

<b>Software Engineering &amp; Project Management</b>		Semester	V
Course Code	<b>BCS501</b>	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	4:0:0:0	SEE Marks	50
Total Hours of Pedagogy	52 hours	Total Marks	100
Credits	04	Exam Hours	03
Examination nature (SEE)	<b>Theory</b>		
<p><b>Course objectives:</b> This course will enable students to,</p> <ul style="list-style-type: none"> <li>• Outline software engineering principles and activities involved in building large software programs. Identify ethical and professional issues and explain why they are of concern to Software Engineers.</li> <li>• Describe the process of requirement gathering, requirement classification, requirement specification and requirements validation.</li> <li>• Recognize the importance of Project Management with its methods and methodologies.</li> <li>• Identify software quality parameters and quantify software using measurements and metrics. List software quality standards and outline the practices involved.</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b> These are sample Strategies; that teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Lecturer method (L) need not be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.</li> <li>2. Use of Video/Animation to explain functioning of various concepts.</li> <li>3. Encourage collaborative (Group Learning) Learning in the class.</li> <li>4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.</li> <li>5. Adopt Problem Based-Learning (PBL), which fosters student's Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.</li> </ol>			
<b>MODULE-1</b>		<b>10 hours</b>	
<p><b>Software and Software Engineering:</b> The nature of Software, The unique nature of WebApps, Software Engineering, The software Process, Software Engineering Practice, Software Myths. <b>Process Models:</b> A generic process model, Process assessment and improvement, Prescriptive process models: Waterfall model, Incremental process models, Evolutionary process models, Concurrent models, Specialized process models. Unified Process , Personal and Team process models</p> <p><b>Textbook 1: Chapter 1: 1.1 to 1.6, Chapter 2: 2.1 to 2.5</b></p>			
<b>MODULE-2</b>		<b>12 hours</b>	
<p><b>Understanding Requirements:</b> Requirements Engineering, Establishing the ground work, Eliciting Requirements, Developing use cases, Building the requirements model, Negotiating Requirements, Validating Requirements. <b>Requirements Modeling Scenarios, Information and Analysis classes:</b> Requirement Analysis, Scenario based modeling, UML models that supplement the Use Case, Data modeling Concepts, Class-Based Modeling. <b>Requirement Modeling Strategies :</b> Flow oriented Modeling , Behavioral Modeling. <b>Textbook 1: Chapter 5: 5.1 to 5.7, Chapter 6: 6.1 to 6.5, Chapter 7: 7.1 to 7.3</b></p>			
<b>MODULE-3</b>		<b>10 hours</b>	

**Agile Development:** What is Agility?, Agility and the cost of change. What is an agile Process?, Extreme Programming (XP), Other Agile Process Models, A tool set for Agile process .  
**Principles that guide practice:** Software Engineering Knowledge, Core principles, Principles that guide each framework activity.

**Textbook 1: Chapter 3: 3.1 to 3.6, Chapter 4: 4.1 to 4.3**

**MODULE-4**

**10 hours**

**Introduction to Project Management:** Introduction, Project and Importance of Project Management, Contract Management, Activities Covered by Software Project Management, Plans, Methods and Methodologies, Some ways of categorizing Software Projects, Stakeholders, Setting Objectives, Business Case, Project Success and Failure, Management and Management Control, Project Management life cycle, Traditional versus Modern Project Management Practices.

**Project Evaluation:** Evaluation of Individual projects, Cost-benefit Evaluation Techniques, Risk Evaluation

**Textbook 2: Chapter 1: 1.1 to 1.17 , Chapter 2: 2.4 to 2.6**

**MODULE-5**

**10 hours**

**Software Quality:** Introduction, The place of software quality in project planning, Importance of software quality, Defining software quality, Software quality models, product versus process quality management.

**Software Project Estimation:** Observations on Estimation, Decomposition Techniques, Empirical Estimation Models.

**Textbook 2: Chapter 13: 13.1 to 13.5, 13.7, 13.8, Text Book 1: Chapter 26: 26.5 to 26.7**

**Course Outcomes**

At the end of the course, the student will be able to:

- **Differentiate** process models to judge which process model has to be adopted for the given scenarios.
- **Derive** both functional and nonfunctional requirements from the case study.
- **Analyze** the importance of various software testing methods and agile methodology.
- **Illustrate** the role of project planning and quality management in software development.
- **Identify** appropriate techniques to enhance software quality.

**Assessment Details (both CIE and SEE)**

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

**Continuous Internal Evaluation:**

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at

the end of the semester if two assignments are planned.

- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

**The Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.**

**Semester-End Examination:**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**).

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.

Marks scored shall be proportionally reduced to 50 marks. .

**Suggested Learning Resources:**

**Textbooks**

1. Roger S. Pressman: Software Engineering-A Practitioners approach, 7th Edition, Tata McGraw Hill.
2. Bob Hughes, Mike Cotterell, Rajib Mall: Software Project Management, 6th Edition, McGraw Hill Education, 2018.

