PENETRATION TESTING AND CYBER OPERATIONS

VI Semester: CSE (CS)

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
ACCC09	Core	3	0	0	3	30	70	100
Contact Classes:45	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 45		

Prerequisite: Foundations 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.COURSE OBJECTIVES:

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 vulnerabilities associated with various network applications and database system.

III.COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Make use of** different OSINT Tools, Techniques and Resources thatreturn better results for different kind of queries. .	Apply
CO 2	**Compare** different port scanning techniques to find out which systems are active and which software is reliable.	Understand
CO 3	**Demonstrate** wide variety of methodologies and standards of penetration testing that the vulnerabilities were discovered.	Understand
CO 4	**Illustrate** the attacking networks that deploy various security protocols in Wireless Security.	Understand
CO 5	**Choose** different techniques, protocols that can be used to performthe vulnerability analysis of web-based applications.	Apply
CO 6	**List** the different types of factors, control measures, mechanisms that defend against database security issues.	Remember

IV. SYLLABUS:

MODULE 1:INFORMATION GATHERING AND DETECTING VULNERABILITIES (09)

Open source intelligence gathering – port scanning – nessus policies – web application scanning manual analysis-traffic capturing.

MODULE 2:ATTACKS AND EXPLOITS (09)

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 3: WIRELESS SECURITY (09)

Wired vs wireless Privacy Protocols – Wireless Frame Generation Encryption Cracking Tools-Wireless DoS Attacks

MODULE 4:COMMON VULNERABILITY ANALYSIS OF APPLICATION PROTOCOLS (09)

Simple Mail Transfer Protocol – File Transfer Protocol – Trivial File Transfer Protocol-Hyper Text Transmission Protocol- ICMP SMURF-UDP-DNS-PING-SYN.

MODULE 5: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. GeorgiaWeidman, "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, 2008.

VI. REFERENCE BOOKS

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