FACULTY OF COMPUTER SCIENCE & IT

SYLLABUS

of

Master of Science (Information and Network Security)
(Semester I - IV)

(Under Continuous Evaluation System)

Session: 2020-21

The Heritage Institution

KANYA MAHA VIDYALAYA
JALANDHAR
(Autonomous)

PROGRAMME SPECIFIC OUTCOMES

Master of Science (Information and Network Security)

Students of this Post Graduation will be able to:

PSO1: Highlight the need of security architecture and its relevance to system, services, continuity and reliability.

PSO2: Identify the trade-offs for functionality usability and security and to differentiate between controls to protect system availability and reliability: controls to protect information.

PSO3: Measure the performance of security systems within an enterprise-level information system and to troubleshoot, maintain and update an enterprise-level information security system.

PSO4: Comprehend the role of forensics, cyber incidents, intrusions and investigations in revealing how an attack was carried out and understand how to support investigation.

PSO5: Apply skills gained for evaluation and protection of computer networks and security system.

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2020-21

Master of Science (Information and Network Security)Semester - I							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-1111	Computer Networks	C	100	80	-	20	3
MINL-1112	Network Protocols	C	100	80	-	20	3
MINL-1113	Network Operating System	C	100	80	-	20	3
MINL-1114	Information Security and Threats	C	100	80	-	20	3
MINL-1115	Java Programming	C	100	80	-	20	3
MINP-1116	Lab on NOS and Java Programming	C	100	-	80	20	3
		Total	600				

Note:

C - Compulsory

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2020-21

Master of Science (Information and Network Security) Semester - II							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-2111	Network Planning, Analysis and Performance	C	100	80	-	20	3
MINL-2112	Network Security Practices	C	100	80	-	20	3
MINL-2113	Computer Forensic Fundamentals	C	100	80	-	20	3
MINL-2114	Secure Code Development	C	100	80	-	20	3
MINL-2115	Mobile Application Development and Security	C	100	80	-	20	3
MINP-2116	Lab on Mobile Application Development and Security	C	100	-	80	20	3
			600				

Note:

C - Compulsory

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2020-21

Master of Science (Information and Network Security) Semester - III							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-3111	Cyber Incident Handling and Reporting	C	100	80	-	20	3
MINL-3112	Cloud Computing and its Security	C	100	80	-	20	3
MINL-3113	Proactive Security Tools and Technology	C	100	80	-	20	3
MINL-3114	Penetration Testing and Auditing	C	100	80	-	20	3
MINL-3115	Cryptography and Network Security	C	100	80	-	20	3
MINP-3116	Lab on Penetration Testing and Virtualization	C	100	-	80	20	3
			600				

Note:

C - Compulsory

Kanya Maha Vidyalaya, Jalandhar (Autonomous)

SCHEME AND CURRICULUMOF EXAMINATIONS OF TWO YEAR DEGREE PROGRAMME

Master of Science (Information and Network Security)

Session 2020-21

Master of Science (Information and Network Security) Semester - IV							
COURSE CODE	**COURSE NAME**	**COURSE TYPE**	**Marks**				**Examination Time (in Hours)**
			Total	**Ext.**		**CA**	
				L	**P**		
MINL-4111	Intrusion Detection System	C	100	80	-	20	3
MINL-4112	Reverse Engineering and Malware	C	100	80	-	20	3
MINL-4113	Ethical Hacking	C	100	80	-	20	3
MINL-4114	Blockchain for Enterprise Applications	C	100	80	-	20	3
MIND-4115	Major Project / Dissertation	C	200	-	160	40	6
	Total		600				

Note:

C - Compulsory

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE: MINL-1111
COMPUTER NETWORKS

Course Outcomes:

CO1: The student will understand the fundamental concepts of computer networking and will be familiarized with the basic taxonomy and terminology of the computer networking area.

CO2: The student will be able to understand the physical and logical as well as the electrical characteristics of digital signals and the basic methods of data transmission.

CO3: To understand the organization of computer networks, factors influencing computer network development and the reasons for having variety of different types of networks.

CO4: To study the basic taxonomy and terminology of the computer networking and enumerate the layers of OSI model and TCP/IP model in order to have a good understanding of various Reference Models and protocols.