**Reference Book:**

3. Pankaj Jalote: An Integrated Approach to Software Engineering, Wiley India.
4. "Software Engineering: Principles and Practice", Hans van Vliet, Wiley India, 3rd Edition, 2010.

**Web links and Video Lectures (e-Resources):**

- [https://onlinecourses.nptel.ac.in/noc20\\_cs68/preview](https://onlinecourses.nptel.ac.in/noc20_cs68/preview)
- [https://onlinecourses.nptel.ac.in/noc24\\_mg01/preview](https://onlinecourses.nptel.ac.in/noc24_mg01/preview)

**Activity Based Learning (Suggested Activities in Class)/Practical-Based Learning**

- Demonstration of Agile tool: The students are expected to learn any of the popular agile tool. (10 marks)
- Field Survey (In Team): The students' team may of the size of 2 or 4. Students are expected to visit their library and understand the Library Automation Software. **OR** they have to understand the working of ERP or any inventory management, and then they have to prepare a report and then to be submitted to the concerned staff. Prepare a document/report which includes all the phases of SDLC and to be submitted accordingly (15 marks)

<b>COMPUTER NETWORKS</b>		Semester	V
Course Code	<b>BCS502</b>	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:2:0	SEE Marks	50
Total Hours of Pedagogy	40 hours Theory + 8-10 Lab slots	Total Marks	100
Credits	04	Exam Hours	03
Examination nature (SEE)	Theory/practical		
<p><b>Course objectives:</b> This course will enable students to,</p> <ul style="list-style-type: none"> <li>• Study the TCP/IP protocol suite, switching criteria and Medium Access Control protocols for reliable and noisy channels.</li> <li>• Learn network layer services and IP versions.</li> <li>• Discuss transport layer services and understand UDP and TCP protocols.</li> <li>• Demonstrate the working of different concepts of networking layers and protocols.</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b> These are sample Strategies; that teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Lecturer method (L) need not to be only traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.</li> <li>2. Use of Video/Animation to explain functioning of various concepts.</li> <li>3. Encourage collaborative (Group Learning) Learning in the class.</li> <li>4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.</li> <li>5. Adopt Problem Based Learning (PBL), which fosters student's Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.</li> </ol>			
<b>MODULE-1</b>			
<p>Introduction: Data Communications, Networks, Network Types, Networks Models: Protocol Layering, TCP/IP Protocol suite, The OSI model, Introduction to Physical Layer: Transmission media, Guided Media, Unguided Media: Wireless. Switching: Packet Switching and its types. <b>Textbook:</b> Ch. 1.1 - 1.3, 2.1 - 2.3, 7.1 – 7.3, 8.3.</p>			
<b>MODULE-2</b>			
<p>Data Link Layer: Error Detection and Correction: Introduction, Block Coding, Cyclic Codes. Data link control: DLC Services: Framing, Flow Control, Error Control, Connectionless and Connection Oriented, Data link layer protocols, High Level Data Link Control. Media Access Control: Random Access, Controlled Access. Check Sum and Point to Point Protocol <b>Textbook:</b> Ch. 10.1-10.4, 11.1 -11.4, 12.1 - 12.2</p>			
<b>MODULE-3</b>			
<p>Network Layer: Network layer Services, Packet Switching, IPv4 Address, IPv4 Datagram, IPv6 Datagram, Introduction to Routing Algorithms, Unicast Routing Protocols: DVR, LSR, PVR, Unicast Routing protocols: RIP, OSPF, BGP, Multicasting Routing-MOSPF <b>Textbook:</b> Ch. 18.1, 18.2, 18.4, 22.2,20.1-20.3, 21.3.2</p>			
<b>MODULE-4</b>			
<p>Introduction to Transport Layer: Introduction, Transport-Layer Protocols: Introduction, User Datagram Protocol, Transmission Control Protocol: services, features, segments, TCP connections, flow control, Error control, Congestion control. <b>Textbook:</b> Ch. 23.1- 23.2, 24.1-24.3.4, 24.3.6-24.3.9</p>			
<b>MODULE-5</b>			

Introduction to Application Layer: Introduction, Client-Server Programming, Standard Client-Server Protocols: World Wide Web and HTTP, FTP, Electronic Mail, Domain Name System (DNS), TELNET, Secure Shell (SSH)  
**Textbook:** Ch. 25.1-25.2, 26.1-26.6

### PRACTICAL COMPONENT OF IPCC

Sl.NO	Experiments
1	Implement three nodes point – to – point network with duplex links between them. Set the queue size, vary the bandwidth, and find the number of packets dropped.
2	Implement transmission of ping messages/trace route over a network topology consisting of 6 nodes and find the number of packets dropped due to congestion.
3	Implement an Ethernet LAN using n nodes and set multiple traffic nodes and plot congestion window for different source / destination.
4	Develop a program for error detecting code using CRC-CCITT (16- bits).
5	Develop a program to implement a sliding window protocol in the data link layer.
6	Develop a program to find the shortest path between vertices using the Bellman-Ford and path vector routing algorithm.
7	Using TCP/IP sockets, write a client – server program to make the client send the file name and to make the server send back the contents of the requested file if present.
8	Develop a program on a datagram socket for client/server to display the messages on client side, typed at the server side.
9	Develop a program for a simple RSA algorithm to encrypt and decrypt the data.
10	Develop a program for congestion control using a leaky bucket algorithm.

