M.Sc. Computer Sc. (Cyber Security)
Session 2020-21
Examination 2021-22

ELIGIBILITY FOR ADMISSION

Graduates possessing 50% marks 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 M.Sc. Cyber Security Course (Relaxation to SC/ST etc. as per Prevailing Rules)

PASS CRITERIA

For passing in the examination, a candidate is required to obtain at least 25% in each paper (Internal + External) and 36% marks in the total aggregate in theory and 36% marks in practical separately (in each semester examination).

CLASSIFICATION OF SUCCESSFUL CANDIDATES

As per university norms

Scheme of Examination

1. English shall be the medium of instructions and examination.
2. Examinations shall be conducted at the end of course as per the Academic Calendar notified by the Maharaja Ganga Singh University of Bikaner.

Instructions for Paper setters

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

4.1 The duration of written examination for each paper shall be of three hours and Practical examination shall be for 3 hours duration.

4.2 The minimum attendance required by a candidate will be as per university rules.

5. With regard to dissertation/project/training, the scheme of evaluation shall be as follows:

5.1.1 The candidate has to submit a dissertation in a bound form in three copies at the end of course which would be evaluated by an external examiner. Total marks for dissertation shall be 50 (40 external + 10 internal marks).

5.1.2 The dissertation/case study/project/training/review will be evaluated at the end of course by an external examiner.

5.1.3 Students are advised to complete dissertation/project/training (Review or experimental) preferably in some outside research institute or industry or otherwise in the University.

6. An educational tour may be organized for students within or outside the State under the supervision of faculty members of the department. Traveling expenses of the teacher/s will be borne by the university as per rules.

Teaching and Examination scheme for
M.Sc. Cyber Security
Semester I

Paper Code	Paper Name	Exam Hours	Maximum Marks		Minimum passing Marks
			Internal Marks	External Marks	
MCSEC 101	Mathematical Foundations for Cyber Security	3	10	40	13
MCSEC 102	Cyber Crime, Cyber Laws and IPR	3	10	40	13
MCSEC 103	Computer Networks	3	10	40	13
MCSEC 104	C++ and Data Structures	3	10	40	13
MCSEC 105	Combined Practical	3	25	75	36
Grand Total(Theory+ Practical)				**300**	

Teaching and Examination scheme for
M.Sc. Cyber Security
Semester II

Paper Code	Paper Name	Exam Hours	Maximum Marks		Minimum passing Marks
			Internal	External	
MCSEC 201	Information Security and Cryptography	3	10	40	13
MCSEC 202	Ethical Hacking	3	10	40	13
MCSEC 203	DBMS	3	10	40	13
MCSEC 204	Python	3	10	40	13
MCSEC 205	Combined Practical	3	25	75	36
Grand Total(Theory+ Practical)				**300**	

Teaching and Examination scheme for
M.Sc. Cyber Security
Semester III

Paper Code	Paper Name	Exam Hours	Maximum Marks		Minimum passing Marks
			Internal	External	
MCSEC 301	Cyber Forensics, Audit and Investigation	3	10	40	13
MCSEC 302	Biometric Security	3	10	40	13
MCSEC 303	Wireless LAN and Mobile Computing	3	10	40	13

MCSEC 304	Operating Systems	3	10	40	13
MCSEC 305	Combined Practical	3	25	75	36
Grand Total(Theory+ Practical)				**300**	

Teaching and Examination scheme for
M.Sc. Cyber Security
Semester IV

Paper Code	Paper Name	Exam Hours	Maximum Marks		Minimum Passing Marks
			Internal	External	
MCSEC 401	Malware Analysis	3	10	40	13
MCSEC 402	Mobile and wireless security	3	10	40	13
MCSEC 403	Intrusion Detection and Prevention Systems	3	10	40	13
MCSEC 404	Project/Dissertation	3	10	40	13
MCSEC 405	Combined Practical	3	25	75	36
Grand Total(Theory+ Practical)				**300**	

Note:

