GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code: BE04045011
Subject Name: Introduction to cyber security

w. e. f. Academic Year:	2024-25
Semester:	4
Category of the Course:	Professional Core Course

Prerequisite:	None
Rationale:	Cyber crime is a global problem and cyber threats are increasing as the Digital landscape is ever increasing. Every entity from Government to individual citizen and private industry depends on Information Technology. Cyber security plays an important role in Information Technology.

Course Outcomes:

Sr. No.	CO statement	Marks% weightage
CO-1	Classify the types of cyber crime	20
CO-2	Understand the network level and application level security	20
CO-3	Perform vulnerability, Malware analysis	20
CO-4	Perform network scanning	20
CO-5	Explore and Exploit Linux operating system	20

Teaching and Examination Scheme:

Teaching - Learning Scheme (in Hours per Semester)					Total Credits = TH/30	Assessment Pattern and Marks					Total Marks
						Theory		Tutorial / Practical			
L	T	P	PBL*	TH		ESE (E)	PA (M)	PA (I)	PBL (I)	ESE (V)	
45	0	30	45	120	04	70	30	20	30	50	200

Content:

Sr. No.	Content	Total Hrs
1	Introduction to cyber security, CIA triad, Reasons for cyber crime, Need for cyber security, Damage to the organization, History of cyber crime – evolution of cyber crime, Cyber crime classification, Types of cyber crime – phishing scams, cyber bullying, Identity theft, cyber stalking, hacking, logic bombs, DDos attack, salami attack, Email bombing, Piracy	8

2	Cyber security components – OSI layer, Zero day attack – Network security, Basics of Network, Network terminology Types of Network attacks – types of attacks, common types of network attacks, Unauthorized access, Man in the middle attack, code and SQL injection attacks, privilege escalation, Insider threats Application security – Types of application security, End point security, Identity and access management, Mobile security, Data security	**8**
3	Scanning and Enumeration. Exploring scanning techniques – Ping, Traceroute Ports, Port scan, Port scanning issues, scanning countermeasures Nmap – scanning tool	**5**
4	Vulnerability assessment, Types of vulnerability assessment, vulnerability assessment life cycle, Vulnerability scanning tool, vulnerability assessment report The elements of threat modeling, Threat modeling framework, Threat modeling tools, threat forecasting	**8**
5	Linux, Basic linux commands, Metasploit framework, Exploiting the Linux operating system, Exploring Linux file system, Exploiting Linux networking, Exploiting Linux Authentication	**8**
6	Exploring types of Malware – Virus, Worms, Trojans, Ransomware, Bots/Botnets, Adware, Spyware, Malvertising, Fileless malware, Backdoors, rootkits Analysis of Malware – static analysis, Dynamic analysis, Detecting Malware, Malware Prevention	**8**
	TOTAL	**45**

Suggested Specification table with Marks (Theory): (For B.E. only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**50**	**10**			

R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (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:

1. INRODUCTION TO CYBER SECURITY Paperback – 25 April 2024 by Ajay Singh Universities Press

2. Hands-On Ethical Hacking Tactics: Strategies, tools, and techniques for effective cyber defenseby Shane Hartman Packt Publication

2. Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts by Ethem Mining (Author)

List of Experiments:

1. Install Kali Linux.
2. Perform port scanning
3. Install OpenVAS and perform vulnerability assessment.
4. Perform security testing and vulnerability management with Metasploit
5. Perform application security testing with Burp suite.
6. Create a network of 3 laptops/Desktops and perform DoS attack on one laptop and observe the behavior.
7. Study the E-mail headers against E-mail bombing.
8. Perform active attack. Create network of 3 laptops/desktops. Inject packets while the data is being transferred from one computer to another.

Major Equipment:
Laptop,Desktop

List of Open Source Software/learning website:
1) https://www.kali.org/
2) https://www.metasploit.com/
3) https://openvas.org/

List of suggested activities for Term Work / Self Learning:

1. Mini Project (10 hours):
1) Create a tool that measures the password strength. Also integrate it with operating system.
2) Create a tool that creates Brute force attack on password.

2. Prepare presentation/case study on cyber attacks in different countries across Globe that includes Government offices, Private organizations and citizens.(6 hours)

3. https://youtube.com/playlist?list=PLFW6lRTa1g80JCqzslAXGHMFIo2AJ_qyb&si=X9hoYgfsYi-kAsOw – NPTEL cyber security course by Prof. Sandeep Shukla

- **List of suggested activities for Problem Based Learning:**

Sl. No.	Name of the activity	No. of hours	Evaluation Criteria
1	Assignment writing. Numerical based assignment is preferable.	5 assignments of 3h each. Total = 15h	Based on the assignment submitted.

2	Problem solving/Coding using C, C++, Python, SCILAB, MATLAB, MS-EXCEL or any other relevant software	5 small coding-based problems of 3h each. Total = 15h	Based on the coding solution submitted.
3	Technical Video based learning related to the subject	Duration of video = 5h Report preparation & Presentation = 10h Total = 15h	Report /presentation based on the video learning outcomes.
4	Discussion on research paper based on relevant subject	3 research paper = 15h	Summarize research paper and evaluation critical parameters
5	Poster/chart/power point preparation on technical topics	Duration = 10 h	Based on poster/chart preparation and presentation skills
6	Application/Software development	Duration = 15 h	Depending on the complexity of the Application/Software
7	Group Discussion on emerging/trending technical topics based on subject	Duration = 1 h each	Based on performance in group discussion, technical depth, knowledge etc.
8	Seminar / Presentation	Duration for study and preparation=5h Report writing=3h Presentation=2h Total=10h	Topic can be selected technical content beyond syllabus
9	Real world case studies-based learning	Duration of data collection/study = 5h Report preparation = 10h Total = 15h	Based on in-depth study, technical depth, data collected, fact finding, etc.
10	Working/non-working model on technical topics	Working = 12 h Non- working = 8 h	Based on inter department/external evaluation
11	Self-learning on-line course	Minimum duration of the course should be 15h.	Examination based assessment at the end of course. Based on the certificate produced.
12	Complex problem solving	Maximum 3 problem. Study of the problem and solution finding, Total = 15h	Based on the depth of the solution submitted.
13	Industry/Research laboratory visit	Visit = 5h, Report preparation = 5h Total = 10h	Based on report submitted. Report should contain observations and calculations based on industry/ lab data.
14	Videos on Industrial safety aspects based on subject	Duration of video = 5h Report preparation = 5h Total = 10h	Based on quiz/report submitted

15	Industrial exposure for 2-3 days to observe and provide tentative solutions on society/environment /health/any other issue	Duration = 15 h for industrial exposure Problem identification and tentative solution = 10 h Total = 20 h	Based on evaluation of critical problems and solutions

Note:

- All the suggested activity should be related to the subject.
- Min 3 activities must be carried out as per the availability of faculties and students.
- The number of hours is suggestive. Faculty can sub-divide the number of hours based on the activity. However, total number of hours is fixed.
- Rubrics for the evaluation can be prepared by the faculty.

****