#### Course outcomes (Course Skill Set):

At the end of the course, the student will be able to:

- **Explain** the fundamentals of computer networks.
- **Apply** the concepts of computer networks to demonstrate the working of various layers and protocols in communication network.
- **Analyze** the principles of protocol layering in modern communication systems.
- **Demonstrate** various Routing protocols and their services using tools such as Cisco packet tracer.

**Note: For the Simulation experiments modify the topology and parameters set for the experiment and take multiple rounds of reading and analyze the results available in log files. Plot necessary graphs and conclude using NS2 or NS3. Installation procedure of the required software must be demonstrated, carried out in groups, and documented in the report. Non simulation programs can be implemented using Java.**

#### Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE

(Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

### **CIE for the theory component of the IPCC (maximum marks 50)**

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are **25 marks** and that for the practical component is **25 marks**.
- 25 marks for the theory component are split into **15 marks** for two Internal Assessment Tests (Two Tests, each of 15 Marks with 01-hour duration, are to be conducted) and **10 marks** for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.
- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for **25 marks**).
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC.

### **CIE for the practical component of the IPCC**

- **15 marks** for the conduction of the experiment and preparation of laboratory record, and **10 marks** for the test to be conducted after the completion of all the laboratory sessions.
- On completion of every experiment/program in the laboratory, the students shall be evaluated including viva-voce and marks shall be awarded on the same day.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to **15 marks**.
- The laboratory test (**duration 02/03 hours**) after completion of all the experiments shall be conducted for 50 marks and scaled down to **10 marks**.
- Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for **25 marks**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the practical component of the IPCC.

### **SEE for IPCC**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored by the student shall be proportionally scaled down to 50 Marks

**The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper may include questions from the practical component.**

### **Suggested Learning Resources:**

#### **Textbook:**

1. Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, Tata McGraw-

Hill,2013.

**Reference Books:**

1. Larry L. Peterson and Bruce S. Davie: Computer Networks – A Systems Approach, 4th Edition, Elsevier, 2019.
2. Nader F. Mir: Computer and Communication Networks, 2nd Edition, Pearson Education, 2015.
3. William Stallings, Data and Computer Communication 10th Edition, Pearson Education, Inc., 2014.

**Web links and Video Lectures (e-Resources):**

1. <https://www.digimat.in/nptel/courses/video/106105183/L01.html>
2. <http://www.digimat.in/nptel/courses/video/106105081/L25.html>
3. <https://nptel.ac.in/courses/10610>

**Activity Based Learning (Suggested Activities in Class)/ Practical Based learning**

- Implementation of various protocols using open source simulation tools. (5 marks)
- Simulation of Personal area network, Home area network, achieve QoS etc. (5 marks)

<b>THEORY OF COMPUTATION</b>		Semester	V
Course Code	<b>BCS503</b>	CIE Marks	50
Teaching Hours/Week (L: T:P: S)	(3:2:0:0)	SEE Marks	50
Total Hours of Pedagogy	50	Total Marks	100
Credits	04	Exam Hours	3
Examination type (SEE)	Theory		
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>● Introduce core concepts in Automata and Theory of Computation.</li> <li>● Identify different Formal Language Classes and their Relationships.</li> <li>● Learn concepts of Grammars and Recognizers for different formal languages.</li> <li>● Prove or disprove theorems in automata theory using their properties.</li> <li>● Determine the decidability and intractability of Computational problems.</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b>            These are sample Strategies which teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.</li> <li>2. Use of Video/Animation to explain functioning of various concepts.</li> <li>3. Encourage collaborative (Group Learning) Learning in the class.</li> <li>4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.</li> <li>5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyse information rather than simply recall it.</li> <li>6. Introduce Topics in manifold representations.</li> <li>7. Show the different ways to solve the same problem with different approaches and encourage the students to come up with their own creative ways to solve them.</li> <li>8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.</li> </ol>			
<b>Module-1</b>		<b>10 Hours</b>	
Introduction to Finite Automata, Structural Representations, Automata and Complexity. The Central Concepts of Automata Theory. Deterministic Finite Automata, Nondeterministic Finite Automata, An Application: Text Search, Finite Automata with Epsilon-Transitions. <b>TEXT BOOK: Sections 1.1, 1.5, 2.2,2.3,2.4,2.5</b>			
<b>Module-2</b>		<b>10 Hours</b>	
Regular Expressions, Finite Automata and Regular Expressions, Proving Languages not to be Regular. Closure Properties of Regular Languages, Equivalence and Minimization of Automata, Applications of Regular Expressions <b>TEXT BOOK: Sections 3.1, 3.2 (Except 3.2.1), 3.3, 4.1, 4.2, 4.4</b>			
<b>Module-3</b>		<b>10 Hours</b>	



