ALAGAPPA UNIVERSITY

(A State University Established in 1985)

Karaikudi - 630003. Tamil Nadu, India

2017 Accredited with A+ Grade by NAAC (CGPA : 3.64)

2018 MHRD Govt. of India UGC Granted as Category - I & Graded Autonomy

2018 MHRD Swachh Campus Rank : 4

2021 nirf National Institutional Ranking Framework Rank : 33

2021 QS University Rankings Asia Rank : 199

FACULTY OF EDUCATION

ALAGAPPA INSTITUTE OF SKILL DEVELOPMENT

PG DIPLOMA IN CYBER SECURITY

REGULATIONS AND SYLLABUS

(For the candidates admitted from the Academic Year 2022 - 2023)

ALAGAPPA INSTITUTE OF SKILL DEVELOPMENT
ALAGAPPA UNIVERSITY, KARAIKUDI.
SYLLABUS UNDER CBCS PATTERN (w.e.f. 2018-19)

Post-Graduate Diploma in Cyber Security (Course Code: 248)

Degree	Sem	Subject code	Course Name	Credits		Hrs./ Week	Marks		Total
				Skill	General		Int.	Ext	
PG Diploma in Cyber Security	I	2248101	**Core – I** – Introduction to Communication Networks and Security	--	4	4	25	75	100
		2248102	**Core – II** – Principles of Cyber Forensics	-	4	4	25	75	100
		2248103	**Core-III-** Security Operations and Countermeasures	--	4	4	40	60	100
		2248104	**Core – IV** – Risk Management and Security Auditing	-	4	4	40	60	100
		2248105	**Core – V** – **Practical –** Security Counterintelligence Lab	-	5	5	25	75	100
		2248106	**Core – VI** – **Practical –** Security Architecture and Engineering Lab	-	5	5	25	75	100
		2248501/ 2248502	**Elective – I**	-	4	4	25	75	100
			Sub-Total		**30**	**30**			**700**
			Total for Semester - I	**30**		**30**	**--**	**--**	**700**
	II	2248201	**Core – VII** – Information Security Standards & Cyber Laws	-	4	4	25	75	100
		2248202	**Core – VIII** – **Practical –** Security Assessment &Penetration Testing Lab	-	6	6	25	75	100
		2248999	**Core –IX** – Industrial Internship with Project	-	20	20	25	75	100
			Sub-Total	-	**30**	**30**			**300**
			Total for Semester – II	**30**		**30**	**--**	**--**	**300**

Elective – I

1. Wireless Network Forensics	–	2248501
2. Virus Programming	–	2248502

Semester-I					
CORE	Course Code 2248101	Introduction to Communication Networks and Security	T	C	H/W
				4	4

Unit -I		
Objective1	To know the fundamental concepts of big data and analytics.	
Principles of Communication Networks and Media Basics of Communications: Analog vs. Digital Signals - Basic Data Communications Links - Circuit Sharing (Multiplexing) - Data compression. Wired media and technologies: Twisted- Pair - Coaxial Cable - Fiber Optic Cable. LAN- Topologies, Ethernet, Token Ring, Fiber, COAX, CAT5e, CAT6. Wireless media and technologies: Modes of Wireless Cellular Radio Protocols - Microwave - Satellite - GPS - Cellular technology.		
Outcome 1	Work with big data tools and its analysis techniques	K1&K2
Unit - II		
Objective 2	To explore tools and practices for working with big data	
Architecture, Models and Standards Architecture and Standards - Layered models – OSI Model - The TCP/IP model – Protocols in each layers in OSI and TCP/IP models – IP Addressing – Classifications - Routing - Network Connectivity Basics – Topology – Network equipment – Reach of networks – Connectivity in networks – Firewalls – Network storage. VOIP: Introduction- VoIP architecture and Protocols- Threats and Attacks-VoIP Vulnerabilities-VoIP and Network security controls.		
Outcome 2	Analyze data by utilizing clustering and classification algorithms	K3
Unit - III		
Objective 3	To learn about stream computing.	
Broadband Technology and Wireless Networks Networks for large areas – WAN Technologies - Putting a Graphical Interface on the Internet Protocols - Access Points to the Internet. Wireless Networks: Traditional Wireless Formats WAN or LAWN - Wireless Broadband Technologies - Wireless Metropolitan Area Networks - Wireless Wide Area Networking – Wireless Networking issues and management. WAN - Carrier, Authentication, Tunnelling, Packet and Circuit Switching. The raise of Software Defined Networks (SDN)		
Outcome 3	Learn and apply different mining algorithms and recommendation systems for large volumes of data	K4
Unit IV		
Objective 4	To know about the research that requires the integration of large amounts of data.	
Network Security Risk Assessment – Disaster planning – Network security - Parameters of a Valuable Network- Power for Network Equipment - Security Issue Threats and Responses - Prevention Measures – Disaster recovery – Next generation virus defense		
Outcome 4	Perform analytics on data streams	K3&K6
Unit-V		
Objective5	To know about the database and Management	
Cloud Computing and Security Cloud Computing - PaaS, SaaS, IaaS, Hybrid Cloud, Private and Public Cloud. Cloud Security – Software as a Service Security – Standards for application developers –Ajax, XML, JSON, LAMP, LAPP – Standards for Messaging –SMTP, POP, IMAP, HTTP, SIMPLE, XMPP – Standards for Security –SAML oAuth, OpenID, SSL/TLS, Collaborating via Blogs and Wikis – Mobile Platform Virtualization –KVM, VMWare		
Outcome 5	Learn NoSQL databases and management	K5&K6

