

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

COURSE MODULE OF THE SUBJECT TAUGHT FOR THE SESSION 2026-27 - (ODD SEM)

Faculty Name: Chetan G			Academic Year: 2026 - 2027				
Department: CSE-Cyber Security							
Course Code	Course Title	Core/Elective	Prerequisite	Contact Hours			Total Hrs/ Sessions
				L	T	P	
BCY702	ETHICAL HACKING	Core	Computer Fundamentals, Networking Basics, Linux Commands	3	0	2	40 hours Theory + 8-10 Lab slots
Course Learning Objectives: This course (BCO601) will enable students to:							
- Grasp the ethical implications, legal considerations and best practices associated with ethical hacking - Learn various methodologies for conducting penetration tests, including reconnaissance, enumeration and exploitations - Gain hands-on experience with industry-standard tools (e.g., Nmap, Metasploit, Burp Suite) and techniques for vulnerability assessment, network scanning and exploitation - Learn how to effectively document and present penetration testing results, including creating detailed reports and presentations that outline vulnerabilities, potential impacts etc.							
Module 1							Contact Hours
Introduction: Hacking Impacts, The Hacker The Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration. Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking. Textbook: Ch. 2, Ch. 3, Ch. 5.							08
Module 2							
The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges. Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement. Textbook: Ch. 6, Ch. 7.							08
Module 3							
Preparing for a Hack: Technical Preparation, Managing the Engagement. Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance. Textbook: Ch. 8, Ch. 9.							08
Module 4							
Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase. Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, Applications, Wardialing, Network, Services and Areas of Concern. Textbook: Ch. 10, Ch. 12.							08

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

Module 5	
The Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation. The Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy. Textbook: Ch. 13, Ch.14.	08
Textbook: 1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing” , Auerbach Publications, CRC Press.	
Reference Books: 1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases” , Cengage Learning. 2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.	
Course Outcomes: At the end of the course, the student will be able to: • Explain a comprehensive ethical hacking framework, integrating planning, reconnaissance, exploitation and risk analysis to identify vulnerabilities within information security systems. • Develop a strategic plan for a controlled ethical hacking engagement that aligns with business objectives and security policies, effectively navigating inherent and imposed limitations. • Model an ethical hacking engagement by effectively conducting reconnaissance through social engineering, physical security assessments and internet reconnaissance techniques. • Develop proficiency in employing enumeration techniques to gather critical information and prepare for exploitation, utilizing intuitive testing methods, evasion strategies and a variety of tools and applications. • Develop a comprehensive deliverable that effectively communicates the findings of an ethical hacking engagement, including documentation and structured reporting, while integrating results into actionable mitigation strategies.	
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.	

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

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.

The Correlation of Course Outcomes (CO's) and Program Outcomes (PO's)

Subject Name and Code:	Ethical Hacking-BCY702											
Faculty Name:	Chetan G											
List of Course Outcomes (RBT)	Program Outcomes											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	Total
CO-1(L3)	3	3		2	2	-	2	-	-	-	2	14
CO-2(L3)	2	3	3		2	-	3	-	-	-	2	15
CO-3(L3)	2	3	2	3	3	-	2	-	-	-	2	17
CO-4(L3)	2	3	2	3	3	-	3	-	-	-	2	18
CO-5(L3)	-	-	-	-	-	-	-	-	3	-	2	5
Total	9	12	7	8	10	-	10	-	3	-	10	69

Note: 3 = Strong Contribution, 2 = Average Contribution, 1 = Weak Contribution, - = No Contribution

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

The Correlation of Course Outcomes (CO's) and Program Specific Outcomes (PO's)

Subject Code:	BCY702	Ethical Hacking		Faculty Name:	Chetan G
List of Course Outcomes	Program Specific Outcomes			Total	
	PSO1	PSO2	PSO3		
CO-1	-	3	3	6	
CO-2	-	3	3	6	
CO-3	-	3	3	6	
CO-4	-	2	2	4	
CO-5	-	-	-	-	
Total	-	-	-	22	

Course Co-ordinator

HoD