JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

Vision and Mission of the University

VISION

The University is primarily promoting quality of education in the areas of Science, Technology, Engineering and Mathematics (STEM) as four academic pillars of education, to excel in teaching, learning, research, consultancy and placements through innovative practices with global perspective.

MISSION

1. Design an Industry relevant curriculum from time to time with a Global perspective
2. Promoting quality education by embracing ICT delivery mechanism with continuous pedagogy through e-learning mechanism
3. Spread across for industry collaborations with a focus to pre-training and placements for technology transfer to society
4. Establishing centers of excellence to promote research and innovations in multidisciplinary areas to bring in patent culture and consultancy practices
5. International Collaborations for student outreach
6. Facilitating international students to study in JNTUK to infuse cross culture learning practices.

Vision and Mission of the Institute

Vision and Mission of the Department

Programme Education Objectives (PEOs) of the M.Tech CSE(Cyber Security)

PEO1: Graduates will possess deep technical knowledge and problem-solving skills to design, develop, and deploy secure computing systems, networks, and applications.

PEO2: Graduates will apply research and innovation to solve emerging cyber security challenges in cloud, IoT, AI, data privacy, and biometric security.

PEO3: Graduates will uphold legal, ethical, and societal responsibilities while ensuring privacy, safety, and security in the cyber domain.

Mapping of Mission statements to PEOs

Mission Statement	PEO1	PEO2	PEO3
MS1	✓	✓	
MS2	✓	✓	
MS3		✓	
MS4	✓		
MS5	✓	✓	
MS6			✓

Programme Outcomes (POs)

PO1: An ability to independently carry out research /investigation and development work tosolve practical problems.

PO2: An ability to write and present a substantial technical report/document.

PO3: Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: Apply computational, mathematical, and analytical skills to design and implement secure computing solutions.

PO5: Design and evaluate effective security solutions for diverse cyber threats.

PO6: Conduct cyber investigations and risk management in compliance with legal and ethical standards**.**

Note: Program may add up to three additional POs

Mapping of Programme Outcomes to PEOs

	PO1	PO2	PO3	PO4	PO5	PO6
PEO1	L	M	H	H	H	M
PEO2	L	M	H	H	H	M
PEO3	M	L	M	M	H	H

M.TECH

CSE (CYBER SECURITY)

PROGRAMME COURSE STRUCTURE & SYLLABUS

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

Programme Structure

I Semester

S.No	Course Title	L	T	P	C
1	**Program Core-1** Mathematical Foundations for Security	3	1	0	4
2	**Program Core-2** Advanced Data Structures	3	1	0	4
3	**Program Core-3** Principles of Cyber Security	3	1	0	4
4	**Program Elective-1** • Operating System Security • Firewall and VPN Security • Intrusion Detection	3	0	0	3
5	**Program Elective-2** • Database and Web Application Security • Secure Software Design and Development • Wireless Network Security	3	0	0	3
6	**Laboratory-1** Advanced Data Structures Lab	0	1	2	2
7	**Laboartory-2** Cyber Security Lab	0	1	2	2
8	**Seminar-1**	0	0	2	1
	Total Credits	15	5	6	23

List of Professional Elective Courses in I Semester (Electives – I & II)

S.No.	Course Title
1	Operating System Security
2	Firewall and VPN Security
3	Intrusion Detection
4	Database and Web Application Security
5	Secure Software Design and Development
6	Wireless Network Security

@ Minimum 2/3 themes per elective

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester

S.No	Course Title	L	T	P	C
1	**Program Core-4** • Vulnerability Assessment and Penetration Testing	3	1	0	4
2	**Program Core-5** • Malware Analysis & Reverse Engineering	3	1	0	4
3	**Program Core-6** • Cyber Crime Investigation & Digital Forensics	3	1	0	4
4	**Program Elective-3** • Cloud and IoT Security • AI for Cyber security • Data Privacy	3	0	0	3
5	**Program Elective-4** • Principles of Secure Coding • Security Assessment and Risk Analysis • Biometric Security	3	0	0	3
6	**Laboratory-3** • Vulnerability Assessment and Penetration Testing Lab	0	1	2	2
7	**Laboartory-4** • Digital Forensics Lab	0	1	2	2
8	**Seminar-2**	0	0	2	1
	Total Credits	15	5	6	23

*During the summer break, students need to pursue Summer Internship/ Industrial Training, it will be evaluated in the III Sem.

List of Professional Elective Courses in II Semester (Electives III & IV)

S.No.	Course Title
1	Cloud and IoT Security
2	AI for Cyber security
3	Data Privacy
4	Principles of Secure Coding
5	Security Assessment and Risk Analysis
6	Biometric Security

@ Minimum 2/3 themes per elective

III Semester

Sl. No.	Course Title	L	T	P	C
1	Research Methodology and IPR / *Swayam 12 week MOOC course – RM&IPR*	3	0	0	3
2	Summer Internship/ Industrial Training (8-10 weeks)*	-	-	-	3
3	Comprehensive Viva#	-	-	-	2
4	Dissertation Part – A$	-	-	20	10
	TOTAL	**3**	**-**	**20**	**18**

* Student attended during summer / year break and assessment will be done in 3rd Sem.
# Comprehensive viva can be conducted courses completed upto second sem.
$ Dissertation – Part A, internal assessment

IV Semester

S. No.	Course Title	L	T	P	C
1	Dissertation Part – B%	-	-	32	16
	TOTAL	**-**	**-**	**32**	**16**

% External Assessment

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	MATHEMATICAL FOUNDATIONS FOR SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

1. To understand the mathematical fundamentals in probabilistic and statistical concepts
2. To develop the understanding of the mathematical and logical basis of various modern techniques in information technology like machine learning, programming language design, and concurrency.
3. To study various Graph Theory problems.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Understand the basic notions of discrete and continuous probability	K2
CO2	Apply the methods of statistical inference, and learn application of sampling distributions in Data mining and Machine Learning	K2, K3
CO3	Apply statistical analysis to algorithmic problems of simple to moderate complexity in different domains	K3
CO4	Model different applications of Computer science as graph theory problems	K2, K3
CO5	Evaluate modular exponentiation for cryptographic applications.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		M	H		
CO2	H		H	H	M	
CO3	H		H	H	M	
CO4			H	H	M	
CO5			M	H	H	M