Context-Free Grammars, Parse Trees, Ambiguity in Grammars and Languages, Ambiguity in Grammars and Languages, Definition of the Pushdown Automaton, The Languages of a PDA, Equivalence of PDA's and CFG's, Deterministic Pushdown Automata.  <b>TEXT BOOK: Sections 5.1, 5.2, 5.4, 6.1,6.2,6.3.1,6.4</b>
<b>Module-4</b> <span style="float: right;"><b>10 Hours</b></span>
Normal Forms for Context-Free Grammars, The Pumping Lemma for Context-Free Languages, Closure Properties of Context-Free Languages.  <b>TEXT BOOK: Sections 7.1, 7.2, 7.3</b>
<b>Module-5</b> <span style="float: right;"><b>10 Hours</b></span>
Introduction to Turing Machines: Problems That Computers Cannot Solve, The Turing Machine, Programming Techniques for Turing Machines, Extensions to the Basic Turing Machine, Undecidability: A Language That Is Not Recursively Enumerable. <b>TEXT BOOK: Sections 8.1,8.2, 8.3,8.4, 9.1, 9.2</b>
<b>Course outcome (Course Skill Set)</b> At the end of the course, the student will be able to: <ol style="list-style-type: none"> <li>1. Apply the fundamentals of automata theory to write DFA, NFA, Epsilon-NFA and conversion between them.</li> <li>2. Prove the properties of regular languages using regular expressions.</li> <li>3. Design context-free grammars (CFGs) and pushdown automata (PDAs) for formal languages.</li> <li>4. Design Turing machines to solve the computational problems.</li> <li>5. Explain the concepts of decidability and undecidability.</li> </ol>

**Assessment Details (both CIE and SEE)**

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

**Continuous Internal Evaluation:**

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 220B2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

**The Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.**

**Semester-End Examination:**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**).

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks.

**Suggested Learning Resources:****Books**

1. John E Hopcroft, Rajeev Motwani, Jeffrey D. Ullman," Introduction to Automata Theory, Languages and Computation", Second Edition, Pearson.

**Reference:**

1. Elaine Rich, "Automata, Computability and complexity", 1st Edition, Pearson Education, 2018.
2. K.L.P Mishra, N Chandrashekar, 3rd Edition, "Theory of Computer Science", PHI, 2012.
3. Peter Linz, "An introduction to Formal Languages and Automata", 3rd Edition, Narosa Publishers, 1998.
4. Michael Sipser : Introduction to the Theory of Computation, 3rd edition, Cengage learning, 2013.
5. John C Martin, Introduction to Languages and The Theory of Computation, 3rd Edition, Tata McGraw –Hill Publishing Company Limited, 2013.

**Web links and Video Lectures (e-Resources):**

- <https://archive.nptel.ac.in/courses/106/105/106105196/>
- <https://archive.nptel.ac.in/courses/106/106/106106049/>
- <https://nptelvideos.com/course.php?id=717>

**Activity Based Learning (Suggested Activities in Class)/ Practical Based Learning**

- Open source tools (like JFLAP) to make teaching and learning more interactive [<https://www.jflap.org/>] (10 Marks)
- Assignments at RBTL-4 (15 marks)

<b>Advanced Cyber Security Lab</b>		Semester	5
Course Code	<b>BCYL504</b>	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		
<b>Course objectives:</b>			
<ul style="list-style-type: none"> <li>● To learn concepts of web application pen testing</li> <li>● To identify and exploit vulnerabilities</li> <li>● To understand the OWASP top 10 vulnerabilities and other common web security threats</li> <li>● To learn concept of digital forensics</li> </ul>			
<b>Sl.NO</b>	<b>Experiments</b>		
1	<b>Password Cracking</b> Objective: To understand password vulnerabilities and the importance of strong passwords Tools: Hashcat, John the Ripper		
2	<b>Cross-Site Scripting (XSS)</b> Objective: To learn about XSS attacks and how to mitigate them Tools: DVWA		
3	<b>Insecure Direct Object References (IDOR)</b> Objective: To identify and exploit IDOR vulnerabilities Tools: Burp Suite, DVWA, custom web application		
4	<b>File Upload Vulnerabilities</b> Objective: To understand the risks associated with file uploads Tools: DVWA, Burp Suite, a vulnerable web application		
5	<b>Command Injection</b> Objective: To learn how command injection attacks work Tools: DVWA, Burp Suite, custom vulnerable web application		
6	<b>Man-in-the-Middle (MITM) Attack</b> Objective: To understand how MITM attacks intercept and manipulate network traffic. Tools: Ettercap, Wireshark		
7	<b>Privilege Escalation</b> Objective: To learn techniques to escalate privileges on a compromised system Tools: Metasploit, Linux/Windows VMs with known vulnerabilities		
8	<b>Buffer Overflow Exploitation</b> Objective: To understand how buffer overflow vulnerabilities can be exploited Tools: Immunity Debugger, Metasploit, vulnerable application (e.g., VulnServer)		
9	<b>XML External Entity (XXE) Injection</b> Objective: To learn about XXE vulnerabilities and how to exploit them Tools: Burp Suite, a vulnerable XML-based application		
10	<b>Session Hijacking and Fixation</b> Objective: To learn how session hijacking and fixation attacks work Tools: DVWA, Burp Suite, browser developer tools		
11	<b>Digital Forensics</b> Objective: To learn the basics of digital forensics and evidence collection Tools: Autopsy, FTK Imager		
12	<b>Acquisition of Mobile Data</b> Objective: To learn the methods for acquiring data from mobile devices		

Tools: ADB (Android Debug Bridge)

**Course outcomes (Course Skill Set):**

At the end of the course the student will be able to:

- Design the experiment for the given problem using cyber-security tools.
- Develop the solution for the given real world cyber-security problem.
- Analyze the results and produce substantial written documentation.

