BCSE319L	PENETRATION TESTING AND VULNERABILITY ANALYSIS	L	T	P	C
		2	0	0	2
Pre-requisite	**NIL**	**Syllabus version**			
		1.0			

Course Objectives

1. To understand the system security-related incidents and insight on potential defenses, countermeasures against common vulnerabilities.
2. To provide the knowledge of installation, configuration, and troubleshooting of information security devices.
3. To make students familiarize themselves with the tools and common processes in information security audits and analysis of compromised systems.

Course Outcome

After completion of this course, the student shall be able to:

1. Familiarized with the basic principles for Information Gathering and Detecting Vulnerabilities in the system.
2. Gain knowledge about the various attacks caused in an application.
3. Acquire knowledge about the tools used for penetration testing.
4. Learn the knowledge into practice for testing the vulnerabilities and identifying threats.
5. Determine the security threats and vulnerabilities in computer networks using penetration testing techniques.

Module:1	**Pentesting Fundamentals**	**5 hours**
Vulnerability Assessment (VA)- Pentesting Analysis (PTA) **-T**ypes of Vulnerability Assessments-Modern Vulnerability Management Program-Ethical Hacking terminology- Five stages of hacking- Vulnerability Research - Impact of hacking - Legal implication of hacking - Compare Vulnerability Assessment (VA) and Penetration Testing (PT) Tools.		
Module:2	**Information Gathering Methodologies**	**5 hours**
Competitive Intelligence- DNS Enumerations- Social Engineering attacks - Scanning and Enumeration. Port Scanning: Network Scanning, Vulnerability Scanning, scanning tools- OS and Fingerprinting Enumeration - System Hacking Password.		
Module:3	**System Hacking**	**3 hours**
Password cracking techniques- Key loggers- Escalating privileges- Hiding Files, Active and Passive sniffing - ARP Poisoning - IP Poisoning and MAC Flooding.		
Module:4	**Wireless Pentesting**	**4 hours**
Wi-Fi Authentication Modes - Bypassing WLAN Authentication - Types of Wireless Encryption - WLAN Encryption Flaws – Access Point Attacks - Attacks on the WLAN Infrastructure - Buffer Overloading.		
Module:5	**The Metasploit Framework**	**3 hours**
Metasploit User Interfaces and Setup - Getting Familiar with MSF Syntax - Database Access - Auxiliary Modules- Payloads - Staged vs Non-Staged Payloads - Meterpreter Payloads - Experimenting with Meterpreter.		
Module:6	**Web Application Attacks**	**4 hours**
Web Application Assessment Methodology – Enumeration - Inspecting URLs - Inspecting Page Content - Viewing Response Headers - Inspecting Sitemaps - Locating Administration Consoles.		
Module:7	**Exploiting Web-Based Vulnerabilities**	**4 hours**
Exploiting Admin Consoles - Cross-Site Scripting (XSS) - SQL Injection.		
Module:8	**Contemporary Issues**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)			
1.	Najera-Gutierrez G, Ansari JA. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux., 2018, 3rd Edition, Packt Publishing Ltd, United Kingdom.		
2.	Hadnagy C. Social engineering: The science of human hacking, 2018, 2nd Edition, John Wiley & Sons, United States.		
Reference Books			
1.	Weidman G. Penetration testing: a hands-on introduction to hacking,2014, 1st Edition, No Starch Press, United States		
2.	Engebretson P. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy, 2013, 2nd Edition, Elsevier.		
Mode of Evaluation: CAT / written assignment / Quiz / FAT			
Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No.65	Date	17-03-2022