Suggested Readings:

Mike Chapple, James Michael Stewart and Darril Gibson (2018), "CISSP Certified Information Systems Security Professional Official Study Guide" , Eighth Edition, Sybex (A Wiley Brand)

Houston H. Carr, Charles A. Snyder (2006), "Data Communications and Network Security", McGraw-Hill Education.

Behrouz A. Forouzan (2017), "Data Communications and Networking", (5th ed.), McGraw-Hill, Inc.,

John W.Rittinghouse and James F.Ransome (2012), "Cloud Computing – Implementation, Management and Security", CRC press.

Online Resources:

1. **https://www.researchgate.net**
2. **https://www.azdocuments.in**

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-I					
CORE	Course Code 2248102	Principles of Cyber Forensics	T	C	H/W
				4	4

Unit -I		
Objective1	To know the fundamental concepts of big data and analytics	
Introduction to Cybercrime Introduction – Definition-Role of Electronic Communication Devices and ICT-Types of Cybercrime -Classifications of Cyber Criminals –Execution of Cybercrime-Tools used in Cybercrime-Strategies to prevent Cybercrimes -Extent of Cyber crime		
Outcome 1	Work with big data tools and its analysis techniques	K1&K2
Unit - II		
Objective 2	To explore tools and practices for working with big data	
Classification of Cybercrime Cyber Crime against Individuals- Cyber Crime against Property-Cyber Crime against Nation-Introduction to Cyber War-Crypto currency –Bitcoin – Ethereum – Blockchain - Ransomware- Deep web and Dark Web - Challenges		
Outcome 2	Analyze data by utilizing clustering and classification algorithms.	K3
Unit - III		
Objective 3	To learn about stream computing	
Introduction to Cyber Forensics Security-Cyber Forensics-Disk Forensics-Network Forensics-Wireless Forensics, Database Forensics-Malware Forensics-Mobile Forensics-GPS Forensics-Email Forensics-Memory Forensics		
Outcome 3	Understand and demonstrate the role of statistics in the analysis of large of datasets	K4
Unit- IV		
Objective 4	To know about the research that requires the integration of large amounts of data.	
Cyber Forensics – The Present and Future Forensics Tools-Cyber Forensics Suite-Drive Imaging and Validation Tools-Forensic Tools for Data Recovery- Forensic Tools for RAM Analysis- Forensic Tools for Analysis of Registry- Forensic Tools for Encryption/Decryption- Forensic Tools for Password Recovery- Forensic Tools for Analysing Networks-Forensic Tools for Meta data processing-E mail Analysis-Need for Computer Forensic Investigators		
Outcome 4	Understand and demonstrate advanced knowledge of statistical data analytics as applied to large data sets	K3&K6
Unit-V		
Objective5	To know about the Hadoop	
Digital Evidence Introduction to Digital evidence and Collection procedure-Sources of Evidence-Digital Evidence from computers-Storage Medium-File System-Windows Registry-Windows Artifacts-Browser Artifacts-Macintosh Artifacts-Linux Artifacts-Digital Evidence on Internet- Challenges with Digital Evidence		
Outcome 5	Select and apply suitable statistical measures and analyses techniques for data of various structure and content and present summary statistics.	K5&K6
Suggested Readings: Dejey, Murugan (2018), “*Cyber Forensics*"– Oxford HigherEducation		

Online Resources:

1. https://www.unodc.org
2. https://www.geeksforgeeks.org

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-I					
CORE	Course Code 2248103	Security Operations and Countermeasures	T	C	H/W
				5	4
Unit -I					
Objective1	To know the basics of Programming				
Fundamentals of Ethical Hacking – Building Your Hack Box: Hardware for Hacking - Gentoo Linux - Arch Linux – Debian - Ubuntu - Kali Linux - Firewall - Password Manager - Setting Up Virtual Box - Virtualization Settings. Bash Scripting: Ping – A Simple Bash Script – Conditional and looping in Bash scripting – Python scripting fundamentals					
Outcome 1	Develop algorithmic solutions to simple computational problems				K1&K2
Unit - II					
Objective 2	To convert an algorithm into a Python program				
Open Source Intelligence Gathering: OSINT Review - OSINT Tools - Grabbing Email Addresses from Google - Google Dorking the Shadows - A Brief Introduction to Passwd and Shadow Files - The Google Hacking Database - OSINT Framework Recon-ng - Recon-ng Under the Hood - Harvesting the Web - Document Metadata - Maltego - Social Media Networks - Shodan - Protecting Against OSINT. Information Gathering: Netcraft - Whois Lookups - DNS Reconnaissance - Searching for Email Addresses – Maltego - Port Scanning: Manual and using Nmap					
Outcome 2	Develop and execute simple Python programs.				K3
Unit - III					
Objective 3	To construct Python programs with control structures.				
Vulnerabilities: The Domain Naming System (DNS) - Implications of Hacking DNS - Electronic Mail: protocols and vulnerabilities - The Nmap Scripting Engine - CVE-2014- 0160: The Heartbleed Bug - Exploiting CVE-2010-4345. The World Wide Web of Vulnerabilities - Vulnerabilities in Virtual Private Networks					
Outcome 3	Develop simple Python programs for solving problems.				K4
Unit IV					
Objective 4	To structure a Python Program as a set of functions				
Foot printing, Scanning, Enumeration, Email Analysis and Spam Mails, Proxy Servers, Spoofing, Banner Grabbing, Social Engineering, Sniffers, Session Hijacking, Defending Virus, Defending Trojans, Backdoor ,Rootkits and Worms, Keyloggers, Cross Site Scripting.(XSS), Cross Site Request Forgery (CSRF) Countermeasures, OWASP Top 10 Vulnerabilities, IP Tracing Hunting Hackers					
Outcome 4	Structure a Python program into functions.				K3&K6
Unit-V					
Objective5	To use Python data structures-lists, tuples, dictionaries.				
Assets Security: Controls - Admin /Management, Physical, Technical - Access Control – Threats - Logging and Accountability - Identity and Access Management (IAM) - Biometrics, Kerberos, SESAME, SAML, MFA and Attacks. Security Operations: Business Continuity – Recovery – Contingency – RAID – Backups - Evidence and Investigations - Power, Media Control - Change Management					
Outcome 5	Read and write data from/to files in Python Programs				K5&K6

Suggested Readings:

Matthew Hickey, Jennifer Arcuri (2020), "Hands-on Hacking", Willy

Georgia Weidman (2014), "Penetration Testing – A Hands-On Introduction to Hacking", No Starch Press, San Francisco

Mike Chapple, James Michael Stewart and Darril Gibson (2018), "CISSP Certified Information Systems Security Professional Official Study Guide" , Eighth Edition, Sybex (A Wiley Brand)

Ankit Fadia (2006), "Ethical Hacking", (2nd ed.), Macmillan India Ltd

Ethical Hacking and Countermeasures: Threats and Defense Mechanisms Ec-Council Press Series: Certified Ethical Hacker, EC- Council(2009)

Online Resources:

1. **https://link.springer.com**
2. **https://www.mdpi.com**

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-I					
CORE	**Course Code** **2248104**	**Risk Management and Security Auditing**	**T**	**C**	**H/W**
				5	**4**
Unit -I					
Objective1	**To Open RStudio. Identify the Console, Script, Environment, and Plots pane.**				
Personnel Security Policies and Procedures - Security Governance - Understand and Apply Risk Management Concepts - Establish and Maintain a Security Awareness, Education and Training program - Manage Security Function					
Outcome 1	**Show the installation of R Programming Environment**				**K1&K2**
Unit - II					
Objective 2	**To Create a ‘Gap Minder’ style plot.**				
Building a Security Assessment and Testing Program - Performing Vulnerability Assessment - Testing your software - Implementing Security Management Process					
Outcome 2	**Utilize and R Data types for developing programs.**				**K3**
Unit - III					
Objective 3	**To Create univariate visualizations with two different R packages.**				
Assessments: NIST 800-53A, System Specifications, Mechanisms, Activities, Individuals. Audits: COBIT, Security, Internal, External, Third Party. DREAD Risk Assessment Model. Frameworks: COBIT, ITIL, COSO, ISO/IEC 270001					
Outcome 3	**Make use of different R Data Structures.**				**K4**
Unit IV					
Objective 4	**To dentify books, websites, and additional sources for further learning and help.**				
The Principles of Auditing - Auditing Tools and Techniques - Auditing Cisco Security Solutions-Policy, Compliance, and Management					
Outcome 4	**Develop programming logic using R Packages.**				**K3&K6**
Unit-V					
Objective 5	**To Load a Workspace containing an R dataframe, edit the dataset, and save the Workspace.**				
Infrastructure Security - Perimeter Intrusion Detection and Prevention - Access Control. Secure Remote Access - Endpoint Protection -Unified Communications					
Outcome 5	**Analyze the datasets using R programming capabilities.**				**K5&K6**