**Assessment Details (both CIE and SEE)**

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

**Continuous Internal Evaluation (CIE):**

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

### **Semester End Evaluation (SEE):**

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.
- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

### **Suggested Learning Resources:**

- <https://www.youtube.com/@CryptoCat>
- <http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf>
- <https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/>
- <https://blackhawkk.medium.com/cross-site-scripting-xss-dvwa-damn-vulnerable-web-applications-36808bff37b3>
- <https://medium.com/@eudorina67/dvwa-file-upload-vulnerabilities-40104b54d488>
- <https://www.youtube.com/@HackerSploit>
- <https://www.youtube.com/@NetworkChuck>
- <https://www.youtube.com/@davidbombal>
- Book: Web Penetration Testing with Kali Linux – Explore the Methods and Tools of Ethical Hacking with Kali Linux by Gilberto Najera-Gutierrez, Juned Ahmed Ansari – 2018, Third Edition, Packt Publishing  
[https://terrorgum.com/tfox/books/webpenetrationtestingwithkalilinux\\_ebook.pdf](https://terrorgum.com/tfox/books/webpenetrationtestingwithkalilinux_ebook.pdf)
- Book: Practical Web Penetration Testing – Secure Web Applications using Burp Suite, Nmap, Metasploit, and more by Gus Khawaja – 2018, Packt Publishing

<https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Practical%20Web%20Penetration%20Testing.pdf>

- Book: Ethical Hacking with Kali Linux – Learn Fast how to Hack like a Pro by Hugo Hoffman, 2020

<https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Ethical%20Hacking%20With%20Kali%20Linux%20Learn%20Fast%20How%20To%20Hack.pdf>

<b>Digital watermarking and Steganography</b>		Semester	5
Course Code	<b>BCY515A</b>	CIE Marks	50
Teaching Hours/Week (L: T:P: S)		SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	3
Examination type (SEE)	Theory/practical/Viva-Voce /Term-work/Others		
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>● To understand the basic principles, and characteristics of digital watermarking and steganography</li> <li>● To study and evaluate various approaches and applications of digital watermarking and steganography.</li> <li>● To apply digital watermarking techniques as an authentication tool for distribution of content over the Internet</li> <li>● To apply steganography techniques for covert communication.</li> <li>● To impart knowledge on the basics of the counter measures like steganalysis for assessing the data hiding methods.</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b> These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Chalk and board</li> <li>2. Presentation and Prezi</li> <li>3. Active Learning.</li> <li>4. Practical based learning</li> </ol>			
<b>Module-1: Introduction</b>			
Digital Watermarking, Digital Steganography, Differences between Watermarking and Steganography, Classification of Digital watermarking: Classification Based on Characteristics, Classification Based on Applications, Mathematical Preliminaries: Least-Significant-Bit Substitution, Discrete Fourier Transform . Discrete Cosine Transform			
<b>Module-2: Digital Watermarking Fundamentals.</b>			
Digital Watermarking Fundamentals : Spatial Domain Watermarking,, Frequency Domain Watermarking, Fragile Watermarks, Robust Watermarks Watermarking Attacks and Tools: Image-Processing Attacks, Geometric Attacks, Cryptographic Attacks, Protocol Attack, Watermarking Tools			
<b>Module-3: Watermarking Based on Genetic Algorithm and Reversible watermarking</b>			
Watermarking Based on Genetic Algorithms.: Introduction to Genetic Algorithms, Concept of GA-Based Watermarking, GA-Based Rounding Error Correction Watermarking, Applications to Medical Image Watermarking, Authentication of JPEG Images Based on Genetic Algorithms Reversible Image Authentication Scheme Based on Chaotic Fragile Watermark .			
<b>Module-4: Steganography - Introduction</b>			



