Scheme of Final Year

B. Tech Computer Science and Engineering (Cyber Security)
Scheme of Studies/Examination (w.e.f. Session 2023-24)

Semester VII

S. No.	Course No.	Subject		/ k	Credits	Examination Schedule				Duration of Exam (Hrs.)
						Major Test	Minor Test	Practical	Total	
1	PC-CS-CYS 401A	Cyber Attacks-OWASP Framework	3:0:0	3	3	75	25	0	100	3
2	HSS-403A	Universal Human Values II: Understanding Harmony	3:0:0	3	3	75	25	0	100	3
3	OEC	OEC Elective -II	3:0:0	3	3	75	25	0	100	3
4	PE-I	Elective*-I	2:0:0	2	2	75	25	0	100	3
5	PE-II	Elective* - II	2:0:0	2	2	75	25	0	100	3
6	PC-CS-CYS 405LA	Cyber Attacks-OWASP Framework Lab	0:0:2	2	1	0	40	60	100	3
7	PC-CS-CYS 407LA	Cloud Security Lab	0:0:2	2	1	0	40	60	100	3
8	PC-CS-CYS	Project-I	0:0:10	10	5	0	100	100	200	3

	409LA									
9	PC-CS-CYS 413LA	Industrial Training	0:0:0	0	3	0	100	0	100	
		Total		**27**	**23**	**375**	**405**	**220**	**1000**	

Code	**PE-I**	**Code**	**PE-II**
PE-CS-CYS-415A	Introduction to cyber laws	PE-CS-CYS-421A	Software Testing
PE-CS-CYS-417A	Advance Computer Architecture	PE-CS-CYS-423A	Cybercrime Forensics and Digital Forensics
PE-CS-CYS-419A	Software Vulnerability Analysis	PE-CS-CYS-425A	Cloud Security

Code	**OEC Elective-II**
OE-CS-CYS -401	Robotics and Intelligent Systems
OE-CS-CYS-403	Ethical Hacking
OE-CS- CYS-405	Privacy and Security in IoT
OE-CS-CYS-407	Digital Electronics
OE-CS-CYS-409	Network Management and Security

B. Tech Computer Science and Engineering (Cyber Security)
Modified Scheme of Studies/Examination (w.e.f. Session 2023-24)
Semester VIII

	. se No.	Subject	L: T:P	Hours/ Week	Credits	Examination Schedule				Duration of Exam (Hrs.)
						Major Test	Minor Test	Practical	Total	
1	PC-CS-CYS 402A	Block Chain in Cyber security	3:0:0	3	3	75	25	0	100	3
2	HSS-404A	Entrepreneurship and Start-ups	3:0:0	3	3	75	25	0	100	3
3	OEC	OEC Elective*-III	3:0:0	3	3	75	25	0	100	3
4	PE-III	Elective*-III	2:0:0	2	2	75	25	0	100	3
5	PE-IV	Elective* - IV	2:0:0	2	2	75	25	0	100	3
6	PC-CS-CYS 406LA	Cyber security Block Chain Lab	0:0:2	2	1	0	40	60	100	3
7	PC-CS-CYS 410LA	Project-II	0:0:10	10	5	0	100	100	200	3
8	PC-CS-CYS	General Fitness &	0:0:0	0	0	0	0	100	100	3

	412LA	Professional Aptitude								
		Total		**25**	**19**	**375**	**265**	**260**	**900**	

Code	**PE Elective* -III**	**Code**	**PE Elective* -IV**
PE-CS- CYS-414A	Penetration Testing	PE-CS- CYS-422A	Intrusion detection and Prevention
PE-CS- CYS-416A	Identity and Access Management	PE-CS- CYS-424A	Introduction to Cyber Crime Investigations
PE-CS- CYS-420A	Biometric Security	PE-CS- CYS-426A	Social Networks

Code	**OEC Elective*-III**
OE-CS- CYS-402	Backup Disaster & Recovery
OE-CS- CYS-404	Cryptographic Fundamentals
OE-CS- CYS-406	Artificial Intelligence
OE-CS- CYS-408	Reasoning, Problem Solving and Robotics
OE-CS- CYS-410	Data Injection

Syllabus Final Year

PC-CS CYS-401A	**Cyber Attacks- OWASP Framework**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hours**
Purpose	To understand web application security course based on OWASP Top 10 web application security risks.						
Course Outcomes (CO)							
CO1	Awareness about OWASP Top 10 web application security risks.						
CO2	Understanding of the most critical security risks to web applications.						
CO3	Identify and mitigate the ten most critical security risks by reviewing vulnerable source code.						
CO4	Understand the need of writing the secure code.						

