The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science & Commerce, Pune. (Autonomous)

Faculty of Science and Technology

Four Year Degree Program

B.Sc. (Cyber Security) Program

With

Major- Cyber Security

Syllabus For

S.Y. B.Sc. (Cyber Security)

Choice Based Credit System (CBCS)
Syllabus Under National Education Policy (NEP) 2020
with effect from Academic Year 2026-27

B. Sc. (Cyber Security)

1. **Name of Program: Cyber Security**

2. **Introduction:**

In today's interconnected world, the proliferation of digital technologies has brought about unprecedented convenience and efficiency. However, this digital transformation has also led to an increase in cyber threats, making cyber security an essential field. Cyber-attacks can cause significant harm to individuals, businesses, and national security. As a result, there is a growing demand for skilled cyber security professionals who can protect sensitive information and critical infrastructure.

The B.Sc. in Cyber Security program is designed to address this demand by providing students with a comprehensive education in the field. Aligned with the National Education Policy (NEP) 2020, this program emphasizes a holistic, flexible, and multidisciplinary approach to education, preparing students for the complexities of the cyber security landscape.

The B.Sc. (Cyber Security) program is for three years duration with six semesters and B.Sc. (Cyber Security) Honors and Research programs are for **four years** duration with eight semesters. It is a full-time degree program. The program will be based on the Choice-Based Credit System comprising 132 credit points for B.Sc. (Cyber Security) and 176 credit points for B.Sc. (Cyber Security) Honors and Research degree.

3. **Objectives:**

- To Develop Proficiency in Cyber Security: Equip students with the skills to protect Information systems against cyber threats and vulnerabilities.
- To provide hands-on experience with current security technologies and tools.
- To an understanding of the ethical, legal, and societal implications of cyber security practices.
- To encourage innovative problem-solving and critical analysis of security issues.
- To develop an understanding of the global context and cultural dimensions of cyber security

4. **Eligibility:**

- Higher secondary school certificate (10+2) in science stream or its equivalent examination in Science stream

OR

- Three-year diploma course from the board of technical education conducted by Government of Maharashtra or its equivalent

PO No.	PO Outcomes
PO-1	Become proficient in Linux administration, as it is essential in today's IT environment.
PO-2	Address and take action to meet the cyber security needs of the modern IT world.
PO-3	Cultivate creative abilities, critical thinking, analytical skills, and research capabilities to tackle real-world problems using cyber security expertise.
PO-4	Understand the Concepts of cyber security, Networking and vulnerability testing and statistical methods.
PO-5	Applying the Concepts of Digital Communication and IOT.
PO-6	Identify and evaluate software vulnerabilities and security solutions to mitigate the risk of exploitation.
PO-7	Acquire essential programming languages such as C and Python
PO-8	Integrate ethics and cyber laws to understand the rules and regulations of the current IT environment.
PO-9	To developing regulations and tactics for cyber security
PO-10	Cloud security protects applications, data, and cloud-based infrastructure.
PO-11	Comprehend security concepts such as cyber threat intelligence, block chain in cyber security, communication systems security, malware analysis, vulnerability assessment and penetration testing (VAPT), intrusion detection and prevention systems (IDS & IPS), and cybercrime reporting.

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER-1

Level- 4.5 (First Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Subject 1 (2T+2P)	CYS-101-MJ-TH	Fundamentals of Linux Administration	2		2		20	30	50
	CYS-102-MJ-PR	Practical based on CYS-101-MJ-TH		2		4	20	30	50
Subject 2 (2T+2P)	CYS-103-MJ-TH	Foundations of C programming	2		2		20	30	50
	CYS-104-MJ-PR	Practical based on CYS-103-MJ-TH		2		4	20	30	50
Subject 3 (2T+2P)	CYS-105-MJ-TH	Information Technology	2		2		20	30	50
	CYS-106-MJ-PR	Practical based on CYS-105-MJ-TH		2		4	20	30	50
IKS (2T)	CYS-101-IKS-TH	Computing in ancient India	2		2		20	30	50
GE/OE* (2T)	OE-101-CYS-TH	Office Automation/ Introduction to Google Tools	2		2		20	30	50
SEC (2P)	SEC-101-CYS-PR	Basics of Digital Communication		2		4	20	30	50
AEC (2T)	AEC-104-ENG-TH	Professional Communication Skills-I	2		2		20	30	50
VEC (2T)	VEC-101-ENV-TH	Environment Education -I	2		2		20	30	50
TOTAL			14	8	14	16			550

* *The subjects offered to other faculty students under OE vertical are* ***OE-101-CYS - TH*** *and* ***OE-102-CYS -TH.***
The students of B.Sc. (Cyber Security) will opt the subjects offered by other faculty given in College GE/OE Basket.

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- II

Level- 4.5 (First Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Subject 1 (2T+2P)	CYS-151-MJ-TH	Cyber Security Fundamentals	2		2		20	30	50
	CYS-152-MJ-PR	Practical based on CYS-151-MJ-TH		2		4	20	30	50
Subject 2 (2T+2P)	CYS-153-MJ-TH	Python Programming	2		2		20	30	50
	CYS-154-MJ-PR	Practical based on CYS-155-MJ-TH		2		4	20	30	50
Subject 3 (2T+2P))	CYS-155-MJ-TH	Computer Networks	2		2		20	30	50
	CYS-156-MJ-PR	Practical based on CYS-153-MJ-TH		2		4	20	30	50
GE/OE * (2P)	OE-151-CYS-PR	Office Automation/ Introduction to Google Tools		2		4	20	30	50
SEC (2P)	SEC-151-CYS-PR	Statistical Methods-I		2		4	20	30	50
AEC (2T)	AEC-154-ENG-TH	Professional Communication Skills-II	2		2		20	30	50
VEC (2T)	VEC-151-ENV-TH	Environment Education -II	2		2		20	30	50
CC (2)	CC-151-PE-TH	University Basket	2		2		20	30	50
TOTAL			14	8	14	16			550

* *The subjects offered to other faculty students under OE vertical are **OE-151-CYS -PR** and **OE-152-CYS -PR.***

The students of B.Sc. (Cyber Security) will opt the subjects offered by other faculty given in College GE/OE Basket.

Exit option:

Award of UG Certificate in Major **with 44 credits and an additional 4 credits** as per college guidelines OR Continue with Major and Minor.

ATKT Rules

Minimum number of credits required to take admission to S.Y.B.Sc. (Cyber Security) is 31 credits [70%].

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- III

Level- 5.0 (Second Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (4T+2P)	CYS-201-MJ-TH	Ethical Cyber Hacking-I	2		2		20	30	50
	CYS-202-MJ-TH	Advance Network Security	2		2		20	30	50
	CYS-203-MJ-PR	Practical based on CYS-201-MJ-TH		2		4	20	30	50
VSC (2T)	CYS-221-VSC-TH	Data Structure using Python	2		2		20	30	50
IKS (2T)	CYS-201-IKS-TH	IKS in Cyber Security	2		2		20	30	50
FP/OJT/ CEP (2)	CYS-231-FP	FP Mini Project		2		4	20	30	50
Minor (2T+2P)	CYS-241-MN-TH	Web Technology	2		2		20	30	50
	CYS-242-MN-PR	Practical based on CYS-241-MN-TH		2		4	20	30	50
GE/OE (2T)	OE-201-CYS-TH Other than Sci. Faculty	Principles of OS	2		2		20	30	50
GE/OE (2T)	OE-201-GER-TH For CYS students	German Language-III	2						
AEC (2T)	AEC-201-MAR-TH Or AEC-201-HIN-TH	Marathi Or Hindi	2		2		20	30	50
CC (2)	CC-201-PE / NSS / NCC	From CC Basket	2		2		20	30	50
TOTAL			16	6	16	12			550

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- IV

Level- 5.0 (Second Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (4T+2P)	CYS-251-MJ-TH	Ethical Cyber Hacking -II	2		2		20	30	50
	CYS-252-MJ-TH	Ethics and Cyber Law	2		2		20	30	50
	CYS-253-MJ-PR	Practical Based on CYS-251-TH		2		4	20	30	50
VSC (2T/P)	CYS-271-VSC-PR	Database Management System	2		2		20	30	50
FP/OJT/ CEP (2)	CYS-281-CEP	CEP Mini Project		2		4	20	30	50
Minor (2T+2P)	CYS-291-MN-TH	Modern Web Development	2		2		20	30	50
	CYS-292-MN-PR	Practical Based on CYS-291-MN-TH		2		4	20	30	50
GE/OE (2T)	OE-251-CYS-TH Other than Sci. Faculty	Basic of Python Programing	2		2		20	30	50
	OE-251-GER-TH For CYS students	German Language-IV							
SEC (2P)	SEC-251-CYS-TH	Cloud Cyber Security	2		2		20	30	50
AEC (2T)	AEC-251-MAR-TH Or AEC-251-HIN-TH	Marathi Or Hindi	2		2		20	30	50
CC (2)	CC-251-PE / NSS / NCC	From CC Basket	2		2		20	30	50
TOTAL			16	6	16	12	220	330	550

Exit option:

Award of UG Diploma in Major and Minor with **88 credits and an additional 4 credits** core as per college guidelines OR Continue with Major and Minor.

