SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

B. Tech. Semester V

Subject Name: **Cyber Security and Ethical Hacking** **Subject Code: BTEC14505**
Type of course: PEC
Prerequisite: Computer Networking and Operating System
Rationale: The cyber security and ethical hacking covers 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	150
3	0	2	4	60	25	15	30	20	

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.	Topics	Teaching Hrs.	Module % Weightage
1.	**Systems Vulnerability Scanning:** Introduction to computer network, Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet.	9	20
2.	**Network Defense Tools:** Network Defense tools Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Introduction Detection System	6	15
3.	**Web Application Tools:** Web Application Tools Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap.	6	15

	DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra.		
4.	**Introduction to Ethical Hacking:** Introduction to ethical hacking. Overview of TCP/IP protocol stacks. Security Fundamental, Security testing, Hacker and Cracker, Test Plans-keeping It legal, Ethical and Legality.	4	10
5.	**The Technical Foundations of Hacking:** The Attacker's Process, The Ethical Hacker's Process, Security and the Stack.	5	10
6.	**Footprinting and scanning for Hacking:** Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface.	5	10
7.	**Hacking and Malware Threats:** Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Countermeasures.	5	10
8.	**Sniffers, Session Hijacking and Denial of Service:** Sniffers, Session Hijacking, Denial of Service and Distributed Denial of Service.	5	10

Suggested Specification table with Marks (Theory/Practical):

% Distribution of Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
30	10	30	20	0	0

Legends: R: Remembrance, **U:** Understanding; **A:** Application, **N:** Analyze, **E:** Evaluate **C:** Create and above Levels **(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 Text Books:

Sr. No.	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1.	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole	Publication Wiley	2011	Latest
2.	Cyber Security and Cyber Law	Alfred Basta, Nadine Basta	publication Cengage	2018	Latest

3.	Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity	Erdal Ozkaya,	Publication Packt	2019	Latest
4.	Certified Ethical Hacker	Michael Gregg	Pearson IT	2011	2nd
5.	Hacking the Hacker	Roger Grimes	Wiley	2017	1st

Course Outcome:

Sr. No.	CO Statement After learning this subject students will be able to,	Marks % weightage
CO-1	Define key concepts and terminology in cyber security.	20
CO-2	Explain various vulnerabilities and cyber-attacks.	20
CO-3	Explain various defense tools to avoid cyber-attacks.	20
CO-4	Differentiate Hacking and Ethical Hacking and identify means used to hack a system.	20
CO-5	List different malwares used in hacking and consequences of such malwares.	10
CO-6	Apply knowledge of this course to protect themselves and society against Cyber Attacks.	10

Mapping with POs:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO-1	3	-	1	-	2	2	2	2	2	-	-	2	-	-	2
CO-2	2	-	2	1	2	2	2	2	2	2	-	2	-	-	2
CO-3	2	-	1	1	3	2	2	2	2	2	-	3	-	-	2
CO-4	2	3	1	2	3	2	2	3	2	-	2	2	-	-	-
CO-5	2	2	2	2	2	1	2	1	2	2	-	3	-	-	-
CO-6	3	2	3	2	3	2	3	3	2	2	-	3	-	-	2

List of practical:

1. Study of basic Unix commands.
2. TCP/UDP connectivity using Netcat.
3. Perform Scan using Nmap.
4. Perform Scan using Zenmap.

5	Perform Network Scan using Wireshark.
6	To study SQLMAP
7	To Study DVWA for Web App Testing and manual SQL Injections.
8	To study XSS using DVWA.
9	Examine software keyloggers and hardware keyloggers.
10	Evaluate network defense tools for following (i) IP spoofing (ii) DOS attack
11	Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber-attack/vulnerability.
12	Perform online attacks and offline attacks of password cracking.

Major Equipment:

- Computer System

List of Open Source/learning websites:

- https://onlinecourses.swayam2.ac.in/nou19_cs08/preview
- https://www.coursera.org/specializations/intro-cyber-security
- www.wireshark.org

List of Open Source software:

- Nmap
- Zenmap
- SQLMap
- DVWA
- Kali Linux