbole, N., "Information Systems Security: Security Management, Metrics, Frameworks and Best Practices". 1st Ed. John Wiley & Sons India, ISBN: 9788126564057.

Reference Books:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 20th Anniversary Edition, Wiley, ISBN: 978-1-119-09672-6.
1. Jeff Koseff , "3rd Edition, Cyber Security Law" Wiley ISBN: 9781119231509

Web references:

1. williamstallings.com/Extras/Security-Notes/
2. www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/
3. http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security
4. http://cs.brown.edu/courses/csci1510/2013_lectures.html
5. NPTEL Course lectures links :- https://nptel.ac.in/courses/106/105/106105031/ (Modern cryptography, ECC andSHA)

Department of Computer Engineering

Program:	B. Tech. (Computer) - Honors in Cyber Security			Semester:		V	
Course:	Cryptography Laboratory			Code:		HCE5984	
Teaching Scheme				**Evaluation Scheme**			
Practical	Tutorial	Credit	Hours	TW	PR	OR	Total
4	-	2	4	50	-	-	50

Prior Knowledge of:
1. Basic algorithm analysis
2. Complexity theory
3. Elementary notions of logic
4. Set theory

is essential.

Course Objectives:
1. To explore the working principles of well-known attacks such as Buffer Overflow, SQL Injection and their countermeasures.
2. To explore the issues security issues in the network and resolve it.
3. To develop the ability to use modern cryptographic utilities to build programs for secure communication.

Course Outcomes:
After learning the course, the students will be able to:
1. Acquire background on well-known Cryptography Digital Signature Techniques
2. Apply various public key cryptography techniques
3. Apply finite field (mathematics) for achieving security
4. Apply security and privacy methods in development of modern applications and in organizations to protect resources and to prevent cyber crimes
5. Evaluate security mechanisms using rigorous approaches by digital signatures and Hash functions.
6. Develop awareness of latest trends and advances in security using quantum computing

Guidelines for Students:

- The laboratory assignments are to be submitted by students in the form of a journal.

- Journal consists of prologue, certificate, table of contents and handwritten write-up of each assignment (Title, Objectives, Problem Statement, Outcomes, Date of Completion, Assessment grade/marks and assessor's sign, Theory- Concept, algorithm, sample input and expected output, conclusion).

- Program codes with sample output of all performed assignments are to be submitted as softcopy.

Guidelines for Laboratory /TW Assessment:
- Continuous assessment of laboratory work is done based on the overall performance and laboratory performance of students.
- Each laboratory assignment assessment should assign grade/marks based on the parameters with appropriate weightage.
- Suggested parameters for overall assessment as well as each laboratory assignment assessment includes- performance, timely completion, innovation, efficiency, punctuality, and neatness.

Guidelines for Laboratory Conduction

- Operating System: 64-bit Open-source Linux or its derivative.
- Programming Tools: Open-Source C, C++, JAVA and PYTHON.
- All assignments are compulsory to perform.

Department of Computer Engineering

Assignment No.	Suggested List of Assignments
1	Given a piece of code with buffer-overflow vulnerability, gain the root privilege by exploiting this vulnerability
2	Demonstrate SQL Injection using SQL Map
3	Demonstrate Cross-site Scripting attack.
4	Demonstrate password cracking using Cain and Abel and John the Ripper tools.
5	Write a program to solve a system of linear congruence by applying the Chinese Remainder Theorem
6	Write a program to implement the MD5/SHA-1 algorithm.
7	Write a program to implement Rabin Cryptosystem.
8	Write a program to implement Knapsack Cryptosystem
9	Write a program to illustrate El-Gamal digital signature.
10	Write a program to illustrate Elliptic curve digital signature algorithm.
11	Write a program to illustrate Schnorr digital signature schemes.
12	Implement shor's public key cryptography algorithm.

Reference Books:

1. William Stallings**,** Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, ISBN13: 9781292158587
2. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, ISBN-13: 978-0070702080
3. Kahate, A**.** Cryptography, and Network Security. McGraw-Hill Higher Ed., ISBN-13: 9789353163303
4. Godbole, N., Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. 1st Ed.John Wiley & Sons India, ISBN: 9788126564057.
5. Riggs, C., Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA, eISBN: 9780429211577.