ATKT Rules:

Minimum number of credits required to take admission to T.Y.B.Sc. (Cyber Security) is 44 credits [100%] to be completed from F.Y.B.Sc. (Cyber Security) and at least 22 credits from S.Y.B.Sc. (Cyber Security)

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- V

Level- 5.5 (Third Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (8T+4P)	CYS-301-MJ-TH	Digital Forensic-I	2		2		20	30	50
	CYS-302-MJ-TH	Malware Analysis	2		2		20	30	50
	CYS-303-MJ-TH	Cyber Threat Intelligence	2		2		20	30	50
	CYS-304-MJ-TH	Advanced Network Security	2		2		20	30	50
	CYS-305-MJ-PR	Practical based on CYS-301-MJ-TH		2		4	20	30	50
	CYS-306-MJ-PR	Practical based on CYS-302-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-310-MJ-TH	Internet of Things	2		2		20	30	50
	CYS-311-MJ-PR	Practical based on CYS-310-MJ-TH		2		4	20	30	50
	OR								
	CYS-312-MJ-TH	Mobile Forensic	2		2		20	30	50
	CYS-313-MJ-PR	Practical based on CYS-312-MJ-TH		2		4	20	30	50
VSC (2T/P)	CYS-321-VSC-PR	Block Chain		2		4	20	30	50
FP/OJT/ CEP (2FP/CEP)	CYS-331-FP	Project		2		4	20	30	50
Minor (2T)	CYS-341-MN-TH	Statistical Methods	2		2		20	30	50
TOTAL			**12**	**10**	**12**	**20**			**550**

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- VI

Level- 5.5 (Third Year)

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (8T+4P)	CYS-351-MJ-TH	Digital Forensic-II	2		2		20	30	50
	CYS-352-MJ-TH	IoT Security	2		2		20	30	50
	CYS-353-MJ-TH	Cyber Crime and Reports	2		2		20	30	50
	CYS-354-MJ-TH		2		2		20	30	50
	CYS-355-MJ-PR	Practical Based on CYS-351-MJ-TH		2		4	20	30	50
	CYS-356-MJ-PR	Practical Based on CYS-352-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-360-MJ-TH	Vulnerability Assessment and Penetration Testing	2		2		20	30	50
	CYS-361-MJ-PR	Practical Based on CYS-360-MJ-TH		2		4	20	30	50
	OR								
	CYS-362-MJ-TH	Fin-Tech Cyber Security	2		2		20	30	50
	CYS-363-MJ-PR	Practical Based on CYS-362-MJ-TH		2		4	20	30	50
VSC(2T/P)	CYS-371-VSC-PR	AI and Machine Learning		2		4	20	30	50
FP/OJT/ CEP (4 OJT)	CYS-381-OJT	On Job Training		4		8	20	30	100
TOTAL			12	10	12	20			550

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- VII

Level- 6 (Fourth Year)

Honors Degree

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (10T+4P)	CYS-401-MJ-TH	Malware Analysis II	2		2		20	30	50
	CYS-402-MJ-TH	Intrusion Detection and Prevention System	2		2		20	30	50
	CYS-403-MJ-TH	Digital Image Processing	2		2		20	30	50
	CYS-404-MJ-TH	Cyber Crime Investigation	2		2		20	30	50
	CYS-405-MJ-TH	Cyber Threat Intelligence	2		2		20	30	50
	CYS-406-MJ-PR	Practical Based on CYS-401-MJ-TH		2		4	20	30	50
	CYS-407-MJ-PR	Practical Based on CYS-402-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-410-MJ-TH	Digital Payments and Its Security	2		2		20	30	50
	CYS-411-MJ-PR	Practical Based on CYS-410-MJ-TH		2		4	20	30	50
	OR								
	CYS-412-MJ-TH	Wireless Security	2		2		20	30	50
	CYS-413-MJ-PR	Practical Based on CYS-412-MJ-TH		2		4	20	30	50
	OR								
	CYS-414-MJ-TH	IT Act 2000 in Cyberspace	2		2		20	30	50
	CYS-415-MJ-PR	Practical Based on CYS-414-MJ-TH		2		4	20	30	50
RM (4T)	CYS-441-RM-TH	Research Methodology	4		4		40	60	100
TOTAL			**16**	**6**	**16**	**12**			**550**

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- VIII

Level- 6 (Third Year)

Honors Degree

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (10T+4P)	CYS-451-MJ-TH	Mobile Application And Services	2		2		20	30	50
	CYS-452-MJ-TH	Incident Handling	2		2		20	30	50
	CYS-453-MJ-TH	Cyber Security Architecture	2		2		20	30	50
	CYS-454-MJ-TH	Introduction to Hardware Security	2		2		20	30	50
	CYS-455-MJ-TH	IT Security Strategy Planning and Leadership	2		2		20	30	50
	CYS-456-MJ-PR	Practical Based on CYS-451-MJ-TH		2		4	20	30	50
	CYS-457-MJ-PR	Practical Based on CYS-452-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-460-MJ-TH	Dark web and Cyber warfare	2		2		20	30	50
	CYS-461-MJ-PR	Practical Based on CYS-460-MJ-TH		2		4	20	30	50
	OR								
	CYS-462-MJ-TH	DecSecOps	2		2		20	30	50
	CYS-463-MJ-PR	Practical Based on CYS-462-MJ-TH		2		4	20	30	50
	OR								
	CYS-464-MJ-TH	Tools and Technology for Cyber Security	2		2		20	30	50
	CYS-465-MJ-PR	Practical Based on CYS-464-MJ-TH		2		4	20	30	50
OJT (4 OJT)	CYS-481-OJT	On Job Training		4		8	40	60	100
TOTAL			12	10	12	20			550

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- VII

Level- 6 (Fourth Year)

Honors with Research

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (6T+4P)	CYS-401-MJ-TH	Malware Analysis II	2		2		20	30	50
	CYS-402-MJ-TH	Intrusion Detection and Prevention System	2		2		20	30	50
	CYS-403-MJ-TH	Digital Image Processing	2		2		20	30	50
	CYS-404-MJ-PR	Practical Based on CYS-401-MJ-TH		2		4	20	30	50
	CYS-405-MJ-PR	Practical Based on CYS-402-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-410-MJ-TH	Digital Payments and Its Security	2		2		20	30	50
	CYS-411-MJ-PR	Practical Based on CYS-410-MJ-TH		2		4	20	30	50
	OR								
	CYS-412-MJ-TH	Wireless Security	2		2		20	30	50
	CYS-413-MJ-PR	Practical Based on CYS-412-MJ-TH		2		4	20	30	50
	OR								
	CYS-414-MJ-TH	IT Act 2000 in Cyberspace	2		2		20	30	50
	CYS-415-MJ-PR	Practical Based on CDS412MJ		2		4	20	30	50
FP/OJT/ CEP/RP (4 RP)	CYS-431-RP-PR	Research Project		4		8	40	60	100
RM (4T)	CYS-441-RM-TH	Research Methodology	4		4		40	60	100
TOTAL			**12**	**10**	**12**	**20**			**550**

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

SEMESTER- VIII

Level- 6 (Fourth Year)

Honors with Research

Course Type	Course Code	Course Title	Credit		Teaching Scheme Hr. / Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Mandatory (6T+4P)	CYS-451-MJ-TH	Mobile Application And Services	2		2		20	30	50
	CYS-452-MJ-TH	Incident Handling	2		2		20	30	50
	CYS-453-MJ-TH	Cyber Security Architecture	2		2		20	30	50
	CYS-454-MJ-PR	Practical Based on CYS-451-MJ-TH		2		4	20	30	50
	CYS-455-MJ-PR	Practical Based on CYS-452-MJ-TH		2		4	20	30	50
Major Elective (2T+2P)	CYS-460-MJ-TH	Dark web and Cyber warfare	2		2		20	30	50
	CYS-461-MJ-PR	Practical Based on CYS-460-MJ-TH		2		4	20	30	50
	OR								
	CYS-462-MJ-TH	DecSecOps (Decentralized Security Operations)	2		2		20	30	50
	CYS-463-MJ-PR	Practical Based on CYS-462-MJ-TH		2		4	20	30	50
	OR								
	CYS-464-MJ-TH	Tools and Technology for Cyber Security	2		2		20	30	50
	CYS-465-MJ-PR	Practical Based on CYS-464-MJ-TH		2		4	20	30	50
FP/OJT/ CEP/RP (8 RP)	CYS-481-RP-PR	Research Project		8		16	80	120	200
TOTAL			**8**	**14**	**8**	**28**			**550**

Syllabus of Semester-III

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) - Sem-III
Subject Code: CYS-201-MJ-TH
Subject: Ethical Cyber Hacking -I

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites:-

- Fundamentals of Cyber Security
- Fundamentals of OSI model and TCP/IP Suite
- Fundamentals of GNU /Linus operating System

Course Objectives: -

- To introduce students to the fundamentals of ethical hacking and cyber security threats.
- To familiarize students with various hacking methodologies and techniques.
- To develop practical skills in penetration testing and vulnerability assessment.
- To educate students on legal and ethical responsibilities in cyber security.
- To enhance students' ability to recognize and mitigate cyber threats effectively.