Unit- I

Getting Started with OWASP, Application Security Risks, OWASP Top 10 Application Security Risks, Introduction to Web Application Security (OWASP A02:2021 Cryptographic Failures, OWASP A04:2021— Insecure Design).

Unit-II

User Authentication (OWASP A07:2021—Identification and Authentication Failures, OWASP A03:2021— Injection, OWASP A02:2021—Cryptographic Failures), Function and Data Access Control (OWASP A01:2021—Broken Access Control).

Unit-III

SQL Injection (OWASP A03:2021—Injection), Cross-Site Scripting (XSS) (OWASP A08:2021— Software and Data Integrity Failures), Handling Data from an Untrusted Source (OWASP A09:2021— Security Logging and Monitoring Failures, A10:2021—Server-Side Request Forgery).

Unit-IV

Processing of Composite Data (OWASP A08:2021—Software and Data Integrity Failures), Configuration Errors (OWASP A05:2021—Security Misconfiguration, A06:2021— Vulnerable and Outdated Components).

Miscellaneous topics: Cross Site Request Forgery (CSRF), JWT security, session hijacking, Local File Inclusion (LFI), Remote File Inclusion (RFI).

Suggested Books:

· OWASP. Top 10 the Most Critical Web Application Security Risks. 2021. Available online: https://owasp.org/Top10/ (accessed on 15 January 2023).

· Troiano, Ernesto, Maurizio Ferraris, and John Soldatos. "Security challenges for the critical infrastructures of the financial sector." Cyber-physical threat intelligence for critical infrastructures security (2020).

HSS-403A	Universal Human Values II: Understanding Harmony						
Lecture	Tutorial P		Credit	Major Test	Minor Test	Total	Time
3	0	0	3.0	75	25	100	3 Hours
Purpose	Purpose and motivation for the course, recapitulation from Universal Human Values-I						
Course Outcomes(CO)							
CO1	Development of a holistic perspective based on self-exploration about						
CO2	themselves(human being),family, society and nature/existence.						
CO3	Understanding(or developing clarity)of the harmony in the human being, family, Strengthening of self-reflection.						
CO4	Society and nature/existence. Development of commitment and courage to act.						

Module1:Course Introduction-Need, Basic Guidelines, Content and Process for Value Education

1. Purpose and motivation for the course, recapitulation from Universal Human Values-I

2. Self-Exploration–what is it? - Its content and process;‘ Natural Acceptance’ and Experiential Validation-as the process for self-exploration

3. Continuous Happiness and Prosperity- Aloo kat basic Human Aspirations

4. Right understanding, Relationship and Physical Facility

The basic requirements for fulfilment of aspirations of every human being with their correct priority

5. Understanding Happiness and Prosperity correctly-A critical appraisal of the current scenario

6. Method to fulfil the above human aspirations: understanding and living in harmony at various levels. Include practice sessions to discuss natural acceptance in human being as the innate acceptance for living with responsibility (living in relationship, harmony and co existence) rather than as arbitrariness in choice based on liking-disliking

Module2:UnderstandingHarmonyintheHumanBeing-HarmonyinMyself!

1. Understanding human being as a co-existence of the sentient 'I' and the material 'Body' 2. Understanding the needs of Self('I') and 'Body'-happiness and physical facility 3. Understanding the Body as an instrument of 'I'(I being the doer, seer and enjoyer) 4. Understanding the characteristics and activities of 'I' and harmony in 'I' 5. Understanding the harmony of I with the Body: Sanyam and Health; correct appraisal of Physical needs, meaning of Prosperity in detail 6. Programs to ensure Sanyam and Health.

Include practice sessions to discuss the role others have played in making material goods available to me. Identifying from one's own life. Differentiate between prosperity and accumulation. Discuss program for ensuring health vs dealing with disease

Module 3: Understanding Harmony in the Family and Society- Harmony in Human Human Relationship

1. Understanding values in human-human relationship; meaning of Justice (nine universal values in relationships)and program for its fulfilment to ensure mutual happiness; Trust and Respect as the foundational values of relationship 2. Understanding the meaning of Trust; Difference between intention and competence 3. Understanding the meaning of Respect, Difference between respect and differentiation; the other salient values in relationship 4. Understanding the harmony in the society(society being an extension of family): Resolution, Prosperity, fearlessness(trust)and co-existence as comprehensive Human Goals 5. Visualizing a universal harmonious order in society- Undivided Society, Universal Order from family to world family. Include practice sessions to reflect on relationships in family, hostel and institute as extended family, real life examples, teacher
Student relationship, goal of education etc. Gratitude as a universal value in relationships. Discuss with scenarios. Elicit examples from students' lives

Module4: Understanding Harmony in the Nature and Existence- Whole existence as Coexistence

1. Understanding the harmony in the Nature 2.Interconnectedness and mutual fulfilment among the four orders of nature- recyclability and self regulation in nature
3. Understanding Existence as Co-existence of mutually interacting units in all-pervasive space 4. Holistic perception of harmony at al levels of existence.

