

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SYLLABUS FOR B.E IV SEMESTER**

**CYBER SECURITY (Open elective-II)
(for other Departments)**

Instruction: 1Hr /week	SEE Marks :40	Course Code :OE410CS
Credits :1	CIE Marks: 30	Duration of SEE : 2Hrs

Course objectives	Course outcomes
Students should be able to	At the end of the course, Students will be able to
•Utilize the concepts of cyber security to safeguard from threats and infection spread through the internet	1. Explain the concepts of confidentiality, availability and integrity 2. Explain the basics of fraud techniques used by a hacker 3. Explore the common exploitation mechanisms and inspect data sniffing over the network 4. Determine the ways an organization attempts to discover threats

UNIT I- CYBER SECURITY FUNDAMENTALS

Network and Security concepts: Information assurance fundamentals, Basic Cryptography, Public key encryption, DNS, Firewalls, Virtualization. Attacker Techniques and Motivations: How hackers cover their tracks, Fraud Techniques, Threat Infrastructure

UNIT II – EXPLOITATION

Techniques to gain foothold: Shellcode, Integer overflow, Stack based buffer overflow, Format String Vulnerabilities, SQL Injection, Web Exploit Tools, Misdirection, Reconnaissance, and Disruption Methods. Malicious Code-Worms, Virus, Rootkits, Spyware, Escalation of privileges, Stealing information – MITM attack.

Suggested Books:

1. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", Auerbach Publications , CRC Press, 2011
2. Mike Shema, "Anti-Hacker Tool Kit (Indian Edition)", Mc Graw Hill, 2014
3. Cyber Security - Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole and SunitBelpure, Publication Wiley , 2011

Online Resources:

1. <https://www.edx.org/micromasters/ritx-cybersecurity>
2. <https://www.coursera.org/specializations/cyber-security>
3. <http://nptel.ac.in/courses/106105031/>