Web references:
1. NPTEL Course lectures links:

   https://nptel.ac.in/courses/106/105/106105031/ (Modern cryptography, ECC and SHA)

Course Syllabus
Semester – VI
Honors in Cyber Security

Department of Computer Engineering

Program:	B. Tech.(Computer) - Honors in Cyber Security		Semester: VI	
Course:	Advance Security and Digital Forensics		Code: HCE6983	

Teaching Scheme				Evaluation Scheme			
Lecture	Tutorial	Credit	Hours	IE1	IE2	ETE	Total
3	-	3	3	20	30	50	100

Prior Knowledge of:
1. Cryptography
2. System Security
is essential.

Course Objectives:

1. To provide the underlying principles of access control mechanisms
2. To make students understand various program flaws and learn control against program threats.
3. To provide foundation of open web application security project and web service security
4. To explore software vulnerabilities, attacks and protection mechanisms of wireless networks and protocols, mobile devicesand web applications.
5. To develop an understanding of current cyber security issues (Computer Security Incident) and analyzed the ways that exploitsin securities.

Course Outcomes:

After learning the course, the students will be able to:
1. Understand cyber-attacks and apply access control policies and control mechanisms
2. Identify malicious code and targeted malicious code
3. Detect and counter threats to web applications
4. Understand the vulnerabilities of Wi-Fi networks and explore different measures to secure wireless protocols, WLAN andVPN networks.
5. Explain the methodology of incident response and various security issues in ICT world, and identify digital forensic tools fordata collection.
6. Use different forensic tools to acquire and duplicate data from compromised systems and analyse the same.

Detailed Syllabus:		
Unit	**Description**	**Duration (H)**
I	**Introduction & Access Control**: Cyber-attacks, Vulnerabilities, and Defence in Depth Strategies. Access Control Policies: DAC, MAC, RBAC, Multi-level Security Models: Biba Model, Bell La Padula Model, and Single Sign on, Federated Identity Management.	7
II	**Program & OS Security**: Malicious and Non-Malicious programming errors, Targeted Malicious codes: Salami Attack, Linearization Attack, Covert Channel, Control against Program threats.	7

	Operating System Security: Memory and Address protection, File Protection Mechanism, User Authentication.	
III	**Web Application Security:** OWASP, Web Security Considerations, User Authentication and Session Management, Cookies, SSL, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Clickjacking, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, Web Service Security, OAuth 2.0	7
IV	**Wireless Security:** Wi-Fi Security, WEP, WPA, WPA-2, Mobile Device Security- Security Threats, Device Security, GSM and UMTS Security, IEEE 802.11/802.11i Wireless LAN Security, VPN Security.	8
V	**Computer Security Incident Response Methodology:** Goals of Incident response, Incident Response Methodology, Formulating Response Strategy, IR Process – Initial Response, Investigation, Remediation, Tracking of Significant ,Investigative Information, Reporting Pre Incident Preparation, Incident Detection and Characterization. Live Data Collection : Live Data Collection on Microsoft Windows Systems: Live Data Collection on Unix-Based Systems	8
VI	**Forensic Duplication:** Forensic Image Formats, Traditional Duplication, Live System Duplication, Forensic Duplication tools **Disk and File System Analysis**: Media Analysis Concepts, File System Abstraction Model The Sleuth Kit : Installing the Sleuth Kit , Sleuth Kit Tools Partitioning and Disk Layouts : Partition Identification and Recovery, Redundant Array of Inexpensive Disks Special Containers : Virtual Machine Disk Images , Forensic Containers Hashing, Carving : Foremost , Forensic Imaging : Deleted Data , File Slack , dd , dcfldd , dc3dd **Data Analysis:** Analysis Methodology Investigating Windows systems , Investigating UNIX systems , Investigating Applications, Web Browsers, Email, Malware Handling: Static and Dynamic Analysis	8
	Total	45

Text Books:

1. Stallings, William, Lawrie Brown, "Computer security: principles and practice", Pearson Education, 2012. ISBN-13: 9780134794105.
2. Pfleeger, Charles P, and Shari Lawrence Pfleeger, "Analyzing computer security: A threat/vulnerability/countermeasure approach", Prentice Hall Professional, 2012, ISBN: 9780132789493

Cole, Eric, "Network security bible", John Wiley & Sons, 2011, ISBN: 978-0-470-57000-5

Reference Books:

1. Gollman, Dieter, "Computer Securuty", John Wiley & Sons, 2009, ISBN: 978-0-470-74115-3
2. Prosise, Chris, Kevin Mandia, and Matt Pepe. "Incident response & computer forensics." McGraw-Hill, 2014, ISBN: 9780071798693

Web references:

1. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Program:	B. Tech. (Computer) - Honors in Cyber Security			Semester:		VI	
Course:	Cyber Forensics Laboratory			Code:		HCE6984	
Teaching Scheme				Evaluation Scheme			
Practical	Tutorial	Credit	Hours	TW	PR	OR	Total
4	-	2	4	50	-	-	50

Prior Knowledge of:
1. Cryptography
2. Network security

is essential.

