INSTITUTE	**FACULTY OF TECHNOLOGY**
PROGRAM	**BACHELOR OF TECHNOLOGY (COMPUTER ENGINEERING)**
SEMESTER	**7**
COURSE TITLE	**CYBER SECURITY**
COURSE CODE	**01CE0726**
COURSE CREDITS	**3**

Objective:

1 To equip students with practical knowledge of cyber threats, security architectures, and industry-standard frameworks for protecting digital systems. To develop skills in attack analysis, security assessment, incident response, and understanding of legal, ethical, and governance requirements in cyber security.

Course Outcomes: After completion of this course, student will be able to:

1 Explain cyber security fundamentals, CIA triad, frameworks, and Zero Trust.

2 Analyze hacker techniques, cyber-attacks, malware, and system exploitation methods.

3 Evaluate social engineering and apply VAPT and security architecture concepts.

4 Analyze digital forensics and incident response processes.

5 Interpret cyber laws, data protection regulations, and ethical practices governing digital systems.

Pre-requisite of course:NA

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Cyber Security** Introduction to Cyber Security & Information Security, Cyberspace & Cyber Threat Landscape, Types of Cyber Attacks, CIA Triad, Cyber Security Frameworks, Introduce Zero Trust Model	6
2	**Hackers, Attacks & System Exploitation** Types of Hackers, Cyber Crimes & Attack Lifecycle, Malware Types, Sniffing & Network Attacks, Gaining Access & Privilege Escalation, Covering Tracks & Log Manipulation, OWASP Top 10 vulnerabilities, Introduction to Ethical Hacking Tools.	6

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
3	**Social Engineering & Security Assessment** Social Engineering Attacks, Insider Threats & Prevention, Threat Modeling Concepts, Information Assurance Principles, Vulnerability Assessment & Penetration Testing (VAPT), Enterprise Security Architecture, Security Awareness & Human Factor Defence.	6
4	**Digital Forensics & Incident Response** Introduction to Cyber Forensics, Digital Evidence & Storage Media, Forensic Investigation Process, Network Forensics & Evidence Collection,, Writing Forensic Reports, Auditing & Logging, Incident Response Lifecycle, Introduction to Security Operations Center.	5
5	**Cyber Laws, Ethics & Governance** Cyber Laws & IT Act 2000 (India),, E-Commerce & E-Governance Security, Cyber Offences & Penalties, Data Protection Law (DPDP Act),, Intellectual Property Rights (IPR), Digital Signatures & Certifying Authorities,, Privacy Laws, Cyber Ethics in AI & Digital Systems.	5
Total Hours		**28**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Introduction to Cyber Security Tools	2
2	**Practical 2** Network Scanning using Nmap	2
3	**Practical 3** Packet Sniffing and Traffic Analysis using Wireshark	2
4	**Practical 4** Vulnerability Scanning Tools	2
5	**Practical 5** Password Cracking Techniques	2
6	**Practical 6** Scripting programming by creating template virus	2
7	**Practical 7** Web Application Security Testing	2
8	**Practical 8** Social Engineering Awareness and Case Study	2
9	**Practical 9** Digital Forensics Basics	2
10	**Practical 10** Firewall Configuration	2

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
11	**Practical 11** Case study about cybercrime	2
Total Hours		**22**

Textbook :

1 Cyber Security, Nina Godbole, Sumit Belapure, Willey India, 2011

References:

1 Hacking the Hacker, Hacking the Hacker, Roger Grimes, Wiley India, 2017

2 Social Engineering: The Science of Human Hacking, Social Engineering: The Science of Human Hacking, Christopher Hadnagy, Willey India, 2018

3 Cyber Law, Bare Act, Govt of India, Cyber Law, Bare Act, Govt of India, -, -, 2000

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	10.00	40.00	30.00	20.00	0.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 https://www.sans.org/security-resources/

2 https://www.nist.gov

3 https://nptel.ac.in/courses/106106146

4 https://codered.eccouncil.org/

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)