Include practice sessions to discuss human being as cause of imbalance in nature (film "Home" can be used), pollution, depletion of resources and role of technology etc.

Module5: ImplicationsoftheaboveHolisticUnderstandingofHarmonyonProfessionalEthics

1. Natural acceptance of human values 2. Definitiveness of Ethical Human Conduct 3. Basis for Humanistic Education, Humanistic Constitution and Humanistic Universal Order 4. Competence

in professional ethics: a .Ability to utilize the professional competence for augmenting universal human order b. Ability to identify the scope and characteristics of people friendly and eco-friendly production systems, c. Ability to identify and develop appropriate technologies and management patterns for above production systems. 5. Case studies of typical holistic technologies, management models and production systems 6. Strategy for transition from the present state to Universal Human Order: a. At the level of individual: as socially and ecologically responsible engineers, technologists and managers b. At the level of society :as mutually enriching institutions and organizations 7. Sumup Include practice Exercises and Case Studies will be taken up in Practice(tutorial)Sessions eg. To discuss the conduct as an engineer or scientist etc.

READINGS:

TextBook

1. Human Values and Professional Ethics by RR Gaur,R Sangal,GP Bagaria, Excel
Books,New Delhi,2010

ReferenceBooks

1. JeevanVidya:EkParichaya, ANagaraj, JeevanVidyaPrakashan,
Amarkantak,1999. 2.
HumanValues,A.N.Tripathi,NewAgeIntl.Publishers,NewDelhi,2004.
3. TheStoryofStuff(Book).

OE-CS-CYS 403	**Ethical Hacking**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hrs.**
Purpose	The course teaches beginners about computer systems with the permission of the organization. People who have a keen interest in the field of technology can opt for this course. Ethical hacking is a process wherein professionals use the vulnerabilities of a network/ system to detect intrusions from malicious hackers.						
Course Outcomes							
CO 1	To gain knowledge about Ethical hacking and penetration testing.						
CO 2 ·	To learn about various types of attacks, attackers and security threats and vulnerabilities present in the computer system.						
CO 3 ·	To examine how social engineering can be done by attacker to gain access of useful & sensitive information about the confidential data.						
CO 4	To learn about cryptography, and basics of web application attacks.						

Unit-I Ethical Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms.

Unit-II Security operations center(SOC), SOC framework, SOC tools, what is QRadar, Incident Detection and Investigation with QRadar, Incident Responder process.

Unit-III Wifi hacking, firewall and honeypots, Snort introduction, Snort implementation, pentration testing, hacking web server, SQL injection, exploit writing in python, Format string

Unit-IV Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking Basic ethical hacking tools and usage of these tools in a professional environment. Legal, professional and ethical issues likely to face the domain of ethical hacking. Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Suggested Books:

<u>Hacking: The Art of Exploitation</u>, Jon Erickson, 2nd edition, No Starch Press

The Basics of Hacking and Penetration Testing, Patrick Engebretson, 2nd edition, Syngress The Web Application Hacker’s Handbook, DafyddStuttard, 2nd edition, Wiley

PE-CS-CYS 415A	Introduction to cyber laws						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	The course deals with all the aspects of Cyber law as per Indian/IT act. It also covers overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.						
Course Outcomes (CO)							
CO 1	To give overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.						
CO 2	To analyze and evaluate existing legal framework and laws on cyber security.						
CO 3	To analyze and evaluate the Intellectual rights and copyrights.						
CO 4	To understand cyber ethics.						

Unit-1

Introduction to Cybercrime and cyber law: Cyber Crimes Categories and kinds, Evolution of the IT Act, IT Act, 2000, various authorities under IT Act and their powers. Penalties & Offences, amendments

Unit-2

Jurisdiction and Ecommerce: Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E – commerce and Laws in India, Digital / Electronic Signature in Indian Laws.

Unit-3

Intellectual rights and copyrights: Intellectual Property Rights, Domain Names and Trademark Disputes, Copyright in Computer Programmes, Concept of Patent Right, Sensitive Personal Data or Information in Cyber Law, Cyber Law an International Perspective.