Steganographic Communication, Information-Theoretic Foundations of Steganography, Information-Theoretic Foundations of Steganography, Minimizing the Embedding Impact, Types of Steganography, Applications of Steganography, Examples of Steganographic Software.
<b>Module-5: Steganalysis</b>
Steganalysis Scenarios- Detection, Forensic Steganalysis, The Influence of the Cover Work on Steganalysis . IQM-Based Steganalytic System, Frequency Domain Steganalytic System LSB Embedding and the Histogram Attack Sample Pairs Analysis . Blind Steganalysis of JPEG Images Using Calibration, Blind Steganalysis in the Spatial Domain
<p><b>Course outcome (Course Skill Set)</b></p> <p>At the end of the course, the student will be able to :</p> <ol style="list-style-type: none"> <li>1. Explain the fundamental concepts, principles, characteristics and performance measures of digital watermarking.</li> <li>2. Illustrate the concepts, types and attacks of digital watermarking.</li> <li>3. Describe various concepts of genetic algorithms on watermarking and explore the use of reversible watermarking.</li> <li>4. Identify the various concepts of steganography to access the sensitive information concealing of message, image, audio or video within another file.</li> <li>5. Design efficient data hiding methods against steganalysis techniques</li> </ol>
<p><b>Assessment Details (both CIE and SEE)</b></p> <p>The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.</p> <p><b>Continuous Internal Evaluation:</b></p> <ul style="list-style-type: none"> <li>• For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.</li> <li>• The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered</li> <li>• Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.</li> <li>• For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.</li> </ul> <p><b>Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.</b></p> <p><b>Semester-End Examination:</b></p> <p>Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (<b>duration 03 hours</b>).</p> <ol style="list-style-type: none"> <li>1. The question paper will have ten questions. Each question is set for 20 marks.</li> <li>2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), <b>should have a mix of topics</b> under that module.</li> <li>3. The students have to answer 5 full questions, selecting one full question from each module.</li> <li>4. Marks scored shall be proportionally reduced to 50 marks</li> </ol>

**Suggested Learning Resources:****Text books**

1. Frank Y. Shih, Digital Watermarking and Steganography Fundamentals and Techniques, 2020, 2nd Ed. CRC Press, United States. (ISBN No. : 9780367656430)
2. I. J. Cox, M. L. Miller, J. A. Bloom, T. Kalker, and J. Fridrich, Digital Watermarking and Steganography, 2008, 2nd Ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-12-372585-1 )

**Reference books**

1. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 2010, 1st Ed. Cambridge: Cambridge University Press, United Kingdom. (ISBN No.: 978-0-52-119019-0 )
2. P. Wayner, Disappearing Cryptography: Information hiding: Steganography and Watermarking, 2008, 3rd ed. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-08-092270-6 )

**Web links and Video Lectures (e-Resources):**

- <https://www.sciencedirect.com/topics/computer-science/digital-watermarking>
- [https://link.springer.com/chapter/10.1007/978-981-19-1412-6\\_39](https://link.springer.com/chapter/10.1007/978-981-19-1412-6_39)
- [https://www.researchgate.net/publication/264048994\\_A\\_Survey\\_of\\_Digital\\_Watermarking\\_Techniques\\_and\\_its\\_Applications](https://www.researchgate.net/publication/264048994_A_Survey_of_Digital_Watermarking_Techniques_and_its_Applications)
- [https://link.springer.com/chapter/10.1007/978-981-10-8536-9\\_32](https://link.springer.com/chapter/10.1007/978-981-10-8536-9_32)
- <https://youtu.be/8MW094OkSpU?feature=shared>
- <https://youtu.be/zQ15474JACs?feature=shared>

**Activity Based Learning (Suggested Activities in Class)/ Practical Based learning**

- Demonstration of tools of watermarking and steganography (10 Marks)
- Implementation of different algorithms in watermarking and steganography (15 Marks)

<b>INFORMATION RETRIEVAL</b>		Semester	V
Course Code	<b>BAI515B</b>	CIE Marks	50
Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	Theory		
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>● Understand the need of an information retrieval system.</li> <li>● Understand various retrieval models and the factors of evaluation.</li> <li>● Explore on text, query and indexed based processing for information retrieval.</li> <li>● Realize the importance of user interfaces for visualization and the web based search.</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b>  These are sample Strategies; which teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.</li> <li>2. Use of Video/Animation to explain functioning of various concepts.</li> <li>3. Encourage collaborative (Group Learning) Learning in the class.</li> <li>4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.</li> <li>5. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.</li> <li>6. Use any of these methods: Chalk and board, Active Learning, Case Studies.</li> </ol>			
<b>Module-1</b>			
<p><b>Introduction:</b> Information retrieval, IR problem, IR System, The web.  <b>User interfaces for search:</b> Introduction, How people search, Search interfaces today, Visualization on search interfaces, Design and evaluation of search interfaces.</p> <p>Textbook: Chapter 1: 1.1 to 1.4, Chapter 2: 2.1 to 2.5</p>			
<b>Module-2</b>			
<p><b>Modeling:</b> IR models, Classic information retrieval, Alternative set theoretic models, Alternative algebraic models, Alternative probabilistic models, Other models.</p> <p>Textbook: Chapter 3: 3.1 to 3.6</p>			
<b>Module-3</b>			
<p><b>Retrieval Evaluation:</b> Retrieval metrics, Reference Collections, User-based evaluation  <b>Relevance feedback and Query expansion:</b> A framework for feedback methods, Explicit relevance feedback, Explicit feedback through clicks, Implicit feedback through local analysis, Implicit feedback through global analysis  <b>Documents - Languages and Properties:</b> Metadata, Document formats, Text properties, Document preprocessing, Organizing documents, Text compression  Textbook : Chapter 4: 4.3 to 4.5, Chapter 5: 5.2 to 5.6, Chapter 6: 6.2 to 6.3, 6.5 to 6.8</p>			