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE: MINL-1111
COMPUTER NETWORKS

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Data Communication, Components, Protocols, Standard Organizations, Applications

Networks Basics & Various Types: Topology, Transmission Mode, Categories of Networks

OSI and TCP/IP Models: OSI Model Layers, Functions of the Layer, TCP/IP Layers and its functions, Comparison of TCP/IP and OSI Models

UNIT – II

Signals, Modulations and Multiplexing: Analog and Digital Signal, Digital to Digital Conversion, Analog to Digital Conversion, Digital to Analog Conversion

Transmission Media: Asynchronous and Synchronous Transmission, Modems, Guided(Twisted pair cable, Coaxial Cable and Optical Fibre) and Unguided Media (Terrestrial Microwave, Satellite and Cellular Telephony, Transmission Disturbance and Performance)

UNIT – III

Detection and Correction of Errors: Error types, Redundancy, Error Detection Methods: VRC,LRC, CRC and Checksum, Error Correction: Single Bit Error Correction, Hamming Code

Data Link Control and Protocols: Line Discipline, Flow Control, Error Control, Asynchronous Protocol, Synchronous Protocol, Character Oriented and Bit Oriented Protocols

UNIT – IV

Quality of Service in Routing & Signaling: Issues, importance, parameters like delay, jitter, end to end service, CoS.

Routing Algorithms: Distance Vector Routing, Link State Routing

Upper OSI Layers: Session Layer, Presentation Layer and Application Layer

References / Textbooks:

1. James F. Kuros and Keith W. Ross, Computer Networking: A Top–Down Approach 2002.
2. Computer Networks Protocols, Standards and Interfaces: Uyless Black, PHI, 2006.
3. Data Communication and Networking, White, Cengage Learning, 2008.
4. Behrouz Forouzan, Data Communications and networking, McGraw Hill, 2007.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE:MINL-1112
NETWORK PROTOCOLS

Course Outcomes:

CO1: To get in depth knowledge about various networking protocols, their working, management and operations.

CO2: To understand the layered approach that makes design, implementation and operation of extensive networks possible.

CO3: Classify the routing protocols and analyze how to assign the IP addresses for the given network.

CO4: To understand the TCP/IP suite of protocols and the networked applications supported by it.

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE: MINL - 1112
NETWORK PROTOCOLS

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Review of networking Technologies & Internetworking Concepts and Architectural Model: Application level and Network level Interconnection, Properties of the Internet, Internet Architecture, Interconnection through IP Routers

Internet Addresses, Mapping internet addresses to Physical addresses (ARP) & Determining an internet addresses at Startup (RARP): Universal identifiers, three Primary classes of IP addresses, network and Broadcast Addresses, Limited Broadcast, Dotted decimal Notation, weakness in Internet addressing, Loopback addresses.

UNIT - II

Internet Addresses, Mapping internet addresses to Physical addresses (ARP) & Determining an internet addresses at Startup (RARP): Address resolution problem, two types of Physical addresses, resolution through Direct Mapping, Resolution through Dynamic Binding. Address Resolution Cache, ARP to other Protocols. Reverse address resolution protocol, timing RARP transaction, Primary and backup RARP severs.

Internet Protocol Connectionless Data Gram Delivery & Internet Protocol: Routing IP Datagrams: The concepts of unreliable delivery, connectionless delivery system, purpose of the internet protocol. The internet datagram.

UNIT - III

Internet Protocol Connectionless Data Gram Delivery & Internet Protocol: Routing in an internet, direct and indirect delivery, table driven IP routing, next Hop Routing, default routes, host specific routes, The IP routing Algorithm, handling incoming datagrams, Establishing routing tables

Internet Protocol: Error and Control Message (ICMP) & Subnet and Supernet Address Extension: The internet, control message protocols, Error reporting versus error detection. ICMP message format. Detecting and reporting various network problems through ICMP. Transparent Router, Proxy ARP, subset addressing, implementation of subnets with masks representation, Routing in the presence of subsets, a unified algorithm.

UNIT - IV

User Datagram Protocol (UDP): Format of UDP message UDP pseudo header UDP encapsulation and Protocols layering and the UDP checksum computation. UDP multiplexing, De–multiplexing and Ports.

Reliable Stream Transport service (TCP): The Transmission control Protocol, pots, Connections and Endpoint, passive and active opens the TCP segment format. TCP implementation issues.