Course Objectives:
1. To explore the working principles of cyber forensics tools.
2. To develop the ability to use various open source tools for network forensics.
3. To explore forensic tools to acquire and duplicate data from compromised systems and analyse the same.

Course Outcomes:
After learning the course, the students will be able to:
1. Explore various password forensics tools for compressed files.
2. Understand the basic network forensics and techniques for conducting the forensic examination on network.
3. Apply forensic analysis tools to recover deleted files.
4. Explore various forensics tools in Kali Linux and use them to acquire, duplicate and analyze data and recover deleted data.
5. Analyse forensic images using open source tools
6. Apply steganography tools to detect data hiding.

Guidelines for Students:
- The laboratory assignments are to be submitted by students in the form of a journal. Journal consists of prologue, Certificate, table of contents, and handwritten write-up of each assignment.
- Each assignment write-up should have Title, Objectives, Outcomes, Theory- Concept in brief, dataset used, data description,
- Conclusion, Assessment grade/marks and assessor's sign.
- Program codes with sample output of all performed assignments are to be submitted as softcopy.

Guidelines for Laboratory /TW Assessment:
- Continuous assessment of laboratory work is done based on overall performance and Laboratory performance of students.
- Each Laboratory assignment assessment should assign grade/marks based on parameters with appropriate weightage.
- Suggested parameters for overall assessment as well as each Laboratory assignment assessment include- timely completion, performance, innovation, efficiency, punctuality, and neatness.

Guidelines for Laboratory Conduction
- Operating System recommended:- 64-bit Open source Linux or its derivative, Kali Linux
Use of open source tools is encouraged.

Assignment No.	Suggested List of Assignments

1	Using a password forensic tools like fcrackzip, rarcrack to crack .zip and .rar password protected files
2	Network Forensics, Investigating Logs and Investigating Network Traffic
3	Recovery of deleted files using winhex, Foremost
4	Detect SQL injection vulnerabilities in a website database using SQLMap.
5	Explore open source tools like Autopsy, FTK Imager, etc. for acquiring, analyzing and duplicating data.
6	Explore forensics tools in Kali Linux for acquiring, analyzing and duplicating data: dd, dcfldd, foremost, scalpel, debugfs, wireshark, tcptrace, tcpflow
7	Memory forensics to capture the physical memory of a suspect's computer using open source tools likeMAGNET RAM Capture etc.
8	Windows Registry forensics using open source Registry Analysis tools like RegRipper etc.
9	Install and use Android and iOS Mobile Forensics Open Source Tools.
10	Analysis of forensic images using open source tools like Autopsy: SIFT, and commercial tool FTK Imager.
11	Analysis of photograph using open source Image forensic tools like Forensically etc.
12	Use of steganographic tools like OpenStego, to detect data hiding or unauthorized file copying

Reference Books:

1. Kevin Mandia, Chris Prosise, "Incident Response & Computer Forensics", McGraw-Hill, 2014, ISBN: 9780071798693
2. C. Altheide& H. Carvey, "Digital Forensics with Open Source Tools", Syngress, 2011. ISBN: 9781597495868.

Web references:
1. http://www.opentechinfo.com/learn-use-kali-linux/

Course Syllabus
Semester – VII
Honors in Cyber Security

Department of Computer Engineering

Program:	**B.Tech.(Computer) - Honors in Cyber Security**			Semester:		**VII**
Course:	**Blockchain Architecture Design**			Code:		**HCE7982**

Teaching Scheme				Evaluation Scheme			
Lecture	**Tutorial**	**Credit**	**Hours**	**IE1**	**IE2**	**ETE**	**Total**
3	-	3	3	20	30	50	100

Prior Knowledge of :
1. Data Structures
2. cryptography techniques
3. Programming Concepts

is essential.

