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

COURSE CONTENT

PENETRATION TESTING AND CYBER OPERATIONS								
VI Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCD10	CORE	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisite: Essentials of Cyber security								

I. COURSE OVERVIEW:
This course mainly focuses on port scanning and web application scanning. It also gives information about different attacks like password attacks and detection of vulnerabilities. This covers wireless security and penetration tools like Trace routes and Neo trace. Information about Database access and security at different levels is also defined.

II. COURSESOBJECTIVES:
The students will try to learn

I. The tools that can be used to perform information gathering.
II. The various attacks in various domains of cyberspace.
III. The various operating systems and wireless environment.
IV. The vulnerability assessment can be carried out by means of automatic tools or manual investigation.

III. COURSE OUTCOMES:
At the end of the course students should be able to:

CO1 Make use of different OSINT Tools, Techniques and Resources that return better results for different kind of queries.
CO2 Compare different port scanning techniques to find out which systems are active and which software is reliable
CO3 Demonstrate wide variety of methodologies and standards of penetration testing that the vulnerabilities were discovered
CO4 Illustrate the attacking networks that deploy various security protocols in Wireless Security.
CO5 Choose different techniques, protocols that can be used to perform the vulnerability analysis of web- based applications.
CO6 List the different types of factors, control measures, mechanisms that defend against database security Issues

IV.COURSE CONTENT:

MODULE I: INFORMATION GATHERING AND DETECTING VULNERABILITIES (10)
Open-source intelligence gathering – port scanning – Nessus policies – web application scanning manual analysis- traffic capturing.

MODULE II: ATTACKS AND EXPLOITS (10)
Password Attacks Client-side Exploitation Social Engineering – By passing Antivirus Applications. Metasploit Payloads Open php My Admin-Buffer overflow: Windows and Linux, Web scanning exploits, port scanning exploits, SQL exploits.

MODULE III: WIRELESS SECURITY (09)
Wired vs Wireless Privacy Protocols: Understand the differences in security requirements between wired and wireless networks, Study of WEP, WPA, WPA2, and WPA3 protocols. Wireless Frame Generation: the structure and types of IEEE 802.11 wireless frames and Data frames.

Encryption Cracking Tools: Tools used to assess and break wireless encryption, Air cracking, Reader, Kismet, Wireshark, and other tools, Understanding ethical hacking and penetration testing in wireless environments.

MODULE IV: COMMON VULNERABILITY ANALYSIS OF APPLICATION PROTOCOLS (10)
Simple Mail Transfer Protocol – File Transfer Protocol – Trivial File Transfer Protocol-Hyper Text Transmission Protocol- ICMP SMURF-UDP-DNS-PING-SYN.

MODULE V: PENETRATION TOOLS AND DATABASE SECURITY (09)
Trace routes, Neo trace, What web. Database Security: Access control in database systems – Inference control, Multilevel database security.

V. TEXT BOOKS:

1. Georgia Weidman, "Penetration Testing: A Hands on Introduction to Hacking", No Startch Press, 1st Edition, 2014.
2. B. Singh, H. Joseph and Abhishek Singh, "Vulnerability Analysis and Defense for the Internet", Springer, 1st Edition, 2008.

VI. REFERENCE BOOKS:

1. Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 1st Edition, 2015,
2. Dr.Patrick Engebretson, "The Basics of Hacking and Penetration Testing", Syngress Publications Elseveir, 1st Edition, 2013.
3. Prakhar Prasad, "Mastering Modern Web Penetration Testing", Packtet Publishing, 1st Edition, 2016.

VII. ELECTRONIC RESOURCES:

1. https://www.udemy.com/course/learn-website-hacking-penetration-testing-from-scratch/
2. https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/
3. https://www.eccouncil.org/train-certify/certified-penetration-testing-professional-cpent/

VIII. MATERIALS ONLINE

1. Course Template
2. Tutorial Question Bank
3. Tech talk Topics
4. Assignments
5. Definition and Terminology
6. Model Question Paper – I
7. Model Question Paper - II
8. Lecture Notes

9. Early Lecture Readiness Videos
10. Power point presentation