Unit-4

Cyber Ethics: Cyber Ethics and Code, Net Neutrality, Free speech and Censorship in Cyberspace, Intellectual Property in Cyberspace, Privacy Rights and Surveillance.

Suggested Books:

1. Sushma Arora, Raman Arora, Cyber Crimes & Laws, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, Technology Laws Decoded, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723 3. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House New Delhi
4. P.M. Bukshi and R.K. Suri, Guide to Cyber and E –Commerce Laws, Bharat Law House, New Delhi 5. Rodney D. Ryder, Guide to Cyber Laws; Wadhwa and Company, Nagpur

Note: The Examiner will be given the question paper template and will have to set the question paper according to the template provided along with the syllabus.

PE-CS- CYS- 425A	**Cloud Security**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To enable students to learn various computational models, design paradigms of advanced computer architecture, parallelism approaches and techniques for static and dynamic interconnections.						
Course Outcomes (CO)							
CO1	Classify and interpret various paradigms, models and micro-architectural design of advanced computer architecture as well as identify the parallel processing types and levels for achieving optimum scheduling						
CO2	Identify the roles of VLIW & superscalar processors and branch handling techniques for performance improvement						
CO3	Analyze and interpret the basic usage of various MIMD architectures and relative importance of various types of static and dynamic connection networks for realizing efficient networks.						
CO4	Examine the various types of processors and memory hierarchy levels and cache coherence problem including software and hardware-based protocols to achieve better speed and uniformity.						

Unit - 1

Introduction to AWS Security by Design, AWS Key Management Best Practices, A Deep Dive into AWS Encryption Services, Security at Scale: Logging in AWS, AWS WAF, AWS Security Incident Response.

Unit - 2

Common attacks on cloud infrastructure: Unauthorized Access, SQL injection, XSS, Misconfiguration, DOS - DDOS, Data Loss/Leakage, Data Privacy/Confidentiality, Incident Response, counter measure to protect cloud infrastructure.

Unit - 3

Data Protection for Cloud Infrastructure and Services: Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Data protection laws of India, Common attack vectors and threats, Data Protection Strategies.

Unit - 4

Monitoring, Auditing and Management: Proactive activity monitoring, Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts.

Reference books
Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9 o
Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563

PC-CS-CYS 405LA	**Cyber Attacks- OWASP Framework Lab**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hours**
Purpose	Understand the OWASP Top 10 and how to use them to minimize risk.						
Course Outcomes (CO)							
CO1	Apply the OWASP Top 10 to ensure your applications minimize the security risks in the list.						
CO2	Explore how Web Applications are built and delivered on top of the HTTP protocol.						
CO3	Explore threat agents, attack vectors, and impact of the ten most critical web application security risks.						
CO4	Explore common exploitation techniques used to test software security.						

LIST OF PRACTICALS*:*

Lab1: Introduction to Web Application Security- In this lab, there is creation of an environment for testing the security of WWW applications and for performing basic tasks such as data preview and modification of the transmitted HTTP requests. Virtual laboratories in this topic are based on OWASP A02:2021—Cryptographic Failures and OWASP A04:2021—Insecure Design. The exercises involved in this lab are-- Response Headers Preview (*), Manipulating HTTP Parameters (*), Launch and Configuration of Proxy in a browser (**), Automatic Application Scan (*), Modification of HTTP Requests (*), Repeating HTTP Request (*), Finding the Right Parameter Value by Brute Force Method (**).

Lab2: User Authentication- This topic concerns authentication-related attacks. Authentication describes the procedure to verify one’s identity. On most websites, it is encountered in the form of a username and password combination that is needed to log in. Session management, on the other hand, comes into play when we are successfully authenticated. Upon login, a unique session key is generated. This unique key ensures that our logged-in session is held upright as we browse the application, so we do not have to re-authenticate each time we switch the endpoint. Broken authentication denotes that there is an issue with the authentication or the way that the session is handled. In this module, students can detect broken authentication using manual methods and can exploit them using automated tools with password lists and dictionary attacks. They can examine and compromise session tokens. Virtual laboratories in this topic are based on OWASP A07:2021—

Identification and Authentication Failures, OWASP A03:2021—Injection, and OWASP A02:2021—Cryptographic Failure and consist of five exercises, which are described as: Low-Complexity User Password (**), Weak Randomness Session Identifier (**), Client-Side Authentication (*), Incorrect password reset implementation (**), User Enumeration Based on Response Time (**).