Instructions for Paper setters

1. The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).
2. Each practical exam is to be conducted by two examiners one External and one Internal. External examiner should be senior lecturer from jurisdiction of other universities. Marks distribution for Practical of 40 marks is as under
   a) Practical Examination exercise of 3 questions 30 marks
   b) Viva-Voce 5 marks
   c) Laboratory Exercise File 5 marks
3. Marks distribution for Project of 40 marks is as under
   a. External Evaluation-
      i. Project Dissertation 30 marks
      ii. Presentation 5 marks
      iii. External Viva Voce 5 marks
   b. Internal Evaluation- Dissertation 10 marks
4. The student has to complete two months 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 dissertation under the supervision of any of the faculty in his college.
5. The student who has opted 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 dissertation, has to submit his/her dissertation report with a certificate from his supervisor.
6. In both the cases a student has to present his work in front of all the faculty members and fellow students at the starting of the next session.
7. At least 3 hours for lectures and one hour for tutorial should be allotted per week for each theory paper.
8. A slot of at least 2 hours per week should be allotted for each practical paper.

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

MCSEC-101 Mathematical Foundations for Cyber Security

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Note: Scientific Calculator may be allowed in the examination.

Unit I

Overview of Sets, Basics of counting, Permutations and Combinations, Relations-equivalence and partial orders. Concept of time complexity and asymptotic notations . **Graph Theory**: Euler graphs, Hamiltonian paths and circuits, planar graphs, rooted and binary trees, cut sets, graph colorings and applications, chromatic number, chromatic partitioning and polynomial, matching.

Unit II

Analytic Number Theory: Prime numbers, Euclid's lemma, Euclidean algorithm, basic properties of congruences, residue classes and complete residue systems, Euler-Fermat theorem, Lagrange's theorem and its applications, Chinese remainder theorem, primitive roots. Algebra: groups, cyclic groups, rings, fields, finite fields, lattices and their applications to cryptography.

Unit III

Linear Algebra: vector spaces and subspaces, linear independence, basis and dimensions, linear transformations and applications. **Probability theory**: basics, conditional probability, Bayes theorem, random variables – discrete and continuous, normal probability distribution, central limit theorem, stochastic process, Markov chain. **Coding Theory**: equivalence of codes, linear codes. Overview of Pseudorandom Number Generation.

Suggested Readings:

1. Discrete Mathematics and its applications by K. H. Rosen, seventh edition, TMH
2. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
3. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
4. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
5. H. Anton, "Elementary Linear Algebra", John Wiley & Sons, 2010.
6. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
7. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
8. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.
9. D.S. Malik, J. Mordeson, M.K.Sen, Fundamentals of abstract algebra,TataMcGrawHill

Duration: 3 Hours | Maximum Marks: 50

Minimum Passing Marks: 13

MCSEC-102 Cyber Crime, Cyber Laws and IPR

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Introduction to cyber crime and cyber law, cyberspace and information technology, Nature and scope of cyber crime, Jurisdiction of cybercrime. Important definitions under IT Act 2000, Cyber crime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, Cyberstalking, voyeurism, obscenity in internet, Software piracy

Unit II

IT Act 2000, offences under IT Act and IT(amendment) Act, 2008. CRPC overview, Role Of Intermediaries, Electronic Evidence, Cyberterrorism, espionage, warfare and protection system. Overview of amended laws by the IT Act, 2000: The Indian Penal Code, 1860, The Reserve Bank of India Act 1934, Cyber Theft and the Indian Telegraph Act,1885. Digital Signatures and certificate-legal issues.

Unit III

Intellectual Property rights: Introduction to IP, Copyright, Related Rights, Trademarks, Geographical Indications, Industrial Design, Patents, Licensing and transfer of technology, WIPO Treaties , CopyrightsAct, PatentsAct, Trademark Act.

