SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B.Tech III (Semester V)

Subject Name: Ethical Hacking and Penetration Testing **Subject Code:** BTEA19523
Type of course: Honors
Prerequisite: Computer Network, Database Management System, Operating System

Rationale: The security of digital infrastructure is an utmost need for an organization. The variety of security attacks makes it compulsion to analyze the way newer attacks are formed and their understanding is important to prevent or detect such attacks. The ethical hacking and penetration testing covers the theory and practices of finding the vulnerabilities through forming the different attacks and then defining the appropriate security policy including the action to detect or prevent the attacks and thus reduce the damages.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
4	0	2	5	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No	Contents	Total Hours
1.	**An Introduction to ethical Hacking:** Introduction to ethical hacking. Overview of TCP/IP protocol stack. Security Fundamental, Security testing, Hacker and Cracker, Descriptions, Test Plans-keeping It legal, Ethical and Legality	05
2.	**The Technical Foundations of Hacking:** The Attacker's Process, The Ethical Hacker's Process, Security, and the Stack	05

3.	**Foot printing and scanning:** Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface	07
4.	**Enumeration, System Hacking and Malware Threats:** Enumeration, System Hacking, Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Countermeasures	07
5.	**Sniffers, Session Hijacking and Denial of Service:** Sniffers, Session Hijacking, Denial of Service and Distributed Denial of Service	07
6.	**Web Server Hacking, Web Applications and Database Attacks:** Web Server Hacking, Web Application Hacking, Database Hacking	07
7.	**Wireless Technologies, Mobile Security and Attacks:** Wireless Technologies, Mobile Device Operation and Security, Wireless LANs	07
8.	**IDS, Firewalls and Honeypots:** Intrusion Detection Systems, Firewalls, Honeypots	05
9.	**Penetration Testing:** Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap, mapping, discovery, and exploitation	10

Suggested Specification table with Marks (Theory): (For B.Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
10	20	20	05	05	0

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

Sr. No	Title of Book /Article	Author(s)	Publisher and details like ISBN	Year of Publication	Publication Edition
1	Certified Ethical Hacker	Michael Gregg	Pearson IT Certification	August 2011	1st Edition
2	Hacking the Hacker	Roger Grimes	Wiley	July 2017	2nd Edition
3	The Unofficial Guide to Ethical Hacking	Ankit Fadia	Premier Press	January 2006	2nd Edition
4	The Basics of Hacking and Penetration Testing	Patrick Engebretson	Syngress	2013	2nd Edition

Course Outcomes (CO):

Sr. No	CO statements	Marks % weightage
CO-1	Understand the basics of ethical hacking.	15%
CO-2	Perform the foot printing and scanning.	15%
CO-3	Demonstrate the techniques for system hacking.	20%
CO-4	Characterize the malware and their attacks and detect and prevent them.	20%
CO-5	Perform security audit using penetration testing.	30%

List of Open learning website:

1. https://hackaday.com/
2. https://breakthesecurity.cysecurity.org/
3. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
4. https://www.hackthissite.org/

List of Open-Source Software:

- NMAP
- Metasploit
- Burp Suite
- Ettercap

List of Experiments:

Sr. No	Practical
1.	List the tools for Ethical Hacking.
2.	Implement Footprinting and Reconnaissance using tools 3d Traceroute, Alchemy Eye, DNS Tools and Network Solution Whois.
3.	Implement Network Scanning using tools Advanced Port Scanner, Colasoft Ping Tool, Hide Your IP Address, Nessus and Nmap.
4.	Implement Enumeration using tools Default Password List, Default Password List, OpUtil Network Monitoring Tool and OpUtil Network Monitoring Tool.
5.	Implement system hacking using tools Actual spy, Alchemy Remote Executor, Armor Tool and F-Secure BlackLight.
6.	Implement Trojan and Backdoors using tools Absolute Startup Manager, Absolute Startup Manager, Netwirx Services Monitor and StartEd Lite.
7.	Implement Viruses and Worms using tools Anubis Analyzing UnknownBinaries, Filterbit, Sunbelt CWSandbox and ThreatExpert.
8.	Implement sniffers using tools Colasoft Capsa Network Analyzer, EffeTech HTTP Sniffer, Packet Sniffer and PRTG Network Monitor.
9.	Write a research paper in which Ethical Hacking tools are used to address any problem definition in cyber security.