Course Outcomes: - Student will be able to: -

CO1: Explain the fundamentals of ethical hacking, cyber security threats, and the importance of ethical responsibilities in hacking practices

CO2: Perform reconnaissance techniques using various foot printing and information-gathering tools to identify vulnerabilities in a target system.

CO3: Conduct network scanning operations to detect live hosts, open ports, and potential security flaws using advanced scanning techniques.

CO4: Demonstrate system hacking techniques such as password cracking, privilege escalation, and malware attacks while understanding countermeasures.

CO5: Analyze and exploit common web application vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), and CSRF, using ethical hacking tools.

CO6: Evaluate wireless network security by performing attacks on WEP, WPA, and WPA2 encryption and implementing security best practices.

Course Contents

Chapter 1	**Introduction to Ethical Hacking**	**6 hours**

- Overview of Cyber security and Ethical Hacking
- Understanding Hacking: Types and Phases
- Ethical Hacking vs. Malicious Hacking
- Cyber Laws and Ethical Responsibilities
- Setting up a Lab Environment for Ethical Hacking.

Chapter 2	**Foot printing and Reconnaissance**	**5 hours**

- Basics of Foot printing
- Active vs. Passive Reconnaissance
- Information Gathering Techniques
- WHOIS Lookup, DNS Enumeration, Google Dorking
- Tools: Maltego, Shodan, Nmap, Recon-ng

Chapter 3	Scanning Networks	5 hours

- Network Scanning Fundamentals
- Types of Scanning (Port, Vulnerability, Service)
- Identifying Live Systems and Open Ports
- Scanning Techniques: TCP/UDP Scans, SYN Scans
- Tools: Nmap, Netcat, Angry IP Scanner

Chapter 4	System Hacking and Gaining Access	6 hours

- Exploiting System Vulnerabilities
- Password Cracking Techniques (Brute Force, Dictionary Attack)
- Privilege Escalation and Maintaining Access
- Malware: Keyloggers, Trojans, Rootkits
- Tools: Metasploit, John the Ripper, Hydra

Chapter 5	Web Application Hacking Basics	4 hours

- Common Web Vulnerabilities (SQL Injection, XSS, CSRF)
- OWASP Top 10 Overview
- Basics of Website Enumeration
- Tools: Burp Suite, SQLmap, ZAP Proxy

Chapter 6	Wireless Hacking Basics	4 hours

- Fundamentals of Wireless Networks and Security
- Cracking WEP/WPA/WPA2 Encryption
- MITM (Man-in-the-Middle) Attacks in Wireless Networks
- Tools: Aircrack-ng, Wireshark, Kismet

Reference Books:

1. Certified Ethical Hacker (CEH) v12 Study Guide – Matt Walker
2. Hacking: The Art of Exploitation – Jon Erickson
3. The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
4. Online Labs: TryHackMe, Hack The Box, PentesterLab

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-III
Subject Code: CYS-202-MJ-PR
Subject: Advance Network Security

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites:-

- To understand process of data communication using protocols and standards
- To learn various topologies and applications of network.

Course Objectives: -

- To prepare students with basic networking concept.
- To understand process of data communication using protocols and standards
- To understand the concept of network security, networking attacks, cryptography.

Course Outcomes: - Student will be able to :-

- Understand Network Security Concepts
- Identify Security Threats and Vulnerabilities
- Implement Cryptographic Technique
- Monitor and Analyze Network Traffic:

Course Contents

Chapter 1	**Introduction**	**5 Hours**

- Communication models- OSI Overview, TCP/IP Overview
- Communication protocol overview
- Bridging and Switching Overview
- Virtual Private Networks Overview
- Introduction Attacks on Computers and Computer Security

Chapter 2	**TCP/IP Protocol Overview**	**5 Hours**

- Over of IP Addressing-Architecture
- Class of Address- Example of Addressing, Special Addresses
- Addressing and Networks
- Introduction to Subnetting - Simple Subnets, Complex subnets , Variable Length Subnets
- IP Addressing Design

Chapter 3	**Network Fundamental and Security**	**8 Hours**

- Need for Security
- Security Attacks (Active and Passive attacks)
- Services and Mechanisms
- Network Security
- Network Security Mode

- Internet Standards and RFCs
- Symmetric Key Cryptography

Chapter 4	User Authentication and security at Application and Transport Layer	12 Hours

- Pretty Good Privacy (PGP) and S/MIME.
- User Authentication 1. Remote User-Authentication Principles
- Remote User-Authentication Using Symmetric Encryption
- Application Layer Security:
- Email privacy: PGP and S/MIME,
- SSL Architecture –Handshake ,Change Cipher Space, Alert And Record Protocols SSL Message Formats
- Transport Layer Security: Transport Layer Security, HTTPS, Secure Shell (SSH)

Reference Books:

1. Certified Ethical Hacker (CEH) v12 Study Guide – Matt Walker
2. Cryptography & Network Security – William Stallings
3. TCP / IP Protocol Suite Fourth Edition – Behrouz A. Forouzan.

E- Books and Online Learning Material

- http://www.w3schools.com/html/html5_intro.asp.
- Network Security Essentials by William Stallings.
- Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, and Mike Speciner.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) – Sem-III
Subject Code: CYS-203-MJ-PR
Subject: Practical based on CYS-201-MJ-TH

Teaching Scheme	No. of Credits	Examination Scheme
04 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites None

Course Objectives: -

- To provide hands-on experience in ethical hacking techniques and tools.
- To develop skills in reconnaissance, scanning, and exploitation of system vulnerabilities.
- To familiarize students with penetration testing methodologies.
- To analyze and secure web applications and wireless networks against cyber threats.
- To enhance understanding of cyber security best practices and ethical considerations.

Course Outcomes: - Student will be able to :-

CO1: Set up and configure an ethical hacking lab environment using virtualization tools.
CO2: Perform reconnaissance techniques and information gathering using open-source intelligence (OSINT) tools.
CO3: Conduct network scanning and identify vulnerabilities in target systems.
CO4: Execute system hacking techniques including password cracking, privilege escalation, and malware deployment.
CO5: Identify and exploit common web application vulnerabilities like SQL Injection and XSS.
CO6: Assess wireless network security and conduct attacks on WEP, WPA, and WPA2 encryption.

Practical List

Exp 1	**Introduction to Ethical Hacking Environment**	

Objective: Set up an ethical hacking lab using a virtualized environment
Task:

- Install Virtual Box /VMware on the system.
- Set up kali Linux and Metasploitable VM.
- Configure network settings for penetration testing.
- Verify installation of essential hacking tools (Nmap, Metasploit, Wireshark)

Exp 2	**Information Gathering & Foot printing**	

Objective: Perform reconnaissance and gather information about a target system.
Task:

- Perform WHOIS lookup and analyze results.
- Conduct DNS enumeration using nslookup and dig.
- Use Google Dorking techniques to find sensitive information.
- Use tools like Maltego and Shodan to gather intelligence.

Exp 3	**Network Scanning Techniques**	

Objective: Identify live hosts, open ports and running services on a target network
Task:

- Perform a basic Nmap scan on a target machine.
- Conduct SYN, TCP connect and UDP scans.
- Detect operating system and version details.
- Analyze scan results using Wireshark

Exp 4	**System Hacking and Password Craking**	

Objective: Exploit system vulnerabilities and crack passwords.
Task:

- Use John the Ripper to crack hashed passwords.
- Perform a brute-force attack using Hydra on SSH.
- Demonstrate privilege escalation techniques.
- Deploy Keyloggers and analyze logs.

Exp 5	**Web Application Hacking Basics**	

Objective: Exploit common web vulnerabilities like SQL Injection and XSS.
Task:

- Perform SQL Injection attacks using SQL map.
- Demonstrate XSS attacks using Burp Suite.
- Analyze OWASP Top 10 vulnerabilities.
- Use ZAP Proxy to intercept and modify HTTP requests.

Exp 6	**Wireless Network Security & Attacks**	

Objective: Analyze and exploit weaknesses in wireless networks.
Task:

- Capture Wi-Fi packets using Wireshark.
- Perform WEP/WPA2 cracking using Aircrack-ng.
- Conduct a deauthentication attack.
- Simulate a MITM attack in a controlled lab environment.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-III
Subject Code: CYS-221-VSC-TH
Subject: Data Structure in Python

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites: -

- Introductory Programming (in Python)
- Basic Discrete Mathematics (helpful, but not strict required)

Course Objectives: -

- Understand and implement fundamental data structures such as arrays, linked lists, stacks, queues, and hash tables.
- Analyze the time and space complexity of basic algorithms.
- Apply appropriate data structures to solve security-related problems.
- Develop proficiency in Python programming for secure coding practices.
- Understand the importance of efficient data handling in cyber security contexts.