References / Textbooks:

1. Douglas E. Comer, Internetworking with TCP/IP, Pearson Prentice Hall, 2006.
2. Behrouz A. Forouzan, TCP/IP Protocol Suite, McGraw Hill Education, 2010.
3. Douglas E. Comer, David L. Stevens, Internetworking with TCP/IP, Vol. III: Client-Server Programming and Applications, Linux/Posix Sockets Version, Pearson, 2000.
4. W. Richard Stevens, Unix Network Programming, PHI, 1998.
5. William Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Addison-Wesley, 1999.
6. Craig Hunt, TCP/IP Network Administration, O'Reilly & Associates, 2002.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE: MINL - 1113
NETWORK OPERATING SYSTEM

Course Outcomes:

A student will be able to do the following:

CO1: Understand the installation, configuration and administration of Network Operating Systems.

CO2: The student will gain and will improve the capabilities in:

- Installing, configuring and administering network operating system
- Remote administration using network operating systems
- Connecting client computers to the network
- Linux working

CO3: This course aims to provide an understanding of the general security concepts of windows and Linux systems, network security tools and implementation of organizational security.

CO4: To learn the fundamentals and gain knowledge of Operating Systems.

Master of Science (Information and Network Security) Semester – I
(Session 2020-21)
COURSE CODE: MINL - 1113
NETWORK OPERATING SYSTEM

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Introduction to LINUX, Installing LINUX, Partitions, LILO, Installing softwarepackages. Updating with Gnome, Updating with KDE, Command line installing.

File Structure: LINUX files, File structure, File & Directory permission, Operations on a file.

UNIT - II

Window 2003 File System, Active Directory, DHCP, IIS, DNS

Administering Linux: Creating a user A/C, modifying a user A/C, Deleting a user A/C,Checking Disk Quotas, System Initialization, System start–up & shutdown, Installing & managing H/W devices.

UNIT - III

Disk Management: Managing Basic & Dynamic Disks, Disk quotas, Disk Fragmentation, Remote Storage, RAID all levels

Administrating window 2003: User group & Computer Accounts, Creating & Managing Users and Groups

Backup & Disaster Recover: Concepts, Creating Backing Plan, Choosing & Managing Backup Media, Setting backup Options, Scheduling Backup.

UNIT - IV

Backup & Disaster Recover: Jobs, Disaster Recovery Plan, Assessing Threats, Restoring

Data using Backup

Case & Comparative Studies: Windows 2003 Server & Linux Server

Troubleshooting : Troubleshooting LINUX in GRUB mode, Windows 2003 Server.

References / Textbooks:

1. Christopher Negus, Red Hat Linux(10) Bible, Wiley, 2003.
2. Tim Parker, Linux Unleashed, Sams, 2006.
3. Charles Fisher, Red Hat Linux Administration Tools, 2007.
4. Kathy Ivens, Windows Server 2003: The Complete Reference, McGraw-Hill, 2003.
5. William R. Stanek, Microsoft Windows Server 2003 Inside Out, Microsoft Press, 2004.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I

(Session 2020-21)
COURSE CODE: MINL - 1114
INFORMATION SECURITY AND THREATS

Course Outcomes:

CO1: To understand the network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic networking defense tools.

CO2: The student will be able to differentiate between organizational security policies and security mechanism and will be able to analyze the security needs of a small enterprise, design a strategic plan to address those security requirements and select the appropriate tools to implement the organizational policies.

CO3: To be able to explain various Information security threat and controls for it.

CO4: The student will be able to explain the mechanism to protect confidentiality and completeness of data.

Master of Science (Information and Network Security) Semester – I

(Session 2020-21)
COURSE CODE: MINL - 1114
INFORMATION SECURITY AND THREATS

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Essential terminology, Hardware, Software, Malware, Defining security, Need for security Cyber crime vs Computer based crime, Information Security statistics, Three pillars of Security,

UNIT - II

Security myths, Identity of a Web Site, http vs https, Operating System fingerprinting, Hardening operating system, updates, patches, CAN and CVEs, Host based firewall vs Network based firewall, deploying firewall, sniffing network traffic.

UNIT - III

Recognizing Security Threats and attacks, Phishing and its countermeasures, Virus, Trojan Horse, Worms, Spyware, Adware, Keylogger, Social engineering, Denial of Service, Spamming, Port Scanning, Password cracking, Security measures

UNIT - IV

Creating isolated network presence using virtualization, hosting different operating systems virtually and networking amongst these, Identify website's identity, Finding and understanding CVEs, deploying firewall, Understanding phishing, using NMAP, netcat, using tcp dump and wireshark,

generating digital certificates, understanding CAs.