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Density, and cumulative distribution functions, Expected value, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains.	12
UNIT –	Random samples, sampling distributions of estimators, and Maximum	12

2	Likelihood	
UNIT – 3	Statistical inference, Introduction to multivariate statistical models: classification problems, principal component analysis, The problem of over fitting model assessment	12
UNIT – 4	Graph Theory: Isomorphism, Planar graphs, graph coloring, Hamilton circuits and Euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems	12
UNIT – 5	Number Theory: Elementary number theory, unique factorization, Euler's function, modular arithmetic, Fermat's little theorem, Chinese remainder theorem, modular exponentiation, RSA public key encryption	12
	Total	60

Text Books:

1. John Vince, Foundation Mathematics for Computer Science, Springer, 2015.
2. K. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Wiley, 2001.

Reference Books:

1. M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, 2005.
2. Alan Tucker, Applied Combinatorics, Wiley, 2012.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	ADVANCED DATA STRUCTURES	L	T	P	C
		3	1	0	4

Course Objectives: The course is taught with the objectives of enabling the student to:

- Understand the ADT/libraries and choose appropriate data structures to design algorithms for a specific problem.
- Understand the necessary mathematical abstraction to solve problems.
- To familiarize students with advanced problem-solving paradigms and data structure used to solve algorithmic problems.
- Analysis of efficiency and proof of correctness

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Understand the implementation of symbol table using hashing techniques	K2
CO2	Develop and analyze algorithms for red-black trees, B-trees and Splay trees.	K3
CO3	Develop algorithms for text processing applications.	K3
CO4	Identify suitable data structures and develop algorithms for computational geometry problems.	K3
CO5	Use k-d trees for multi-dimensional search problems.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		M	H		
CO2	H		H	H		
CO3	H		H	H		
CO4	H		H	H		
CO5	H		H	H		

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Dictionaries: Definition, Dictionary Abstract Data Type, Implementation of Dictionaries. Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.	12

UNIT – 2	Skip Lists: Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists.	12
UNIT – 3	Trees: Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees	12
UNIT – 4	Text Processing: String Operations, Brute-Force Pattern Matching, The Boyer-Moore Algorithm. The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem	12
UNIT – 5	Computational Geometry: One Dimensional Range Searching, Two-Dimensional Range Searching, constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad trees, k-D Trees.	12
	Total	60

Text Books:

1. Data Structures: A Pseudo-code Approach, 2/e, Richard F.Gilberg, BehrouzA.Forouzon, Cengage
2. Data Structures, Algorithms and Applications in java, 2/e, SartajSahni, University Press

Reference Books:

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
2. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	PRINCIPLES OF CYBER SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

- To learn threats and risks within context of the cyber security architecture.
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply cyber security architecture principles	K3
CO2	Describe risk management processes and practices	K2
CO3	Appraise cyber security incidents to apply appropriate response	K4
CO4	Distinguish system and application security threats and vulnerabilities	K4
CO5	Identify security tools and hardening techniques	K1

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M		H	M
CO2	H		M		H	H
CO3	M		M	H	H	
CO4	M		M	H	H	M
CO5						

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction to Cyber security- Cyber security objectives, Cyber security roles, Differences between Information Security & Cyber security, Cyber security Principles-Confidentiality, integrity, &availability Authentication & non- repudiation.	12
UNIT – 2	Information Security (IS) within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate lifecycle management concepts, Risks & Vulnerabilities-Basics of risk management, Operational threat environments, Classes of attacks.	12
UNIT – 3	Incident Response- Incident categories, Incident responseIncident recovery, and Operational security protection: Digital and data assets, ports and protocols, Protection technologies, Identity and access	12

	Management, configuration management.	
UNIT – 4	Threat Detection and Evaluation (DE):Monitoring- Vulnerability Management, Security Logs and Alerts, Monitoring Tools and Appliances. Analysis- Network traffic Analysis, packet capture and analysis	12
UNIT – 5	Introduction to backdoor System and security-Introduction to metasploit, Backdoor, demilitarized zone(DMZ),Digital Signature, Brief study on Harding of operating system.	12
	Total	60

Text Books:

1. NASSCOM: Security Analyst Student Hand Book Dec 2015.
2. Information Security Management Principles **Updated Edition** by David Alexander, Amanda Finch, David Sutton ,Published by BCS, June 2013.

Reference Books:

1. CSX- cyber security fundamentals 2 nd edition, Published by ISACA, Cyber security, Network Security, Data Governance Security.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	OPERATING SYSTEM SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Students will learn and apply basic concepts and methodologies of System Administration and Security by building from the ground up a miniature corporate network.
- To know some basic security measures to take in system administration.
- To prepare for possible disasters, including an understanding of backup and restoration of file systems.

Course Outcomes:

On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain the overview of operating system	K2
CO2	Demonstrate the Access control matrix, access control list and Lampson's access matrix	K3
CO3	Identify the Encryption Techniques, Authentication and Password Security issues	K2
CO4	Identify the Encryption Techniques and apply the real time applications	K3
CO5	Know the role and responsibilities of a system administrator and Create and administer user accounts on both a Linux and Windows platform	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M			
CO2	M		M	H	H	
CO3	M		M	H	H	M
CO4	H		M	H	H	M
CO5	M		M	H	H	

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT –	Overview of Operating Systems-Introduction, Computer system	12

1	organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Inter-process Communication(TB1)	
UNIT – 2	Operating Systems Protection: Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition(TB2)	12
UNIT – 3	Operating System Security-Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defences, UNIX and Windows security(TB2)	12
UNIT – 4	System Administration: Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment.(TB3)	12
UNIT – 5	Linux Networking: Networking Technologies: DHCP, DNS, NFS/ISCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. Case Studies: Security and Protection-MULTICS, UNIX, LINUX and Windows, Windows and Linux Coexisting.(TB4)	12
	Total	60

