SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech II (Semester IV)

Subject Name: Fundamentals of Cyber Security **Subject Code:** BTEA19423
Type of course: Honors (Group: Cyber Security)
Prerequisite: -

Rationale: Cyber Security course aims to equip students with the knowledge and skills required to defend computer operating systems, networks and data from cyber-attacks. Cyber Security as a profession is evolving over the years, reason being the increasing rate of cyber-crimes.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	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.	**Fundamentals of cyber-crimes and security** Overview, what is Cybercrime? Computer Intrusions and Attacks (Unauthorized Access) Computer Viruses, Time Bombs, Trojans, Malicious Code (Malware), Online Fraud and Identity Theft; Intellectual Property Theft; Virtual Crime, Online Vices, International Aspects and Jurisdiction	07
2.	**Systems Vulnerability Scanning** Introduction to computer networks, 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	12
3.	**Network Defense tools**	08

	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	
4.	**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. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	08
5.	**Cyber Crime and Cyber law** Introduction to Cyber Crime and law Cyber Crimes, Types of Cyber Crime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data, Indian IT ACT 2000	05
6.	**Cyber Crime Investigation** Introduction to Cyber Crime Investigation, Keyloggers and Spyware, Virus and Worms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless networks	05

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**
20	25	10	05	00	00

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	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole and Sunit Belpure	Wiley	2011	1st Edition
2	Cyber Security and Cyber Laws	Alfred Basta, Nadine Basta , Mary Brown, Ravinder Kumar	Cengage	2018	1st Edition
3	Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity	Erdal Ozkaya	Packt	2019	1st Edition
4	Anti-Hacker Tool Kit	Mike Shema	McGraw Hill	2014	4th Edition

Course Outcomes (CO):

Sr. No.	CO Statements	Marks % weightag
CO-1	Explain key concepts and terminology in cyber security.	30
CO-2	Describe various vulnerabilities and cyber-attacks.	25
CO-3	Differentiate between types of cyber-crimes.	25
CO-4	Analyze everyday cyber frauds and take precautions to remain safe.	10
CO-5	Utilize knowledge of this course to protect themselves and society against Cyber Attacks.	10

List of Open learning website:

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

List of Open-Source Software:

- Nmap
- Zenmap
- SQLMap
- DVWA

List of Experiments:

Sr. No	Practical
1.	Hands-on basic Unix commands.
2.	Illustrate TCP/UDP connectivity using Netcat.
3.	Perform Scan using Nmap.
4.	Perform Scan using Zenmap.
5.	Perform Network Scan using Wireshark.
6.	Demonstrate SQLMAP
7.	Working DVWA for Web App Testing and manual SQL Injections.
8.	Perform XSS using DVWA.
9.	Analyze software keyloggers and hardware keyloggers.
10.	Evaluate network defence 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.