<b>Module-4</b>
<p><b>Indexing and Searching:</b> Inverted indexes, Signature files, Suffix trees and suffix arrays, Sequential searching, Multi-dimensional indexing. Textbook: Chapter 9: 9.2 to 9.6</p>
<b>Module-5</b>
<p><b>Web retrieval:</b> The web, Search engine architectures, Search engine ranking, Managing web data, Search engine user interaction. <b>Structured Text Retrieval:</b> Structuring Power, Early text retrieval models, XML retrieval, XML retrieval evaluation. Textbook: Chapter 11: 11.2 to 11.7, Chapter 13: 13.2 to 13.5</p>
<p><b>Course outcome (Course Skill Set)</b></p> <p>At the end of the course, the student will be able to:</p> <ol style="list-style-type: none"> <li>1. Identify the models and the tools for building an Information Retrieval system.</li> <li>2. Apply query based operations for information retrieval.</li> <li>3. Use of text based operations for information retrieval from the documents.</li> <li>4. Apply indexing and searching techniques for information retrieval.</li> <li>5. Design user interface for search and retrieval of information from the web/documents.</li> </ol>
<p><b>Assessment Details (both CIE and SEE)</b></p> <p>The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.</p> <p><b>Continuous Internal Evaluation:</b></p> <ul style="list-style-type: none"> <li>● For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.</li> <li>● The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered</li> <li>● Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.</li> <li>● For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.</li> </ul> <p><b>Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.</b></p> <p><b>Semester-End Examination:</b></p> <p>Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (<b>duration 03 hours</b>).</p> <ol style="list-style-type: none"> <li>1. The question paper will have ten questions. Each question is set for 20 marks.</li> <li>2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), <b>should have a mix of topics</b> under that module.</li> <li>3. The students have to answer 5 full questions, selecting one full question from each module.</li> <li>4. Marks scored shall be proportionally reduced to 50 marks</li> </ol>

**Suggested Learning Resources:****Text Books:**

1. Ricardo BaezaYates and BerthierRibeiroNeto, Modern Information Retrieval, 2<sup>nd</sup> Edition, Pearson 2011

**Reference Books:**

1. Stefan Buettcher, Charles L. A. Clarke and Gordon V. Cormack, –Information Retrieval: Implementing and Evaluating Search Engines, The MIT Press, 2010.
2. Information Storage and Retrieval Systems: Theory and Implementation, Kowalski, Gerald, Mark T Maybury, Springer, 2<sup>nd</sup> Edition, 2002
3. Modern Information Retrieval, Ricardo Baeza-Yates, Pearson Education, 2007.

**Web links and Video Lectures (e-Resources):**

- <https://www.youtube.com/watch?v=cv7ztWiIaAM>
- <https://www.youtube.com/watch?v=ecRMy60oBrA>
- <https://www.youtube.com/watch?v=dXHxPvAlwcl>
- [https://www.youtube.com/playlist?list=PLpwnR8mPhhf8m7L\\_b9cSRLdjPW2soerAd](https://www.youtube.com/playlist?list=PLpwnR8mPhhf8m7L_b9cSRLdjPW2soerAd)
- <https://www.youtube.com/watch?v=m0oiAOGSQFw>
- <https://www.youtube.com/watch?v=yIuvahNq3wk>

**Activity Based Learning (Suggested Activities in Class)/ Practical Based learning**

- Design and development of Question-Answering System/Social media analytic etc... - 15 Marks
- Implementation of Web based/XML based retrieval applications - 10 Marks

<b>HACKER TECHNIQUES, TOOLS, AND INCIDENT HANDLING</b>		Semester	V
Course Code	<b>BCY515C</b>	CIE Marks	50
Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	Theory		
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>● To understand ethical hacking, penetration testing and physical security controls</li> <li>● To identify the various footprinting and port scanning tools and techniques</li> <li>● To study enumeration and wireless vulnerabilities exploited by hackers</li> <li>● To learn about common types of malware, Trojans, backdoors, spyware, ransomware and sniffers</li> <li>● To study various incident response and defensive technologies</li> </ul>			
<p><b>Teaching-Learning Process (General Instructions)</b></p> <p>These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.</p> <ol style="list-style-type: none"> <li>1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.</li> <li>2. Utilize video/animation films to illustrate the functioning of various concepts.</li> <li>3. Promote collaborative learning (Group Learning) in the class.</li> <li>4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.</li> <li>5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.</li> <li>6. Introduce topics through multiple representations.</li> <li>7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.</li> <li>8. Discuss the real-world applications of every concept to enhance students' comprehension.</li> <li>9. Use any of these methods: Chalk and board, Active Learning, Case Studies.</li> </ol>			
<b>Module-1</b>			
<p><b>Hacking: The Next Generation:</b> Profiles and Motives of Different Types of Hackers, History of Computer Hacking, Ethical Hacking and Penetration Testing, Common Hacking Methodologies, Performing a Penetration Test, The Role of the Law and Ethical Standards.</p> <p><b>Physical Security:</b> Basic Equipment Controls, Physical Area Controls, Facility Controls, Personal Safety Controls, Physical Access Controls, Avoiding Common Threats to Physical Security, Defense in Depth.</p> <p><b>Textbook: Chapter 1, Chapter 4</b></p>			

