Post Graduate Diploma in Cyber Security
Choice Based Credit System

Learning Outcome-based Curriculum Framework (LOCF)

for

Post Graduate Diploma in Cyber Security (PGDCS)

Session 2024-25
Exam Dec 2024 - June 2025

Department of Computer Science
Maharaja Ganga Singh University, Bikaner

Table of Contents

S.No.	Item	Page No
1	Background	3
2	Program Outcomes (POs)	5
3	Program Specific Outcomes (PSOs)	6
4	Post Graduate Attributes	6
5	Structure of Masters' Courses	7
6	Learning Outcome Index	9
7	Semester-wise Courses & Credit Distribution	11
8	Course Level Learning Outcomes	11
9	Teaching-Learning Process	29
10	Assessment & Evaluation	29

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Background

Considering the curricular reforms as instrumental for desired learning outcomes, all the academic departments of Maharaja Ganga Singh University Bikaner, made a rigorous attempt to revise the curriculum of postgraduate programs in alignment with National Education Policy-2020 and UGC Quality Mandate for Higher Education Institutions-2021. The process of revising the curriculum could be prompted with the adoption of the "Comprehensive Roadmap for Implementation of NEP-2020". The Roadmap identified the key features of the Policy and elucidated the Action Plan with well-defined responsibilities and an indicative timeline for major academic reforms.

The process of revamping the curriculum started with a series of webinars and discussions conducted by the University to orient the teachers about the key features of the Policy, enabling them to revise the curriculum in sync with the Policy. Proper orientation of the faculty about the vision and provisions of NEP-2020 made it easier for them to appreciate and incorporate the vital aspects of the Policy in the revised curriculum focused on creating holistic thoughtful, creative, and well-rounded individuals equipped with the key 21st-century skills 'for the development of an enlightened, socially conscious, knowledgeable, and skilled nation'.

With NEP-2020 in the background, the revised curricula articulate the spirit of the Policy by emphasising upon - an integrated approach to learning; innovative pedagogies and assessment strategies; multidisciplinary and cross-disciplinary education; creative and critical thinking; ethical and Constitutional values through value-based courses; 21st century capabilities across the range of disciplines through life skills, entrepreneurial and professional skills; community and constructive public engagement; social, moral, and environmental awareness; Organic Living and Global Citizenship Education (GCED); holistic, inquiry-based, discovery-based , discussion-based and analysis-based learning; exposure to Indian knowledge system, cultural traditions and literature through relevant courses offering "Knowledge of India, fine blend of modern pedagogies with indigenous and traditional ways of learning; flexibility in course choices, student-centric participatory learning; imaginative and flexible curricular structures to enable creative combinations of disciplines for study; offering multiple entry and exit points, alignment of Vocational courses with the International Standard Classification of Occupations maintained by the International Labor Organization; breaking the silos of disciplines; integration of extra-curricular and curricular aspects, exploring internships with local industry, businesses and artists and craft persons; closer collaboration between industry and higher education institutions for technical, vocational, and science programs, and formative assessment tools to be aligned with the learning outcomes, capabilities, and dispositions as specified for each course. The university has also developed a consensus on Blended Learning with 10% component of online teaching and 60% face-to-face classes for each program.

The revised curricula of various programs could be devised with concerted efforts of the faculty, Heads of the Departments, and the Deans of Schools of Study. The draft prepared by each department was discussed in a series of discussion sessions conducted at the Department, School, and University levels. The leadership of the University has been a driving force behind the entire exercise of developing the uniform template and structure for the revised curriculum. The Vice-Chancellor of the University conducted series of meetings with Heads and Deans to deliberate upon the vital parameters of the revised curriculum to

formulate a uniform template featuring Background, Programme Outcomes, Programme Specific Outcomes, Postgraduate Attributes, Structure of Masters Course, Learning Outcome Index, Semester-wise Courses and Credit Distribution, Course-level Learning Outcomes, Teaching-Learning Process, Blended Learning, Assessment and Evaluation, Keywords, References, and Appendices. The experts of various Board of Studies and School Boards contributed to a large extent in giving the final shape to the revised curriculum of each program.