Course Outcomes: - Student will be able to:-

CO1 : Implement efficient algorithms using appropriate data structures.
CO2 : Analyze the performance of algorithms and select suitable data structures for specific problems.
CO3 : Apply data structures to solve practical cyber security challenges.
CO4 : Write well-structured and documented Python code.
CO5 : Demonstrate an understanding of the trade-offs between different data structures in terms of performance.
CO6 : Evaluate and implement secure data handling practices to protect sensitive information in data structures

Course Contents

Chapter 1	**Introduction to Data Structures and Python Review**	**7 Hours**

- Introduction to Data Structures: Definition, Classification, and Applications
- Python Review: Basic syntax, data types, control structures, functions, and modules.
- Object-Oriented Programming in Python: Classes, objects, inheritance, and polymorphism.
- Basic Security Considerations in Python.

Chapter 2	**Arrays and Strings**	**7 Hours**

- Arrays: Static and dynamic arrays, multi-dimensional arrays.
- Array Operations: Insertion, deletion, searching, and sorting.
- Strings: String manipulation, pattern matching.
- Applications: Implementing simple ciphers, storing cryptographic keys.

Chapter 3	**Linked Lists**	**7 Hours**

- Linked Lists: Singly linked lists, doubly linked lists, circular linked lists.
- Linked List Operations: Insertion, deletion, traversal, and searching.
- Applications: Implementing dynamic data structures, memory management.

Chapter 4	**Stacks and Queues**	**6 Hours**

- Stacks: LIFO principle, stack operations.
- Queues: FIFO principle, queue operations.
- Applications: Expression evaluation, backtracking algorithms, network packet queuing

Chapter 5	**Security Considerations and Data Structures**	**3 Hours**

- Secure Coding Practices with Data Structures
- Common Vulnerabilities: Buffer overflows, injection attacks.

Reference Books:

- Data Structures and Algorithms in Python by Michael T. Goodrich, Roberto Tamassia, and Michael H. Goldwasser
- Algorithms and Data Structures in Python by Day Nicholas
- Data Structures and Algorithms Using Python by Rance D. Necaise
- Algorithms for Sorting and Searching by Thomas H. Cormen

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-III
Subject Code: CYS-201-IKS-TH
Subject: IKS in Cyber Security

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites: -

- Basic of Indian Knowledge System

Course Objectives: -

- Integrate Indian Knowledge Systems with core concepts of Cyber Security.
- Provide historical and philosophical foundations of cryptography, ethics, governance, and security from Indian texts.
- Strengthen ethical decision-making and legal awareness in cyber security practices.
- Enhance critical thinking by mapping traditional Indian principles to modern cyber security challenges.

Course Outcomes: - Student will be able to:-

CO1 : Describe the fundamentals of Indian Knowledge Systems relevant to cyber security
CO2 : Explain ancient Indian approaches to cryptography and secure communication.
CO3 : Apply Indian ethical principles to cyber security and cyber law scenarios
CO4 : Analyze cyber security issues using Indian ethical and governance frameworks.
CO5 : Evaluate modern cyber practices based on IKS values and ethics

Course Contents

Chapter 1	**Indian Knowledge Systems and Foundations of Security**	**5 Hours**

- Overview of Indian Knowledge Systems (IKS)
- Knowledge protection and transmission in ancient India
- Concept of Dharma and responsibility in governance
- Relevance of IKS in modern cyber security

Chapter 2	**Cryptography and Secure Communication – Indian Perspective**	**5 Hours**

- Cryptography references in Arthashastra
- Ancient Indian cipher methods and secret communication
- Intelligence gathering and information security
- Comparison with modern encryption techniques

Chapter 3	**Indian Ethics and Cyber Ethics**	**7 Hours**

- Ethical principles: Dharma, Karma, Satya, Ahimsa
- Professional ethics in Indian philosophy
- Privacy, confidentiality, and data protection
- Ethical hacking vs unethical hacking (IKS perspective)

Chapter 4	Governance, Law, and Digital Society	6 Hours
• Governance models in ancient India • Raj Dharma and accountability • Indian cyber laws and digital governance • Legal and ethical responsibilities of cyber professionals		
Chapter 5	**Applications of IKS in Cyber Security**	**7 Hours**
• Indigenous approaches to cyber security • Digital sovereignty and Atmanirbhar Bharat • Ethical cyber defense strategies • Future role of IKS in cyber security education		
Reference Books:		
• Bimal N. Patel et al., Indian Knowledge Systems, AICTE / MoE • Kapil Kapoor, Indian Knowledge Systems: Approaches and Applications • Markus Christen et al., The Ethics of Cybersecurity • Pankaj Agarwal, Cyber Law and Cyber Crimes • Mary Manjikian, Cybersecurity Ethics • William Stallings, Cryptography and Network Security • Matt Walker, Certified Ethical Hacker (CEH) v12 Study Guide		

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) – Sem-III
Subject Code: CYS-231-FP-PR
Subject: FP Mini Project

Teaching Scheme	No. of Credits	Examination Scheme
04 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites None

Course Objectives: -

- To provide hands-on experience in ethical hacking projects.
- To enhance problem-solving skills in identifying and mitigating cyber threats.
- To enable students to apply ethical hacking tools and techniques in real-world scenarios.
- To develop analytical skills in vulnerability assessment, penetration testing, and system security.
- To promote ethical considerations and responsible hacking practices.

Course Outcomes: - Student will be able to :-

CO1: Identify and define cyber security challenges and propose ethical hacking solutions.
CO2: Apply ethical hacking methodologies to conduct security assessments.
CO3: Demonstrate the ability to analyze vulnerabilities in networks, web applications, and systems.
CO4: Develop and document a structured approach to penetration testing and risk mitigation.
CO5: Implement security measures to counteract identified threats.
CO6: Present findings and recommendations in a professional security report format.

Project Guidelines:

- Projects should be performed in a controlled lab environment using ethical hacking tools.
- Each project should include problem definition, objectives, methodology, tools used, results and conclusion.
- The final project report should include screenshots, observations, and security recommendations.
- Group size Maximum of 2 students per project.

Suggested Mini Projects List:

- **Vulnerability Assessment of a Web Application** – Perform penetration testing on a dummy website using OWASP tools like Burp Suite and SQLmap.
- **Network Scanning and Exploitation** – Conduct an in-depth analysis of a local network, identify vulnerabilities, and demonstrate controlled exploitation.
- **Wireless Security Testing** – Analyze security flaws in Wi-Fi networks and perform WEP/WPA cracking in a test environment.
- **Phishing Attack Simulation** – Create an awareness-based phishing simulation and analyze user response rates.
- **Reverse Engineering Malware** – Analyze a harmless malware sample, detect its functionality, and implement countermeasures.
- **Social Engineering Attack Simulation** – Design and test social engineering attacks like email spoofing and USB baiting to demonstrate awareness.
- **Developing a Keylogger** – Create a simple keylogger for educational purposes and analyze security measures to counteract it.
- **Security Audit of a Linux System** – Perform a security audit of a Linux system and recommend hardening measures.

Submission Guidelines:

- Each lab should be documented with objective, tools used, procedure, observations, and conclusion.
- Screenshots must be included for each step of the practical.
- The completed lab book must be submitted before the deadline.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) – Sem -III
Subject Code: CYS-241-MN-TH
Subject : Web Development Technology

Teaching Scheme	No. of Credits	Examination Scheme
02 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites :-

- Fundamentals of Web development
- Fundamentals of developing web site using HTML,CSS and JavaScript

Course Objectives: -

- To learn about the Internet, World Wide Web (WWW), and web technologies.
- To know and understand the concept of web designing.
- To understand how to develop web-based applications using HTML and CSS
- To implement Interactivity with JavaScript
- To develop Real-World Web Applications

Course Outcomes: - Student will be able to:-

CO1: Explain the concepts of the Internet, World Wide Web (WWW), web browsers, and web servers and understand client-server architecture and HTTP/HTTPS protocols.
CO2: Create Basic Web Pages Using HTML and Develop structured web pages using HTML5 elements, forms, and multimedia tags.
CO3: Apply CSS for Web Page Styling and use CSS to design visually appealing and responsive web pages, implement layouts, colors, fonts, and animations using CSS.
CO4: Implement Basic Interactivity with JavaScript, Use JavaScript for simple form validation, user interaction, and DOM manipulation.
CO5: Understand Web Hosting and Deployment, learn the basics of web hosting, domain names, and deploying static websites.
CO6: Work on a Basic Web Project, develop a small project applying HTML, CSS, and JavaScript concepts.

Course Contents

Chapter 1	**Introduction to HTML**	**6 Hours**

- Introduction to HTML, Basic HTML Structure ,Common HTML Tags.
- Physical and Logical HTML ,Types of Images, client side and server-side Image mapping,
- List, Table, Frames, Embedding Audio, Video, HTML form and form elements.

