

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

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

Faculty Name: Dr Pavithra M S			Academic Year: 2026 - 2027				
Department: CSE-Cyber Security							
Course Code	Course Title	Core/Elective	Prerequisite	Contact Hours			Total Hrs/ Sessions
				L	T	P	
BCY701	VULNERABILITY ASSESSMENT AND PENETRATION TESTING	Core	Computer Networks, Programming Basics, Security Fundamentals, Web Technologies Basics Linux Commands, Basic use of Virtual Machines	3	0	2	40 hours Theory + 10 Lab slots
Course Learning Objectives: This course (BCY701) will enable students to:							
- Introduce Vulnerability Assessment and Penetration Testing - To be familiar with the Penetration Testing and Tools - To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit - To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.							
Module 1							Contact Hours
Introduction to Ethics of Ethical Hacking: Why You Need to Understand Your Enemy’s Tactics, Recognizing the Gray Areas in Security, Vulnerability Assessment and Penetration Testing.							
Penetration Testing and Tools: Social Engineering Attacks: How a Social Engineering Attack Works, Conducting a Social Engineering Attack, Common Attacks Used in Penetration Testing, Preparing Yourself for Face-to-Face Attacks, Defending Against Social Engineering Attacks.							
Textbook: Ch. 1, Ch. 4.							
Module 2							
Physical Penetration Attacks: Need of Physical Penetration, Conducting a Physical Penetration, Common Ways into a Building, Defending Against Physical Penetrations.							
Insider Attacks: Conducting an Insider Attack, Defending Against Insider Attacks.							
Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit’s Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.							
Textbook: Ch. 5, Ch. 6, Ch. 8							
Module 3							

Managing a Penetration Test: Planning a Penetration Test, Structuring a Penetration Testing Agreement, Execution of a Penetration Test, Information Sharing During a Penetration Test, Reporting the Results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XP SP3, Vista 7 And Server 2008), Bypassing Windows Memory Protections. Textbook: Ch. 9, Ch. 11, Ch. 15.	
Module 4	
Web Application Security Vulnerabilities: Overview of Top Web Application Security Vulnerabilities, Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities, The Rest of the OWASP Top Ten, SQL Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities. Vulnerability Analysis: Passive Analysis: Source Code Analysis, Binary Analysis. Textbook: Ch. 17, Ch. 20.	
Module 5	
Client-Side Browser Exploits: Why Client-Side Vulnerabilities are Interesting, Internet Explorer Security Concepts, History of Client-Side Exploits and Latest Trends, Finding New Browser-Based Vulnerabilities, Heap Spray to Exploit, Protecting Yourself from Client-Side Exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware. Textbook: Ch. 23, Ch. 28.	

PRACTICAL COMPONENT OF IPCC

Sl.NO	Experiments
1	Monitoring Network Traffic Objective: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.
2	Host & Services Discovery using Nmap Objective: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.
3	Vulnerability Scanning using OpenVAS Objective: To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.

4	Internal Penetration Testing - Mapping - Scanning - Gaining Access through CVEs - Sniffing POP3/FTP/Telnet Passwords - ARP Poisoning - DNS Poisoning Objective: To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential security risks effectively.
5	External Penetration Testing - Evaluating External Infrastructure - Creating Topological Map & Identifying IP Address of Target - Lookup Domain Registry for IP Information - Examining Use of IPv6 at Remote Location Objective: To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defenses against external threats.
6	Different Types of Vulnerability Scanning Objective: To explore and compare various vulnerability scanning techniques and tools, assessing their effectiveness in identifying and prioritizing security risks.
7	Vulnerability Scanning with Nessus Objective: To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.
8	Web Application Assessment with Nikto & Burp Suite Objective: To evaluate web applications for security vulnerabilities using Nikto and Burp Suite, identifying issues such as misconfigurations and common vulnerabilities in web applications.

Course outcomes (Course Skill Set):

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

- Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
- Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes.
- Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections.
- Illustrate web application security vulnerabilities to conduct vulnerability analysis.
- Inspect protection against client-side browser exploits.

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.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

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

Subject Name and Code:	VULNERABILITY ASSESSMENT AND PENETRATION TESTING - BCY701											
Faculty Name:	Dr Pavithra M S											
List of Course Outcomes (RBT)	Program Outcomes											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	Total
CO-1(L3)	3	2	1	2	2	3	3	2	2	1	3	24
CO-2(L3)	2	3	2	3	3	2	2	3	2	2	2	26
CO-3(L3)	3	3	3	3	3	2	2	2	2	2	3	28
CO-4(L3)	2	3	3	3	3	2	2	2	2	1	2	25
CO-5(L3)	2	3	2	3	3	2	2	2	2	1	3	25
Total	12	14	11	14	14	11	11	11	10	07	13	128

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

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

Subject Code:	BCY701	VULNERABILITY ASSESSMENT AND PENETRATION TESTING		Faculty Name:	Dr Pavithra M S
List of Course Outcomes	Program Specific Outcomes			Total	
	PSO1	PSO2	PSO3		
CO-1	2	3	3	8	
CO-2	2	3	2	7	
CO-3	3	3	2	8	
CO-4	2	3	2	7	
CO-5	2	3	2	7	
Total	11	15	11	37	

Course Co-ordinator

HoD