1.	Title of the course	Computer Systems Security
2.	Course number	CS531L
3.	Structure of credits	3-0-0-3
4.	Offered to	PG
5.	New course/modification to	Modification To CS5029/17
6.	To be offered by	Department of Computer Science and Engineering
7.	To take effect from	January 2022
8.	Prerequisite	Nil
9.	**Course Objective(s):** To acquire the basic knowledge of cyber security systems, by learning through exploiting system vulnerabilities. To reinforce the understanding of programming and systems concepts from the perspective of different hacking methods. To learn the basic security techniques to prevent system exploitations.	
10.	**Course Content:** Review of programming and systems concepts; Introduction to code disassembly; Common exploitation: buffer overflow attacks, code reuse attacks, shellcode based attacks; Session and log management exploitations; Web exploitation: XSS attacks, XSRF attacks, SQL injection attacks; OS exploitation: privilege escalation attack, rootkits, side- and covert-channel attacks, virtualization and container exploitations; Countermeasures and detection methods: randomizing stack space, memory bounds checking, control flow integrity, taint analysis, rootkit detection, chrooting, isolations using namespace, KPTI defense; Introduction to network attacks and countermeasures.	
11.	**Textbook(s):** 1. Anderson R, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley (2021). 2. Erickson J, *Hacking: The Art of Exploitation*, 2nd Edition, No Starch Press (2008).	
12.	**Reference(s):** 1. Jaeger T, *Operating System Security*, 1st Edition, Morgan and Claypool (2008). 2. Matrosov A, Rodionov E and Bratus S, *Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats*, 1st Edition, No Starch Press (2019). 3. Messier R, *Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking*, 1st Edition, O Reilly (2018). 4. Rice L, *Container Security*, 1st Edition, O Reilly (2020).	