Suggested Readings:

Mike Chapple, James Michael Stewart and Darril Gibson (2018), "CISSP Certified Information Systems Security Professional Official Study Guide", Eighth Edition, Sybex (A Wiley Brand)

Chris Jackson, "Network Security Auditing", O'Reilly, Cisco Press (2010) ISBN: 9781587053528 (https://www.oreilly.com/library/view/network-security- auditing/9781587059407/)

https://www.azeusconvene.com/wp-content/uploads/white-papers/Cybersecurity-Risk- Management.pdf

Online Resources:

1. https://www.techtarget.com
2. https://www.cert-in.org.in

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

<table>
<tr><th colspan="6">Semester-I</th></tr>
<tr><td rowspan="2">CORE</td><td>Course Code</td><td rowspan="2">Security Counterintelligence Lab</td><td rowspan="2">P</td><td>C</td><td>H/W</td></tr>
<tr><td>7BD1G1</td><td>5</td><td>5</td></tr>
<tr><td colspan="6">Unit -I</td></tr>
<tr><td>Objective1</td><td colspan="5">To Identify and comprehend the needs, preferences, and behaviors of the target market</td></tr>
<tr><td colspan="6">1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis, SQL Injection Attacks, XSS, CSRF.</td></tr>
<tr><td>Outcome 1</td><td colspan="4">Identify, define and analyse problems and identify or create processes to solve them</td><td>K1&K2</td></tr>
<tr><td colspan="6">Unit - II</td></tr>
<tr><td>Objective 2</td><td colspan="5">To Evaluate the strengths, weaknesses, strategies, and market positioning of competitors to identify opportunities and threats</td></tr>
<tr><td colspan="6">1. Password guessing and Password Cracking.
2. Wireless Network attacks, Bluetooth attacks
3. Firewalls, Intrusion Detection and Honey pots</td></tr>
<tr><td>Outcome 2</td><td colspan="4">Identify and apply new ideas, methods and ways of thinking</td><td>K3</td></tr>
<tr><td colspan="6">Unit - III</td></tr>
<tr><td>Objective 3</td><td colspan="5">To Recognize and capitalize on market trends, unmet needs, and emerging opportunities for growth</td></tr>
<tr><td colspan="6">1. Malware – Key logger, Trojans, Key logger countermeasures
2. Understanding Data Packet Sniffers – Wireshark, CACE Pilot, TCP dump/Win Dump, Network View, The Dude Sniffer, Ace, Capsa Network Analyzer.</td></tr>
<tr><td>Outcome 3</td><td colspan="4">Demonstrate skills in time management</td><td>K4</td></tr>
<tr><td colspan="6">Unit IV</td></tr>
<tr><td>Objective 4</td><td colspan="5">To Assess the efficiency and effectiveness of distribution channels to ensure products reach the target audience</td></tr>
<tr><td colspan="6">1. Implementing Web Data Extractor and Web site watcher. Hacking Web Application
2. Programming and Reverse Engineering - Basics of coding in Ruby</td></tr>
<tr><td>Outcome 4</td><td colspan="4">Work effectively with others, capitalizing on their different thinking, experience and skills</td><td>K3&K6</td></tr>
<tr><td colspan="6">Unit-V</td></tr>
<tr><td>Objective5</td><td colspan="5">To Assess the efficiency and effectiveness of distribution channels to ensure products reach the target audience</td></tr>
<tr><td colspan="6">1. Simple application with OWASP Juiceshop / DVWA
2. Simple application with Web Services Security (AWS)</td></tr>
<tr><td>Outcome 5</td><td colspan="4">Exercise critical judgement in creating new understanding.</td><td>K5&K6</td></tr>
</table>

Suggested Readings:

Security Analysis, Seventh Edition: Principles and Techniques Hardcover – Import, 18 July 2023 by Benjamin Graham (Author), David Dodd (Author), Seth A. Klarman (Author)

Lab Notes Guide To Lab And Diagnostic Tests by Tracey Hopkins, F.A. Davis Company Books from same Author: Tracey Hopkins

Online Resources:

1. **https://sandia.gov**
2. **https://en.wikipedia.org**

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-I					
CORE	**Course Code** **2248106**	**Security Architecture and Engineering Lab**	**T**	**C**	**H/W**
				5	**5**