Lab3: Function and Data Access Control- In this module, students are introduced to the weaknesses and vulnerabilities available in broken access control. Access control, also known as authorization (not to be confused with authentication), is a process that determines whether users can gain access to a resource. Authorization is a basic security service that appears in most applications. Decisions regarding access control are generally enforced on the basis of rules (called policies) set down by the user. Virtual laboratories in this topic are based on OWASP A01:2021—Broken Access Control and consist of the five exercises described in detail below as: Access to Hidden Pages (**), Security Flaw in Access to API (**), HTTP Parameter Manipulation (**), Path Traversal Vulnerability (**), Insecure Direct Object Reference Vulnerability (**).

Lab4: SQL Injection- Injection attacks are discussed in the OWASP injection module. According to the OWASP authors, injection flaws are very prevalent and are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. They can be easily discovered using automated tools such as scanners and fuzzers. In the exercises prepared for this topic, we mostly focused on SQL-based attacks. SQL injection is an attack that inserts (injects) a malicious part of an SQL query to a database in a loaded request that is created by an application. Virtual laboratories in this topic are based on OWASP A03:2021-Injection and consist of the five exercises described in detail below as: Classic SQL Injection Vulnerability (*), Reading the Database Schema (**), Identification of the Database Server Version (**), Blind SQL Injection Vulnerability (***), Time-Based SQL Injection Vulnerability (***).

Lab5: Cross-Site Scripting (XSS)-According to OWASP, cross-site scripting (XSS) attacks can be found in around two-thirds of all web applications. Cross-site scripting (XSS) attacks are a type of attack involving injection, where malicious input data (such JavaScripts) are inserted in the HTML code of WWW pages. There are three forms of XSS, usually targeting users' browsers: reflected XSS (injecting code to the HTTP request), stored XSS (injecting code into a data source that provides data for the page), and DOM XSS (used when an application uses JavaScript to dynamically create the page content). Virtual laboratories in this topic are based on OWASP A08:2021—Software and Data Integrity Failures and consist of the seven exercises described in detail below as: Stored XSS Vulnerability (*), Reflected XSS Vulnerability (*), DOM XSS Vulnerability (*), XSS Vulnerability (Other Vector) (**), XSS Vulnerability (Filtering Out Tags) (**), XSS Vulnerability (Improved Tag Filtering) (**), XSS Vulnerability (Input Validation) (***).

Lab6: Handling Data from an Untrusted Source-- Data coming from external sources (such as data entered by application users) cannot be recognized by the application as trusted; the application should verify their correctness (e.g., format). One of the most common web application security vulnerabilities is an incorrect check of the correctness of the input data from a client or environment. Data that are modified or prepared unexpectedly can be used for application logic abuse attacks, denial of service (a DoS type of attack), or execution of any code after deserialization of the data. In this section, students learn about common security gaps that emerge from incorrect or unimplemented data validation mechanisms. Virtual laboratories in this topic are based on OWASP A09:2021—

Security Logging and Monitoring Failures and OWASP A10:2021—Server-Side Request Forgery and consist of 10 exercises as described in detail below as: Reading an Unexpected File (*), Reading an Unexpected File with the Use of PHP Filters (**), Running a Malicious Command by Uploading a File (**), Secure File Upload (***), Remote Reading of an Unexpected File (**), Standard Web Application Firewall (WAF) (***), Protected Files Download (WAF) (****), Insecure Log Browser (*), Secure Log Browser (****), Sending E-mails (****).

Lab7: Processing of Composite Data— XML external entities (XXE) attacks can cause denial of service, file scans, and remote code execution that undermine the security of the system. Understanding the relationship between XML files, parsing, and weak parsing is imperative to understanding what an XXE attack is and why such an attack can put the system at risk. Virtual laboratories in this topic are based on OWASP A08:2021—Software and Data Integrity Failures and consist of the six exercises described in detail below as: Unprotected Parsing of XML Files (*), Denial-of-Service Attack with the Use of an XML Bomb (*), Unprotected Object Deserialization (*), Protected Parsing of XML Files (**), From Deserialization of the Object to Code Execution on the Server (***), Real Attack on the Framework Using Object Deserialization (****).

Lab8: Configuration Errors-- Security misconfiguration vulnerabilities can occur when a web application component is susceptible to attack due to misconfiguration or an insecure configuration option. Virtual laboratories in this topic are based on OWASPA05:2021—Security Misconfiguration and OWASP A06:2021—Vulnerable and Outdated Components and consist of the six exercises described in detail below as: Publicly Accessible Administration Panel (**), Insecure Database Server Configuration (**), Publicly Accessible Development Server (**), Using Default Passwords (**), Outdated Software with Known Vulnerabilities (**), Publicly Available Backup (**).