Text Books:

1. Operating System Concepts, 9th Edition, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley Publication, 2008
2. Operating Systems: A Concept-Based Approach, 3rd Edition, Dhananjay M. Dhamdhere, McGraw- Hill, 2015
3. Windows Server 2003 Security, A Technical Reference, Roberta Bragg, Addisson-Wesley
4. Linux Administration Handbook, Second Edition, Evi Nemeth, Garth Snyder, Trent R. Hein. Prentice Hall

Reference Books:

1. An Introduction to Operating Systems: Concepts and practice, 4th Edition, Promod Chandra P Bhat, Prentice Hall of India, 2014.
2. Operating System: Internals and Design Principles, 7th Edition, William Stalling, Prentice Hall, 2014Linux System Administration, Tom Adelstein and Bill Lubanovic, First Edition, O'Reilly Media, Inc.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	FIREWALL AND VPN SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	To show the fundamental knowledge of Firewalls and it types	K1
CO2	Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization	K3
CO3	Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection	K2
CO4	Infer the design of Control Systems of SCAD, DCS, PLC's and ICS's	K4
CO5	Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		M	H	H	
CO2	H		H	H	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	M		H	H	H	M

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Firewall Fundamentals: Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed	12

	and Triple-Homed Firewalls, Placement of Firewalls.	
UNIT – 2	VPN Fundamentals: VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, Digital Certificates, VPN Authorization.	12
UNIT – 3	Exploring the Depths of Firewalls: Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements, and Management Interfaces	12
UNIT – 4	Overview of Industrial Control Systems: Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies.	12
UNIT – 5	SCADA Protocols: Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis- Stuxnet, Duqu.	12
	Total	60

Text Books:

1. Michael Stewart “Network Security, Firewalls, and VPNs” Jones & Bartlett Learning September 2010.
2. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.
3. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.

Reference Books:

1. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
2. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. CRC Press, 2013.
3. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.D. Bailey, Practical SC

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	INTRUSION DETECTION	L	T	P	C
		3	0	0	3

Course Objectives:

The outcome of this course is to:

● Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.

● Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.	K3
CO2	Evaluate the security of an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security	K3
CO3	Classify intrusion detection systems and apply signature- and anomaly-based detection techniques.	K3
CO4	Analyze and implement Snort rules, installation procedures, and alert modes for intrusion detection.	K4
CO5	Evaluate advanced IDS models, malware detection methods, and security issues including insider threats and future collaborative defense strategies.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	M	H	M
CO2	H		H	H	H	H
CO3	M		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	The state of threats against computers, and networked Systems-Overview of computer security solutions and why they Fail-Vulnerability assessment, firewalls, VPN's –Overview of Intrusion	12

	Detection and Intrusion Prevention- Network and Host-based IDS.	
UNIT – 2	Classes of attacks – Network layer: scans, denial of service, penetration – Application layer: software exploits, code Injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, Viruses.	12
UNIT – 3	A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS Anomaly Detection Systems and Algorithms-Network Behaviour Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection.	12
UNIT – 4	Attack trees and Correlation of Alerts-Autopsy of Worms and Botnets-Malware Detection-Obfuscation, Polymorphism-Document vectors. Email/IM security Issues-Viruses/Spam-From signatures to thumbprints to zero day. Detection-Insider Threat Issues-Taxonomy Masquerade and Impersonation-Traitors, Decoys and Deception-Future: Collaborative Security.	12
UNIT – 5	Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes	12
	Total	60

Suggested Readings:

1. Szor, P. (2010). The Art of Computer Virus Research and Defense, United States: Symantec Press.
2. Jakobsson, M., and Ramzan, Z. (2008). Crimeware, Understanding New Attacks and Defenses,United States: Symantec Press.
3. Research Articles from SCI & Scopus indexed Journals.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	DATABASE AND WEB APPLICATION SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To design security applications in the field of Information technology.
- To understand the fundamentals of database design, DB security and SQL extensions to security.
- To learn the basic concepts of Penetration testing.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain threats, vulnerabilities and breaches to design database	K2
CO2	Discuss Relational Data Model and concurrency controls and locking, SQL extensions to security	K2
CO3	Demonstrate the Browser security principles.	K3
CO4	How to provide software centric security and mobile web browser security in real time applications	K3
CO5	Construct the penetrating testing workflows with examples.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H	H	M
CO2	M		H	H	H	
CO3	M		H	H	H	M
CO4	H		H	H	H	M
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Database security**-Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security, concepts, approaches and challenges, types of access controls, Oracle VPD. **Discretionary and Mandatory access control**-Principles, applications and poly instantiation, Database inference problem, types of inference attacks, distributed database, security levels, **SQL-injection:** types and	12

	advanced concepts	
UNIT – 2	**Relational Data Model-**Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, secure data outsourcing.	12
UNIT – 3	**Web application security-**Basic principles and concepts, Authentication, Authorization, Browser security principles; XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 -Detailed treatment, IoT security.	12
UNIT – 4	**Mobile device security**-Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security. **Application security:** Concepts, CIA Triad, Hexad, types of cyber-attacks, Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers.	12
UNIT – 5	**Penetration testing-**Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates.	12
	Total	60

Text Books:

1. Bryan and Vincent, “Web Application Security, A Beginners Guide ”,McGraw-Hill, 2011
2. Alfred Basta, Melissa Zgola, “Database Security”, Course Technology, 2012.