References / Textbooks:

1. Atul Kahate, Cryptography and Network Security, McGraw Hill, 2010.
2. Mark S. Merkow, Jim Breithaupt, Information Security: Principles and Practices, Pearson Prentice Hall, 2006.
3. Michael E Whitman, Herbert J Mattord, Principles of Information Security, Cengage Learning, 2018.
4. Christopher T. Carlson, How to Manage Cybersecurity Risk, Universal-Publishers, 2019.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I

(Session 2020-21)
COURSE CODE: MINL-1115
JAVA PROGRAMMING

Course Outcomes:

CO1: To understand the fundamentals of object-oriented programming in Java, including defining classes, invoking methods, using class libraries, variables, conditional and iterative execution, methods, etc.

CO2: To be aware of the important topics and principles of software development and have the ability to write a computer program to solve specified problems in order to test, document and prepare a professional looking package for each business project.

CO3: To be able to use the Java SDK environment to create, debug and run simple Java programs and to model of object oriented programming: abstract data types, encapsulation, inheritance and polymorphism

CO4: To understand how to take the statement of a business problem and from this determine suitable logic for solving the problem; then be able to proceed to code that logic as a program written in Java.

Master of Science (Information and Network Security) Semester – I

(Session 2020-21)
COURSE CODE: MINL-1115
JAVA PROGRAMMING

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Java Fundamentals: Features, Objects Oriented Basis, Java Virtual Machine, Character Set, Operators, Data Types, Control Structures, Classes, Inheritance, Polymorphism, Packages & Interfaces, Abstract Classes, Stream IO Classes, Exception Handling.

Java I/O: I/O Basics, Streams, reading Console input and writing console output, Print Writer Class, Reading & Writing Files, Byte Streams, Character Streams & Serialization.

UNIT - II

Multithreading: Java Thread model, Thread Priorities, Synchronization, Interthread communication, Suspending, resuming & stopping thread.

Event Handling: The Delegation Event Model, Event Classes, Event Listener Interfaces

UNIT - III

AWT: Window Fundamentals, Working with Frame Windows, Graphics, Color and Fonts.

Swings: Basics of Swing, JButton class, JRadio Button, JText Area class, JCombo Box class JTable class. Layout Managers Border Layout, Grid Layout, Flow Layout, Card Layout.

UNIT - IV

JDBC: JDBC Drivers, Steps to connect to the database, Connectivity with Oracle, Driver Manager, Connection interface, Statement interface, ResultSet interface, Prepared Statement, ResultSet MetaData, Database MetaData.

References / Textbooks:

1. Patrick Naughton & Herbert Schildt, JAVA 2: The Complete Reference, McGraw-Hill Education, 1999.
2. Mary Campione, Kathy Walrath, Alison Huml, The Java Tutorial Continued: The Rest of the JDK, Addison Wesley, 1998.
3. Bruce Eckel, Thinking in Java, Prentice Hall, 2006.
4. D.T. Editorial Services, Java 8 Programming Black Book, Dreamtech Press, 2015.
5. Cay S. Horstmann, Core Java Vol I & II, Prentice Hall, 2013.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – I

(Session 2020-21)

COURSE CODE: MINP-1116

LAB ON NOS AND JAVA PROGRAMMING

Examination Time: 3 Hrs **Max. Marks: 100**

Practical: 80

CA:20

Lab on NOS: Installation & Configuration of NOS (Windows 2003, Linux) and their Administration. User account creation, group creation, DHCP settings, Backup & Recovery plan.

Lab on Java Programming

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2111
NETWORK PLANNING, ANALYSIS AND PERFORMANCE

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend design of computer and communication network.

CO2: Evaluate network planning, including minimum cost and maximum flow methodologies.

CO3: Analyze network performance through design tools, traffic matrix, etc.

CO4: Comprehend and tune various network design.

CO5: Design hypothetically security measures in Network.

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2111
NETWORK PLANNING, ANALYSIS AND PERFORMANCE

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Requirements, Planning & Choosing Technology: Business requirements, technical requirement user requirements, traffic sizing characteristics time & delay consideration

Traffic Engineering and Capacity Planning: Throughout calculation traffic characteristics & source models.