Lab9: Cross Site Request Forgery (CSRF)-- The objective of this lab is to help students understand the Cross-Site Request Forgery (CSRF) attack. A CSRF attack involves a victim user, a trusted site, and a malicious site. The victim user holds an active session with a trusted site while visiting a malicious site. The malicious site injects an HTTP request for the trusted site into the victim user session, causing damages.

Lab10: JWT security and session hijacking

Lab11: Local File Inclusion (LFI) and Remote File Inclusion (RFI).

Lab Practical Resources:

1. Ksiezopolski, Bogdan, et al. "Teaching a Hands-On CTF-Based Web Application Security Course." *Electronics* 11.21 (2022): 3517.

2. Cross Site Request Forgery (CSRF), Available online: https://seedsecuritylabs.org/Labs_16.04/PDF/Web_CSRF_Elgg.pdf (accessed on 15 January 2023).

NOTE: A student must perform at least ten experiments. Seven experiments should be performed from the above list. Remaining three experiments may either be performed from the above list or designed & set by the concerned institution as per the scope of the syllabus.

PC-CS-CYS 407LA	**Cloud Security Lab**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hours**
Purpose	Understand the cloud deployment and security tools						
Course Outcomes (CO)							
CO1	Learn various cloud deployment tools						
CO2	Learn about Cloud security metrics.						
CO3	Explore threat in cloud services & application.						
CO4	To get the knowledge about work with cloud management Platform						

LIST OF PRACTICALS

1. **Installation and configuration of Microsoft Azure/AWS/Cloud Stack environment**

2. **Implement Service deployment & Usage over cloud.**

3. **Perform Management actions of cloud resources and prepare report.**

4. **Using existing cloud characteristics & Service models deploy various services.**

5. **Perform Cloud Security Management Operations**

6. **Performance evaluation of services over cloud.**

HSS-404A	**Entrepreneurship and Start-ups**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hour**
Purpose	To expose students to the joys and skills of being an entrepreneur.						
Course Outcomes (CO)							
CO1	To understand the basics of Entrepreneurship.						
CO2	To learn the basics of Creative and Design Thinking.						
CO3	To apply the Business Enterprises.						
CO4	To know about business models.						

Unit I

Introduction to Entrepreneurship, Meaning and concept of entrepreneurship, the history of entrepreneurship development, role of entrepreneurship in economic development, Myths about entrepreneurs, types of entrepreneurs.

Unit II

The skills/ traits required to be an entrepreneur, Creative and Design Thinking, the entrepreneurial decision process, entrepreneurial success stories.

Unit III

Crafting business models and Lean Start-ups: Introduction to business models; Creating value propositions conventional industry logic, value innovation logic; customer focused innovation; building and analysing business models; Business model canvas, Introduction to lean start-ups, Business Pitching.

Unit IV

Institutions Supporting Small Business Enterprises: Central level institutions. State level institutions. Other agencies. Industry Associations. Class exercise- discussions on current government schemes supporting entrepreneurship and finding out which scheme will most suit the business plan devised by the student.

Text Books:

· Kuratko, D , Hornsby J.S. (2017) New Venture Management: Entrepreneur's roadmap

· Hisrich, R.D., Manimala, M.J., Peters, M.P., Shepherd, D.A.: Entrepreneurship, Tata McGraw Hill · Ries, Eric(2011)The lean Start-up: How constant innovation creates radically

· S. Carter and D. Jones-Evans (2012), Enterprise and small business- Principal Practice and Policy, Pearson Education (2006)

PC-CS **CYS-402A**	**Block Chain in Cyber Security**						
L	**T**	**P**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 hrs**
Purpose	***Purpose To provide knowledge of various*** **Blockchain** ***& Cyber Security***						
Course Outcomes (CO)							
CO 1	*To learn the basics of Blockchain Concepts & Architecture.*						
CO 2	*To explore knowledge of various process of Cyber attacks on blockchain*						
CO 3	To understand the basics of security issues						
CO 4	To implies the basic of solidity and its deployment						

UNIT I- Blockchain and Smart Contract Fundamentals: Introduction to Blockchain, Importance of Blockchain, need of Blockchain, types of blockchain, Decision Tree, Consensus Mechanism

Cryptography, Hashing, and Digital Signatures: Introduction, Hashing, Hash Function Characteristics, Digital Signatures, Data Encryption, Denial of Serviceman-in-The-Middle Attack, System Resiliency, Infrastructure Hardening.

Unit II-Consensus Protocols: Proof of Work, Security Issues in Proof of Work, Proof of Stake, Security Issues in Proof of Stake, Other Consensus Types

Blockchain Vulnerabilities and Attacks: Network and Consensus Security Issues, Smart Contract and Code Security Issues, Wallet and Client Security Issues, Centralization Security Issues, User Security Issues.