Reference Books:

1. Michael Gertz and SushilJajodia, “Handbook of Database Security— Applications and Trends”, Springer, 2008.
2. Bhavani Thuraisingham, “Database and Applications Security”, Integrating Information Security and Data Management, Auerbach Publications, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	SECURE SOFTWARE DESIGN AND DEVELOPMENT	L	T	P	C
		3	0	0	3

Course Objectives:

- To fix software flaws and bugs in various software.
- To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic.
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Differentiate between various software vulnerabilities.	K4
CO2	Explain the Software process vulnerabilities for an organization.	K2
CO3	Demonstrate the Monitor resources consumption in software.	K3
CO4	Explain the Interrelate security and software development process.	K2
CO5	Discuss the Case study of DNS server, DHCP configuration and SQL injection attack.	K2

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H	H	M
CO2	M		H	H	H	
CO3	M		H	H	H	M
CO4	H		H	H	H	M
CO5	H		H	H	H	H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Secure Software Design-**Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.	12
UNIT – 2	**Enterprise Application Development**- Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation,	12

	business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.	
UNIT – 3	**Enterprise Systems Administration-**Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services(DNS/DHCP/Terminal Services/Clustering/Web/Email).	12
UNIT – 4	Obtain the ability to manage and troubleshoot a network running multiple services, understand the requirements of an enterprise network and how to go about managing them.	12
UNIT – 5	Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws, Case study of DNS server, DHCP configuration and SQL injection attack.	12
	Total	60

Text Books:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	WIRELESS NETWORK SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the concepts of network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.
- Student should learn and Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX and Windows NT.
- To learn and understand wireless technologies and apply real time applications

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain the History of wireless Technologies and Rogue Network Access Points	K2
CO2	Demonstrate the wireless LAN Security Protocols and SSL/TLS	K3
CO3	Describe the concepts of FDMA,GSM Security and Algorithm Analysis	K2
CO4	Explain Current and Future Technologies and Standards	K2
CO5	Identify the Basic specifications in Bluetooth Security.	K1

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	H
CO3	M		H	H	H	M
CO4	M		H	M	H	
CO5	M		H	M	H	M

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Introduction to Wireless**: History of Wireless Technologies, History of Wireless Security, State of the Wireless Security Industry, **Wireless Threats:** Uncontrolled Terrain, Communications Jamming, DoS Jamming, Injections and Modifications of Data, Man-in-the-Middle (MITM) Attack, Rogue Client, Rogue Network Access Points, Attacker Equipment, Covert Wireless Channels, Roaming Issues, Cryptographic Threats	12
UNIT –	**Introduction to Wireless Security Protocols and Cryptography:**	12

2	Recovery the FUD, OSI Model, OSI Simplified, Internet Model, Wireless LAN Security Protocols, Cryptography, SSL/TLS, Secure Shell Protocols, Terminal Access and File Transfer, Port Forwarding a Word of Caution,Man-in-the-Middle of SSL/TLS and SSH, WTLS, WEP,802.1x, IP Security. **Security Considerations to Wireless Devices:** Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure	
UNIT – 3	**Wireless Technologies and Applications:** Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats, GSM Security, GSM Algorithm Analysis. **Introduction to Wireless Data Networks:** Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex- Mobitex Architecture, Mobitex Security Architecture, General Packet Radio Service (GPRS)- GPRS Architecture, Security Issues, Introduction to the Wireless Application Protocol (WAP)- WAP Device, Gateway, Security Model	12
UNIT – 4	**Wireless Standards and Technologies:** Current and Future Technologies- Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802, 802.11, The ABC's of 802.11, 802.11b, 802.11a, 802.11g, 802.11j, 802.11h and 5GPP, 802.11e, 802.11i, 802.11f, IEEE 802.15, IEEE 802.16, IEEE 802.1x, ETSI, Home RF, Ultra wideband Radio (UWB). **Wireless Deployment Strategies:** Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing Design, Small Office/Home Office Design (SOHO)	12
UNIT – 5	**Bluetooth Security:** Basic specifications, Pico-nets, Bluetooth security architecture, Scatter-nets, Security at the baseband layer and link layer, Frequency hopping, Security manager, Authentication, Encryption, And Threats to Bluetooth security	12
	Total	60

Text Books:

1. Merritt Maxim and David Pollino, "Wireless Security", Osborne/McGraw Hill, New Delhi, 2005
2. Nichols and Lekka, "Wireless Security-Models, Threats and Solutions", Tata McGraw – Hill, New Delhi, 2006.
3. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

Reference Books:

1. BehrouzA.Forouzan, ―Cryptography & Network Security, Tata McGraw Hill, India, New Delhi, 2009.
2. William Stallings, ―Cryptography and Network Security, Prentice Hall, New Delhi, 2006.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	ADVANCED DATA STRUCTURES LAB	L	T	P	C
		0	1	2	2

Course Objectives:

From the course the student will learn

- Knowing about oops concepts for a specific problem.
- Various advanced data structures concepts like arrays, stacks, queues, linked lists, graphs and trees.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Identify classes, objects, members of a class and relationships among them needed for a specific problem.	K1
CO2	Examine algorithms performance using Prior analysis and asymptotic notations.	K4
CO3	Organize and apply to solve the complex problems using advanced data structures (like arrays, stacks, queues, linked lists, graphs and trees.)	K3
CO4	Implement B-Tree operations, perform binary tree traversals (DFT, BFT).	K3
CO5	Apply Kruskal's algorithm to find a minimum-cost spanning tree and analyze functions of Dictionary	K3

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	H		
CO2	M		H	H		
CO3	H		H	H		
CO4	M		H	H		
CO5	H		H	H		

- (Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment	CONTENTS
Experiment 1:	Implement Multi stacks.
Experiment 2:	Implement Double Ended Queue (Dequeues) & Circular Queues.
Experiment 3:	Implement various Recursive operations on Binary Search Tree.
Experiment 4:	Implement various Non-Recursive operations on Binary Search Tree.
Experiment 5:	Implement BFS for a Graph
Experiment 6:	Implement DFS for a Graph.
Experiment 7:	Implement Merge & Heap Sort of given elements.
Experiment 8:	Implement Quick Sort of given elements.

