INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER SECURITY TECHNIQUES AND TOOLS								
VI Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCD11	**Elective**	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: There is no prerequisite to take this course								

I. COURSE OVERVIEW:

This course aims to provides a comprehensive introduction to cybersecurity, focusing on practical skills in ethical hacking and penetration testing. Students will learn techniques for password cracking, steganography, and anonymous browsing, as well as setting up virtual environments with tools like Kali Linux and VMware. It also covers essential topics such as Linux command line usage, managing network services, and exploiting vulnerabilities using the Metasploit framework. Additionally, it explores mobile security, including attack vectors and post-exploitation techniques. Through hands-on labs and real-world scenarios, students will develop the skills needed for ethical hacking and cybersecurity defense.

II. COURSE OBJECTIVES:

The students will try to learn:

I	The foundational knowledge of cybersecurity threats, hacking techniques, and methods of securing systems.
II	The practical skills for setting up virtual environments (using VMware) to simulate real-world penetration testing scenarios.
III	The metasploit frame work for hacking and assess the security in mobile devices

III. COURSE OUTCOMES:

CO1	**Acquire** the ability to apply various cybersecurity techniques and tools, such as password cracking, steganography, and anonymous browsing using TOR
CO2	**Gain** hands-on experience in installing and configuring virtual environments, including VMware, Kali Linux, and target VMs (Windows XP, Ubuntu, Windows 7).
CO3	**Develop** proficiency in the Kali Linux environment**,** including command-line operations, managing files and packages, handling user privileges, and executing network configurations.
CO4	**Make Use** the Metasploit Framework to identify vulnerabilities**,** configure and launch payloads, and exploit systems to enhance penetration testing capabilitie
CO5	**Identify and exploit** vulnerabilities in mobile devices**,** focusing on attack vectors, remote attacks, client-side attacks, and mobile post-exploitation.
CO6	**Develop** the ability to conduct ethical hacking activities using a wide range of tools and techniques across both desktop and mobile platforms.

IV. COURSE CONTENT:

MODULE–I: CYBER ISSUES (09)

Window Password Hacking and Cracking, Steganography, Hiding Secret Message, Anonymous Call, Message and Email Header Analysis, Access Darknet or Darkweb Using TOR: Anonymous Browsing, Access Darknet or Darkweb Using TOR: Anonymous Browsing

MODULE–II: VIRTUAL LAB SET UP (09)

Installing VMware, Setting Up Kali Linux - Target Virtual Machines, Creating the Windows XP Target, Setting Up the Ubuntu 8.10 Target - Creating the Windows 7 Target.

MODULE–III: ROUTING PROTOCOLS (10)

Linux Command Line, The Linux File system, User Privileges, File Permissions, Editing Files, Data Manipulation - Managing Installed Packages.

Processes and Services - Managing Networking- Netcat: The Swiss Army Knife of TCP/IP Connections- Automating Tasks with cron Jobs.

MODULE–IV: TRANSPORT LAYER PROTOCOLS (10)

Starting Metasploit, inding Metasploit Modules, Setting Module Options, Payloads, Types of Shells – Setting a Payload Manually, Msfcli, Creating Standalone Payloads with Msfvenom, Usingan Auxiliary Module.

MODULE-V: SENSOR NETWORK SECURITY (09)

Mobile Attack Vectors, The Smartphone Pentest Framework, Remote Attacks, Client, Side Attacks, Malicious Apps, Mobile Post Exploitation, Password Attacks: Password Management, Online Password Attacks, Offline Password Attacks.

V. TEXTBOOKS:

1. G. Kumawat, Ethical Hacking & Cyber Security Course: A Complete Package, Online Course, 1st Edition., Udemy, 2017.
2. G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 1st Edition, San Francisco, CA, USA: No Starch Press, 2014.

VI. REFERENCE BOOKS:

1. **G**. Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 1st Edition. San Francisco, CA, USA: No Starch Press, 2014.
2. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, “Security in Computing”, 5th Edition, Pearson Education, 2015.

VII. ELECTRONIC RESOURCES:

1. https://www.w3schools.com/cybersecurity/cybersecurity_web_applications_attacks.php
2. https://www.cybrary.it
3. https://www.kali.org/docs
4. https://www.offensive-security.com/metasploit-unleashed

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)