BCA308 Cyber Ethics

Teaching Scheme	Examination Scheme	
Lectures: 1 hr/Week	Class Test	– 6 Marks
Tutorials: 1 hr/Week	Teachers Assessment	– 3 Marks
	Attendance	– 6 Marks
Credits: 2	End Semester Exam	– 35 Marks

Prerequisite: Data Networks, Network Security

Course Objectives:
The course intends to
1. Introduce concepts of cyber-security.
2. Discuss about threats and solutions proposed.
3. Illustrate the values and value conflicts in cybersecurity.
4. Differentiate between ethical and unethical hacking

Detailed Syllabus:

Unit-1

Basic concepts and models of cyber-security: Introduction to cybersecurity, system security, information security, Security vs. Safety, Security as Risk Management, Relationship between vulnerability and risk, Approaches for attack and defense: Attackers and their motives, defenses, Stages of an intrusion

Unit-2

Threats and Solutions: Threats and solutions in Data security, Case Study- Secure HTTP Malware threats and solutions: Propagation and Delivery, Payloads, countermeasures, Threats and solutions in Software Security: Case Study-Buffer Overflows, Case Study- SQL Injections, Finding and handling vulnerabilities, Threats and Solutions in Network Security: Case Study: Denial of Service Attacks, Continuous Testing

Unit-3

Core values and Value conflicts in cybersecurity: introduction, what are values? value clusters, value clusters in cybersecurity: security, privacy, fairness, accountability, Value conflicts? Value conflicts in cybersecurity, privacy vs. security, privacy vs. fairness, privacy vs. accountability, security vs accountability, Security vs. privacy (and democracy)

Unit-4

Ethical and Unethical hacking: What actually is a hacker, hackers in early days vs. modern hackers, taxonomy for hackers' classification: based on expertise and legal goals, Inethical, Unethical and Ethical Hacking, Competing ethical values

Reference book:

Markus Christen, Bert Gordijn, Michele Loi, The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology book series (ELTE, volume 21)

Course Outcomes:

After completing the course, students will be able to:

1. To recall and understand the basic concepts of cyber security.
2. Demonstrate the threats applicable in various domains of cyber security.
3. Explain conflicts in values applicable in cyber-security.
4. Enlist the differences between ethical hacking and unethical hacking