GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering

Level: UG

Subject Name: Cyber Security

Subject Code: BE05016041

w.e.f. Academic Year:	2024-25
Semester:	5
Category of the Course:	Professional Elective Course - 2

Prerequisite:	DBMS, Operating system
Rationale:	With the proliferation of digital technology, there is a critical need to understand the security challenges and mitigation strategies associated with modern communication. Th e course addresses the shifting landscape of cybercrime, from traditional offences to complex social engineering attacks on social media and botnet architectures. By mastering networking fundamentals and tools like Nmap and Metasploit, students gain the hands-on expertise required to conduct vulnerability scanning and penetration testing

Course Outcome:

After Completion of the Course, Student will be able to:

No	Course Outcomes	RBT Level
1	**Identify** the global perspectives of cybercrime to understand its impact on individuals and society with mechanism involved in cybercrime.	U
2	**Illustrate** security challenges and mitigation strategies for mobile and wireless devices, including credit card fraud prevention.	A
3	**Demonstrate** the use of various cybercrime in a controlled environment.	A
4	**Analyze** different cyber-attack methods to develop effective prevention techniques.	AN
5	**Execute** network scanning and vulnerability assessments using tools like Nmap and the Metasploit framework.	AN

**Revised Bloom's Taxonomy (RBT)*

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	15	90	03	70	30	20	30	50	200

* Problem Based Learning (PBL) aims to accommodate learning beyond syllabus as per clause 9.4 of NBA manual.

Course Content:

Unit No.	Content	No. of Hours
1	Introduction to cyber crime Definition and origins, introduction, Classifications of cybercrime – crime against individual, property, government and society Global perspective on cybercrime – cybercrime transcends national boundaries, case studies, Global struggle with cyber security – case study, international cooperation to combat cybercrime – case study, Planning of cyber offences by criminals	6
2.	Cybercrime and social media Structure, objective Social Engineering – Evolution of social engineering, types of social engineering attacks – phishing, pretexting, baiting, quid pro quo, tailgating or piggybacking, impersonation, scareware Social media platforms – case study Cyber stalking – types of cyber staking behavior, Direct cyber stalking, indirect cyber stalking, Prevention and protection strategy Cybercrimes – taxonomies of cybercrime, social media as a cyber crime ecosystem, cyber crime as a service model, economic impact of cybercrime, challenges in cybercrime investigation Botnets – Botnet architecture and evolution, Botnet capabilities and criminal applications, Botnet monetization strategies, case study Attack vectors – classification	8
3.	Cyber crime with mobile and wireless devices Introduction, proliferation of mobile and wireless devices, Trends in mobility Credit card fraud – types, impact, strategies to prevent credit card fraud Security challenges, Mitigation strategies Registry setting for mobile devices, authentication service security Attacks on mobile devices Organizational measures for handling mobile security – Implementing strong mobile device management policy, enforcing strong authentication and access controls, securing mobile applications and data, Protecting wireless network connections, Educating employees	8
4.	Tools used in cybercrime Introduction to proxy servers – introduction to cyber crime tools, types of proxy servers, tools used in proxy-based cybercrime, proxy detection and mitigation Anonymizers – types, technical functions, Tor network architecture, Operation Bayonet and Alphabay takedown Phishing – attack lifecycle, types, advanced phishing techniques Password cracking – methods, popular tools, password hash types and relative security Keyloggers and spyware – types of keyloggers, spyware capabilities, spyware distribution, detection and prevention Viruses and worms – comparison, virus types, worm types, virus or worm anatomy Trojan horses – Trojan types and functions, Trojan architecture components, Trojan detection methods	8