Chapter 2	**Basics of Style Sheets**	**6 Hours**

- Need for CSS, Introduction to CSS, What is CSS? ,Importance of CSS in Web Development
- Types of CSS: Inline CSS, Internal CSS ,External CSS
- Basic CSS Syntax and Structure

Chapter 3	**Advanced Styling and Layouts in CSS**	**8 Hours**

- **CSS Selectors:** Element Selector Class Selector ,ID Selector ,Group Selector Universal Selector
- **CSS Properties:** Colors (color, background-color),Fonts (font-family, font-size, font-style)
- ,Text Formatting (text-align, text-decoration, text-transform)
- **Box Model and Layouts:** Understanding the Box Model (Margin, Border, Padding, Content) Width, Height, and Overflow, Display Property (block, inline, inline-block, none),Positioning Elements (static, relative, absolute, fixed, sticky)
- Styling Lists, Links, and Tables: Customizing Lists (ordered, unordered, nested lists), Styling Links (hover, active, visited, focus),Table Styling (borders, spacing, background)

Chapter 4	**Introduction to JavaScript**	**6 Hours**

- Introduction to Java Script, What is JavaScript?
- Importance of JavaScript in Web Development
- How JavaScript Works (Client-Side vs. Server-Side)
- Writing and Running JavaScript (Inline, Internal, and External JS)
- Comments in JavaScript, Alert, Prompt, and Console.log(),
- Identifier & operator,
- Control Structure, Conditional Statements (if, if-else, switch-case),Loops (for, while, do-while),Break and Continue Statements,
- Functions ,Predefined functions, math & string functions ,Array in Java scripts
- Introduction to Arrays ,Creating, Accessing, Modifying ,Array Methods (push, pop, shift, unshift, for Each, map) ,Introduction to Objects (Properties and Methods) ,Accessing Object Data (Dot Notation vs. Bracket Notation)

Chapter 5	**DOM Manipulation (Document Object Model)**	**4 Hours**

- What is the DOM?, Selecting Elements (getElementById, querySelector)
- Changing HTML and CSS with JavaScript ,Handling Events (onclick, onmouseover, onkeyup) , Event Listeners (add Event Listener) ,Keyboard and Mouse Events.
- Form Validation Basics.

Reference Books: -

- HTML and CSS: Design and Build Websites – Jon Duckett
- CSS: The Missing Manual – David Sawyer McFarland
- Mastering CSS: A Beginner's Guide – Rich Finelli
- JavaScript and JQuery: Interactive Front-End Web Development – Jon Duckett
- JavaScript: The Definitive Guide – David Flanagan.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) – Sem-III
Subject Code: CYS-242-MN-PR
Subject: Practical based on CYS-241-MJ-TH

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisite:

Course Objectives: -

- Learn about the fundamental components of web development (HTML, CSS, JavaScript).
- Understand the difference between front-end and back-end development.
- Develop structured web pages using HTML.
- Apply CSS for styling and layout designs.
- Implement interactive features using JavaScript

Practical

1. Creating a JavaScript code block, which checks the contents entered in a form's Text element. If the text entered is in the lower case, convert to upper case.
2. Design a login form with fields username, password and login button.
3. Write a JavaScript to accept username and password, validate login details and display a message accordingly.
4. Creating a web page using two image files, which switch between one another as the mouse pointer moves over the images.
5. Creating a web page, which accepts user information and user comments on the web site to check if all the Text fields have being entered with data else display an alert.
6. Write a program in JavaScript and DOM to update the background Color dynamically.
7. Write a java script function that reverse a input number.
8. Write a JavaScript code to accept a string from the user and display the occurrences of every vowel character from the string.
9. Write a JavaScript to read a number from user, store its factors into the array and display that array. (Handle onClick event).
10. Write a JavaScript function that retrieves the first and last name values, concatenates them, and displays the full name in an alert.
11. Write a JavaScript function that prevents the default form submission and displays the form values in a designated div element.
12. Write a JavaScript program to set paragraph background color.
13. Write a JavaScript program to remove items from a drop-down list.
14. Write a JavaScript program to display a random image (clicking on a button).
15. Write a JavaScript program to find all HTML elements that match a specified CSS selector (id, class names, types,

Syllabus of Semester-IV

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-IV
Subject Code: CYS-251-MJ-TH
Subject : Ethical Cyber Hacking -II

Teaching Scheme	No. of Credits	Examination Scheme
02 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites:-

- Basic Knowledge of Ethical Hacking
- Networking Fundamentals
- Web Application Security Basics

Course Objectives: -

- To provide advanced knowledge of ethical hacking techniques.
- To explore complex attack vectors and countermeasures.
- To enhance practical skills in penetration testing and red teaming.
- To introduce forensic analysis in cyber investigations.
- To ensure ethical compliance and best security practices.

Course Outcomes: - Student will be able to: -

CO1: Explain advanced network penetration testing techniques, including bypassing firewalls, IDS/IPS evasion, and exploiting network vulnerabilities.
CO2: Perform advanced web application exploitation using techniques such as SQL injection, XML External Entity (XXE) attacks, and Server-Side Request Forgery (SSRF
CO3: Analyze and exploit vulnerabilities in wireless networks and IoT devices, including WPA3 attacks, RFID exploitation, and Bluetooth security flaws
CO4: Evaluate security risks in cloud environments by identifying and exploiting misconfigurations in AWS, Azure, and GCP.
CO5: Apply digital forensic techniques to perform memory and disk analysis, log investigation, and malware analysis for cyber security incident response.
CO6: Demonstrate red teaming methodologies, privilege escalation, lateral movement, and social engineering tactics used in advanced penetration testing.

Course Contents

Chapter 1	**Advanced Network Penetration Testing**	**6hours**

- Advanced Scanning Techniques and Bypassing Firewalls
- Exploiting Network Vulnerabilities (SMB, SNMP, FTP, SSH)
- Man-in-the-Middle (MITM) Attacks & DNS Spoofing
- IDS/IPS Evasion Techniques
- Tools: Wireshark, Scapy, Bettercap

Chapter 2	**Web Application Exploitation**	**5 hours**

- Advanced SQL Injection Techniques
- Exploiting XML External Entity (XXE) and Server-Side Request Forgery (SSRF)
- Advanced Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF)
- Server-Side Template Injection (SSTI)
- Tools: Burp Suite Pro, OWASP ZAP, SQLmap

Chapter 3	**Wireless and IoT Hacking**	**5 hours**

- WPA3 & Advanced Wireless Attacks
- Exploiting IoT Devices: Smart Home Security Risks
- Bluetooth and RFID Hacking Techniques
- Drone and Embedded System Security
- Tools: Aircrack-ng, Kismet, Bettercap, HackRF

Chapter 4	**Cloud Security and Hacking**	**5 hours**

- Cloud Security Architecture (AWS, Azure, GCP)
- Exploiting Cloud Misconfigurations (S3 Bucket, IAM Policies)
- Server less & Container Security (Docker, Kubernetes)
- Cloud Forensics & Incident Response
- Tools: Pacu, Scout Suite, Cloud Sploit

Chapter 5	**Cyber Forensics and Incident Response**	**4 hours**

- Memory and Disk Forensics
- Log Analysis and Malware Reverse Engineering
- Threat Hunting and SOC Operations
- Digital Evidence Handling and Chain of Custody
- Tools: Autopsy, Volatility, FTK, Splunk

Chapter 6	**Red Teaming and Advanced Exploitation**	**4 hours**

- Red Team vs. Blue Team Methodologies
- Exploiting Privilege Escalation and Lateral Movement
- Social Engineering Tactics and Physical Security Bypass
- Post-Exploitation and Data Exfiltration
- Tools: Cobalt Strike, Empire, Blood Hound

Reference Books:

- The Hacker Playbook 3 – Peter Kim
- Black Hat Python: Python Programming for Hackers and Pentesters – Justin Seitz
- The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
- Online Platforms: Hack The Box, TryHackMe, PentesterLab

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security) – Sem-IV
Subject Code: CYS-252-MJ-TH
Subject: Ethics and Cyber Law

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites:

- Basic knowledge of computer systems and networking.
- Awareness of cyber security concepts.
- Interest in digital security laws and ethics

Course Objectives: -

- To understand the ethical and legal issues in cyber security.
- To familiarize students with national and international cyber laws.
- To examine ethical frameworks for digital security.
- To analyze case studies on cybercrime and legal consequences.

Course Outcomes: - Student will be able to: -

CO 1: Recognize ethical concerns in cyber security.
CO 2: Understand key cyber laws in India and globally **CO 3**: Apply legal frameworks to cybercrime cases.
CO 4: Develop ethical decision- making skills.
CO 5: Analyze cyber forensic techniques in legal contexts.
CO 6: Evaluate international cyber laws and their impact on digital security.

Course Contents

Chapter 1	**Introduction to Cyber Ethics**	**9 Hours**

- Ethics in Cyber security
- Ethical Theories (Utilitarianism, Deontology, Virtue Ethics)
- Ethical Hacking , Malicious Hacking
- Digital Rights and Responsibilities
- Intellectual Property Rights (IPR) in Cyberspace

Chapter 2	**Cybercrime and Cyber Law**	**7 Hours**

- Cybercrimes and Their Types
- Social Engineering and Cyberbullying
- Basics of Cyber Forensics
- Role of Law Enforcement
- Overview of IT Act, 2000

Chapter 3	**Indian Cyber Law Framework**	**7 Hours**

- IT Act, 2000: Objectives, Scope, and Amendments
- Cyber Law and E-Governance
- Digital Signatures and Electronic Authentication
- Cybercrime Cases in India: Analysis and Legal Consequences
- Right to Privacy and Data Protection Laws.