Unit -I		
Objective1	**To Apply logical checks to ensure data accuracy, consistency, and reliability before analysis**	
1. Study Bell-LaPadula Access Control Model and implement multi-level security on a database security and perform auditing. • Ensure information confidentiality • Propose solution to Trojan Horse • Analyze Simple Security property and Star Property		
Outcome 1	**Analyze and evaluate the cyber security needs of an organization**	**K1&K2**
Unit - II		
Objective 2	**Formulate and test hypotheses using mathematical logic to validate or refute assumptions about data patterns.**	
1. Control Secrecy and Integrity with Biba Model. 2. Study Exercise on other Models and compare their performances • Access Matrix/Lattice • Clark-Wilson • Brewer-Nash • Graham-Denning		
Outcome 2	**Measure the performance and troubleshoot cyber security systems.**	**K3**
Unit - III		
Objective 3	**To understand market segmentation, targeting, mapping market structure and product design**	
1. Review the TCSEC Orange Book. Prepare a consolidated report on security assessment of hardware products of different vendors. 2. Study Experiment - Securing data at the application level with PKI (https://blog.cloudflare.com/how-to-build-your-own-public-key-infrastructure/)		
Outcome 3	**Conduct a cyber-security risk assessment.**	**K4**
Unit IV		
Objective 4	**To understand the Parameters of a Valuable Network**	
1. Use GPG, OpenSSL to demonstrate symmetric and asymmetric encryption/decryption and MD5, SHA1 to demonstrate hash functions. 2. Study ITSEC and understand the purpose behind Functionality Rating and Assurance Rating.		
Outcome 4	**Implement cyber security solutions.**	**K3&K6**

Unit-V

Objective5	**To know about the Mobile Platform Virtualization**	

1. Demonstrate Steganography with a simple application.

2. Implement as a Service - Confidentiality, Integrity, Authentication, Authorization, Non-repudiation

Outcome 5	**Identify the key cyber security vendors in the marketplace.**	**K5&K6**

Suggested Readings:

Security Analysis, Seventh Edition: Principles and Techniques Hardcover – Import, 18 July 2023 by Benjamin Graham (Author), David Dodd (Author), Seth A. Klarman (Author)

Lab Notes Guide To Lab And Diagnostic Tests by Tracey Hopkins, F.A. Davis Company Books from same Author: Tracey Hopkins

Online Resources:

1. **https://sandia.gov**
2. **https://en.wikipedia.org**

K1- Remember	K2-Understand	K3 - Apply	K4 - Analyze	K5 - Evaluate	K6 – Create

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-II					
CORE	**Course Code**	**Information Security Standards & Cyber Laws**	**T**	**C**	**H/W**
	2248201			**4**	**4**
Unit -I					
Objective1	**To provide comprehensive knowledge to address fundamental marketing decision problems**				
Security basics, legal response to security, legal standard for compliance, developing a compliant security program, security controls, role of standards					
Outcome 1	**Understand the theory and basis of data analytics (including computing, statistics and mathematics) to be able to apply in the practice of data analytics.**				**K1&K2**
Unit - II					
Objective 2	**To Provide strong core training so that graduates can adapt easily to changes and new demands from industry.**				
Governance and risk management, IT regulatory Compliance, Information and Continuity risk, Internal control frameworks, Project Governance, Components of IT Governance, ISO/IEC 38500, IT Governance Frameworks and Standards, The Calder- Moir Framework, Implementing IT Governance.					
Outcome 2	**Identify, locate, evaluate, collect, compile and responsibly (ethically, legally, socially, professionally, and securely) use data and associated materials from multiple sources relevant for Data Analytics**				**K3**
Unit - III					
Objective 3	**To Enable students to understand not only how to apply certain methods, but when and why they are appropriate.**				
Build and maintain a secure network, Protect Card holder Data, Maintain a vulnerability Management programme, Implement strong access control measures, regularly monitor and test networks, maintain an Information security policy.					
Outcome 3	**Customize and utilize data analytics and data management software packages in order to manage and apply exploratory, descriptive and inferential data analytics techniques to complex data sets**				**K4**
Unit IV					
Objective 4	**To Integrate fields within computer science, optimization, and statistics to create adept and well-rounded data scientists.**				
Modern Era : the Scene and Problems – Need for Cyber Laws – Impact of Internet & Information Technology – The Character and Use of Internet Technologies.					
Outcome 4	**Appropriately define Data problems, formulate questions, develop and design an analysis plan, and interpret the results of these analyses.**				**K3&K6**
Unit-V					
Objective5	**To Expose students to real-world problems in the classroom and through experiential learning.**				
Reorganization of Electronic Records - UNICITRAL Model Law, Legal Aspects of Electronic Records / Digital Signatures - UNICITRAL Model Law, UNICITRAL Model Law :relating TO THE retention of Data Messages, Attributes of Data Messages, Acknowledgement of Data Messages, Time and Place receipt of Data Messages – Securing Electronic Record and electronic / Digital Signature in India – Verification of electronic Signature in India.					
Outcome 5	**Work with a team of students in consultation with a client to apply a full range of Data Analytics techniques drawn from computer science, mathematics and statistics to address a real-world application problem.**				**K5&K6**