Experiment 9:	Implement various operations on AVL trees.
Experiment 10:	Implement B: Tree operations.
Experiment 11:	Implementation of Binary trees and Traversals (DFT, BFT)
Experiment 12:	Implement Krushkal's algorithm to generate a min-cost spanning tree.
Experiment 13:	Implement Prim's algorithm to generate a min-cost spanning tree.
Experiment 14:	Implement functions of Dictionary using Hashing.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

I Semester	CYBER SECURITY LAB	L	T	P	C
		0	1	2	2

Course Objectives:

- Student to get the knowledge about audit and information security management, which makes the student to get the real world experience.
- To learn and implement Data leakage in a website database

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Analyze and implement Audit security policy in windows environment, create a Demilitarized zone creation in Network environment	K4
CO2	Illustrate the Resource harvesting attack and mitigation, Window Patch management policy, Trojans and mitigation strategies	K2
CO3	Apply the knowledge of metasploit, Access control list creation and content filtering limiting the traffic	K3
CO4	Explain the Data leakage in a website database, Password policy and verification, Patch management using MBSA tool on windows machine	K2
CO5	Build an Audit Policy management, Media handling policy and event log analysis and Installation of Trojan, Network DOS attack and proof of bandwidth utilization	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H	H	H
CO2	M		H	H	H	H
CO3	M		H	H	H	H
CO4	M		H	H	H	M
CO5	H		H	H	H	H

2) (Please fill the above with Levels of Correlation, viz., L, M, H)

Exercise	CONTENTS
Exercise – 1:	Audit security policy implementation in windows environment.
Exercise – 2:	Create a Demilitarized zone creation in Network environment for information security.
Exercise – 3:	Implement Resource harvesting attack and mitigation.
Exercise – 4:	Implement Window Patch management policy.
Exercise – 5:	Knowing the Behaviour of Trojans and mitigation strategies.
Exercise – 6:	Create a metasploit and make it to implement.
Exercise – 7:	Access control list creation and content filtering limiting the traffic.
Exercise – 8:	Data leakage in a website database and preventive measures.

Exercise – 9:	Password policy implementations and verification.
Exercise – 10:	Patch management implementation using MBSA tool on windows machine
Exercise – 11:	Audit Policy management for users and computers log analysis.
Exercise – 12:	Media handling policy implementation and event log analysis.
Exercise – 13:	Installation of Trojan and study of different options.
Exercise – 14:	Network DOS attack and proof of bandwidth utilization and preventive steps.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	VULNERABILITY ASSESSMENT & PENETRATION TESTING	L	T	P	C
		3	1	0	4

Course Objectives:

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools.
- To understand the impact of hacking in real time machines.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain Penetration testing phases	K2
CO2	Illustrate information gathering methodologies	K2
CO3	Apply System Hacking Techniques in real time applications	K3
CO4	Describe Bypassing WLAN Authentication	K2
CO5	Analyze and test wireless network security using authentication bypass, attack simulation, and traffic analysis techniques.	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	M	H	M
CO2	M		H	M	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction-Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies	12
UNIT – 2	Information Gathering and Scanning-Information gathering methodologies- Foot printing, Competitive Intelligence- DNS Enumerations- Social Engineering attacks, Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS	12

	Fingerprinting- Enumeration.	
UNIT – 3	System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files, Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding- SQL Injection - Error- based, Union-based, Time-based, Blind SQL, Out-of-band. Injection Prevention Techniques.	12
UNIT – 4	Advanced System Hacking: Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Code, XSS - Stored, Reflected, DOM Based	12
UNIT – 5	**Wireless Pentest:** Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Misassociation, Wireless Hacking Methodology, Wireless Traffic Analysis	12
	Total	60

Text Books:

1. Kali Linux
2. Windows Penetration Testing, 1st Edition, By Wolf Halton, Bo Weaver, June 2016 ,Packt Publishing

Reference Books:

1. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing.
2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	MALWARE ANALYSIS & REVERSE ENGINEERING	L	T	P	C
		3	1	0	4

Course Objectives:

- To understand the purpose of computer infection program.
- To implement the covert channel and mechanisms.
- To test and exploit various malware in open source environment.
- To analyze and design the famous virus and worms.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Explain the characteristics of Malware and its effects on Computing systems.	K2
CO2	Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	K3
CO3	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	K4
CO4	Demonstrate the Malware functionalities.	K3
CO5	How to apply anti-reverse engineering in different Applications	K3

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	H
CO3	H		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Malware Basics**- General Aspect of Computer infection program, Non Self Reproducing Malware, How does Virus Operate, Virus Nomenclature, Worm Nomenclature, Recent Malware Case Studies.	12
UNIT – 2	**Basic Analysis-** Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries &	12

	Functions, PE Header File &Section.	
UNIT – 3	**Advanced Static & Dynamic Analysis**-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures.	12
UNIT – 4	**Malware Functionalities-**Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis.	12
UNIT – 5	**Reverse Engineering Malware (REM)**: REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV-Signatures.	12
	Total	60

Text books:

1. Michael Sikorski, Andrew Honig “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” publisher Williampollock

Reference Books:

1. ErciFiliol, “Computer Viruses: from theory to applications”, Springer, 1st edition, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	CYBER CRIME INVESTIGATION & DIGITAL FORENSICS	L	T	P	C
		3	1	0	4

Course Objectives:

- Able to identify security risks and take preventive steps
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Acquire the definition of computer forensics fundamentals.	K1
CO2	Describe the types of computer forensics technology	K2
CO3	Analyze various computer forensics systems.	K4
CO4	Illustrate the methods for data recovery, evidence collection and data seizure.	K2
CO5	Summarize duplication and preservation of digital evidence.	K2

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M		M
CO2	M		H	M		M
CO3	H		H	H		H
CO4	H		H	H		H
CO5	M		H	M		H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Introduction:** Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.	12
UNIT – 2	**Cyber Crime Issues**: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.	12

UNIT – 3	**Investigation:** Introduction to Cyber Crime Investigation, Investigation Tools, e-Discovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.	12
UNIT – 4	**: Digital Forensics:** Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.	12
UNIT – 5	**Laws And Acts:** Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.	12
	Total	60

Reference Books:

1. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics“, Tata McGraw-Hill, New Delhi, 2006.
   Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	**CLOUD AND IOT SECURITY**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