To ensure the implementation of curricular reforms envisioned in NEP-2020, the University has decided to implement various provisions in a phased manner. Therefore, the curriculum may be reviewed annually so as to gradually include all relevant provisions of NEP-2020.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Program Outcomes

On completing Masters in the Faculty of Science, the students shall be able to realize the following outcomes:

PO1: Acquired knowledge with facts and figures related to various subjects in pure sciences such as Physics, Chemistry, Botany, Zoology, Mathematics, etc.
PO2: Understood the basic concepts, fundamental principles, and scientific theories related to various scientific phenomena and their relevance in day-to-day life.
PO3: Acquired the skills in handling scientific instruments, planning, and performing laboratory experiments The skills of observations and drawing logical inferences from the scientific experiments.
PO4: Analyzed the given scientific data critically and systematically and the ability to draw objective conclusions.
PO5: Been able to think creatively (divergent and convergent) to propose novel ideas in explaining facts and figures or providing new solutions to problems.
PO6: Realized how developments in any science subject help develop other science subjects and vice-versa and how interdisciplinary approach helps provide better solutions and new ideas for sustainable outcomes.
PO7: Developed scientific outlook concerning science subjects and all aspects related to life.
PO8: Realized that knowledge of subjects in other faculties such as humanities, performing arts, social sciences, etc., can have greatly and effectively influence, which inspires in evolving new scientific theories and inventions.
PO9: Imbibed ethical, moral, and social values in personal and social life, leading to a highly cultured and civilized personality.
PO10: Developed various communication skills such as reading, listening, speaking, etc., which will help express ideas and views clearly and effectively.
PO11: Realized that pursuit of knowledge is a lifelong activity and in combination with untiring efforts and positive attitude and other necessary qualities leads towards a successful life.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Program Specific Outcomes

On completing Masters in the M.Sc. in Computer Science, the students shall be able to realize the following outcomes:

PSO1. Communicate cyber security concepts, designs, and solutions effectively and professionally
PSO2. Apply knowledge of computing to produce effective designs and solutions for specific problems
PSO3. Use software development tools, software systems, and modern computing platforms to solve cyber security related issues
PSO4: To have the knowledge and the ability to develop creative solutions for security solutions
PSO5: To develop skills to learn new technology related to cyber security
PSO6: To develop critical reasoning
PSO7: To apply computer science theory and software development concepts to construct computing-based solutions
PSO8: To acquaint with computer programs/computer-based systems in the area related to algorithms, network security, web security, cloud security, Artificial Intelligence, Mobile and wireless security
PSO9: The ability to understand and use computer programs in the areas related to information security to design solutions of varying complexity
PSO10: The ability to understand the evolutionary changes in the security domain and to understand the real-world problems and meet the challenges of the future
PSO11: The ability to employ modern computer languages, environments, and platforms in creating innovative career paths to be an entrepreneur, lifelong learning and a zest for higher studies and also to act as a good citizen by inculcating in them moral values & ethics

Postgraduate Attributes

- Disciplinary Knowledge
- Creative & Critical Thinking
- Reasoning and Analytical abilities
- Logic/Discrete Mathematics knowledge
- Logical Thinking
- Problem analysis and solving abilities
- Life Skills
- Moral & Ethical Values
- Research Skills

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Structure of Masters' Programme

Session 2024-25

Semester I Exam Dec 2024										
	Course Code	**Course Title**	**Exam Hours**	**Max. Marks**		**Min. Marks**	**L**	**T**	**P***	**Credits**
				Int. Marks	**Ext. Marks**					
Core Courses										
1	FS-COMP-MSC-CY-CC-101	Introduction to Cyber Security	3	10	40	18 (36%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-102	Security Threats	3	10	40	18 (36%)	3	1	1	5
3	FS-COMP-MSC-CY-CC-103	Cyber Laws and Security Policies	3	10	40	18 (36%)	3	1	1	5
4	FS-COMP-MSC-CY-CC-104	Intrusion Detection and Prevention System	3	10	40	18 (36%)	3	1	1	5
5	FS-COMP-MSC-CY-CP-105	Combined Practical	3	25	75	18 (36%)	*combined practical of above subjects			

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Semester II Exam June 2025										
	Course Code	**Course Title**	**Exam Hours**	**Max. Marks**		**Min. Marks**	**L**	**T**	**P***	**Credits**
				Int. Marks	**Ext. Marks**					
Core Courses										
1	FS-COMP-MSC-CY-CC-201	Information Security & Cryptography	3	10	40	18 (36%)	3	1	1	5
2	FS-COMP-MSC-CY-CC-202	Cyber Forensics, Audit and Investigation	3	10	40	18 (36%)	3	1	1	5
3	FS-COMP-MSC-CY-CC-203	Malware Analysis	3	10	40	18 (36%)	3	1	1	5
4	FS-COMP-MSC-CY-CC-204	Software Vulnerability Analysis	3	10	40	18 (36%)	3	1	1	5
5	FS-COMP-MSC-CY-CP-205	Combined Practical & project	3	25	75	36 (36%)	*combined practical of above subjects			

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Learning Outcome Index

Learning Outcomes are statements of knowledge, skills, and abilities a student should possess and demonstrate upon completion of learning experiences.