Course Objectives:
1. To provide conceptual understanding of working of Blockchain Technology.
2. To familiarize various types of Blockchian.
3. To familiarize different platforms of Blockchain such as Ethereum, Hyperledger, Bitcoin etc.
4. To impart knowledge of smart contracts for development of Blockchian based systems.

Course Outcomes:

After learning the course, the students will be able to:
1. Describe working of Blockchain system.
2. Demonstrate different types of Consensus algorithms.
3. Classify public, private and consortium Blockchain
4. Design Ethereum based smart contracts for different applications
5. Explore different Consortium Blockchain techniques using Hyperledger Fabric and Ripple.
6. Develop and Deploy different ideas using block chain technology in different domain.

Detailed Syllabus:

Unit	Description	Duration (H)
I	Fundamentals of Blockchain : Introduction, Origin of Blockchain, key Blockchain concepts, Components of Blockchain- Node, Nonce, Hash, mining, Wallet, Ledger, Block in a Blockchain, Blockchain layers, Pros & Cons of Blockchain.	7
II	Consensus Mechanisms and Blockchain Types : Different consensus mechanisms, Public Blockchain & Private Blockchain : Public Blockchain, Blockchain Layers, Popular public Blockchain. Ethereum Blockchian, Private Blockchain & Permission ed Blockchain, RAFT Consensus algorithm	7

III	Smart Contracts : Introduction to smart contracts, Characteristics of smart contracts, Types of smart contracts, Smart contracts in Ethereum, Smart contracts in Industry(healthcare, Supply chin etc). Smart contracts in Private Blockchain.	**8**
IV	Consortium Blockchain : Key characteristics of consortium Blockchain, Need of consortium Blockchain, Challenges of Consortium Blockchain, Introduction to Hyperledger : Fabric, sawtooth , Tools, Hyperledger fabric, Overview of Ripple	**7**
V	Blockchain Security: Pseudo-anonymity vs. anonymity, Introduction to Zcash and Zk-SNARKS for anonymity preservation. Attacks on Blockchains: Sybil attacks, selfish mining and 51% attacks.	**8**
VI	Applications of Blockchain and Cryptocurrency: Blockchain in Banking & Finance- Challenges, Know your customer (KYC), Cross border payments, Trade finance. Blockchain in Healthcare- Challenges in Healthcare, Heath Records Management. Future of Blockchain for cryptocurrencies.	**8**
	Total	**45**

Text Books:

1. Chanframouli Subramanian, Asha George, Abhilash K A, Meena Karthikeyan, " Blockchain Technology", University Press (Indis)Pvt.Ltd. 2021, ISBN: 9789389211634
2. Bashir, Imran, "Mastering Blockchain : Distributed ledger technology, decentralization, and smart contracts explained", 2nd Edition, Birmingham : Packet Publishing, 2018, ISBN 9781788838672 178883867X 1788839048 9781788839044

Reference Books:

1. Melanie Swan, "Block Chain: Blueprint for a New Economy", O'Reilly, 2015
2. Ritesh Modi, "Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum and Block Chain", Packt Publishing
3. Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, "Hands-On Block Chain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer", Import, 2018
4. Daniel Drescher, "Block Chain Basics", Apress; 1st edition, 2017

Department of Computer Engineering

Program:	B.Tech.(Computer) - Honors in Cyber Security			Semester:			VII
Course:	Ethical Hacking			Code:			HCE7983
Teaching Scheme				**Evaluation Scheme**			
Practical	Tutorial	Credit	Hours	TW	PR	OR	Total
4	-	2	4	50	-	-	50

Prior Knowledge of:
1. Cryptography
2. Network security
is essential.

Course Objectives:
1. Investigate reconnaissance: Information gathering for the ethical hacker
2. Evaluate various techniques and tools used in network scanning
3. Determine the techniques and tools used in system hacking

Course Outcomes:
After learning the course, students will be able to:

1. Identify footprinting techniques and tools for network scanning and analysis
2. Use tools to simulate intrusion detection system and firewalls
3. Explore open source tools to identify network vulnerability
4. Simulate various attacks like DoS and SQL Injection attack
5. Analyze static code and program vulnerabilities using open source tools
6. Analyze different security tools to detect web application and browser vulnerabilities

Guidelines for Students:
- The laboratory assignments are to be submitted by students in the form of a journal. Journal consists of prologue,Certificate, table of contents, and handwritten write-up of each assignment.
- Each assignment write-up should have Title, Objectives, Outcomes, Theory- Concept in brief, dataset used, datadescription,
- Conclusion, Assessment grade/marks and assessor's sign.
- Program codes with sample output of all performed assignments are to be submitted as softcopy.