- Student learn and understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.
- Student learns differentKey components of Amazon Web Services, Cloud Backup and solutions.
- Student able to discuss the main threats and attacks on IoT products and services
- Be able to learn secure a connected IoT product from scratch.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Define Cloud Computing and memorize the different Cloud services and deployment models	K1
CO2	Assessing the financial, technological, and organizational capacity of employer's for actively initiating and installing cloud-based applications.	K5
CO3	Explain how IOT can be used in different Industries.	K2
CO4	Discuss how companies can plan for the future of technologies.	K2, K4
CO5	How to apply smart applications in real world.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**
CO1	M		H	M		M
CO2	M		H	M		M
CO3	H		H	H		H
CO4	H		H	H		H
CO5	M		H	M		H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Cloud Computing Fundamental-**Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds,	12

	role of virtualization in enabling the cloud	
UNIT – 2	**Cloud Applications-**Development environments for service development; Amazon, Azure, Google App. Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud	12
UNIT – 3	**The Internet of Things-**An Overview of Internet of things, Internet of Things Technology, behind IoTs Sources of the IoTs, M2M Communication, Examples OF IoTs, Design Principles For Connected Devices Internet Connectivity Principles, Internet connectivity, Application Layer Protocols: HTTP, HTTPS, FTP, Telnet	12
UNIT – 4	**IOT Design**-Business Models for Business Processes in the Internet of Things ,IoT/M2M systems LAYERS AND designs standardizations ,Modified OSI Stack for the IoT/M2M Systems ,ETSI M2M domains and High-level capabilities ,Communication Technologies, Data Enrichment and Consolidation and Device Management Gateway Ease of designing and affordability	12
UNIT – 5	**IOT Security Issues-** Secure constrained devices, Authorize and authenticate devices, Manage device updates, secure communication, Ensure data privacy and integrity, secure web, mobile, and cloud applications, Ensure high availability**,** Detect vulnerabilities and incidents, Manage vulnerabilities, Predict and preempt security issues.	12
	Total	60

Text Books:

1. Internet of Things: Architecture, Design Principles And Applications, Raj kamal, McGraw Hill Higher Education
2. Internet of Things, A. Bahgya and V. Madisetti, Univesity Press, 2015

Reference Books:

1. Gautam Shroff, Enterprise Cloud Computing Technology Architecture Applications
2. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach
3. IOT Security Issues by Alasdair Gilchrist, O'Reilly Publishers, 2017.
4. Tim Mather, Subra Kumara swamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	AI FOR CYBER SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The course is taught with the objectives of enabling the student to:

- Understand the importance of AI in cyber security and their limitations
- Understand detection methods for image spam and threat analysis
- Apply Time Series Analysis and Ensemble Modeling in practical applications
- Perform experiments Using Data Science to Catch Email Fraud and Spam

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply AI principles in cyber security and relevant applications	K3
CO2	Detection the threats and image spams and its impact	K4, K5
CO3	Apply the Time Series Analysis and Ensemble Modeling methods for practical applications	K3
CO4	Demonstrate the experiments Using Data Science to Catch Email Fraud and Spam	K3
CO5	Apply ML and data science methods to detect and prevent fraud in emails and networks.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H	H	M
CO2	H		H	H	H	H
CO3	H		H	H		
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	Introduction to AI for Cyber security Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms ofautomated learning, The characteristics of algorithm training and optimization, Introducing AI in the context of cyber security.	12
UNIT – 2	AI for Cyber security Arsenal Classification, Regression, Dimensionality reduction,Clustering, Speech recognition, Video	12

	anomaly detection, Natural language processing (NLP), Large-scale image processing, Social media analysisDetecting Cyber security Threats with AI, How to detect spam with Perceptrons, Image spam detection with Support Vector Machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, Spam detection adoptingNLP.	
UNIT – 3	Basics of Machine Learning in Cyber security, Delving into machine learning in the cyber security world, Different types of machine learning systems, Different data preparation techniques, Machine learning architecture, statistical models and machine learning models, Model tuning to ensure model performance and accuracy, Machine learning toolsTime Series Analysis and Ensemble Modeling Time series and its different classes, Time series decomposition, Analysis of time series in cyber security, Prediction of DDoS attack, Ensemble learning methods and voting ensemble methods to detect cyber-attacks.	12
UNIT – 4	Segregating Legitimate and Lousy URLs Understanding URLs and how they fit in the internet address scheme, Introducing malicious URLs, Looking at the different ways malicious URLs propagate, Using heuristics to detect malicious URLs, Using machine learning to detect malicious URLsKnocking Down CAPTCHAs Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Types of CAPTCHA, Solving CAPTCHAs with neural networks.	12
UNIT – 5	Fraud Prevention with Cloud AI Solutions How to leverage machine learning (ML) algorithms for fraud detection, How bagging and boosting techniques can improve an algorithm's effectiveness, How to analyze data with IBM Watson and JupyterNotebook,Using Data Science to Catch Email Fraud and Spam and Efficient Network Anomaly Detection Using k-means Fraudulent emails and spoofs, Types of email fraud, Spam detection using the Naive Bayes algorithm, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression.	12
	Total	60

Text Books:

1. Alessandro Parisi, Hands-On Artificial Intelligence for Cyber security: Implementsmart AIsystems for preventing cyber-attacks and detecting threats and network anomalies, Packt Publication, 2019.

Reference Books:

1. ClarenceChio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms O‟REILLY Publications, 2018.
2. McKinney, W Brij B. Gupta and Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication, 2019.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	DATA PRIVACY	L	T	P	C
		3	0	0	3

Course Objectives:

- The objective of this course is to create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals
- Student able to learn the concepts of confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Understand basic privacy concepts, data privacy attacks, access control models, and privacy policies in various domains.	K2
CO2	Analyze data explosion challenges and apply mathematical and protection models to safeguard personal information	K3, K4
CO3	Evaluate privacy protection techniques, disclosure control methods, and their strengths and weaknesses.	K5
CO4	Apply computational tools and methods to protect structured and textual data.	K3
CO5	Analyze web privacy issues and related legal protections under the Freedom of Information Act and search warrant requirements.	K4

- #Based on suggested Revised BTL
- Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	H		H	H	H	M
CO3	H		H	H	H	M
CO4	M		H	H	H	M
CO5	H		H	M	H	H

- (Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	**Introduction**- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc.	12

