

CCY4202 Ethical Hacking and Penetration Testing**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY3201	4	7	2	--	2	3

COURSE AIM

To get the students to:

- Understand and apply ethical theories to cybersecurity issues.
- Gain practical experience with penetration testing tools and techniques.
- Learn about common cyber attacks and corresponding defensive measures.
- Develop skills in secure coding to prevent vulnerabilities.
- Master methodologies for identifying, exploiting, and mitigating security flaws

COURSE WEEKLY CONTENTS

- 1 Introduction to Ethical Hacking and Penetration Testing
- 2 Overview of Cyber Attacks
- 3 Defensive Measures and Incident Response
- 4 Secure Coding Practices
- 5 Race Conditions and Format String Vulnerabilities
- 6 Vulnerability Discovery Techniques
- 7 7th week Assessment
- 8 Exploitation Techniques
- 9 Fuzzing Techniques
- 10 Penetration Testing Methodologies
- 11 Network Security Assessment
- 12 12th week Assessment
- 13 Operating System Security Assessment
- 14 Application Security Assessment
- 15 Project Presentations

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook Rafay Baloch, Ethical Hacking and Penetration Testing Guide, Auerbach Publications