	Backdoors – types, common backdoor techniques, Backdoor communication methods Dos and DDos attack – types	
5.	Cyber attack methods and different technique SQL injection – attack vectors, prevention techniques, working Buffer overflow – types of attacks, process, Prevention technique Introduction to phishing – types, techniques, Detection and prevention Identity theft – types of identity theft, common theft methods, prevention, incidence response Online fraud detection – social engineering, manipulating the human element, phishing websites and fake apps, Malware and spyware attacks, one time password bypass techniques, cloning and spoofing, fake identities and deepfakes, QR code scam, fake customer support scam	4
6.	Networking fundamentals for hackers – Basic networking concepts – IP addresses, TCP/IP, Ports, Protocol Understanding firewalls, intrusion detection system, intrusion prevention system How network affects scanning and Exploitation Mastering network scanning with Nmap – introduction, basic scanning, Ping scan, TCP syn scan, UDP scan, stealth and timing option, scan specific ports and ranges, port scanning and service detection, OS fingerprinting and version detection, vulnerability scanning, scan outputs, identifying potential vulnerabilities	6
7.	Introduction to Metasploit framework – exploits, payloads, auxiliary, post-exploitation, Meterpreter shell, Handling sessions and commands, basic post exploitation techniques	5

Suggested Specification Table with Marks %(Theory):

Distribution of Theory Marks (in%)					
RLevel	**ULevel**	**Alevel**	**NLevel**	**E Level**	**CLevel**
20	**40**	**30**	**10**	**--**	**-**

WhereR:Remember;U:Understanding;A:Application,N:AnalyzeandE:EvaluateC: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Cybercrime and Digital Security: Understanding threats, attacks, and defenses in the connected world by Mayank Bhushan , Dr. Aatif Jamshed , BPB publication
2. MASTERING HACKING WITH METASPLOIT AND NMAP: A Hands-On Guide to Network Scanning, Vulnerability Exploitation, and Penetration Testing by Elmer wright
3. Cyber Security,
4. by Nina Godbole (Author), Sunit Belapure (Author), WILEY
5. Cyber Security and Network Security (Advances in Cyber Security) 1st Edition, Kindle Edition
6. by Sabyasachi Pramanik (Editor), Debabrata Samanta (Editor), M. Vinay (Editor), Abhijit Guha (Editor), WILEY

(b) Open source software and website:

7. Software: https://nmap.org/download

8. Software: Wireshark (www.wireshark.org)
9. https://www.metasploit.com/

Suggested Course Practical List:(List can be change according to Latest Development)

1. Perform a simulated phishing atack to understand attack vectors and defense mechanisms.
2. Identify vulnerabilities in mobile device settings and implement strong authentication policies.
3. Configure and test various proxy servers and explore the architecture of the Tor network.
4. Use popular tools to perform dictionary and brute-force attacks on various password hash types.
5. Implement Trojan horse or Virus in a sandbox environment to identify its functions.
6. Perform various scans (Ping, TCP SYN, UDP) to identify active hosts and open ports.
7. Navigate the Metasploit framework and understand the use of exploits, payloads, and auxiliary modules.
8. Suppose a keylogger is installed in ATM machine which traps PIN of cards. How the keylogger would be identified?

List of suggested activities for Problem Based Learning:

Sl. No	. Name of the activity	No. of hours	Evaluation Criteria
1	Seminar / Presentation	Duration for study and preparation=10h Report writing=3h Presentation=2h Total=15h	Topic can be selected technical content beyond syllabus
2	Poster/chart/power point preparation on technical topics	Duration = 15h	Based on poster/chart preparation and presentation skills
3	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.
4	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.
5	Application/Software development(Mini Project)	Duration = 15 h	Depending on the complexity of the Application/Software
6	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.

Note:

- All the suggested activity should be related to the subject.
- Min 1 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.
- All records pertaining to the evaluation and assessment of self-learning activities must be properly maintained and preserved at the institute level. These records should be made available to the university upon request.
- Institutes are encouraged to utilize digital platforms, such as Microsoft Teams, for effective record-keeping and to ensure transparency in the evaluation and assessment of self-learning activities.

* * * * * **