UNIT - II

Traffic Engineering and Capacity Planning: Traditional traffic engineering, queued data & packet switched traffic modeling, designing for peaks, delay or latency

Network Performance Modeling and Analysis: creating traffic matrix, design tools, components of design tools, types of design projects

UNIT - III

Technology Comparisons: Generic packet switching networks characteristics, private vs. public networking. Business aspects of packet, frame and cell switching services, High speed LAN protocols comparison, Application performance needs, Throughout, burstiness, response time and delay tolerance, selecting service provider, vendor, service levels, etc.

UNIT - IV

Access Network Design: N/W design layers, Access N/W design, access n/w capacity, Backbone n/w design, Backbone segments, backbone capacity, topologies, Tuning the network, securing the network. Design for network security

References / Textbooks:

1. Piet Van Mieghem, Performance Analysis of Complex Networks and Systems, Cambridge University Press (2014), 2nd Edition.
2. James D McCabe, Network Analysis, Architecture and Design, Morgan Kaufman Series in Networking (2007), 2nd Edition.
3. Youeu Zheng, Shakil Akhtar, Network for Computer Scientists and Engineers, Oxford University Press (2007)
4. Foruzan, Data Communications & Networking, Tata–McGraw Hill (2006).
5. Darren L. Spohn, Co–Authors: Tina L. Brawn and Scott G Rau.

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2112
NETWORK SECURITY PRACTICES

Course Outcomes:

After passing this course the student will be able to:

CO1: Demonstrate various security attacks like Interruption, Interception, Modification, integrity, non–repudiation, etc.

CO2: Analyze the performance of various Classical and Modern Cryptography Techniques.

CO3: Comprehend security requirements and issues at application layer.

CO4: Demonstrate the key exchange and generation through public key infrastructure.

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2112
NETWORK SECURITY PRACTICES

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Introduction: Overview, Security attacks (Interruption, Interception, Modification and Fabrication) and services (confidentiality, authentication, integrity, non–repudiation, access control and availability), types of attacks, model for network security.

Classical and Modern Cryptography Techniques: Conventional encryption model, classical encryption techniques.

UNIT - II

Classical and Modern Cryptography Techniques: Simplified DES, Principles of Block ciphers, DES and its strength, Triple DES, Blowfish, CAST – 128, linear and differential cryptanalysis, steganography.

Confidentiality: Traffic confidentiality, key distribution, random number generation

UNIT – III

Public Key Encryption Methods: Principles, RSA Algorithm, Key management, Diffie–Hellman key exchange, Elliptic curve cryptography

Authentication: Requirements, functions, Authentication codes, Hash functions

UNIT – IV

Digital Signatures: Basics, Digital signature standard, Authentication Protocols

Other Securities:
IP Security: overview and architecture, Authentication Header (AH) and Encryption Security Payload (ESP); Electronic Mail security: Pretty Good Privacy (PGP); Web security: overview.

References / Textbooks:

1. Forouzan, Cryptography and Network Security, McGraw Hill Education (2015).
2. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson Education (2019), 4th Edition
3. Richard Bejtlich, The Practice of Network Security Monitoring, No Starch Press (2013), 1st Edition
4. Atul Kahate, Network Security Practices, McGraw Hill Education (2019), 4th Edition

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)

COURSE CODE: MINL-2113

COMPUTER FORENSIC FUNDAMENTALS

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend the role of digital forensics in the field of information assurance and cyber security

CO2: Apply various principles of effective digital forensics investigation techniques.

CO3: Identify housing, hardware and software requirements for Computer Forensics.

CO4: Comprehend processing of evidence and report preparation

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)

COURSE CODE: MINL-2113

COMPUTER FORENSIC FUNDAMENTALS

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80

CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Computer Forensics Fundamentals: Introduction to Computer Forensics, Cyberspace and Criminal Behavior, Traditional Problems Associated with Computer Crime.

Web-Based Criminal Activity, Malware: Viruses and Worms, DoS and DDoS Attacks, Botnets and Zombie Armies, Spam, Ransomware. Theft of Information, Data Manipulation, and Web Encroachment.

UNIT- II

Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources, Employment Proceedings.
Computer Forensics: Traditional Problems in Computer Investigations, Disk Structure and Digital Evidence, Developing Computer Forensic Science Capabilities.

UNIT- III

Requirements: Housing, Hardware and software requirements.
Sampling of Forensic Software. Searching and Seizing Computer-Related Evidence, Pre-search Activities, On-scene Activities.

