5 years Integrated M.Sc (IT) – Semester 4
Lesson Planning
060010411 – DSE5 Cyber Security

Objective: To acquaint the fundamental knowledge of Cyber Security, be familiar with various security attacks and mechanism, digital forensics and career in cyber security.

Course outcomes: Upon completion of the course, students shall be able to

CO1: Summarize different types of cyber criminals and the motives behind them.
CO2: Study different types of cyber-attacks and steps involved in planning cybercrime.
CO3: Exemplifying the security challenges faced by the mobile workforce and their implications.
CO4: Compare various tools and methods used in cybercrime.
CO5: Classifying different methods of phishing and identity theft.
CO6: Summarize digital forensics careers in cyber security.

Unit	Unit Name	Sub Unit	Topics	No. of Lectures	Reference Chapter/Additional Reading
1	Introduction to Cybercrime	1.1	Cybercrime: Definition & Origins of the word	1	NGSB #1 Page no. 1-4, 6, 12
		1.2	Cybercrime and Information Security	1	NGSB #1 Page no. 13-15
		1.3	Cyber criminals	1	NGSB #1 Page no. 16-17
		1.4	Classifications of Cybercrimes.	1	NGSB #1 Page no. 17-32
		1.5	Categories of cyber crime	1	NGSB #2 Page no. 46-49
2	Cyber offenses	2.1	Attack plans	1	NGSB #2 Page no. 49-50, 54, 58, 61
		2.2	Social Engineering	2	NGSB #2 Page no. 61-65
		2.3	Cyberstalking	1	NGSB #2 Page no. 65-67
		2.4	Cybercafe and Cybercrime	2	NGSB #2 Page no. 67-71
		2.5	Botnets: The Fuel for Cybercrime	2	NGSB #2 Page no. 71-73
		2.6	Attack Vector	1	NGSB #2 Page no. 73-75
		2.7	Cloud Computing	1	NGSB #2 Page no. 75-77
3	Cybercrime: Mobile and	3.1	Trends in mobility	2	NGSB #3 Page no. 84-86
		3.2	Types and Techniques of Credit Card Frauds	2	NGSB #3 Page no. 87-90

	Wireless Devices	3.3	Attacks on Mobile/Cell Phones	3	NGSB #3 Page no. 99-106
		3.4	Authentication Service Security	1	NGSB #3 Page no. 93-98
		3.5	Security Countermeasures: Laptops	1	NGSB #3 Page no. 116-120
4	Tools and Methods Used in Cybercrime	4.1	Password Cracking	2	NGSB #4 Page no. 132-137
		4.2	Keyloggers and Spywares	2	NGSB #4 Page no. 137-142
		4.3	Virus, Worms and Trojan Horses	2	NGSB #4 Page no. 143-154
		4.4	Steganography	1	NGSB #4 Page no. 155-158
		4.5	DoS Attacks and Classification	2	NGSB #4 Page no. 158-163
		4.6	SQL Injection	1	NGSB #4 Page no. 164-167
		4.7	Buffer Overflow	1	NGSB #4 Page no. 168-171
5	Phishing and Identity Theft	5.1	Phishing: Methods and Techniques	2	NGSB #5 Page no. 187-195
		5.2	Spear phishing and whaling	1	NGSB #5 Page no. 195-196
		5.3	Types of Phishing Scams	2	NGSB #5 Page no. 196-201
		5.4	Phishing Countermeasures	2	NGSB #5 Page no. 202-206
		5.5	Personally Identifiable Information	1	NGSB #5 Page no. 209-210
		5.6	Identity Theft: Types and Techniques	2	NGSB #5 Page no. 211-219
		5.7	Countermeasures for Identity Theft	1	NGSB #5 Page no. 220
6	Cyber Laws and Introduction to Digital Forensics	6.1	Cyber Laws in India : ITA 2000	1	NGSB #6 Page no. 254-270
		6.2	Digital Forensics Science	1	NGSB #7 Page no. 320-322
		6.3	Cyber Forensics and Digital Evidence	1	NGSB #7 Page no. 327-331
		6.4	Digital Forensics Life Cycle	1	NGSB #12 Page no. 754-759
		6.5	Chain of Custody Concept	1	NGSB #12 Page no. 759-762
		6.6	IT Security Organization: Roles and Responsibilities	1	NGSB #8 Page no. 762-767
		6.7	Career paths in Cyber Security	2	NGSB #12 Page no. 759-762

Text book:

1. Nina God bole, Sunit Belapure – Cyber Security – Understanding cybercrimes, computer forensics

Reference book:

1. Marjie T. Britz – Computer Forensics and Cyber Crime: An Introduction – Prentice Hall
2. George M. Mohay – Computer and intrusion forensics – Artech House

Course objectives and course outcome mapping:

- To acquaint the fundamental knowledge of cyber security: CO1
- To be familiar with various security attacks and mechanism: CO2, CO3, CO4, CO5
- To acquaint with digital forensics and career in cyber security: CO6