Suggested Readings:

1. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, Raghu Santanam, M. Sethumadhavan, Information Science Reference.
2. Pfleeger, Charles P.and ShariL. Pfleeger.Security in Computing, 4th Edition. Upper Saddle River, NJ:Prentice Hall,2008.
3. Cyber crime:Security and Surveillance in the Information Age,Douglas Thomas; Brian Loader.
4. Computer Crime:A Crime-Fighters Handbook by David Icove.
5. Crime in the Digital Age: Controlling Telecommunications and Cyber space Illegalities,Peter N. Grabosky.
6. Cyber law–The Indian Perspective By Pavan Duggal,Saakshar Law Publications.
7. Jonathan Rosenoer,“Cyber Law:The law of the Internet”, Springer-Verlag, 1997.
8. Mark F Grady,Fransesco Parisi,“The Law and Economics of Cyber Security”,Cambridge University Press,2006.

Duration: 3 Hours Maximum Marks: 50

Minimum Passing Marks: 13

MCSEC-103 Computer Networks

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Introductory Concepts: Goals and Applications of Networks, Network structure and architecture, the OSI reference model, services, networks topology. Physical Layer: The Physical Layer, Theoretical Basis for Data Communication, Guided Transmission Media, Wireless Transmission, Overview of Digital Signal Encoding Formats, Digital Modulation – ASK, FSK, PSK, PSK, Digitization – Sampling Theorem, PCM, DM, Analog Modulation – Introducing AM, FM, PM, The Mobile Telephone System.

Unit II

The Data Link Layer: Data Link Layer Design Issues, Error Detection and Correlation, Flow Control Protocols, Stop-and-wait Flow Control, Sliding – Window Flow Control, Error Control, Stop-and-wait ARQ, Go-back-N; Example of Data Link Protocols-HDLC Medium access sub layer: Channel allocations, ALOHA Protocols, Carrier Sense Multiple Access Protocols, Ethernet, wireless LANs, BlueTooth, Data Link Layer Switching.

Unit III

Network Layer: Point-to-Point network, routing algorithms, congestion control, internetworking, Quality Control, Internetworking, The Network Layer in the Internet, IP packet, IP addresses, IPv6. Transport Layer: Design Issue, connection management, TCP window management, User Datagram Protocol, Transmission Control Protocol, Performance Issues. Application Layer: DNS, E-Mail, WWW, Multimedia, application layer protocols.

Suggested Readings

1. Forouzan, “Data Communication and Networking”, TMH, 4th Edition.

2. A.S. Tanenbaum, “Computer Networks”, PHI, 4th Edition.

3. W. Stallings, “Data and Computer Communication”, Macmillan Press.

4. Comer, “Computer Networks and Internet”, PHI. 5.Comer, “Internetworking with TCP/IP”, PHI.
5. W. Stallings, “Data and Computer Communication”, McMillan.

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-104 C++ and Data Structures

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Basics : Overview of OOPs, if-else statements, loops (for, while). **Functions** : Overview, passing arguments by value and reference, recursive function, pointers. **Arrays**: Overview, array and function, array and pointers. **Class**: Overview, static data members, Inline Function, Constructors and Destructors.

Unit II

Inheritance: usage, types, compile time and run time polymorphism, overloading and overriding, virtual function, friend function, abstract class. String handling, String class, Overview of Templates. **Searching**: Linear Search, Binary Search. **Sorting:** Insertion Sort, Quick sort.

Unit III

Algorithm: Time and Space complexity of Algorithm. **Overview and applications of abstract data types:** Linked List, Stack, Queue. **Trees :** Basic terminologies. **Binary Tree** : Representation as Array, Basic operations, **Tree Traversal** : Inorder, Preorder, Postorder, Application of Binary Tree.

Suggested Readings

1. Object Oriented Programming With C++ By E. Balagurusamy (Tata Mcgraw Hill)
2. C++ The Complete Reference By Herbert Schildt (Tata Mcgraw Hill)
3. Object Oriented Programming With C++ By Schaum Series (Tata Mcgraw Hill)
4. C++11 for Programmers (Deitel Developer) by Paul J. Deitel (Author), Harvey M. Deitel, Prentice Hall; 2nd edition
5. Professional C++ by Marc Gregoire, Nicholas A. Solter and Scott J.Kleper (Goodreads Publications)
6. A Tour of C++ by Bjarne Stroustrup, 2018
7. C++17 in Detail by Bartłomiej Filipek
8. Expert Data Structure with 'C' By R.B Patel (Khana Book Publishing Co.(P))
9. Data structure By Lipschutz (Tata McGraw Hill)
10. Data Structure By Yashvant Kanitkar (BPB)
11. An Introduction to Data Structures with Applications By Jean-Paul Tremblay, Paul G.Sarerson (Tata McGraw Hill)