Guidelines for Laboratory /TW Assessment:
- Continuous assessment of laboratory work is done based on overall performance and Laboratory performance of students.
- Each Laboratory assignment assessment should assign grade/marks based on parameters with appropriate weightage.
- Suggested parameters for overall assessment as well as each Laboratory assignment assessment include- timelycompletion, performance, innovation, efficiency, punctuality, and neatness.

Guidelines for Laboratory Conduction
- Operating System recommended:- 64-bit Open source Linux or its derivative, Kali Linux
- Use of open source tools is encouraged.
- All assignments are compulsory to perform.

Assignment No.	Suggested List of Assignments
1	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather informationabout networks and domain registrars.

2	Study of packet sniffer tools like wireshark, ethereal, tcpdump etc. following need to covered:- 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show the packets can be traced based on different filters.
3	Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do aping scan, tcp port scan, udp port scan, etc.
4	Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark. Use arping tool to generate gratuitous arps and monitor using wireshark
5	Use the NESSUS tool to scan the network for vulnerabilities.
6	Install IDS (e.g. SNORT) and study the logs.
7	Use of iptables in linux to create firewalls.
8	Simulate buffer overflow attack using Ollydbg, Splint, Cppcheck etc
9	Simulate DOS attack using Hping, hping3 and other tools.
10	Explore the website copier HTTrack
11	Static code analysis using open source tools like RATS, Flawfinder etc
12	Explore web-application vulnerabilities using open source tools like Wapiti, browser exploitation framework (BeEf)

Reference Books:

1. Sean-Philip Oriyano, Michael Gregg, "Hacker Techniques, Tools, and Incident Handling." Jones and Bartlett Learning, 2017, ISBN: 9780763791841.
2. Walker, Matt. " CEH Certified Ethical Hacker All-in-One Exam Guide", McGraw-Hill, 2017, ISBN: 9781260454567.
3. Gregg, Michael, "Build Your Own Security Lab: a field guide for network testing (with cd)", John Wiley & Sons, 2008, ISBN: 9780470179864.
4. Stuttard, Dafydd, and Marcus Pinto, "The web application hacker's handbook: Finding and exploiting security flaws", John Wiley & Sons, 2011, ISBN: 9780470170779.

Course Syllabus

Semester – VIII

Honors in Cyber Security

Department of Computer Engineering

Program:	B. Tech.(Computer) - Honors in Cyber Security		Semester:	VIII
Course:	Project		Code:	HCE8982

Teaching Scheme				Evaluation Scheme			
Practical	Tutorial	Credit	Hours	TW	PR	OR	Total
10	-	5	10	100	-	50	150

Course Objectives:
1. To follow SDLC meticulously and meet the objectives of proposed work.
2. To apply recent tools and techniques.
3. To develop the solutions and conduct experimentations.
4. To validate and evaluate the work undertaken.
5. To clearly articulate their research work in a well-written and orally presented project
6. To present project management skills in a team.

Course Outcomes:
After learning the course, the students should be able to:
1. Acquire practical knowledge within the chosen area of technology for project development.
2. Identify, analyze, formulate and handle programming projects with a comprehensive and systematic approach
3. Critically analyze the results and their interpretation.
4. Validate the project outcomes.
5. Contribute as an individual or in a team in development of technical projects
6. Develop effective communication skills for presentation of project related activities

Guidelines for Project:
1. The Project may be carried out in a group of 2 /3 students.
2. The student shall prepare and submit the report of Project work in standard format for satisfactory completion of the work that is duly certified by the concerned guide and head of the Department/Institute.
3. The evaluation of the project shall be on continuous basis.

Vision and Mission of Computer Department

Department Vision

To be a premier Computer Engineering program by achieving excellence in Academics and Research for creating globally competent and ethical professionals.

Department Mission

M1: To develop technologically competent and self-sustained professionals through contemporary curriculum.

M2: To nurture innovative thinking and collaborative research, making a positive impact on society.

M3: To provide state-of-the art computing environment and learning opportunities through Center of Excellence.

M4: To foster leadership skills and ethics with holistic development.