<b>Module-2</b>
<p><b>Footprinting Tools and Techniques:</b> The Information-Gathering Process, The Information on a Company Website, Discovering Financial Information, Google Hacking, Exploring Domain Information Leakage, Tracking an Organization's Employees, Exploiting Insecure Applications, Using Social Networks, Using Basic Countermeasures.</p> <p><b>Port Scanning:</b> Determining the Network Range, Identifying Active Machines, Mapping Open Ports, OS Fingerprinting, Mapping the Network, Analyzing the Results.</p> <p><b>Textbook: Chapter 5, Chapter 6</b></p>
<b>Module-3</b>
<p><b>Enumeration and Computer System Hacking:</b> Windows Basics, Commonly Attacked and Exploited Services, Enumeration, System Hacking, Types of Password Cracking, Using Password Cracking, Using PsTools, Rootkits, Covering Tracks.</p> <p><b>Wireless Vulnerabilities:</b> The Importance of Wireless Security, Working with and Securing Bluetooth, Working with Wireless LANs, Threats to Wireless LANs, Internet of Things (IoT), Wireless Hacking Tools, Protecting Wireless networks.</p> <p><b>Textbook: Chapter 7, Chapter 8</b></p>
<b>Module-4</b>
<p><b>Malware:</b> Malware, Viruses and How they Function, Worms and How they Function, Significance of Trojans, Detection of Trojans and Viruses, Trojan Tools, Distribution Methods, Trojan Construction Kits, Backdoors, Covert Communication, Spyware, Adware, Scareware, Ransomware.</p> <p><b>Sniffers, Session Hijacking, and Denial of Service Attacks:</b> Sniffers, Session Hijacking, Distributed Denial of Service (DDoS) Attacks, Botnets and the Internet of Things (IoT).</p> <p><b>Textbook: Chapter 10, Chapter 11</b></p>
<b>Module-5</b>
<p><b>Incident Response:</b> What is Security Incident? The Incident Response Process, Incident Response Plans, Planning for Disaster and Recovery, Evidence Handling and Administration, Requirements of Regulated Industries.</p> <p><b>Defensive Technologies:</b> Defense in Depth, Intrusion Detection Systems, The Purpose of Firewalls, Honeypots / Honeynets, The Role of Controls, Security Best Practices.</p> <p><b>Textbook: Chapter 14, Chapter 15</b></p>
<p><b>Course outcome (Course Skill Set)</b></p> <p>At the end of the course, the student will be able to:</p> <ol style="list-style-type: none"> <li>1. Explain hacking and penetration testing, including ethical and legal implications and identify basic equipment controls, physical area controls, and facility controls.</li> <li>2. Identify common information gathering tools and techniques and analyze how port scanning and fingerprinting are used by hackers.</li> </ol>

3. Analyze how enumeration is used in conjunction with system hacking and analyze wireless network vulnerabilities exploited by hackers.
4. Identify common types of malware, Trojans, backdoors, and covert communication methods.
5. Perform incident handling by using appropriate methods, compare and contrast defensive technologies.

### **Assessment Details (both CIE and SEE)**

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

### **Continuous Internal Evaluation:**

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

**Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.**

### **Semester-End Examination:**

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**).

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

### **Suggested Learning Resources:**

#### **Text Book:**

1. Sean-Philip Oriyano, Michael G Solomon "Hacker Techniques, Tools, and Incident Systems", Third Edition, Jones & Bartlett Learning, 2020.

#### **Reference Books:**

1. Abhinav Ojha, "Beginners Guide to Ethical Hacking and Cyber Security", Notion Press, 2020.
2. Hugo Hoffman, "Ethical Hacking with Kali Linux - Learn Fast how to Hack like a Pro", 2020.



<b>Web links and Video Lectures (e-Resources):</b>
<ul style="list-style-type: none"><li>• <a href="https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about">https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about</a></li><li>• <a href="https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks">https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks</a></li><li>• <a href="https://www.youtube.com/watch?v=mOOIv8-IuEo">https://www.youtube.com/watch?v=mOOIv8-IuEo</a></li><li>• <a href="https://www.youtube.com/watch?v=R0up9SZJqyQ">https://www.youtube.com/watch?v=R0up9SZJqyQ</a></li><li>• <a href="https://archive.nptel.ac.in/courses/106/105/106105217/">https://archive.nptel.ac.in/courses/106/105/106105217/</a></li></ul>
<b>Activity Based Learning (Suggested Activities in Class)/ Practical Based learning</b>
<ul style="list-style-type: none"><li>• Demonstration of concepts (Hacking techniques, Incident handling and others) with open source tools (Kali Linux, Nmap, Wireshark, Metasploit) etc. – (25 marks)</li></ul>