9. James A Freeman, David M S Kapura, "Neural Networks Algorithms, Applications, and Programming Techniques", Addison Wesley, 2003.

CO's-PO's & PSO's MAPPING

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
1	3	2	3	2	3	1	-	-	2	1	-	-	2	2
2	3	1	2	1	-	-	-	-	-	1	2	2	-	1
3	3	3	3	3	3	1	-	-	2	1	-	-	2	2
4	3	3	3	3	3	-	-	-	2	-	2	3	2	2
5	1	1	3	2	3	-	-	-	2	-	-	-	1	1
AVg.	2.6	2	2.8	2.2	2.4	0.4	0	0	1.6	0.6	0.8	1	1.4	1.6

1 - low, 2 - medium, 3 - high, '-' - no correlation

CCS340	CYBER SECURITY	L T P C
		2 0 2 3

COURSE OBJECTIVES:
- To learn cybercrime and cyberlaw.
- To understand the cyber attacks and tools for mitigating them.
- To understand information gathering.
- To learn how to detect a cyber attack.
- To learn how to prevent a cyber attack.

UNIT I   INTRODUCTION   6

Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for Cyber Crime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

UNIT II   ATTACKS AND COUNTERMEASURES   6

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures.

UNIT III   RECONNAISSANCE   5

Harvester – Whois – Netcraft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches – SYN – Stealth – XMAS – NULL – IDLE – FIN Scans – Banner Grabbing and OS Finger printing Techniques.

UNIT IV   INTRUSION DETECTION   5

Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.

UNIT V   INTRUSION PREVENTION   5

Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations – Intrusion Prevention Systems – Example Unified Threat Management Products.

30 PERIODS

PRACTICAL EXERCISES: **30 PERIODS**
1. Install Kali Linux on Virtual box
2. Explore Kali Linux and bash scripting
3. Perform open source intelligence gathering using Netcraft, Whois Lookups, DNS Reconnaissance, Harvester and Maltego
4. Understand the nmap command d and scan a target using nmap
5. Install metasploitable2 on the virtual box and search for unpatched vulnerabilities
6. Use Metasploit to exploit an unpatched vulnerability
7. Install Linus server on the virtual box and install ssh
8. Use Fail2banto scan log files and ban Ips that show the malicious signs
9. Launch brute-force attacks on the Linux server using Hydra.
10. Perform real-time network traffic analysis and data pocket logging using Snort

COURSE OUTCOMES:
On successful completion of this course, the student will be able to
CO1: Explain the basics of cyber security, cyber crime and cyber law (K2)
CO2: Classify various types of attacks and learn the tools to launch the attacks (K2)
CO3 Apply various tools to perform information gathering (K3)
CO4: Apply intrusion techniques to detect intrusion (K3)
CO5: Apply intrusion prevention techniques to prevent intrusion (K3)

TOTAL:60 PERIODS

TEXTBOOKS
1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021 (Unit 1)
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publishers, 2011 (Unit 1)
3. https://owasp.org/www-project-top-ten/

REFERENCES
1. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013 (Unit 2)
2. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011 (Unit 3)
3. Kimberly Graves, "CEH Official Certified Ethical hacker Review Guide", Wiley Publishers, 2007 (Unit 3)
4. William Stallings, Lawrie Brown, "Computer Security Principles and Practice", Third Edition, Pearson Education, 2015 (Units 4 and 5)
5. Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking", No Starch Press, 2014 (Lab)

COs- PO's & PSO's MAPPING

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
1	1	1	1	1	-	1	-	-	-	-	1	-	2	2

2	1	3	1	3	2	1	-	-	-	-	-	-	2	2
3	2	1	1	1	-	1	-	-	-	-	1	-	2	2
4	3	3	2	2	2	1	-	-	-	-	-	-	2	2
5	3	2	1	1	1	1	-	1	-	-	1	-	2	2
AVg.	2	2	1.2	1.6	1	1	0	0.2	0	0	0.6	0	2	2

1 - low, 2 - medium, 3 - high, '-' - no correlation

CCS359	**QUANTUM COMPUTING**	L T P C
		2 0 2 3

COURSE OBJECTIVES:
- To know the background of classical computing and quantum computing.
- To learn the fundamental concepts behind quantum computation.
- To study the details of quantum mechanics and its relation to Computer Science.
- To gain knowledge about the basic hardware and mathematical models of quantum computation.
- To learn the basics of quantum information and the theory behind it.

UNIT I   QUANTUM COMPUTING BASIC CONCEPTS   6
Complex Numbers - Linear Algebra - Matrices and Operators - Global Perspectives Postulates of Quantum Mechanics – Quantum Bits - Representations of Qubits - Superpositions

UNIT II   QUANTUM GATES AND CIRCUITS   5
Universal logic gates - Basic single qubit gates - Multiple qubit gates - Circuit development - Quantum error correction

UNIT III   QUANTUM ALGORITHMS   7
Quantum parallelism - Deutsch's algorithm - The Deutsch–Jozsa algorithm - Quantum Fourier transform and its applications - Quantum Search Algorithms: Grover's Algorithm

UNIT IV   QUANTUM INFORMATION THEORY   6
Data compression - Shannon's noiseless channel coding theorem - Schumacher's quantum noiseless channel coding theorem - Classical information over noisy quantum channels

UNIT V   QUANTUM CRYPTOGRAPHY   6
Classical cryptography basic concepts - Private key cryptography - Shor's Factoring Algorithm - Quantum Key Distribution - BB84 - Ekart 91

30 PERIODS

PRACTICAL EXERCISES   **30 PERIODS**
1.   Single qubit gate simulation - Quantum Composer
2.   Multiple qubit gate simulation - Quantum Composer
3.   Composing simple quantum circuits with q-gates and measuring the output into classical bits.
4.   IBM Qiskit Platform Introduction
5.   Implementation of Shor's Algorithms
6.   Implementation of Grover's Algorithm
7.   Implementation of Deutsch's Algorithm
8.   Implementation of Deutsch-Jozsa's Algorithm
9.   Integer factorization using Shor's Algorithm