I. Programme Outcomes(PO) and Programme Specific Outcomes (PSO)

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10	PSO11
PO1	x	x	x	x	x	x	x	x		x	x
PO2	x		x		x	x	x	x	x	x	x
PO3	x	x	x		x	x	x	x	x	x	x
PO4	x	x	x	x	x	x		x	x	x	x
PO5	x	x	x	x	x	x	x	x	x	x	x
PO6	x	x	x	x	x	x	x			x	x
PO7				x	x		x		x	x	x
PO8		x		x		x	x	x			x
PO9	x	x		x	x		x	x			x
PO10	x	x	x		x				x		x
PO11	x	x	x		x	x	x	x	x	x	x

II. Programme Specific Outcomes (PSO) and Core Courses (CC)

	MCSEC 101	MCSEC 102	MCSEC 103	MCSEC 104	MCSEC 201	MCSEC 202	MCSEC 203	MCSEC 204	MCSEC 301	MCSEC 302	MCSEC 401	MCSEC 402
PSO1	x	x	x	x	x	x	x	x	x	x	x	x
PSO2	x	x	x	x	x	x	x	x	x	x	x	x
PSO3		x		x	x			x	x	x		x
PSO4	x	x	x	x	x	x	x	x	x	x	x	x
PSO5	x	x	x	x	x	x	x	x	x	x	x	x
PSO6	x		x		x	x	x				x	
PSO7	x	x	x	x	x	x	x	x	x	x	x	x
PSO8		x		x	x			x	x	x		x
PSO9		x	x	x	x			x	x	x	x	x
PSO10	x	x	x	x	x	x	x	x	x	x	x	x
PSO11	x	x	x	x	x	x	x	x	x	x	x	x

Post Graduate Diploma in Cyber Security
Choice Based Credit System

III. Programme Specific Outcomes (PSO) and Core Elective Courses (CEC)

	MCS 305a	MCS 305b	MCS 405a	MCS 405b
PSO1	x	x	x	x
PSO2	x	x	x	x
PSO3	x		x	
PSO4	x	x	x	x
PSO5	x	x	x	x
PSO6		x		x
PSO7	x	x	x	x
PSO8	x		x	
PSO9	x	x	x	x
PSO 10	x	x	x	x
PSO 11	x	x	x	x

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Objectives, Course-level Learning Outcomes, Contents, and Suggested Readings

Semester I
Exam Dec 2024

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-101 **Introduction to Cyber Security**

Course Objectives:
CO1. To identify and classify various attacks
CO2. To encrypt and decrypt messages using block chippers and signs.
CO3. To create a digital signature using multiple algorithms.
CO4. To describe web security, intruders, viruses, and firewalls

Learning Outcomes:
After completing this course, students will be able to-
LO1. Identify and classify various attacks
LO2. Encrypt and decrypt messages using block chippers and signs.
LO3. Create a digital signature using multiple algorithms.
LO4. Describe web security, intruders, viruses, and firewalls

---

Unit I

Computer Security models, Computer Security Terms, Computer Ethics, Business, and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT, Smartphone Operating systems, introduction to compliances, Globalization and borderless world.

Unit II

Basic Python Scripting: Python Basics, Variables, and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules, and Packages.

Unit III

Cyber Laws: Need for Cyber Regulations; Scope and Significance of Cyber laws: Information Technology Act 2000; Network and Network Security, Access and Unauthorised Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass, and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Recommended Readings

1. Behrouz A. Forouzan (2004). Data communication and Networking. Tata McGraw-Hill.
2. Kurose, James F. & Ross, Keith W. (2003). Computer Networking: A Top-Down Approach Featuring the Internet (3rd Ed.). Pearson Education.
3. Langtangen, H.P. (2012). Python Scripting for Computational Science (4th Ed.). Springer
4. Craig, B. (2012). Cyber Law: The Law of the Internet and Information Technology. Pearson. Sharma J. P. & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt Ltd.
5. Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd

Suggested Readings

1. Shema, M. (2012). Hacking Web Apps: Detecting and Preventing Web Application Security Problems.
2. https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
3. Computer Programming And Cyber Security for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cybersecurity Fundamentals, Zach Codings, Independently published

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-102 **Security Threats**

Course Objectives:

CO1. To understand the basic concepts of security threats
CO2. To know about network security
CO3. To have knowledge of various behavioral biometric technologies
CO4. To understand the basics of threat analysis
CO5. To be acquaint with various security elements
CO6. To understand various methods of access control

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the basic concepts of security threats
LO2. Know about the network security
LO3. Having knowledge of various behavioral biometric technologies
LO4. Understanding of the basics of basics of threat analysis
LO5. Acquaintance with various security elements
LO6. Understanding of various methods of access control

Unit I

Security threats: introduction, sources, motives, target assets and vulnerabilities, consequences of threats, email threats, web threats, intruders and hackers, insider threats. **Network Threats:** active/ passive, interference, interception, impersonation, worms, virus, spams, adware, spyware, Trojans. Covert channels, backdoors, bots, IP spoofing, ARP spoofing, session hijacking, sabotage-internal threats, environmental threats, threats to server security.

Unit II

Security threat management: risk assessment, forensic analysis, security threat correlation, threat awareness, vulnerability sources and assessment, vulnerability assessment tools, threat identification, **Threat analysis: t**hreat modelling, model for Information Security planning.

Unit III

Security Elements: authorization and authentication, types, policies and techniques, security certification, security monitoring and auditing, security requirements specifications, security polices and procedures, firewalls, IDS, log files, honey pots. **Access control**: trusted computing and multilevel security, security models, trusted systems, software security issues, physical and infrastructure security, security awareness, training, e-mail, and Internet use policies.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Required Readings

1. Joseph M Kizza, "*Computer Network Security*", Springer Verlag, 2005
2. Swiderski, Frank and Syndex, "*Threat Modeling*", Microsoft Press, 2004
3.

Suggested Readings

4. William Stallings and Lawrie Brown, "*Computer Security: Principles and Practice*", Prentice Hall, 2008.
5. Thomas Calabres and Tom Calabrese, "*Information Security Intelligence: Cryptographic Principles & Application*", Thomson Delmar Learning, 2004.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-103 **Cyber Laws and Security Policies**

Course Objectives:

CO1. To understand the concept of computer security
CO2. To know about the secure system planning and administration
CO3. To have knowledge about information security policies and procedures
CO4. To understand the basics of information security
CO5. To be acquaint with organizational and human security

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the concept of computer security
LO2. Know about the secure system planning and administration
LO3. Having knowledge about information security policies and procedures
LO4. Understanding of the basics of information security
LO5. Acquaintance with organizational and human security

Unit I

Introduction to Computer Security: definitions, threats to security, government requirements, information protection and access controls, computer security efforts, standards, computer security mandates and legislation, privacy considerations, international security activity. **Secure System Planning and administration:** introduction to the orange book, security policy requirements, accountability, assurance and documentation requirements, network security, red book and government network evaluations.

Unit II

Information security policies and procedures: corporate policies- tier1, tier2 and tier3 policies, process management, planning and preparation, developing policies, asset classification, policy-developing standards. **Information security:** fundamentals, employee responsibilities, information classification, information handling, tools of information security, information processing, secure program administration.

Unit III

Organizational and Human Security: adoption of information security management standards, human factors in security, role of information security professionals.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Required Readings

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3.

Suggested Readings

4. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
5. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
6. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
7. James Graham, " Cyber Security Essentials" Averbach Publication T & F Group.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-104 **Intrusion Detection and Prevention Systems**

Course Objectives:

CO1. To understand the requirement of IDS and IPS
CO2. To know about the concepts of IDS and IPS
CO3. To have knowledge about various state-of-art IPS/IDS system available till the date
CO4. To understand the basic architecture and modeling of IDS/IPS
CO5. To be acquaint with installation and configuration procedure of Snort
CO6. To be acquainted with the functioning of Snort

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the requirement of IDS and IPS
LO2. Know about the concepts of IDS and IPS
LO3. Having the knowledge about various state-of-art IPS/IDS system available till the date
LO4. Understanding of the basic architecture and modeling of IDS/IPS
LO5. Acquaintance with installation and configuration procedure of Snort
LO6. Acquainted with the functioning of Snort

Unit I

Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources. Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion.

Unit II

A model for intrusion analysis , techniques, types of responses mapping, responses to policy Vulnerability analysis, credential analysis, non credential analysis; 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.

Unit III

Working with Snort Rules, Rule Headers, Rule Options, The SnortConfiguration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL,Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Required Readings

1. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003.
2. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: "IntrusionDetection and Correlation Challenges and Solutions", 1st Edition, Springer, 2005.
3. Carl Endorf, Eugene Schultz and Jim Mellander "Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.