12. Data Structure Using C and C++ By Yedidyah Langsam, Moshe J.Augenstein, Arora M. Tenenbaum (Prentice- Hall India)

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-201 Information Security and Cryptography

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

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.

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.

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

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-202 Ethical Hacking

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Section I

Introducing Hacking, Different types of hacking, Phases of hacking, Installation and configuration of Kali Linux, Overview of directory structure, Usage of basic commands; Malwares – Virus , Worms, Trojan; Information gathering using NMAP and ZenMAP .

Section II

Metasploit: Exploiting System Software and Privilege, Metasploit Social Engineering Attack. Working and Network analysis with Wireshark , Network and web scanning about target , Packet captures and man-in-the-Middle attacks. Hacking using different social Engineering techniques.

Section III

DoS and DDoS attacks, Hardware hacking, Hijack sessions, Hacking web servers, Website Hacking , SQL Injection and SQLMAP, Database assessment , Router and Wi-Fi attacks, different types of password attacks, phishing attacks.

Suggested Readings:

1. Basic Security Testing with Kali Linux, by Daniel Dieterle, freely available online.

2. Gray Hat Hacking The Ethical Hacker’s Handbook, Branko Spasojevic, TMH, 2018.

2. Ethical Hacking and Penetration Testing Guide, by Rafay Baloch , Auerbach Publications.

3. Kali Linux Revealed,by Raphaël Hertzog, JimO’Gorman, and Mati Aharoni, offsec press,https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

5. Kali Linux - An Ethical Hacker's Cookbook, by Himanshu Sharma , Packt Publishing Limited

Web resources:

1. https://nptel.ac.in/courses/106/105/106105217/

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

MCSEC-203 DBMS

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Introduction: Characteristics of database approach, Advantages, Database system architecture, Overview of different types of Data Models and data independence, Schemas and instances, Database languages and interfaces; **E-R Model** : Entities, Attributes,keys, Relationships, Roles, Dependencies, E-R Diagram; Normalization: Definition, Functional dependencies and inference rules, 1NF, 2NF, 3NF and BCNF.

Unit II

Introduction to Relational model, Constraints: Domain, Key, Entity integrity, Referential integrity; Keys: Primary, Super, Candidate, Foreign; **Relational algebra**: select, project, union, intersection, minus, cross product, different types of join , division operations; aggregate functions and grouping**; SQL**: Data Types, statements: select, insert, update,delete, create, alter, drop; views, SQL algebraic operations, nested queries; Stored procedures: Advantages, Variables, creating and calling procedures, if and case statements, loops, Cursors, Functions, Triggers.

Unit III

Transactions processing: Definition , desirable properties of transactions, serial and non-serial schedules ,concept of serializability , conflict-serializable schedules; **Concurrency Control:** Two-phase locking techniques, dealing with Deadlock and starvation, deadlock prevention protocols, basic timestamp ordering algorithm; Overview of database recovery techniques; concept of data warehousing.

Suggested Readings:

1. Fundamentals of Database Systems,Ramez A. Elmasri, Shamkant Navathe,5th Ed(Pearson)

2. Database System Concepts By Korth, Silberschatz, Sudarshan (Mcgraw Hill)

3. An Introduction to Database Systems By Bipin C. Desai (Galgotia Publication.)

4. SQL, PL/SQL Programming By Ivan Bayross (BPB)

5. Commercial Application Development Using Oracle Developer 2000 By Ivan Bayross (BPB)

Web Resources

1. http://www.mysqltutorial.org/mysql-stored-procedure-tutorial.aspx

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-204 Python

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Basics: Python Interpreter, writing code in Jupyter Notebook, Indentation, comments, importing a module, binary operators, standard scalar data types, type casting, if-else statements, loops(while, for), pass, range, ternary expressions. Data Structures and Sequences: Tuples, Lists and slicing, Built-in Sequence functions, Dictionary, Sets; List, Set, and Dict Comprehensions.

