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

ETHICAL HACKING

IV Semester: CSE (CS)							
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**	
ACCD02	**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: Essentials of Cyber Security							

I. COURSE OVERVIEW:

This course combines an ethical hacking methodology to better help students secure their systems. Introduced to common countermeasures that effectively reduce and/or mitigate attacks. The concept of ethical hacking explained with their importance in protecting corporate and government data from cyber-attacks. Trusted text features new computer security resources, coverage of emerging vulnerabilities and innovative methods to protect networks, a new discussion of mobile security, and information on current federal and state computer crime laws, including penalties for illegal computer hacking are covered in this course. This course helps you gain the knowledge and skills to protect networks using the tools and techniques of an ethical hacker.

II. COURSE OBJECTIVES:
The students will try to learn:
I. The various information security tools given different target systems in different environments;
II. The tools interrelate with each other in an overall penetration testing process;
III. The common ethical hacking methodology to carry out a penetration test;
IV. The penetration testing and ethical hacking fit into a comprehensive enterprise information security program; Implement countermeasures for various types of attacks.

III. COURSE OUTCOMES:
After successful completion of the course, students should be able to:
CO 1   Explain the basic concepts on ethical hacking to overcome an unauthorized attempt and access to a computer system.
CO 2   Extend the password hacking techniques to identify viruses and worms-sniffers.
CO 3   Identify the foot printing concepts and techniques for Web Services and scanning networks.
CO 4   Examine the operating system vulnerabilities to access the devices and system.
CO 5   Illustrate the network protection systems for firewalls to detection and prevention of the systems.
CO 6   Classify the network scanning concepts to identify active hosts, ports and the services used by the target application.

IV. COURSE SYLLABUS:
MODULE – I: INTRODUCTION TO ETHICAL HACKING (09)
Introduction-Ethical hacking Terminology-types of hacking technologies-phases of ethical hacking-Foot Printing-Social Engineering-Scanning and enumeration

MODULE – II: HACKING TECHNIQUES (09)
Understanding the password hacking techniques-Rootkits-Trojans-Backdoors-Viruses and worms-sniffers- denial of service-Session hijacking, Foot printing and Reconnaissance, Scanning Networks – Enumeration.

MODULE – III: FOOT PRINTING AND SCANNING NETWORKS (10)
Foot printing Concepts – Foot printing through Search Engines and Social Engineering, Web Services.

Foot printing Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall.

MODULE – IV: OPERATING SYSTEM VULNERABILITIES (10)
Windows OS vulnerabilities-tools for identifying vulnerabilities in windows-Linux OS vulnerabilities-vulnerabilities of embedded OS.

MODULE – V: NETWORK PROTECTION SYSTEMS (10)
Understanding routers-understanding firewalls-risk analysis tools for firewalls- understanding intrusion and detection and prevention systems-honeypots.

V.TEXT BOOKS:
1. Michael T. Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense" 2016.
2. Steven DeFino, Barry Kaufman, Nick Valenteen, "Official Certified Ethical Hacker Review Guide", 2015.

VI.REFERENCE BOOKS:
1. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy(Syngress Basics Series).

VII.WEB REFERENCES:
1. https://www.nationalcyberwatch.org/resource/ethical-hacking-systems-defense-national-cyberwatch-center-edition/

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)