Suggested Readings

4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rdEdition, New Riders Publishing, 2002.
5. T. Fahringer, R. Prodan, "A Text book on Grid Application Development and Computing Environment". 6th Edition, Khanna Publishers, 2012.
6. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010
7. Paul E. Proctor, "The Practical Intrusion Detection Handbook ",Prentice Hall , 2001.
8. Ankit Fadia and Mnu Zacharia, "Intrusion Alert", Vikas Publishing house Pvt., Ltd, 2007
9. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Semester II
Exam June 2025

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-201 **Information Security and Cryptography**

Course Objectives:

CO1. To understand the concept of CNSS security model
CO2. To know about the life cycle of security systems
CO3. To have knowledge about basic concepts of cryptography
CO4. To understand the basics of symmetric and Asymmetric key cyphers
CO5. To be acquainted with the usage of message authentication and hash functions
CO6. To understand and apply the concept of MAC algorithms
CO7. To know about the concept of cryptanalysis

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding the concept of CNSS security model
LO2. Know about the life cycle of security systems
LO3. Having knowledge about basic concepts of cryptography
LO4. Understanding of the basics of symmetric and Asymmetric key cyphers
LO5. Acquaintance with the usage of message authentication and hash functions
LO6. Understanding and ability to apply the concept of MAC algorithms
LO7. Know about the concept of cryptanalysis

Unit I

Information Security: Introduction, CNSS Security Model, Components of Information System, Approaches to Information Security Implementation, The Security Systems Development Life Cycle. **Cryptography**: Concept, traditional ciphers like Caesar, Substitution, Vigenere, Transposition.

Unit II

Symmetric key Ciphers: Concept and Types, Structure and analysis of DES, Security of DES, Structure and analysis of AES. **Asymmetric key Ciphers**: Concept of public key cryptosystems, RSA algorithm, Diffie-Hellman Key exchange. **Message Authentication and Hash Functions:** Authentication requirements and functions, MAC and Hash Functions.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Unit III

MAC Algorithms: Secure Hash Algorithm, Digital signatures, Kerberos. Concept and applications of IPSec, SSL, TLS, SET, PGP and S/MIME. Concept of steganography. **Cryptanalysis:** Concept, Linear Cryptanalysis, Differential Cryptanalysis.

Required Readings

1. Principles of Information Security : Michael E. Whitman, Herbert J. Mattord, CENGAGE Learning, 4th Edition.
2. Cryptography and Network Security : William Stallings, Pearson Education, 4th Edition.

Suggested Readings

3. Cryptography and Network Security : Forouzan Mukhopadhyay, McGraw Hill, 2nd Edition.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Paper Code:FS-COMP-PGDCS-FC-202
Paper Name : Cyber Forensics, Audit and Investigation

Course Objectives:

CO1. To understand basic concepts of various file systems and write blockers
CO2. To know about the extracting & recovering partitions
CO3. To have knowledge about NTFS file system architecture
CO4. To understand the basics of extended file systems
CO5. To be acquaint with windows forensic analysis
CO6. To understand the concepts of mobile forensics
CO7. To know about various audit functions, frameworks, standards and regulations

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of basic concepts of various file systems and write blockers
LO2. Know about the extracting & recovering partitions
LO3. Having knowledge of NTFS file system architecture
LO4. Understanding of the basics of extended file systems
LO5. Acquaintance with windows forensic analysis
LO6. Understanding of the concepts of mobile forensics
LO7. Know about various audit functions, frameworks, standards and regulations

---

Unit I

Filesystem: CHS, LBA, HPA, write blockers, Extracting & recovering partitions, MBR, DOS partition table, Extended partition table, RAID; NTFS file system:Architecture, File creation,File deletion, Compression, encryption and indexing; Extended file systems: EXT4, Architecture, File creation, File deletion and Journaling; Other Disk structures; Windows and Linux boot process; File system acquisition and recovery.

Unit II

Windows Forensic Analysis: Window artifacts, Evidence volatility, System time, Logged on user(s), Open files, MRUs, Network information, Process information, Service information, Windows Registry, Startup tasks, Memory dumping; Document Forensics:PDF structure,PDF analysis, MS Office Document structure and analysis, Macros, Windows thumbnails.