Suggested Readings:

Thomas J. Smedinghoff ,Information Security Law: The Emerging Standard for Corporate Compliance

Kevin Beaver , Rebecca Herold, The Practical Guide to HIPAA Privacy and Security Compliance

James M Barrow,PCI Compliance: Level 1 Merchant Guide for DSS version 2.0

Harish Chander ,Cyber Law & IT Protection, Eastern Economy Edition

Jonathan Rosenor.Cyber Law : the law of Internet Mark F Grady, FransescoParisi, The Law and Economics of Cyber Security

Online Resources:

1. **https://books.google.com**
2. **https://www.scribd.com**

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-II					
CORE	**Course Code** **2248202**	**Security Assessment & Penetration Testing Lab**	**P**	**C**	**H/W**
				6	**6**
Unit -I					
Objective1	**To Ensure the accuracy and reliability of data through the use of constraints and relationships.**				
1. Network Mapping & Target Identification 2. Interpreting Tool Output - Interpreting output from port scanners, network sniffers and other network enumeration tools.					
Outcome 1	**Analyze and evaluate the high data integrity through the enforcement of constraints and the use of ACID properties.**.				**K1&K2**
Unit - II					
Objective 2	**To Maintain a consistent and coherent view of the data, adhering to predefined rules and constraints.**				
1. Filtering Avoidance Techniques - The importance of egress and ingress filtering, including the Risks associated with outbound connections. 2. Packet Crafting - Packet crafting to meet a particular requirement.					
Outcome 2	**The structured nature of RDBMS helps maintain consistency and accuracy of data through well-defined schemas.**				**K3**
Unit - III					
Objective 3	**To Provide a standardized and powerful query language (SQL) for easy retrieval and manipulation of data.**				
1. OS Fingerprinting - Remote operating system fingerprinting; active and passive techniques. 2. Network Access Control Analysis - Reviewing firewall rule bases and network access control lists.					
Outcome 3	**SQL provides a powerful and standardized language for interacting with the database.**				**K4**
Unit IV					
Objective 4	**To Ensure that transactions are processed reliably and adhere to the ACID properties.**				
1. File System Permissions a. File permission attributes within Unix and Windows file systems and their security implications. b. Analyzing registry ACLs 2. Configuration Analysis - Analyzing configuration files from the following types of Cisco equipment:					
Outcome 4	**Normalization reduces data redundancy, leading to more efficient storage and minimizing update anomalies.**				**K3&K6**
Unit-V					
Objective5	**To Implement access control mechanisms to secure the database and restrict unauthorized access.**				
1. Unix Security Assessment a. User enumeration- Discovery of valid usernames from network services commonly running bydefault. b. Unix vulnerabilities - Common post-exploitation activities c. FTP - FTP access control Anonymous access to FTP servers Risks of allowing write access to anonymoususers d. Send mail / SMTP - Valid username discovery via EXPN Awareness of recent Send mail vulnerabilities; ability to exploit them if possible . Mail relaying					

2. Web Testing Techniques
    a. Web Site Structure Discovery
    b. Cross Site Scripting Attacks
    c. SQL Injection
    d. Session ID Attacks
    e. Data Confidentiality &Integrity
    f. Directory Traversal
    g. Code Injection

Application Logic Flaws

Outcome 5	**RDBMS has a mature and well-established ecosystem with a wide range of tools and technologies.**	**K5&K6**

Suggested Readings:

Ivan Bayross, “SQL,PL/SQL The programming language of Oracle”, 3rd revised edition,BPB Publications, 2010

Kevin Loney, Bob Bryla, Oracle Database 12c: The Complete Reference, Oracle Press2013

Karl Seguin, “The Little MongoDB Book”, 10gen Corporation, 2014

Online Resources:

1. **https://theqalead.com**
2. **https://www.secura.com**

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-II					
CORE	**Course Code** **2248999**	**Industry Internship With Project**	**P**	**C**	**H/W**
				20	**20**
Unit -I					
Objective1	**To Identify underlying patterns and structures within the dataset that may not be apparent when analyzing variables individually.**				