UNIT- IV

Processing of Evidence and Report Preparation: Aspects of Data Analysis, Smart Phones and GPS Forensics, Smart Phones and GPS Forensics.

Report Preparation and Final Documentation.

References / Textbooks:

1. Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education India (2011), 2nd Edition
2. Jason Luttgens and Matthew Pepe, Incident Response and Computer Forensics, McGraw-Hill Education (2014), 3rd Edition
3. Akash Kamal Mishra, Computer Crime Investigation and Computer Forensics, Notion Press (2020), 1st Edition
4. Christopher Steuart, Bill Nelson, Guide to Computer Forensics and Investigations, Cengage (2013), 4th Edition
5. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications (2015), 1st Edition

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)

COURSE CODE: MINL-2114

SECURE CODE DEVELOPMENT

Course Outcomes:

After passing this course the student will be able to:

CO1: Identify and evaluate various process model used for development of software.

CO2: Identify various attacks like buffer overrun, DOS and various principals concerning security.

CO3: Comprehend various securities related techniques and methodologies.

CO4: Apply secure coding practices to maintain the Confidentiality, Integrity and Availability of a data.

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2114
SECURE CODE DEVELOPMENT

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Principles and Motivations: Software development process models waterfall, rapid prototyping, incremental development, spiral models, Agile Software Development.

Software Development Methods: Formal, semi–formal and informal methods; Requirements elicitation, requirements specification; Data, function, and event–based modeling;

UNIT – II

The need for Secure Systems, Proactive Security development process: security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, SD3 (Secure by design, default and deployment), Security principles, Threat modelling.

UNIT III

Security Techniques, authentication, authorization, Buffer Overrun, Access control, least privilege, Cryptographic Foibles, Protecting Secret Data

Input issues: database, web–specific, internationalization.

UNIT – IV

Socket Security, Securing RPC, Protecting Against Denial of Service Attacks.

Security testing, security code review, secure software installation, writing security

documentation.

References / Textbooks:

1. Michael Howard and David LeBlanc, Writing Secure Code, Microsoft Press, (2006).
2. Nithin Haridas, Software Engineering – Security as A Process in the SDLC, Startch Publisher (2007).
3. Pressman, Roger, Software Engineering – A Practitioners Approach, McGraw Hill (2008), 6th Ed.
4. Sommerville, Ian, Software Engineering, Addison–Wesley Publishing Company, (2006), 8th Ed.
5. J.D. Glaser, Secure Code Development for Mobile Apps, Auerbach Publications (2017), 1st Edition

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2115
MOBILE APPLICATION DEVELOPMENT AND SECURITY

Course Outcomes:

After passing this course the student will be able to:

CO1: Setup Integrated Development Environment for developing and configuring mobile applications.

CO2: Comprehend and utilize various UI widgets and components for designing User Interface of application.

CO3: Identify various issues involved in developing mobile application.

CO4: Manage view and navigation in mobile application through intents, activities, services, etc.

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)
COURSE CODE: MINL-2115
MOBILE APPLICATION DEVELOPMENT AND SECURITY

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Introduction to Android: Android Introduction, History and Version, Android Architecture, Core Building Blocks, Android Emulator, Install Android, Setup Eclipse, Hello Android example, Android Project Folder Structure, Hide Title Bar, Screen Orientation.

UNIT – II

Android Widgets: UI Widgets, Working with Button, Toast, Custom Toast, Toggle Button, Check Box, Custom Check Box, Radio Button, Dynamic Radio Button, Custom Radio Button, Alert Dialog, Spinner, Auto Complete Text View, List View, Custom List View, Rating Bar, WebView, Seek Bar, Date Picker, Time Picker, Analog and Digital, Progress Bar, Vertical Scroll View, Horizontal Scroll View.

Image Switcher, Image Slider, View Stub, Tab Layout, Tab Layout with Frame Layout, search View, Search View on Toolbar, Edit Text with Text Watcher.

UNIT – III

Activity and Intents: Activity Life Cycle, Implicit Intent, Explicit Intent, Start Activity For Result, Share App Data

Android Fragments, Android Menu: Option Menu, Context Menu, Popup Menu

UNIT – IV

Managing and Accessing Databases: SQLite.

Mobile Issues and Development Strategies: Issues facing Mobile devices, Securing mobile application development

Android Security: Android Securable IPC Mechanism, Android Security Model, Intents, Activities, Services, Android Security tools.