Unit III

Mobile Forensics: SIM Card, Android architecture, Android File System, Android application; Virtual Machines, Network Forensics; Cyber crime investigation: Pre investigation,SOP for Investigation; Case scenarios:social media crime, Email investigation; CDR Analysis. Auditing: Internal Audit and IT Audit Function, IT Governance, Frameworks, Standards, and Regulations, Identifying information assets, Risk assessment and management.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Required Readings

1. Computer Evidence-Collection and Preservation. Brown,C.L.T. Course Technology Cengage Learning.
2. Guide to Computer Forensics And Investigations Nelson, Bill; Phillips, Amelia; Enfinger,Frank;Steuat,Christopher Thomson Course Technology.
3. Computer Forensics–Computer Crime Scene Investigation. Vacca, John R. Charles River Media

Suggested Readings

4. Bunting, Steveand William Wei.EnCase Computer Forensics:The Official EnCE: EnCase Certified Examiner Study Guide.Sybex, 2006
5. Incident Response: Computer Forensics, Prosise, Chris, Kevin Mandia, and Matt Pepe, McGraw-Hill,2014
6. IT Security Risk Control Management:An Audit Preparation Plan,Raymond Pompon,Apress 2016
7. Carrier, Brian.File System Forensic Analysis. Addison- Wesley Professional.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-203 **Malware Analysis**

Course Objectives:

CO1. To understand the fundamentals of malware
CO2. To know about the reverse engineering
CO3. To have knowledge of advanced dynamic analysis tools and concepts
CO4. To understand the basics of packers
CO5. To know about various kernels
CO6. To understand and apply various rootkit techniques

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the fundamentals of malware
LO2. Know about the reverse engineering
LO3. Having knowledge of advanced dynamic analysis tools and concepts
LO4. Understanding of the basics of basics of packers
LO5. Have knowledge of various kernels
LO6. Understanding of various rootkit techniques

Unit I

Introduction to malware, Types of malwares, Basic Static and Dynamic Analysis, Overview of Windows file format, PEView.exe, Patching Binaries , Disassembly(objdump, IDA Pro), Introduction to IDA, Introduction to Reverse Engineering, Extended Reverse Engineering using GDB and IDA;

Unit II

Advanced Dynamic Analysis - debugging tools and concepts, Malware Behavior - malicious activities and techniques, Analyzing Windows programs – WinAPI, Handles ,Networking , COM, Data Encoding, Malware Countermeasures , Covert Launching and Execution, Anti Analysis - Anti Disassembly, VM, Debugging;

Unit III

Packers – packing and unpacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging, Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation , Rootkit Anti-forensics , Covert analysis.

Suggested Readings

1. Michael Sikorski and Andrew Honig, " Practical Malware Analysis", No Starch Press,2012

2. Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel", Addison-Wesley, 2005

Suggested Readings

3. Dang, Gazet and Bachaalany, "Practical Reverse Engineering",Wiley,2014
4. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition,Jones& Bartlett, 2012.
5.

****

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Duration: 3 Hours | Maximum Marks: 50
Minimum Passing Marks: 13

FS-COMP-PGDCS-CC-204 **Software Vulnerability Analysis**

Course Objectives:

CO1. To understand the concept of security and authentication
CO2. To know about the application security
CO3. To have knowledge about malicious code
CO4. To understand the basics of penetration testing
CO5. To have the knowledge of access control
CO6. To understand basics of buffer overflow and rootkits
CO7. To know about some aspects of network security & intrusion

Learning Outcomes:

After completion of this course the student will be able to-
LO1. Understanding of the the concept of security and authentication
LO2. Know about the the application security
LO3. Having knowledge about malicious code
LO4. Understanding of the basics of penetration testing
LO5. Having the knowledge of access control
LO6. Understanding of basics of buffer overflow and rootkits
LO7. Know about some aspects of network security & intrusion

Unit I

Introduction to security & authentication: software security, security failures, bugtraq, CERT Advisories, technical trends affecting software security, penetrate and patch, security goals, prevention, traceability and auditing, monitoring, privacy and confidentiality, Multilevel security, Anonimity, Authentication, Integrity, software security pitfalls, Software project goals. **Application Security & Malicious Code:** software risk management for security, role of security personnel, risk assessment, development goes astray, code review (tools) , architectural risk analysis, penetration testing, risk-based security testing, abuse cases and security requirements, security operations

Unit II

Access control & physical protection: Linux access control model, Linux Permissions, modifying file attributes, modifying ownership, the umask, programmatic interface, access control in Windows NT, compartmentalization, fine-grained privileges. **Buffer overflow & rootkits**: buffer overflows as security problems, defending against buffer overflow, internal buffer overflows, tools for handling buffer overflows, smashing heaps and stacks, heap overflows, stack overflows, decoding the stack.