Theme of the Project: Security Auditing

The student has to attach himself / herself with an organization related to his / her specialization approved by the (Alagappa Institute of Skill Development) Department for a period of two months for Industrial Internship Training with Project. One personnel of that industry and a faculty of the Department will be external and internal guides of the project respectively. The project theme, work flow and other related guidelines can be had from the Industry. During this Internship period there will be one “Project Reviews” conducted by the Department and the students must present themselves in person and present the project progress in the form of presentation in front of the internal guide. At the end of the internship, the student should prepare a project documentation report (not less than 50 pages, A4 size). Student should also produce a certificate of internship from the organization. The internal guide will award for 100 marks based on the performance in project review and the quality of the project documentation report. The external guide (industry personnel) of the particular student will award for 50 marks. The cumulative of these two marks for 150 will be considered as Internal mark. The final project viva-voce for 50 marks will be conducted by the Department with two examiners and the cumulative 200 marks will be given by the Department.

Description	**Department**	**Industry**	**Total Marks**
Internal Marks	**50**	**25**	**75**
Viva- Voce	**25**	**--**	**25**
Total	**75**	**25**	**100**

Outcome 1	**Multivariate techniques provide a deeper understanding of complex relationships between variables, allowing for more comprehensive insights**	**K1&K2**

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

<table>
<tr><td colspan="6">Semester-II</td></tr>
<tr><td rowspan="2">DSE-I</td><td rowspan="2">Course Code
2248501</td><td rowspan="2">Wireless Network Forensics</td><td rowspan="2">T</td><td>C</td><td>H/W</td></tr>
<tr><td>4</td><td>4</td></tr>
<tr><td colspan="6">Unit -I</td></tr>
<tr><td>Objective1</td><td colspan="5">To Enable systems to scale horizontally to handle massive amounts of data.</td></tr>
<tr><td colspan="6">NETWORK FORENSICS AND INVESTIGATING LOGS
Introduction and Investigating Logs-Network Forensics-Log files as Evidence-Why Synchronize Computer Times. network traffic investigations: Introduction -Network addressing Schemes--Overview of Network Protocols-Types of Network Attacks-Evidence gathering at the Physical Layer-DNS Positioning Techniques-Evidence gathering from ARP Table-Evidence Gathering at the Data Link Layer-Gathering Evidence from IDS</td></tr>
<tr><td>Outcome 1</td><td colspan="4">Improved system performance and responsiveness as data volume grows.</td><td>K1&K2</td></tr>
<tr><td colspan="6">Unit - II</td></tr>
<tr><td>Objective 2</td><td colspan="5">Process and analyze data in real-time or near-real-time for immediate insights.</td></tr>
<tr><td colspan="6">WEB ATTACK INVESTIGATIONS
Types of Web Attack-Overview of Web OSI Reference Model Logs-Investigating a Web Attack-Investigating FTP Server-Investigating IIS Logs- Investigating Apache Logs- Investigating Web Attacks in Windows based Server-Web page defacement-Security Strategies for Web Applications- investigating Static and Dynamic IP Addresses-Tools for Web attack Investigation-Tools for Locating IP Addresses. router forensics: Functions of a Router-Router vulnerabilities-Router Attacks-Router forensics Vs Traditional Forensics-
Investigating Router Attacks-Using Specialized E-Mail Forensics Tools-Laws against E-Mail Crime.</td></tr>
<tr><td>Outcome 2</td><td colspan="4">Quick decision-making and responsiveness to changing conditions or events.</td><td>K3</td></tr>
<tr><td colspan="6">Unit - III</td></tr>
<tr><td>Objective 3</td><td colspan="5">To Integrate and consolidate data from various sources, including structured and unstructured data.</td></tr>
<tr><td colspan="6">WEB SECURITY
Web Security, Email Security, Virtual Private Network, Incident response.</td></tr>
<tr><td>Outcome 3</td><td colspan="4">Comprehensive and unified view of the data for analysis.</td><td>K4</td></tr>
<tr><td colspan="6">Unit IV</td></tr>
<tr><td>Objective 4</td><td colspan="5">To Distribute data processing across multiple nodes to improve performance and reduce processing time.</td></tr>
<tr><td colspan="6">WIRELESS ATTACK INVESTIGATIONS:
Wireless Network technologies-Wireless Attacks-Network Forensics in Wireless Environment PDA forensics: Information stored in PDAs-Palm OS-Windows CE-PDA Generic States-PDA Security Issues-PDA Forensics Steps-PDA Security Counter Measures</td></tr>
<tr><td>Outcome 4</td><td colspan="4">Efficient utilization of resources and faster data processing.</td><td>K3&K6</td></tr>
</table>