Unit-III -Cyber security for Blockchain: *Introduction, CIA Triad, AAA of Security, Non-repudiation, Risk Measurement, Blockchain Governance, Quantum Computing, Smart Contracts.*

Unit-IV-Solidity: Solidity Language Overview, Storage, Memory, and Call Data, Function Selectors, Interacting with EVM Smart Contracts, Compiling and Deploying Contracts

Smart Contract Security Issues: Security Hacks on Ethereum, Common Vulnerabilities and Attacks, Case Study: The DAO Hack, Case Study: The Poly-Network Hack.

Suggested Books:

1) Ashutosh Saxena “Blockchain Technology: Concepts and Applications”
2) Makoto Yano “Blockchain and Crypto Currency
3) Anand Shinde “Introduction to Cyber Security”

OE-CS CYS-404	Cryptographic Fundamentals						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
3	**0**	**0**	**3**	**75**	**25**	**100**	**3 Hours**
Purpose	To Understand various cryptographic algorithm, public-key cryptosystem, and fundamental ideas of public-key cryptography.						
Course Outcomes (CO)							
CO1	Student will be able to understand basic cryptographic algorithms.						
CO2	Able to understand the fundamental ideas of public-key cryptography.						
CO3	Analyze and compare symmetric-key encryption public-key encryption schemes based on different security models						
CO4	Able to understand the PKI infrastructure.						

Unit-I

Cryptography Concept: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks Historical Ciphers, Computational Security, Semantic Security, Pseudorandom Generators (PRGs) PRF, PRP and SPRP.

Unit-II

Symmetric key Ciphers: Block Cipher principles, Modes of Operations of Block Ciphers, DES, AES, Stream ciphers.

Cryptographic Hash Functions: MAC, Information-theoretic Secure MAC, Cryptographic Hash Functions, Birthday Attacks on Cryptographic Hash Functions, Applications of Hash Functions, Generic Constructions of Authenticated Encryption Schemes.

Unit-III

Asymmetric key Ciphers: Discrete-Logarithm Problem, Computational Diffie-Hellman Problem, Decisional Diffie Hellman Problem, Elliptic-Curve Based Cryptography and Public-Key Encryption, El Gamal Encryption Scheme, RSA Assumption, CCA -secure Public-key Hybrid Ciphers Based on Diffie-Hellman Problems and RSA-assumption, Digital Signatures.

Unit-IV

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure, overview of SSL/TLS.

Suggested Books:

1. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill,
3rd Edition. 2. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC
press, 2020.
3. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson
Education, 6th Edition

PE-CS-CYS-414A	**Penetration Testing**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hour**
Purpose	To enable students to learn various computational models, design paradigms of advanced computer architecture, parallelism approaches and techniques for static and dynamic interconnections.						
Course Outcomes (CO)							
CO1	Classify and interpret various paradigms, models and micro-architectural design of advanced computer architecture as well as identify the parallel processing types and levels for achieving optimum scheduling						
CO2	Identify the roles of VLIW & superscalar processors and branch handling techniques for performance improvement						
CO3	Analyze and interpret the basic usage of various MIMD architectures and relative importance of various types of static and dynamic connection networks for realizing efficient networks.						
CO4	Examine the various types of processors and memory hierarchy levels and cache coherence problem including software and hardware-based protocols to achieve better speed and uniformity.						

Unit I*- Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non-Disclosure Agreement Checklist, Phases of hacking, Open source/proprietary Pentest Methodologies. Pentest Scoping: The mindset of the professional Pen Tester, creating effective pen test scopes and rules of engagement.*

Unit -II-*Recon: Detailed Recon Using the Latest Tools, Mining Search Engine Results, google hacking database, shodan, Information gathering methodologies- Foot printing, Competitive Intelligence DNS Enumerations- Social Engineering attacks, Port Scanning- Network Scanning Vulnerability Scanning - NMAP scanning tool.*

Unit -III -*System Hacking: Password cracking techniques - Key loggers - Escalating privileges - Hiding Files, Steganography technologies and its Countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding. SQL Injection - Errorbased, Union-based, Time- based, Blind SQL, SQL Injection Prevention Techniques.*

Unit – IV-*wireless pentest: Wi-Fi Authentication Modes, Bypassing wlan, wep, wps Authentication practically,Attacks on the WLAN Infrastructure, Wi-Fi deauthentication attack, Wireless Hacking Methodology, Wireless Traffic Analysis, packet capturing, aircrack-ng, capturing the handshake, cracking the handshake, Wifi hacking prevention,Legal Documentation and Report Writing: legal documents you may encounter as a penetration tester, Statements of Work, Rules of Engagement, Non Disclosure Agreements, and Master Service Agreements.*

