COURSE TITLE	**CYBER SECURITY**
COURSE CODE	**01CE0516**
COURSE CREDITS	**3**

Objective:

1 The objective of this subject is to protect computer systems, networks, and data from unauthorized access, theft, damage, and other threats.

2 The objective of this subject is to protect computer systems, networks, and data from unauthorized access, theft, damage, and other threats

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

1 Understand the fundamentals of cyber security, its types, threats, and organizational implications.

2 Identify types of hackers, cybercrimes, malware, and exploitation techniques.

3 Analyze social engineering, insider threats, and apply defense and assessment methods.

4 Analyze cyber forensics and evidence handling in information security.

5 Evaluate cyber laws and regulations for legal compliance in cyberspace.

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:** Introduction to Cyber Security, Type of Cyber Security, Introduction to Cyber Security, Cyberspace, Cyber threats, Cyberwarfare, Cyber Terrorism, CIA Triad., Architecture of Cyber Security, Cyber security - Organizational Implications	6
2	**Hackers and Cyber Crimes:** Types of Hackers, Hackers and Crackers, Cyber-Attacks and Vulnerabilities, Type of Malware, Sniffing, Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks	6
3	**Social Engineering:** Types of Social Engineering, Insider Attack, Preventing Insider Threats, Social Engineering Targets and Defense Strategies, Type of Threat, Information Assurance, Threat Modelling, Enterprise Information Security Architecture, Vulnerability Assessment and Penetration Testing	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
4	**Cyber Forensics:** Introduction to Cyber Forensics, Computer Equipment and associated storage media, Role of forensics Investigator, Forensics Investigation Process, Collecting Network based Evidence, Writing Computer Forensics Reports, Auditing, Information Security Management System Management, Introduction to ISO 27001:2013	5
5	**Cyber Ethics and Laws:** Introduction to Cyber Laws, E-Commerce and E-Governance, Certifying Authority and Controller, Offences under IT Act, Computer Offences and its penalty under IT Act 2000, Intellectual Property Rights in Cyberspace	5
Total Hours		**28**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical – 1:** Perform networking commands.	2
2	**Practical – 2:** Explore the port scanning tool.	2
3	**Practical – 3:** : Explore the packet capturing tool.	2
4	**Practical – 4:** Explore the network vulnerability scanning tool.	2
5	**Practical – 5:** Study SQL injection.	2
6	**Practical – 6:** Explore registry tool.	2
7	**Practical – 7:** Understand scripting programming by creating template virus.	2
8	**Practical – 8:** Explore sniffing using social engineering toolkit.	2
9	**Practical – 9:** Explore Secure Socket Layer.	2
10	**Practical – 10:** Study about keyloggers.	2
11	**Practical – 11** Explore password cracking attacks.	2
12	**Practical – 12:** Explore digital signature analysis tool.	2
13	**Practical – 13** Explore data recovery tool.	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
14	**Practical – 14:** Case study about cybercrime.	2
Total Hours		**28**

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 , 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**
25.00	35.00	20.00	20.00	0.00	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)