Unit-V		
Objective5	**To Establish policies and procedures for data management, quality, and compliance.**	
IPOD AND IPHONE FORENSICS iPod and iPhone Forensics-Jail Breaking-Tools for iPod and iPhone Forensics blackberry forensics : Blackberry Security-Blackjacking Attacks- Blackberry Forensics-Additional Blackberry Forensics Tools		
Outcome 5	**Advanced analytics on Big Data yield actionable insights, helping organizations identify opportunities, mitigate risks, and optimize processes.**	**K5&K6**
Suggested Readings: EC-Council (2016), "Computer Forensics : Investigating Network Intrusions and Cyber Crime", Cengage Learning EC-Council (2009), "Computer Forensics: Investigating Wireless Networks and Devices", Cengage Learning Eoghan Casey (2009), "Handbook of Digital Forensics and Investigations", Elsevier Academic Press EC-Council (2010), "Network Defense: Security and Vulnerability Assessment", Cengage Learning		
Online Resources: 1. **https://www.simplilearn.com** 2. **https://www.azdocuments.in**		

K1- Remember	**K2-Understand**	**K3 - Apply**	**K4 - Analyze**	**K5 - Evaluate**	**K6 – Create**

Course Outcome VS Programme Outcomes

CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

Semester-II					
DSE-II	Course Code 7BD2C2	Virus Programming	T	C	H/W
				4	4
Unit -I					
Objective1	To Develop a comprehensive understanding of advanced algorithms used in analytics.				
Introduction – Definitions – Malware Defined - Virus Activity and Operation – Virus Mechanisms.					
Outcome 1	Acquire knowledge about algorithms like machine learning, deep learning, clustering, and optimization.				K1&K2
Unit - II					
Objective 2	To Explore and understand the application of machine learning algorithms in various domains..				
Anti-Malware technology – Malware Management – Risk and Incident management – User Management					
Outcome 2	Understand the principles behind deep learning and its applications in tasks like image recognition and natural language processing.				K3
Unit - III					
Objective 3	To Learn algorithms specific to time series analysis for forecasting and trend analysis.				
Virus Origin and Distribution – Meta viruses, Hoaxes and Related Nuisances – Taxonomy, Techniques and Tools.					
Outcome 3	Acquire skills to analyze and model time-dependent data.				K4
Unit IV					
Objective 4	To Explore algorithms for processing and analyzing human language data.				
Computer viruses in interpreted programming language – Companion viruses - Worms					
Outcome 4	Understand how to extract insights from text data, including sentiment analysis and topic modeling.				K3&K6
Unit-V					
Objective5	To Study algorithms for graph analytics, including centrality, community detection, and link prediction.				
Computer Viruses and Applications – BIOS Viruses – Applied Cryptanalysis of Cipher Systems.					
Outcome 5	Analyze and model relationships in complex networks.				K5&K6

Suggested Readings:

Michael Sikorski and Andrew Honig (2012) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious software

ÉricFiliol (2005) Computer Viruses: from theory to applications (Collection IRIS), Springer-Verlag France

David Harley, Urs E. Gattiker and Eugene H. Spafford (2001), “Viruses Revealed”,

McGraw-Hill / Osborne

Peter Szor (2005) “The Art of Computer Virus Research and Defense”, Addison-Wesley Professional

Online Resources:

1. https://en.wikipedia.org
2. https://www.geeksforgeeks.org

K1- Remember	K2-Understand	K3 - Apply	K4 - Analyze	K5 - Evaluate	K6 – Create

Course Outcome VS Programme Outcomes

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M(2)	S(3)	S(3)	M(2)	L(1)	L(1)	M(2)	S(3)	M(2)	M(2)
CO2	L(1)	M(2)	S(3)	M(2)	M(2)	L(1)	M(2)	S(3)	M(2)	L(1)
CO3	S(3)	L(1)	M(2)	S(3)	S(3)	M(2)	S(3)	L(1)	M(2)	M(2)
CO4	L(1)	L(1)	S(3)	M(2)	M(2)	M(2)	S(3)	M(2)	S(3)	L(1)
CO5	M(2)	M(2)	L(1)	L(1)	S(3)	M(2)	S(3)	M(2)	M(2)	S(3)
W.AV	**1.8**	**1.8**	**2.4**	**2**	**2.2**	**1.6**	**2.6**	**2.4**	**2.2**	**1.8**

S–Strong (3), M-Medium (2), L-Low (1)

Mapping Course Outcome VS Programme Specific Outcomes

CO	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	M(2)	S(3)	M(2)	L(1)	M(2)
CO2	S(3)	M(2)	S(3)	M(2)	L(1)
CO3	L(1)	M(2)	M(2)	S(3)	L(1)
CO4	M(2)	S(3)	L(1)	M(2)	M(2)
CO5	M(2)	S(3)	M(2)	M(2)	M(2)
W.AV	**2**	**2.6**	**2**	**2**	**1.6**

S–Strong (3), M-Medium (2), L-Low (1)

EDUCATION CAMPUS