Chapter 4	**International Cyber Law and Policies**	**7 Hours**

- Global Perspectives on Cyber Law: GDPR, HIPAA, COPPA
- Role of Organizations like ICANN, CERT-In, and UN
- Cyber Warfare and International Treaties
- Ethical Challenges in AI and IoT Security
- Case Studies on Cross-Border Cybercrime

Chapter 5	**Emerging Trends in Cyber Security and Legal Challenges**	**6 Hours**

- AI and Machine Learning in Cyber security
- Block chain and Crypto currency Laws
- Cloud Security and Data Regulations
- Cyber security Threats in the Metaverse
- Future Trends in Cyber Law

Reference Books:

- Cyber Law & Cyber Crimes – Pankaj Agarwal
- Cyber security Ethics – Mary Manjikian
- Information Technology Law and Practice – Vakul Sharma
- Cyber Crime and Legal Framework – Anirudh Rastogi
- The Ethics of Cyber security – Markus Christen et al.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem- IV
Subject Code: CYS-253-MJ-PR
Subject: Practical Based on CYS-251-TH

Teaching Scheme	No. of Credits	Examination Scheme
04 hours / Week	**2**	**CE: 20 marks** **EE: 30 marks**

Prerequisites: - Basic Cyber hacking

Course Objectives: -

- To provide hands-on experience in advanced ethical hacking techniques.
- To develop expertise in penetration testing, digital forensics, and cloud security.
- To analyze and exploit security vulnerabilities in networks, web applications, wireless systems, and IoT devices.
- To understand red teaming methodologies and security countermeasures.
- To ensure compliance with ethical and legal considerations in cyber security testing.

Course Outcomes: - Student will be able to: -

CO1: Perform advanced network penetration testing, including firewall evasion and exploitation of vulnerabilities.
CO2: Conduct in-depth web application security assessments using advanced exploitation techniques.
CO3: Analyze and exploit security flaws in wireless networks and IoT devices.
CO4: Assess security risks in cloud platforms and identify misconfigurations.
CO5: Apply cyber forensic techniques for malware analysis and incident response.
CO6: Implement red teaming methodologies, privilege escalation, and social engineering tactics.

Practical Assignments:

Assignment 1	**Advanced Network Penetration Testing**	

Objective: Conduct network vulnerability assessment and bypass security defenses.
Tasks:

1. Perform Nmap scans with IDS/IPS evasion techniques.
2. Exploit SMB, SNMP, and FTP vulnerabilities using Metasploit.
3. Conduct MITM attacks using Bettercap.
4. Perform DNS spoofing and analyze traffic manipulation.

Assignment 2	**Web Application Exploitation**	

Objective: Exploit web vulnerabilities and perform security assessments.
Tasks:

1. Conduct SQL Injection using SQLmap.
2. Exploit XXE and SSRF vulnerabilities using Burp Suite.
3. Perform advanced XSS and CSRF attacks.
4. Exploit Server-Side Template Injection (SSTI).

Assignment 3	Wireless and IoT Hacking	

Objective: Assess security weaknesses in wireless and IoT networks.
Tasks:

1. Capture Wi-Fi traffic and analyze WPA3 vulnerabilities using Aircrack-ng.
2. Exploit smart home IoT devices and analyze security flaws.
3. Perform Bluetooth and RFID hacking techniques.
4. Simulate drone security testing and embedded system vulnerabilities.

Assignment 4	Cloud Security Assessment	

Objective: Identify security misconfigurations in cloud environments.
Tasks:

1. Perform AWS S3 bucket enumeration and access control testing.
2. Identify and exploit IAM policy misconfigurations.
3. Analyze container security in Docker and Kubernetes.
4. Conduct forensic analysis on cloud logs and threat events.

Assignment 5	Cyber Forensics and Incident Response	

Objective: Perform forensic analysis for cyber security incidents.
Tasks:

1. Conduct memory and disk forensics using Autopsy and Volatility.
2. Perform log analysis and identify malware behaviors.
3. Apply threat-hunting techniques in a simulated Security Operations Center (SOC).
4. Handle digital evidence and maintain chain of custody.

Assignment 6	Red Teaming and Advanced Exploitation	

Objective: Simulate real-world cyber-attacks using red teaming methodologies.
Tasks:

1. Implement privilege escalation and lateral movement techniques.
2. Perform social engineering attacks such as phishing and physical security bypass.
3. Deploy post-exploitation tactics for data exfiltration.
4. Utilize Cobalt Strike and Bloodhound for attack simulations.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-IV
Subject Code: CYS-281-FP-PR
Subject: CEP Mini Project

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 50 marks**

Course Objectives: -

- To provide hands-on experience in ethical hacking projects.
- To enhance problem-solving skills in identifying and mitigating cyber threats.
- To enable students to apply ethical hacking tools and techniques in real-world scenarios.
- To develop analytical skills in vulnerability assessment, penetration testing, and system security.
- To promote ethical considerations and responsible hacking practices.

Course Outcomes: -

Upon successful completion of the mini-projects, students will be able to:

CO1: Identify and define cyber security challenges and propose ethical hacking solutions.
CO2: Apply ethical hacking methodologies to conduct security assessments.
CO3: Demonstrate the ability to analyze vulnerabilities in networks, web applications, and systems.
CO4: Develop and document a structured approach to penetration testing and risk mitigation.
CO5: Implement security measures to counteract identified threats.
CO6: Present findings and recommendations in a professional security report format.

Project Guidelines

1. Projects should be performed in a controlled lab environment using ethical hacking tools.
2. Each project should include **problem definition, objectives, methodology, tools used, results, and conclusions**.
3. The final project report should include **screenshots, observations, and security recommendations**.
4. Group size: **Maximum of 2 students per project**.

Suggested Mini Projects List:

1. **Advanced Web Application Penetration Testing** – Conduct security assessments using automated and manual techniques on a dummy web application.
2. **Cloud Security Audit** – Identify misconfigurations in AWS, Azure, or GCP and provide remediation strategies.
3. **IoT Security Analysis** – Test and exploit vulnerabilities in smart home devices.
4. **Red Teaming Simulation** – Execute a controlled red team engagement, including reconnaissance, exploitation, and privilege escalation.
5. **Wireless Security Assessment** – Perform advanced attacks on WPA3-protected networks and analyze security flaws.
6. **Malware Analysis and Reverse Engineering** – Analyze a sample malware to identify attack vectors and propose mitigation measures.

Submission Guidelines:

- Each lab should be documented with **objective, tools used, procedure, observations, and conclusion**.
- Screenshots must be included for each step of the practical.
- The completed lab book must be submitted before the deadline.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem- IV
Subject Code: CYS-291-MN-TH
Subject: Modern Web Development

Teaching Scheme	No. of Credits	Examination Scheme
02 hours / Week	**2**	**CE: 20 marks EE: 30 marks**

Prerequisites: Fundamentals of HTML

1. Basic knowledge of Java Script.
2. Basics of web application development.
3. Basic Knowledge of what is Client and Server-side programming.

Course Objectives: -

To introduce students for modern web technologies.

- To learn and use server side programming using Node.js
- To introduce structure a Node application in modules
- To build a Web Server in Node and understand how it really works
- To learn how to a SQL or Mongo database in Node

Course Outcomes: - Student will be able to: -

CO1 : Define Node.js and its key features like event loop and non-blocking I/O.
CO2 : Explain how Node.js handles asynchronous operations and manages HTTP requests.
CO3 : Develop a basic server and implement RESTful APIs using Node.js and Express.
CO4 : Analyzing: Break down middleware, routing, and error handling to optimize server performance.
CO5 : Compare Node.js with other backend technologies to determine the best use cases.
CO6 : Build and deploy a secure, full-stack web application using Node.js and databases.

Chapter 1	**Introduction to Node**	**4 Hours**

- Introduction
- What is Node JS and its advantages
- Traditional Web Server Model
- Node JS Process model
- Installation of Node JS
- Node JS event loop

Chapter 2	**Node JS Modules**	**4 Hours**

- Functions
- Buffer
- Module
- Module Types
- Module. Exports

Chapter 3	**Node Package Manager**	**4 Hours**

- What is NPM?
- Installing package locally

- Adding dependencies in package. Son
- Installing packages globally
- Updating packages
- Managing Dependencies

Chapter 4	Web Server	3 Hours

- Creating web server
- Handling http requests
- Sending requests

Chapter 5	File System	5 Hours

- FS Model
- Files and Directories
- Streams
- Reading and Writing Files
- Reading and Writing Directories
- Other File Operations

Chapter 6	Working with Databases	5 Hours

- Working with Databases
- Connection String
- Configuring
- Working with Select command
- Various database operations

Chapter 7	Express JS	5 Hours

- Introduction to Express JS
- The MVC pattern
- Routing
- HTTP requests and responses
- Middleware
- Error handling.