UNIT – 2	**Data explosion**- Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness, **Protection Models**- Null-map, k-map, Wrong map	12
UNIT – 3	**Survey of techniques**- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.	12
UNIT – 4	**Computation systems for protecting delimited data**- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.	12
UNIT – 5	**Technology, Policy, Privacy and Freedom**- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	12
	Total	60

Text Books:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation,1st Edition, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	**PRINCIPLES OF SECURE CODING**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

- Understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities.
- Knowledge of outline of the techniques for developing a secure application.
- Recognize opportunities to apply secure coding principles.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	List of secure systems and various security attacks	K1
CO2	Demonstrate the development of process of software leads to secure coding practices	K3
CO3	Apply Secure programs and various risk in the software's	K3
CO4	Classify various errors that lead to vulnerabilities	K4
CO5	Design Real time software and vulnerabilities	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**
CO1	M		H	M	H	M
CO2	H		H	H	H	M
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Introduction:** Need for secure systems, Proactive security development process, Security principles to live by and threat modelling.	12
UNIT – 2	**Secure Coding in C:** Character strings- String manipulation errors, String Vulnerabilities and exploits Mitigation strategies for strings, Pointers, Mitigation strategies in pointer based vulnerabilities Buffer Overflow based vulnerabilities	12
UNIT – 3	**Secure Coding in C++ and Java:** Dynamic memory management, Common errors in dynamic memory management, Memory managers,	12

	Double –free vulnerabilities, Integer security, Mitigation strategies	
UNIT – 4	**Database and Web Specific Input Issues:** Quoting the Input, Use of stored procedures, Building SQL statements securely, XSS related attacks and remedies	12
UNIT – 5	**Software Security Engineering:** Requirements engineering for secure software: Misuse and abuse cases, SQUARE process model Software security practices and knowledge for architecture and design	12
	Total	60

Text Book:

1. Michael Howard, David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition, 2003.

Reference Books:

1. Robert C. Seacord, “Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.
2. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security Engineering: A guide for Project Managers”, Addison-Wesley Professional, 2008.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	SECURITY ASSESSMENT AND RISK ANALYSIS	L	T	P	C
		3	0	0	3

Course Objectives

- Student able to learn basic concepts of risk management
- Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations.
- Able understand and discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Understand the concepts of contingency strategies including data backup and recovery and alternate site selection for business resumption planning	K2
CO2	Evaluate the escalation process from incident to disaster in case of security disaster.	K5
CO3	Analyze designing process of a Disaster Recovery and Business Continuity Plan for sustained organizational operations.	K4
CO4	Apply physical, personnel, and administrative security measures to safeguard organizational assets.	K3
CO5	implement OPSEC and INFOSEC principles, including cryptography, key management, and threat assessment, to protect information systems	K3, K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	H
CO2	H		H	M	H	H
CO3	H		H	H	H	H
CO4	M		H	H	H	M
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	**Security Basics**-Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security counter measures education, training and awareness, critical information 1characteristics – confidentiality critical information characteristics – integrity, information states – storage,	12

	information states – transmission, security counter measures policy, procedures and practices, threats, vulnerabilities.	
UNIT – 2	**Threats to and Vulnerabilities of Systems**: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment	12
UNIT – 3	**Security Planning: directives and procedures for policy mechanism, Risk Management:** acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation	12
UNIT – 4	**Policies And Procedures**: Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (need to know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing , Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs	12
UNIT – 5	**Operations Security (OPSEC):** OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography encryption (e.g., point to point, network, link), cryptography key management (to include electronic key),cryptography strength (e.g., complexity,	12

	secrecy, characteristics of the key) Case study of threat and vulnerability assessment	
	Total	60

Text Books:

1. Principles of Incident Response and Disaster Recovery, 1st Edition, Whitman & Mattord, Course Technology,2006

Web Link Reference:http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

- Introduce Bio-metric and traditional authentication methods.
- Describe the background theory and types of features used in biometric techniques and algorithms related to various biometrics.
- Evaluate the performance of various biometric systems.

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Describe the various modules constituting a bio-metric system. Compare and contrast the different bio-metric traits and appreciate their relative significance.	K2, K4
CO2	Classify the different feature sets used to represent some of the popular bio-metric traits.	K4
CO3	Evaluate and design security systems incorporating bio-metrics.	K5, K6
CO4	Use multi-biometric and multi-factor methods to authenticate and protect biometric data	K3
CO5	Analyze biometric technologies, applications, vulnerabilities, and legal aspects in various sectors.	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	M		H	M	H	M
CO2	M		H	H	H	M
CO3	H		H	H	H	H
CO4	H		H	H	H	H
CO5	H		H	M	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	Contact Hours
UNIT – 1	Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies. Introduction to Image Processing, Image Enhancement Techniques: Spatial Domain Methods: Smoothing, sharpening filters, Laplacian filters, Frequency domain filters, Smoothing and sharpening filters.	12
UNIT – 2	Image Restoration & Reconstruction: Model of Image Degradation/restoration process, Noise models, spatial filtering, inverse	12

	filtering, Minimum mean square Error filtering. Introduction to image segmentation: Image edge detection: Introduction to edge detection, types of edge detectors. Introduction to image feature extraction	
UNIT – 3	Bio-metric technologies: Fingerprint, Face, Iris, Hand Geometry, Gait recognition, Ear, Voice, Palm print, OnLine Signature Verification, 3D Face, Recognition, Dental Identification and DNA	12
UNIT – 4	The Law and the use of multi bio-metrics systems. Statistical measurement of Bio-metric. Bio-metrics in Government Sector and Commercial Sector. Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities. Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D face recognition and DNA matching.	12
UNIT – 5	Signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – dataacquisition - feature extraction - characteristics - strengths –weaknesses-deployment.Multi biometrics and multi factor biometrics - two-factor authenticationwith passwords - tickets and tokens – executive decision -implementation plan.	12
	Total	60

Suggested Readings:

