INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

ETHICAL HACKING								
VII Semester: CSE | CSE (DS) | CSE(CS) | IT								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACSD53	Open Elective	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Basic understanding of operating systems, computer networks, and Network Security and Cryptography".								

I. COURSE OVERVIEW:

The Ethical Hacking course is designed to provide students with comprehensive knowledge and practical skills to identify, analyze, and mitigate security vulnerabilities in computer systems and networks. The course introduces the fundamental principles of cybersecurity, ethical hacking methodologies, and the legal and professional responsibilities of ethical hackers. Students will gain hands-on experience with tools and techniques used for reconnaissance, scanning, system hacking, malware analysis, and penetration testing. Emphasis is placed on understanding real-world attack scenarios, securing network infrastructure, and implementing effective defense strategies. By the end of the course, learners will be equipped to think like attackers to proactively protect information systems while adhering to ethical and legal standards.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The methodologies, frameworks, and best practices of ethical hacking for enhancing organizational and information security.
II. The impacts of hacking, various types of hackers, and key information security models.
III. The components of an information security program from a business perspective.
IV. The planning and execution of controlled attacks using a structured framework, including reconnaissance, enumeration, vulnerability analysis, exploitation, deliverables, and integration.

III. COURSE OUTCOMES:

CO1 Demonstrate knowledge of tools, techniques, and resources available to support ethical hacking activities.
CO2 Analyze and interpret the results of controlled attacks to assess system vulnerabilities effectively
CO3 Understand the influence of organizational politics, inherent and imposed limitations, and metrics in planning and executing penetration tests.
CO4 Apply structured frameworks for planning and executing penetration tests, including reconnaissance, enumeration, vulnerability analysis, exploitation, and reporting.
CO5 Evaluate the role of organizational policies, limitations, and metrics in planning and conducting ethical hacking exercises.
CO6 Recognize and mitigate the risks, ethical concerns, and legal implications associated with penetration testing.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION TO ETHICAL HACKING (10)

Introduction: Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration. Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

MODULE – II: THE BUSINESS PERSPECTIVE (10)

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

MODULE – III: PREPARING FOR HACK (09)

Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.

Rules of Engagement (scope, objectives, permissions, legal considerations), penetration testing planning and target prioritization, passive and active reconnaissance techniques, OSINT gathering, footprinting and target profiling, DNS and WHOIS analysis, network and service discovery.

MODULE – IV: ENUMERATION AND EXPLOITATION (09)

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

MODULE – V: DELIVERABLE (10)

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

V. TEXTBOOKS:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press.
2. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning.
3. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.

VI. REFERENCE BOOKS:

1. Dafydd Stuttard & Marcus Pinto. “The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, 2nd edition, 2011.
2. Christopher Hadnagy, “Social Engineering: The Science of Human Hacking”, 2nd edition, 2018.
3. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd edition, 2015.

VII. WEB REFERENCES

1. NPTEL – Introduction to Ethical Hacking – by IIT Kharagpur.
2. NPTEL – Cyber Security and Privacy – by IIT Madras.
3. Cybrary – Ethical Hacking Courses and Labs.
4. OWASP – Web Application Security Resources and Top 10.
5. PortSwigger – Web Security Academy (Free Hands-on Labs).

VIII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)