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Unit III

Network Security & Intrusion: OSI model, sockets, socket functions, socket addresses, network byte order, internet address conversion, simple server and web clients, Tinyweb server. Peeling back the lower layers, network sniffing, raw socket sniffer, libpcap sniffer, decoding the layers, active sniffing, Denial of Service, SYN Flooding, ping of death, teardrop, ping flooding, amplification attacks, Distributed DoS Flooding, TCP/IP hijacking, RST hijacking, continued hijacking, port scanning, stealth SYN Scan, FIN, X-mas, and Null scans, spoofing Decoys, idle scanning, proactive defence (shroud), reach out and hack someone.

Required Readings

1. John Viega & Gary McGraw: *Building Secure Software: How to Avoid Security Problems the Right Way* (Addison-Wesley Professional Computing Series)
2. Gary McGraw: *Software Security: Building Security In* (Addison-Wesley Professional Computing Series)
3.

Suggested Readings

4. Michael Howard, David LeBlanc, John Viega: *19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off)* (Addison-Wesley Professional Computing Series)
5. Jon Erickson: *Hacking: The Art of Exploitation*, 2nd Edition (No Starch Press, San Fransico)
6. Richard Sinn " Software Security , Theory Programming and Practice" Cengage Learning

****

FS-COMP-PGDCS-CC-205 **Combined Practical & project**

After completing this course, students will be able to:
LO1. Identify and define the problem statement
LO2. Define and justify the scope of the proposed problem
LO3. Gather and analyze system requirements
LO4. Propose an optimized solution among the existing solutions
LO5. Practice software analysis and design techniques
LO6. Develop technical report writing and oral presentation skills
LO7. Develop a functional application based on the software design
LO8. Apply to code, debugging, and testing tools to enhance the quality of the software
LO9. Prepare the proper documentation of software projects following the standard guidelines
LO10. Become a master in specialized technology

LO11. Become updated with all the latest changes in the technological world.
LO12. Ability to communicate efficiently.
LO13. Ability to be a multi-skilled engineer with sound technical knowledge, management, leadership, and entrepreneurship skills.
LO14. Capability and enthusiasm for self-improvement through continuous professional development and life-long learning
LO15. Awareness of the social, cultural, global, and environmental responsibility of an engineer.

Practical Training and Project Work:

1. Project Work may be done individually or in groups in case of bigger projects. However if the project is done in a group each student must be given a responsibility for a distinct module and care should be taken to monitor the individual student.
2. Project Work can be carried out in the college or outside with prior permission of college.
3. The Student must submit a synopsis of the project report to the college for approval. The Project Guide can accept the project or suggest modification for resubmission. Only on acceptance of the draft project report the student should make the final copies.
4. **The Project Report should be hand written**

Submission Copy:
The Student should submit a spiral bound copy of the project report.
Format of the Project:

(a) Paper:
The Report shall be typed on White Paper of A4 size.

(b) Final Submission:
The Report to be submitted must be original.

(c) Typing:
Font:- Times New Roman
Heading:- 16 pt., Bold
Subheading:- 14 pt, Bold
Content:- 12 pt.
Line Spacing:- 1.5 line.
Typing Side :-One Side
Font Color:- Black.

(d) Margins:
The typing must be done in the following margin:
Left : 0.75”
Right: 0.75”
Top: 1”
Bottom: 1”
Left Gutter: 0.5”

(e) Binding:
The report shall be Spiral Bound.

(f) Title Cover:
The Title cover should contain the following details:

Top: Project Title in block capitals of 16pt.
Centre: Name of project developer's and Guide name.
Bottom: Name of the university, Year of submission all in block capitals of 14pt letters on separate lines with proper spacing and centering.

(g) Blank sheets:

At the beginning and end of the report, two white blank papers should be provided, one for the Purpose of Binding and other to be left blank.

(h) Content:

I). Acknowledgement
II). Institute/College/Organization certificate where the project is being developed.
III). Table of contents
IV). A brief overview of project
V). Profiles of problem assigned
VI). Study of Existing System
VII). System Requirement
VIII). Project plan
- Team Structure
- Development Schedule
- Programming language and Development Tools

IX). Requirement Specification
X). Design
- Detailed DFD and Structure Diagram
- Data structure, Database and File Specification

XI). Project Legacy
- Current Status of project
- Remaining Areas of concern
- Technical and Managerial Lessons Learnt
- Future Recommendations

XII). Nomenclature and Abbreviations.
XIII). Bibliography
XIV). Source Code.

