COURSE CONTENT

PENETRATION TESTING AND CYBER OPERATIONS LABORATORY								
VI Semester: CSE(CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACCD18	**Core**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		0	0	2	1	40	60	100
Contact Classes: Nil	**Tutorial Classes: Nil**	**Practical Classes: 45**				**Total Classes: 45**		
Prerequisite: There are no prerequisites to take this course.								

I. COURSE OVERVIEW:

The purpose of this course is to provide a clear understanding of assessing an application or infrastructure for vulnerabilities in an attempt to exploit those vulnerabilities, and circumvent or defeat security features of system components through rigorous manual testing.

II. COURSES OBJECTIVES:

The students will try to learn

I. The usage of tools that can be used to perform information gathering.
II. The Various attacks in various domains of cyberspace.
III. How vulnerability assessment can be carried out by means of automatic tools or manual investigation.
IV. The vulnerabilities associated with various network applications and database system.

III. COURSE OUTCOMES:

At the end of the course students should be able to:

CO 1 Make use of Google and Whois tools to gather information about the target specification.
CO 2 Apply appropriate tools to perform encrypt and decrypt passwords in network.
CO 3 Make Use of vulnerability detection tools to identify vulnerabilities and monitor the networking mechanism.
CO 4 Compare different OSINT tools to gather detailed network information of the target.
CO 5 Make use of Virus Total tool to scan the network and detect malware on the network.
CO 6 Apply Ettercap tool to scan the network and performing an ARP poisoning attack.

IV. COURSE CONTENT:

Week – 1:
Make use of Google and who is tools to gather information about the target specification.

Week – 2:
Apply Crypt tool to perform encryption and decryption of the data with algorithms.

Week – 3:
Make use of Password cracking tools and techniques to crack the passwords on wireless network.

Week – 4:
Make use of Nmap tool to find the vulnerabilities of the target system on network.

Week – 5:
Make use of Wayback Machine Tool to save the digital history of the target on network.

Week – 6:
Install and use Nessus tool to perform web application Scanning on network.

Week – 7:
Install Acunetix tool to understand and perform scanning for variety of vulnerabilities in web Application.

Week – 8:
Perform ARP Poisoning with Ettercap Tool with Two machines on Network.

Week – 9:
Install Burp suite tool perform security testing of Web applications on network.

Week – 10:
Install OWASP ZAP tool to perform web application testing and launching attacks on target machine.

Week – 11:
Install Metasploit framework to perform various exploitation tasks about the security vulnerabilities of target machine.

Week – 12:
Make use of Virus total tool for Analyze suspicious files on URL of the target.

Week – 13:
Post-Exploitation and Lateral Movement.

Week – 14:
Exploiting Web Application Vulnerabilities using Nmap tool.

V. TEXT BOOKS:

1. Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Wiley, 2nd Edition, 2011.
2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, "Metasploit: The Penetration Tester's Guide", No Starch Press, 1st Edition, 2011.

VI. REFERENCE BOOKS:

1. Jon Erickson, "Hacking: The Art of Exploitation", No Starch Press, 2nd Edition, 2008.
2. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson, 7th Edition, 2016.
3. Gordon Fyodor Lyon, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning", Insecure.Com LLC, 1st Edition, 2009.
4. Chris McNab, "Network Security Assessment: Know Your Network", O'Reilly Media, 3rd Edition, 2016.
5. Michael Sikorski, Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", No Starch Press, 1st Edition, 2012.

VII. ELECTRONICS RESOURCES:

1. https://www.virtualhackinglabs.com/labs/penetration-testing-lab
2. https://en.wikipedia.org/wiki/SANS_Institute
3. https://www.virtualhackinglabs.com/labs/penetration-testing-lab/
4. https://pentestlab.blog/
5. https://pentesterlabs.in/

VIII. MATERIALS ONLINE:

1. Course Outline Description
2. Lab Manual