Reference Books:

- Node.js complete reference guid , velentin Bojinov, David Herron, Dioge Resende,
- packt Publishing Ltd
- Mastering Nod.js By Sandro Pasquali , packt Publishing
- Smashing Node.js, Java Script Everywhere , Guillermo Rauch, John wiley & Sons
- Web Development with Node and Express by Ethen brown
- Beginning Node.js, Express & MongoDB Development by Greg Lim

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)- Sem-IV
Subject Code: CYS-292-MN-PR
Subject: Practical course based on CYS-291-MN-TH

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	**2**	**CE: 20 Marks EE: 30 Marks**

Course Objectives:

- Set up Node.js, run scripts, and understand basic syntax.
- Use built-in and custom modules to structure code efficiently.
- Build an HTTP server to handle basic requests and responses.
- Connect Node.js with databases like MySQL/Mongo DB for data storage.
- Create a web server using express with routes and middleware.

Practical Assignments

1. Create a Node.js application that will convert the output "Hello World!" into upper-case letters.
2. Create a Node.js application that uses user defined Module to return the factorial of given number.
3. Create a Node.js application that uses user defined module circle.js which exports functions area () and circumference () and display the details on console.
4. Create Node.js application that uses user defined module Rectangle.js to find area of rectangle and display the details on console.
5. Create a Simple Web Server using node js.
6. Create a Simple Web Server using Node.js that shows the college information.
7. Create a Node.js application that demonstrates database Student and student table (rno, name, percentage) in MySQL.
8. Create a Node.js file that Insert Multiple Records in "Student" table, and display the result object on console.
9. Create a Node.js file that Select all records from the "Student" table, and delete the specified record.
10. Create a Node.js Application that Update Marks of given student rno in "student" table and display the result.
11. Using Node.js create Application that contains Voters details and check proper validation for (name, age, and nationality), as Name should be in upper case letters only, Age should not be less than 18 yrs and Nationality should be Indian and store the data in database.
12. Using Node.js create a web page to read two file names from user and append contents of first file into second file.
13. Using Node.js create a web page to read two file names from user and combine in third file with all content in Upper case.
14. Create a Node.js file that opens the requested file and returns the content to the client. If anything goes wrong, throw a 404 error
15. Create a Node.js Application to count number of lines in a file and display the count on console.
16. Create a Node.js Application to count occurrence of given word in a file and display the count on console.
17. Create a Node.js Application for validating student registration form.
18. Create an Node.js Application that contain the Student Registration details and validate Student first and last name should not contains any special symbols / digits and also age should be between 6 to 25.
19. Create a User Login System using Node.js.
20. Crate an Electricity bill calculation System using Node.js.

Haribhai V. Desai College of Arts, Science and Commerce, Pune
(Autonomous)
S.Y.B.Sc.(Cyber Security)-Sem-IV
Subject Code: SEC-251-CYS-TH
Subject: Cloud Cyber Security

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	**2**	**CE: 20 Marks EE: 30 Marks**

Prerequisites

Understanding of operating systems (Windows/Linux)

- Basic understanding of TCP/IP, HTTP/HTTPS
- Knowledge of cloud service models (IaaS, PaaS, SaaS)
- Awareness of cyber threats (phishing, malware, ransomware

Course Objectives: -

- To introduce students to Provide foundational knowledge of cloud security.
- To equip learners with skills to identify and mitigate cloud security threat.
- To develop an understanding of network and data security principles in the cloud.
- To Offer hands-on experience with cloud security tools.
- To Train learners in incident response and disaster recovery planning.

Course Outcomes: - Student will be able to: -

CO1: Demonstrate an understanding of cloud computing models and security principles, including IaaS, PaaS, SaaS, and various cloud deployment strategies.
CO2: Identify and analyze cloud security threats and vulnerabilities, such as data breaches, insecure APIs, and misconfigurations.
CO3: Implement cloud security measures, including encryption, access control, identity and access management (IAM), and secure authentication methods..
CO4: Evaluate compliance and regulatory frameworks (GDPR, IT Act 2000, ISO 27001, NIST) and apply best practices for cloud security governance.
CO5: Utilize cloud security tools and technologies, such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center, to monitor and mitigate risks..
CO6: Design and apply incident response and disaster recovery strategies for handling security breaches and ensuring business continuity in cloud environments..

Course Contents

Chapter 1	**Fundamentals of Cloud Security**	**4 hours**

- Introduction to Cloud Computing
- Cloud Service Models (IaaS, PaaS, SaaS)
- Cloud Deployment Models (Public, Private, Hybrid, Multi-Cloud)
- Shared Responsibility Model in Cloud Security
- Key Cloud Security Challenges and Risks.

Chapter 2	**Cloud Security Threats and Risk Management**	**6 hours**

- Common Cloud Threats: Data Breaches, Insecure APIs, Account Hijacking
- Risk Management Strategies in Cloud Environments
- Identity and Access Management (IAM) Best Practices
- Data Protection, Encryption, and Secure Data Storage in the Cloud
- Security Compliance and Regulatory Frameworks (GDPR, IT Act 2000, ISO 27001).

Chapter 3	Network Security in Cloud Environments	6 hours

- Cloud Network Architecture and Security
- Virtual Private Cloud (VPC) and Network Segmentation
- Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS)
- Secure Communication Protocols (HTTPS, TLS, VPNs
- Denial-of-Service (DoS/DDoS) Attack Prevention in Cloud

Chapter 4	Introduction to AWS Security	7 hours

- Overview of Amazon Web Services (AWS) and Cloud Security Features
- AWS Identity and Access Management (IAM)
- AWS Security Tools: AWS Shield, AWS WAF, AWS CloudTrail
- Securing AWS Storage (S3) and Databases (RDS, DynamoDB)
- AWS Compliance and Best Practices for Cloud Security

Chapter 5	Incident Response and Disaster Recovery in Cloud Security	7 hours

- Understanding Security Incidents in Cloud Environments
- Cloud-Based Security Monitoring and Logging
- Incident Response Planning and Execution
- Disaster Recovery Strategies for Cloud-Based Systems
- Case Studies on Cloud Security Breaches and Mitigation

Reference Books:

- Practical Cloud Security: A Guide for Secure Design and Deployment" - by Chris Dotson Publisher: O'Reilly Media
- Cloud Security Handbook: A Hands-on Guide to Securing Your Cloud Environment" - by Eyal Estrin Publisher: Packt Publishing
- "Security in Computing (6th Edition) - by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies Publisher: Pearson
- Cloud Computing Security: Foundations and Challenges" - John R. Vacca Publisher: CRC Press

Eligibility:

- Higher secondary school certificate (10+2) in science stream or its equivalent examination in Science stream

OR

- Three-year diploma course from the board of technical education conducted by Government of Maharashtra or its equivalent

Objectives:

- To Develop Proficiency in Cyber Security: Equip students with the skills to protect Information systems against cyber threats and vulnerabilities.
- To provide hands-on experience with current security technologies and tools.
- To an understanding of the ethical, legal, and societal implications of cyber security practices.
- To encourage innovative problem-solving and critical analysis of security issues.
- To develop an understanding of the global context and cultural dimensions of cyber security

Workload

1. Each theory credit is equivalent to 15 clock hours of teaching (i.e. for 2 Credits – 30 Clock Hours) and each practical credit is equivalent to 30 clock hours (i.e. for 2 Credits – 60 Clock Hours) of teaching in a semester.
2. There is 15 weeks of teacher-student interaction during the semester.
3. The 15 week is divided into 12 weeks teaching and 3 weeks for continuous assessment including preparation time to students during the semester.
4. The workload will be calculated based on 12 weeks teaching only.
5. For the purpose of computation of work-load the following mechanism may be adopted as per UGC guidelines.
6. Workload as per credit is as follows:
    i. 1 Credit = 1 Theory period of one hour duration per week.
    ii. 1 Credit = 1 Tutorial period of one hour duration per week.
    iii. 1 Credit = 1 Practical period of two-hour duration per week.
7. Each theory Lecture time for FY, SY, TY is of 60 min. (2 Lectures per week for 2 credit courses)
8. Each practical session time for FY/ SY /TY is of 4 hour i.e. 240 min.

The Poona Gujarati Kelvani Mandal's

Haribhai V. Desai College of Arts, Science and Commerce, Pune

(Autonomous)

Structure of UG Program as per NEP-2020

Program Name: - B.Sc. (Cyber Security)

Major Course: - Cyber Security

Credit Framework

Level /Difficulty	Sem	Subject-1	Subject-2	Subject-3	GE/ OE	SEC	IKS	AEC	VEC	CC	Total
4.5/100	I	2(T)+2(P)	2(T)+2(P)	2(T)+2(P)	2(T)	2(T/P)	2(T) Generic	2(T)	2	-	22
	II	2(T)+2(P)	2(T)+2(P)	2(T)+2(P)	2(P)	2(T/P)	-	2(T)	2	2	22

Exit Option: Award of UG ***Certificate*** in Major with **44** credits and an additional **4** credits core **NSQF** Course/Internship **OR** Continue with Major and Minor

Continue Option: Student will select one subject among the (Subject-1, Subject-2, and Subject-3) as major and another as minor and third subject will be dropped.