Unit II

Functions: Namespaces, Scope, and Local Functions; Returning Multiple Values, Anonymous (Lambda) Functions, Partial Argument Application, Generators, Errors and Exception handling. Basic File Handling. Objects and Methods in Python. NumPy: creating N-dimensional arrays, arithmetic with NumPy arrays, basic indexing and slicing, Psuedorandom number generation.

Unit III

Pandas: Overview of Series and DataFrames, reading data from csv file, DataFrame operations- working with data using functions like head, tail , info, shape, reshape, columns, isnull, dropna, mean, sum, describe, value_counts, corr, loc, iloc, apply. Matplotlib- plotting basic figures, subplots, line plots, bar plots, histograms, scatter plots. Overview of Scikit-learn, SciPy, networkx. Applications of python.

Suggested Readings:

1. Python for Data Analysis: Data Wrangling with Pandas, NumPy, and Ipython, by Wes McKinney, O'Reilly Media, 2017
2. Python All-in-One for Dummies, by John Shovic and Alan Simpson, John Wiley & Sons, Inc., 2019
3. Programming in Python 3: A Complete Introduction to the Python Language, Mark Summerfield, Pearson.
4. Swaroop, C. H. (2003). A Byte of Python. Python Tutorial.
5. Introduction to Computation and Programming Using Python. By John V. Guttag, MIT Press.
6. Learning Python , Mark Lutz, David Ascher, O'Reilly
7. T. Budd, Exploring Python, TMH, 1st Ed, 2011

Web Resources

1. https://www.learnpython.org/
2. https://nptel.ac.in/courses/106/106/106106212/
3. http://greenteapress.com/thinkpython/thinkpython.pdf
4. Python tutorial: https://docs.python.org/3/tutorial/index.html

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-301 Cyber Forensics, Audit and Investigation

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

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.

Suggested 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
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.

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-302 Biometric Security

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.

Unit II

Physiological Biometric Technologies: Fingerprints- characteristics, strengths and weaknesses; Facial scan- characteristics, strengths and weaknesses; Iris scan- characteristics, strengths and weaknesses; Retina vascular pattern- characteristics, strengths and weaknesses; Hand scan - characteristics, strengths and weaknesses; DNA biometrics.

Unit III

Behavioral Biometric Technologies: Handprint Biometrics, overview of DNA Biometrics. Signature and handwriting technology- description, classification, keyboard/keystroke dynamics; Voice- data acquisition, feature extraction, characteristics, strengths and weaknesses. Multi biometrics and multi factor biometrics.

Suggested Readings:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : "Biometrics -Identity verification in a network", 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul :"Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.
3. John Berger: "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.
4. Paul Reid, Biometrics for network security, Hand book of Pearson, 2004

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-303 Wireless LAN and Mobile Computing

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Wireless Networks: Introduction, Architecture, Wireless SwitchingTechnology, Wireless Communication problem, Wireless Network Reference Model, Wireless, Wireless LAN: Infrared vs radio transmission, Infrastructure and Ad-hoc Network, IEEE 802.11:System Architecture,Protocol Architecture, 802.11b, 802.11a, Bluetooth: User Scenarios, Architecture.

Unit II

Global System for Mobile Communications (GSM): Mobile Services, SystemArchitecture, Protocols, Localization & Calling, Handover, Security. GPRS: GPRS System, Architecture, UMTS: UMTS System Architecture. LTE: Long Term Evolution. Mobile Computing: Mobile communication, Mobile computing, Mobile Computing Architecture, Mobile Devices, Mobile System Networks, Mobility Management;

Unit III

Mobile Network Layer: Mobile IP: Goals, Assumptions, Entities and Terminology, IP Packet Delivery, Agent Discovery, Registration, Tunneling and Encapsulation, Optimizations, DHCP. Mobile Transport Layer: Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission /time-out freezing, Selective retransmission, Transaction oriented TCP, TCP over 2.5G/3G Wireless Networks.