1. 1.Reid, P. (2004). Biometrics for network security, Pearson Education.
2. 2.Maltoni, D., Maio, D., Jain, A.K., and Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer Verlag.
3. 3.Jain, A. K., Bolle, R., and Pankanti S. (1999). BIOMETRICS: Personal Identification in Networked Society. Kluwer Academic Publishers.
4. Wayman, J., Jain, A. K., Maltoni, D., and Maio D. (2004). Biometric Systems: Technology, Design and Performance Evaluation. Springer.
5. Jain, A. K., Ross, A. A., &kumar, K. N. (2011). Introduction to Biometric, Springer.
6. Jain, A. K., Maltoni, D., and Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Springer.
7. Gonzalez, R. C., and Woods, R. E. (2018). Digital Image Processing India: Person Education. 8. Research Articles from SCI & Scopus indexed Journals.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB	L	T	P	C
		0	1	2	2

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Perform penetration testing using systematic phases and industry-standard methodologies.	K3
CO2	Use specialized security tools to detect and analyze system, network, and web application vulnerabilities.	K3, K4
CO3	Exploit common vulnerabilities such as SQL injection, XSS, CSRF, and insecure file handling.	K3
CO4	Analyze network traffic, perform port scanning, and identify security weaknesses using packet analysis tools	K4
CO5	Demonstrate advanced exploitation techniques using frameworks, rootkits, and tunneling methods.	K3, K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	H	H	H
CO2	M		H	H	H	H
CO3	H		H	H	H	H
CO4	M		H	H	H	H
CO5	H		H	H	H	H

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment	CONTENTS
Experiment 1:	Implement penetration testing and phases of penetration testing
Experiment 2:	Make use of different types of tools available in kali and parrot O.S
Experiment 3:	Practice different SQL injection attacks
Experiment 4:	Implement and use GHDBC and Microsoft Vulnerabilities (Common CVE)
Experiment 5:	Implement Exploit insecure file handling, upload web shells, deface using upload file mechanism
Experiment 6:	Perform XSS attacks on client side application
Experiment 7:	Implement a case on actions on-behalf users by CSRF, Test websites for Clickjacking

Experiment 8:	Implement port scanning by using NMAP and other tools to find the open ports
Experiment 9:	Text for wire shark and tcp dumps to analyze various types of packets
Experiment 10:	Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating
Experiment 11:	Implement metasploit frameworks
Experiment 12:	Implement Trojan horse root kits backdoors
Experiment 13:	Practice ARP spoofing and buffer overflow exploitation with ETERCAP ANDSHELL'S
Experiment 14:	Perform Port Redirection, SSL Encapsulation - Stunnel, HTTP CONNECT Tunneling, Proxy Tunnel, SSH Tunneling.

List of open Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

II Semester	**DIGITAL FORENSICS LAB**	**L**	**T**	**P**	**C**
		0	**1**	**2**	**2**

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Apply forensic tools and techniques to recover deleted files and create forensic disk images.	K3
CO2	Collect, preserve, and analyze digital evidence from emails, browsers, and USB devices	K3, K4
CO3	Perform live forensic investigations using specialized tools to capture and analyze system activity	K3, K4
CO4	Analyze network traffic and packet data using Wireshark to extract forensic evidence.	K4
CO5	Use system monitoring tools to track processes, network activity, and memory usage for forensic purposes.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**
CO1	H		H	H		H
CO2	H		H	H		H
CO3	H		H	H		H
CO4	M		H	H		H
CO5	M		H	H		H

(Please fill the above with Levels of Correlation, viz., L, M, H)

Experiment	CONTENTS
Experiment-1	Study of Computer Forensics and different tools used for forensic investigation
Experiment – 2	How to Recover Deleted Files using Forensics Tools
Experiment – 3	How to make the forensic image of the hard drive using EnCase Forensics.
Experiment – 4	How to Collect Email Evidence in Victim PC
Experiment – 5	How to Extracting Browser Artifacts
Experiment-6	Find Last Connected USB on your system (USB Forensics)
Experiment-7	Live Forensics Case Investigation using Autopsy
Experiment-8	Capturing and analyzing network packets using Wireshark
Experiment-9	Analyze the packets provided in lab and solve the questions using Wireshark a) What web server software is used by www.uceou.com

	b) About what cell phone problem is the client concerned? c) How many webservers are running in Apache webserver.
Experiment-10	Using Sysinternals tools for Network Tracking and Process Monitoring • Check Sysinternals tools • Monitor Live Processes • Capture RAM • Capture TCP/UDP packets • Monitor Hard Disk • Monitor Virtual Memory • Monitor Cache Memory
Experiment-11	Email Forensics • Mail Service Providers • Email protocols • Recovering emails • Analyzing email header
Experiment-12	Analyzing data of android mobile using MOBILedit.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

R25 M.TECH CSE (CYBER SECURITY) SYLLABUS

III Semester	RESEARCH METHODOLOGY AND IPR	L	T	P	C
		3	0	0	3

Course Outcomes: On completion of this course, the student will be able to:

		Knowledge Level (K)#
CO1	Identify and formulate research problems, design investigative approaches, and apply appropriate data collection and analysis methods.	K3,K4
CO2	Conduct effective literature reviews, maintain research ethics, and prepare structured technical reports and research proposals.	K2,K6
CO3	Explain the nature and types of Intellectual Property Rights and processes for patenting innovations nationally and internationally.	K2
CO4	Analyze patent rights, licensing processes, technology transfer, and the use of patent databases.	K4
CO5	Evaluate recent developments in IPR, including biological systems, software, and traditional knowledge through case studies.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1	H		H	M		M
CO2	H	H	H			M
CO3	M		H			M
CO4	M		H			M
CO5	M		H			M
CO6						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT	CONTENTS	**Contact Hours**
UNIT – 1	Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations	12
UNIT – 2	Effective literature studies approaches, analysis Plagiarism, Research ethics, Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee	12
UNIT – 3	Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research,	12

	innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.	
UNIT – 4	Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.	12
UNIT – 5	New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.	12
	Total	60

REFERENCES:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
5. Mayall, "Industrial Design", McGraw Hill, 1992.
6. Niebel, "Product Design", McGraw Hill, 1974.
7. Asimov, "Introduction to Design", Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in NewTechnological Age", 2016.T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008.