

**SES's L.S. RAHEJA COLLEGE OF ARTS AND COMMERCE
(AUTONOMOUS)**



BOARD OF STUDIES: Information Technology and Data Science

Programme: B.Sc. (Cyber Security & Digital Forensics)

Semester: I

Nomenclature of the Course: Introduction to Cyber Security Tools

NEP Vertical: SEC

Credit: 02

Total Marks: 50

Academic Year: 2026–27

(As per Choice Based Credit System under NEP 2020)



Unit-wise Detailed Syllabus

Unit	Detailed Contents	Andragogy	Hours
Unit I: Fundamentals of Cyber Security Tools	1. Introduction to Cyber Security Tools 2. Categories of Security Tools – Network, Web, System 3. Overview of Kali Linux Environment 4. Basics of Network Scanning Concepts 5. Introduction to Vulnerability Assessment 6. Ethical Usage of Security Tools	Concept explanation with tool demonstrations. Hands-on Activities: • Installation of Kali Linux (Virtual Machine Demonstration) • Basic Linux terminal commands • Introduction to Nmap interface and basic scan • Understanding scan results	15
Unit II: Basic Tool Exposure & Analysis	1. Nmap – Network Scanning (Basic Commands) 2. Wireshark – Packet Capture Basics 3. Introduction to Burp Suite (Overview) 4. Basic Log File Analysis 5. Antivirus & Malware Detection Tools 6. Report Generation Basics	Guided lab-based sessions. Hands-on Activities: • Perform basic network scan • Capture simple HTTP packet using Wireshark • Analyze captured packets • Perform simple log file analysis • Prepare basic scan report	15

Learning Objectives

1. To understand different types of cyber security tools.
2. To learn basic network scanning techniques.
3. To analyze simple packet captures.
4. To develop ethical understanding of tool usage.

Course Outcomes (CO)

CO No.	Course Outcome	Bloom's Level
CO1	Explain categories of cyber security tools	Understand (L2)
CO2	Perform basic network scanning using security tools	Apply (L3)
CO3	Analyze captured network packets	Analyze (L4)
CO4	Demonstrate ethical and responsible use of security tools	Apply (L3), Analyze (L4)

Suggested Readings

Sr. No.	Title	Author / Source
1	Kali Linux Revealed	Offensive Security
2	Nmap Network Scanning	Gordon Lyon
3	Wireshark Network Analysis	Laura Chappell
4	Cybersecurity Essentials	Charles J. Brooks

QUESTION PAPER PATTERN

(A) Continuous Evaluation – 20 Marks

Particulars	Marks
Class Test	10
Tool-based Assignment / Activity Journal	10
Total	20

(B) Semester End Examination – 30 Marks

Duration: 1 Hour

Question No.	Description	Total Marks
Q1	Attempt Unit I	15
	A – Remembering	
	B – Analysing	
	C – Applying	
OR		
	P – Remembering	15
	Q – Analysing	
	R – Applying	
Q2	Attempt Unit II	15
	A – Remembering	
	B – Analysing	
	C – Applying	
OR		
	P – Remembering	15
	Q – Analysing	
	R – Applying	