Teaching-Learning Process

The teaching learning process may include the following-

- Lectures
- Discussions
- Simulations
- Virtual Labs
- Role Playing
- Participative Learning
- Interactive Sessions
- Seminars
- Research-based Learning/ Dissertation/ Case Study/ Project Work

The Blended Learning mode of teaching and learning is preferable in which offline (face-to-face) and online learning both are used to provide learners the opportunity to enjoy both of the worlds. Teachers can share instructions, lecture notes, and assignments online. On the other hand, students can share information/work/assignments with teachers and other students directly in a collaborative setting. This may have a more enriched learning experience, and collaboration between students can be improved upon if group activities rely on information gathered from online resources or lessons. Students who complete online coursework followed by interactive, face-to-face class activities have richer educational experiences.

Assessment and Evaluation

- A comprehensive and continuous evaluation by mid-semester examinations at regular intervals to find out each course level learning outcome
- Formative assessment on the basis of activities of a learner throughout the program instead of one assessment. for this provision of internal exams, student seminars, and assignments is included
- Open book exam is suggested for internal/ mid-term exams to better facilitate the understanding of the knowledge required
- Group examinations are recommended on problem-solving exercises and in major projects to enhance teamwork capabilities of the learner
- Collaborative/Individual assignments are useful to enhance the capability of learners to gain domain-specific knowledge
- Student Seminars and Quizzes are recommended for the continuous learning and evaluation process

ELIGIBILITY FOR ADMISSION

Graduates possessing 55% marks (As per Admission Policy of Govt. of Rajasthan) in any faculty of any statutory university who have studied Computer Science/ Computer Application as a main or vocational subject for three years shall be eligible for admission to the Post Graduate Diploma in Cyber Security Course (Relaxation to SC/ST etc. as per Prevailing Rules)

Post Graduate Diploma in Cyber Security
Choice Based Credit System

PASS CRITERIA

For passing in the examination, a candidate is required to obtain at least a Satisfactory Grade in each paper (Internal + External) and also acquire a Satisfactory Grade in theory and practical separately (in each semester examination).

CLASSIFICATION OF SUCCESSFUL CANDIDATES

As per university norms

INSTRUCTIONS TO PAPER SETTER

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit). **Section-B** will consist of 9 questions (3 questions from each unit). **Section-C** will consist of 6 questions (2 questions from each unit).
The word limit of parts A, B, and C are 50, 200, and 500 respectively

1. INSTRUCTIONS FOR PRACTICAL EXAMINATION

Marks Distribution for Practical Exam -

1. Each practical exam is to be conducted by two examiners one External and one Internal. The external examiner should be a senior lecturer from the jurisdiction of other universities. Credit Weightage distribution for external practical of 4 credits is as under
   a) Practical Examination exercise of 3 questions 2 credits
   b) Viva-Voce 1 credit
   c) Laboratory Exercise File 1 credit
2. Marks distribution for External Project report of 40 marks is as under
   a. External Evaluation-
      i. Research Project/ Case Study 2 credits
      ii. Presentation 1 credit
      iii. External Viva Voce 1 credit
   b. Internal Evaluation- Dissertation 1 credit

2. INSTRUCTIONS FOR STUDENTS

- The student has to complete two months of career-oriented summer training from any firm/organization. If the student does not get a chance to go for training, he/she can choose a research topic and can complete the dissertation under the supervision of any of the faculty in his college.
- The student who has to opt for training has to provide a signed certificate from the firm/ organization authority stating that the student has spent two months as a trainee in his organization/firm. The student who has opted for a dissertation has to submit his/her dissertation report with a certificate from his supervisor.
- In both cases, the student has to present his work in front of all the faculty members and fellow students at the starting of the next session.
- In terms of credits, every one-hour session of L amounts to 1 credit per semester and a minimum of two-hour sessions of T or P amounts to 1 credit per semester.

*** An Academic/ Industrial Tour shall be organized by the college/department in every session. A Tour Report shall be prepared and submitted by the students after a study tour to industries/academic institutions of repute.**

Post Graduate Diploma in Cyber Security
Choice Based Credit System

Key Features of Revised Curriculum

Following are the key features of the revised curriculum-

- Student Centric Teaching and Learning approach
- Technology oriented approach of teaching
- Hand-on Practical/ Laboratory Sessions
- Problem-oriented teaching and learning
- Problem-analysis oriented assignments and evaluation
- Enhance logical thinking and analytical capabilities

Appendice

List of Open Electives offered by the University -