Level /Difficulty	Sem	Credits related to major				Minor		GE/ OE	SEC	IKS	AEC	VEC	CC	Total
		Discipline Specific Core (DSC) Major Core	Discipline Specific Elective (DSE) Major Elective	VSC	FP/ OJT /CEP									
5.0/200	III	4(T)+2(P)	-	2(T/P)	2 (FP)	2(T)+2(P)	-	2(T)	-	2(T)	2(T)	-	2	22
	IV	4(T)+2(P)	-	2(T/P)	2(CEP)	2(T)+2(P)	-	2(P)	2(T/P)	-	2(T)	-	2	22

Exit Option: Award of UG ***Diploma*** in Major and Minor with **88** credits and an additional **4** credits core **NSQF** Course/Internship **OR** Continue with Major and Minor.

5.5/300	V	8(T)+4(P)	2(T)+2(P)	2(T/P)	(FP/ CEP)	2(T)	-	-	-	-	-	-	-	22
	VI	8(T)+4(P)	2(T)+2(P)	2(T/P)	4(OJT)	-	-	-	-	-	-	-	-	22
Total 3 Years		**44**	**8**	**8**	**10**	**18**	**8**	**8**	**6**	**4**	**8**	**4**	**6**	**132**

Exit Option: Award of UG ***degree*** in Major with **132** credits

OR Continue with Major and Minor.

6.0/400	VII	6(T)+4(P)	2(T)+2(P)	-	4(RP)	4(T)(RM)	-	-	-	-	-	-	-	22
	VIII	6(T)+4(P)	2(T)+2(P)	-	8(RP)	-	-	-	-	-	-	-	-	22
Total 4 Years		**64**	**16**	**8**	**22**	**22**	**8**	**8**	**6**	**4**	**8**	**4**	**6**	**176**

Exit Option: Award of UG ***Honors with Research*** Degree in Major and Minor with **176** credits.

-OR-

6.0/400	VII	10(T)+4(P)	2(T)+2(P)	-	-	4(T)(RM)	-	-	-	-	-	-	-	22
	VIII	10(T)+4(P)	2(T)+2(P)	-	4(OJT)	-	-	-	-	-	-	-	-	22
Total 4 Years		**72**	**16**	**8**	**14**	**22**	**8**	**8**	**6**	**4**	**8**	**4**	**6**	**132**

Exit Option: Award of UG ***Honors Degree*** in Major and Minor with **176** credits.

Reference Books

1. **Ethical Cyber Hacking**
   1. *Matt Walker, Certified Ethical Hacker (CEH) v12 Study Guide*
   2. *Jon Erickson, Hacking: The Art of Exploitation*
   3. *Dafydd Stuttard & Marcus Pinto, The Web Application Hacker's Handbook*
   4. *Peter Kim, The Hacker Playbook 3*
   5. *Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters*
   6. *Online Learning Platforms: TryHackMe, Hack The Box, PentesterLab*

2. **Ethics and Cyber Law**
   1. *Pankaj Agarwal, Cyber Law and Cyber Crimes*
   2. *Mary Manjikian, Cybersecurity Ethics*
   3. *Vakul Sharma, Information Technology Law and Practice*
   4. *Anirudh Rastogi, Cyber Crime and Legal Framework*
   5. *Markus Christen et al., The Ethics of Cybersecurity*

3. **Advanced Network Security**
   1. *Matt Walker, Certified Ethical Hacker (CEH) v12 Study Guide*
   2. *William Stallings, Cryptography and Network Security*
   3. *Behrouz A. Forouzan, TCP/IP Protocol Suite (Fourth Edition)*

4. **Data Structures in Python**
   1. *Michael T. Goodrich, Roberto Tamassia & Michael H. Goldwasser, Data Structures and Algorithms in Python*
   2. *Nicholas Day, Algorithms and Data Structures in Python*
   3. *Rance D. Necaise, Data Structures and Algorithms Using Python*
   4. *Thomas H. Cormen et al., Algorithms for Sorting and Searching.*

5. **Web Development Technology**
   1. *Jon Duckett, HTML and CSS: Design and Build Websites*
   2. *David Sawyer McFarland, CSS: The Missing Manual*
   3. *Rich Finelli, Mastering CSS: A Beginner's Guide*
   4. *Jon Duckett, JavaScript and jQuery: Interactive Front-End Web Development*
   5. *David Flanagan, JavaScript: The Definitive Guide*
   6. *Valentin Bojinov et al., Node.js: The Complete Reference Guide, Packt Publishing*
   7. *Sandro Pasquali, Mastering Node.js, Packt Publishing*
   8. *Guillermo Rauch, Smashing Node.js: JavaScript Everywhere, John Wiley & Sons*
   9. *Ethan Brown, Web Development with Node and Express*
   10. *Greg Lim, Beginning Node.js, Express & MongoDB Development*

6. Cloud Cyber Security

1. *Chris Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly Media*
2. *Eyal Estrin, Cloud Security Handbook: A Hands-on Guide to Securing Your Cloud Environment, Packt Publishing*
3. *Charles P. Pfleeger, Shari Lawrence Pfleeger & Jonathan Margulies, Security in Computing (6th Edition), Pearson*
4. *John R. Vacca, Cloud Computing Security: Foundations and Challenges, CRC Press.*

7. IKS in Cyber Security

1. *Bimal N. Patel et al., Indian Knowledge Systems, AICTE / MoE*
2. *Kapil Kapoor, Indian Knowledge Systems: Approaches and Applications*
3. *Markus Christen et al., The Ethics of Cybersecurity*
4. *Pankaj Agarwal, Cyber Law and Cyber Crimes*
5. *Mary Manjikian, Cybersecurity Ethics*
6. *William Stallings, Cryptography and Network Security*
7. *Matt Walker, Certified Ethical Hacker (CEH) v12 Study Guide*

Examination Pattern

1. Exam pattern is 60-40 i.e. Semester End Examination (SEE) is of 60 % and Continuous Internal Assessment is of 40 %.

   Theory, Practical/Project: -

   Continuous Internal Assessment (CIA): 40 % [20 Marks]

   1. Written Test- 50 % [10 Marks]
   2. Presentation/Assignment: - 25% [5 Marks]
   3. Project/Activity Oriented Learning: -25 % [05 Marks]

   Semester End Examination (SEE): - 60 % [30 Marks]

2. For Internal examination, written test should be conducted of 10 marks for 2 credits.

Paper Pattern

Internal Examination

Que-1: Answer the following questions (Short answer questions) (any 4 out of 5) – **4 Marks.**

Que-2: Answer the following questions (Short answer questions) (any 2 out of 3)- **4 Marks**

Que-3: Answer the following questions (Logical Question) (any 1 out of 2)– **2 Marks.**

External Examination

Que-1: [**06 Marks**]
Answer the following questions (Short answer/Definition/Problems/Diagram, etc.) (Any 6 out of 8)
Que-2: [**08 Marks]**
A] Answer the following questions (Short answer questions- 2 Que out of 3) [6 Marks]
B] Answer the following questions (Long answer questions/Problems- 1 Que out of 2) [2 Marks]
Que-3: [**08 Marks]**
A] Answer the following questions (Short answer questions- 1 Que out of 2 [3 Marks]
B] Answer the following questions (Long answer questions/Problems- 1 Que out of 2) [5 Marks]
Que-4: [**08Marks]**
A] Answer the following questions (Short answer questions- 1 Que out of 2 [3 Marks]
B] Answer the following questions (Long answer questions/Problems- 1 Que out of 2) [5 Marks]

Completion of Degree

1. A student who earns 44 credits at First year with additional 4 credits core NSQF Course/Internship shall be eligible for the award of UG Certificate in Major subject. OR May continues with Major and Minor.
2. A student who earns 88 credits at Second year with additional 4 credits core NSQF Course/Internship shall be eligible for the award of UG Diploma in Major subject with Minor (Selected at SY). OR May continues with Major and Minor.
3. A student who earns 132 credits at Third year shall be eligible for the award of UG Degree in Major subject with Minor (Selected at SY). OR May continues with Major and Minor.
4. A student who earns 176 credits in Four years shall be eligible for the award of UG Honors or Honors with Research in Major subject with Minor (Selected at SY).

Award of Degree:

CGPA will be calculated for students who completed 132/176 credits, grades are given as per the following table.

Sr. No.	Grade Letter	Grade Point	Marks
1.	O (Outstanding)	10	90<= Marks <= 100
2.	A+ (Excellent)	9	75<= Marks <= 89
3.	A (Very Good)	8	60<= Marks <= 74
4.	B+ (Good)	7	55<= Marks <= 59
5.	B (Above Average)	6	50<= Marks <= 54
6.	C (Average)	5	45<= Marks <= 49
7.	D (Pass)	4	40<= Marks <= 40
8.	F (Fail)	0	Marks <40
9.	AB (Absent)	0	-