Suggested Readings:

1. Schiller, J. 2008. Mobile Communications. 2nd ed. India: Pearson Education.
2. Kumar,S. and Kakkasageri, M.S. “Wireless and Mobile Networks: Concepts and Protocols”, Wiley India.
3.Kamal R. 2011. “Mobile Computing”, 2ndEd.Oxford University Press.
4. Talukder, A. K., Ahmed, H. andYavagal,R.R. 2010.Mobile Computing: Technology, Applications and Service Creation, 2ndEd. Tata McGraw Hill
5.Gast, M.S. “802.11 Wireless Networks: The Definitive Guide”, O'Reilly Media.

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-304 Operating Systems

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

Introduction to Operating System, layered Structure, Functions, Types; Process: Concept, Process States, PCB; Threads, System calls; Process Scheduling: types of schedulers, context switch, CPU Scheduling, Pre-Emptive Scheduling, Scheduling Criteria- CPU Utilization, Throughput, Turnaround Time, Waiting Time, Response Time; Scheduling Algorithms- FCFS, SJF, Priority Scheduling, Round Robin Scheduling, MLQ Scheduling, MLQ With Feedback.

Unit II

Synchronization: Critical Section Problem, Requirements for a solution to the critical section problem; Semaphores,simple solution to Readers-Writers Problem. Deadlock: Characterization, Prevention, Avoidance, Banker's Algorithm, Recovery from Deadlock. Memory Management: Physical and virtual address space, Paging, Overview of Segmentation;Virtual Memory Management: Concept,Page Replacement techniques- FIFO, LRU, Optimal

Unit III

Linux:features of Linux, steps of Installation, Shell and kernel, Directory structure, Users and groups,file permissions, commands- ls, cat, cd, pwd, chmod, mkdir, rm, rmdir, mv, cp, man, apt, cal, uname, history etc. ; Installing packages; Shell scripts: writing and executing a shell script,shell variables, read and expr, decision making (if else,case), for and while loops.

Suggested Readings

1. Operating System Principles By Abraham Silberschatz, Peter Baer Galvin (John Wiley And Sons Inc.)
2. Operating System Concepts And Design By Milan Milen Kovic (Tata Mcgraw Hill)
3. Modern Operating System Andrew S. Tanenbaum, Herbert Bos
4. Linux in easy steps, Mike McGrath, in easy steps limited
5. Unix concepts and applications , TMH, Sumitabha Das

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-401 Malware Analysis

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

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
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.

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-402 Mobile and Wireless Security

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

Unit I

INTRODUCTION: Security and Privacy for Mobile and Wireless Networks: Introduction- State of the Art- Areas for Future Research- General Recommendation for Research. Pervasive Systems: Enhancing Trust Negotiation with Privacy Support: Trust Negotiation- Weakness of Trust Negotiation- Extending Trust Negotiation to Support Privacy.

Unit II

MOBILE SECURITY: Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security. SECURING WIRELESS NETWORKS: Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks;

Unit III

Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Zigbee Security, Zigbee Attacks; ADHOC NETWORK SECURITY: Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks

Suggested Readings:

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, Prentice Hall, x ISBN 9788131706885, 2007.
2. Noureddine Boudriga,”Security of Mobile Communications”, ISBN 9780849379413, 2010
3. KMakki, PReiher, et. al. “Mobile and Wireless Network Security and Privacy”, Springer, 2007
4. Levente Buttyan, JPHubaux. “Security and Cooperationin Wireless Networks”,Cambridge University Press,2008.

Duration: 3 Hours

Maximum Marks: 50
Minimum Passing Marks: 13

MCSEC-403 Intrusion Detection and Prevention Systems

Instructions for Paper setters

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

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.

Suggested 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.
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.

Duration: 3 Hours Maximum Marks: 50

Minimum Passing Marks: 13

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.