Suggested Books:

The hacker playbook:-Practical guide to penetration testing Author: Kim ISBN -10: 149-4932636/ISBN-13: 978-1494932633

PE-CS CYS-422A	Intrusion Detection and Prevention						
Lecture	**Tutorial**	**Practical**	**Credit**	**Major Test**	**Minor Test**	**Total**	**Time**
2	**0**	**0**	**2**	**75**	**25**	**100**	**3 Hours**
Purpose	To understand the intrusion detection and prevention technologies and various types of network behaviour analysis.						
Course Outcomes (CO)							
CO 1	To understand the intrusion detection and prevention technologies, various types of network behaviour analysis.						
CO 2	To understand the honeypots, multiple IDS methods, tools to analyse various types of attacks like wireless attacks and their detection.						
CO 3	To understand the attack source and provides practical knowledge for dealing with intrusions in real world applications.						

Unit-1

Introduction to IDPS: Introduction of Intrusion detection and Prevention Systems (IDPS), Components and Architecture Implementation, Uses of IDPS Technologies, Key Functions, Common Detection Methodologies-- Signature, Anomaly and Stateful Protocol Analysis, Types of IDPS Technologies.

Host and Network IDPS: Application, Transport, Network and Hardware Layer attacks, Sniffing Network Traffic, Replay Attacks, Command Injection, Internet Control Message Protocol Redirect, DDoS, Dangers and defences with Man-in the Middle, Secure Socket Layer attacks, DNS Spoofing, Defence- in-Depth Approach, Port Security, Use Encrypted Protocols.

Unit-2

Network Behaviour Analysis: Components and Architecture Typical, Network Architecture, Sensor Locations. **Honeypots:** Honeynets- Gen I, II and III, Detecting the Attack - Intrusion Detection, Network Traffic Capture, Monitoring on the box, Setting up the Realistic Environment, OpenCanary, Cowrie honeypots deployment.

Unit-3

Working with SNORT IDS: Introduction to Snort, Snort Alert Modes and Format, Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc, Plugins, Pre-processors and Output Modules, Using Snort with MySQL.

Multiple IDPS Technologies: Need for multiple IDPS Technologies, Integrating Different IDPS Technologies - Direct and Indirect, Firewalls, Routers and Honeypots, IPS using IP Trace back - Probabilistic and Deterministic Packet Marking, Marking.

Unit-4

Wireless IDPS: Exception WLAN Standards, WLAN Components, Threats against WLANs, 802.11 Wireless Infrastructure Attacks, WEP Attacks, Wireless Client Attacks, Bluetooth Attacks, Cell phones, Personal Digital Assistance and Other Hybrid Devices Attack Detection, Jailbreaking.

Suggested Books:

1. Shui Yu, Distributed Denial of Service Attack and Defense, Springer, 2014.
2. Bradd Lhotsky, OOSEC Host based Intrusion detection, PACKT Publication, 2013.
3. Sandeep Kumar Shukla, Manindra Agrawal, Cyber Security in India, Springer, 2020.

Note: The Examiner will be given the question paper template and will have to set the question paper according to the template provided along with the syllabus.

PC-CS **CYS-406LA**	**Cyber Security Block Chain Lab**						
Lecture	**Tutorial**	**Practical**	**Credit**	**Minor Test**	**Practical**	**Total**	**Time**
0	**0**	**2**	**1**	**40**	**60**	**100**	**3 Hrs.**
Purpose	To implement the concepts of Blockchain Network in Cyber security.						
Course Outcomes-Attend of the course students will be able to:							
CO1	Implement solidity programming language.						
CO2	Implement various process of blockchain network.						
CO3	Implement meta mask to execute the smart contract.						
CO4	Implement various type of smart contract and its deployment.						

1) Write a program in remix that calculate the prime number in solidity.

2) Write a program to implement various hash function used in cryptography Technique.

3) Deposit some Ether in your MetaMask accounts.

4) Create several accounts and make some transactions between these accounts on Rinkeby Network.

5) Test some properties of cryptographic hashing like small change in input results in big change in output.

6) Write a smart contract in remix that execute different data types in solidity.

7) Write a smart contract in remix that execute different Error handling functions in solidity.

8) Write a smart contract in remix that execute concept of inheritance in solidity.

9) Write a smart contract in remix that execute different loops in solidity.

10) Write a program in remix that execute different events in solidity.