

Branch Name:	COMPUTER ENGINEERING (Software Engineering)
Program Code:	ET203
Course Title:	Cyber Security Practical
Course Code:	2ET2030205P
Pre-requisite Course:	Basic networking knowledge and a familiarity with data communication principles.

Course Objectives:

A cyber security practicals lab aims to equip students with hands-on experience in securing digital systems. By simulating real-world scenarios, it enhances skills in threat detection, vulnerability assessment, and incident response. The course fosters a deep understanding of cyber security tools and techniques, preparing students to tackle contemporary cyber threats effectively.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1		-	2	2	-	-	-	-	10	25	10	25	50

Course Contents:

Unit	Details	Contact Hours
1	Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber attack/vulnerability.	4
2	Evaluate network defense tools for following (i) IP spoofing (ii) DOS attack	3
3	Explore the Nmap tool and list how it can be used for network defence.	4
4	Explore the NetCat tool.	2
5	Use Wireshark tool and explore the packet format and content at each OSI layer	3
6	Examine SQL injection attack.	3
7	Perform SQL injection with SQLMap on vulnerable website found using google dorks	4
8	Examine software keyloggers and hardware Keyloggers.	2
9	Perform online attacks and offline attacks of password cracking.	2
10	Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker..	2

Reference Books:

1. <https://www.scribd.com/doc/110015407/Hi-Speed-Networks-Syllabus>
2. <https://www.studocu.com/in/document/gujarat-technological-university/cyber-security/cyber-security2150002-lab-manual/18844423>
3. https://www.mbit.edu.in/wp-content/uploads/syllabus/5sem_ITCE_NewSyllabus_GTU/3150714_CS_ITCE.pdf
4. <https://set.gtu.ac.in/wp-content/uploads/2022/12/GTU-Cyber-Security-Certification-Course-26.12.22.pdf>

Course Outcomes:

At the end of the course, students will be able to:

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Understanding and Determine the most effective tool for identifying cyber attacks and vulnerabilities.	Understanding (2), Applying (3)
CO2	Evaluate network defense tools against common threats like IP spoofing and DOS attacks.	Understanding (2), Applying (3)
CO3	Analyze packet formats and content across different OSI layers using Wireshark.	Understanding (2), Applying (3)
CO4	Actively engage in hands-on activities, such as conducting SQL injection attacks.	Understanding (2), Applying (3)
CO5	Analyze a case study involving online credit card fraud.	Understanding (2), Applying (3)

Mapping of CO with PO and PSO

Course Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3	PS O4
CO1	H	M	M	L	M						L	M				
CO2	H	M	L	L	M						L	L				
CO3	H	M	M	L	L						L	M				
CO4	M	M	M	M	L						H	L				
CO5	H	L	L	M	M						H	L				

H: High, M: Medium, L: Low