References / Textbooks:

1. Allen, Grant, Nikhil Gopal, and Michael Thomas. Beginning Android 4. Apress, 2012.
2. Horton, John. Android Programming for Beginners. Packt Publishing Ltd, 2015.
3. Hardy, Brian, and Bill Phillips. Android Programming: The Big Nerd Ranch Guide. Addison-Wesley Professional, 2013.
4. Himanshu Dwivedi, Chris Clark, David Thiel, Mobile Application Security, Tata McGraw Hill, 1st Edition, 2010.
5. Neil Bergman, Mike Stanfield, Jason, Rouse , Joel Scambray , Sarath Geetha kumar , Swapnil Deshmukh, Scott Matsumoto , John Steven , Mike Price, Hacking Exposed Mobile Security Secrets & Solutions, McGraw-Hill Osborne Media,1st Edition ,2013.
6. https://developer.android.com

Master of Science (Information and Network Security) Semester – II

(Session 2020-21)

COURSE CODE: MINP-2116

LAB ON MOBILE APPLICATION DEVELOPMENT AND SECURITY

Examination Time: 3 Hrs **Max. Marks: 100**

Practical: 80

CA:20

Lab on Mobile Application Development & Security

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3111
CYBER INCIDENT HANDLING AND REPORTING

Course Outcomes:

CO1: Obtain the basic knowledge on dealing with system security related incidents.

CO2: Gain experience using tools and common processes in performing the analysis of compromised systems.

CO3: Increase knowledge on potential defenses and counter measures against common threats / vulnerabilities.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3111
CYBER INCIDENT HANDLING AND REPORTING

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Concept of Computer security Incident, Types of Incident-denial of service-malicious code, unauthorized access, Inappropriate Usage. Need for incident Response, Policies, Plans and Procedure related to incident Response, Incident reporting organization.

UNIT - II

Incident Detection and Analysis: Profiling, Behaviors, Centralized logging , Event Correlation, Diagnosis matrix , Incident Analysis – Incident Documentation ,incident Prioritization, Incident Response SLA Matrix , Incident Notification.

UNIT - III

Handling denial of Service Incident: DoS attacks, Concept of DDoS, Types of DDoS- Reflector Attacks, Amplifier Attacks and Floods, Prevention of DDoS-Incident Handling Preparation, Containment Strategy, Handling Unauthorized Access Incidents, Malicious Code Incidents.

UNIT - IV

Incident Handling Tools: Disk Digger, NTFS Walker, LOG Auditing

References / Textbooks:

1. Barbara Guttman, Edward Roback, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, 1995.
2. Julie Lucas, Brian Moeller, The Effective Incident Response Team, Addison-Wesley Professional, 2004.
3. Michael E. Whitman, Herbert J. Mattord, Principles of Incident Response and Disaster

Recovery, Thomson Course Technology, 2007.
4. E. Eugene Schultz, Russell Shumway, Incident Response: A Strategic Guide to Handling System and Network Security Breaches, New Rider Publishing, 2002.
5. Chris Prosise, Kevin Mandia, Incident Response & Computer Forensics, Tata McGraw-Hill Education, 2003.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3112
CLOUD COMPUTING AND ITS SECURITY

Course Outcomes:

CO1: Analyze the Cloud computing setup and applications using different architectures.

CO2: Design different workflows according to requirements

CO3:Analyze the Virtualization concept

CO4: Access cloud Storage systems and Cloud security, the risks involved, its impact and develop cloud application

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3112
CLOUD COMPUTING AND ITS SECURITY

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Cloud Computing, Advantage & Disadvantage, History of Cloud, Cloud Computing Architecture, Cloud Computing Technologies, Cloud Computing vs Grid Computing, working of Cloud, Cloud Computing Applications, Security Risks of Cloud Computing, Essential Characteristics of Cloud Computing, Cloud deployment model.

Cloud Computing: Cloud Service Models, cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing.

UNIT - II

Virtualization: What is Virtualization, Data Virtualization, Hardware Virtualization, Software virtualization, Server Virtualization, Storage Virtualization, OS Virtualization, Linux Virtualization, Windows virtualization

Cloud security: Cloud Security challenge, Principal Characteristics of Cloud Computing security, Data center security Recommendations, Encryption and key management in the cloud, identity and access management, trust models for cloud, Cloud forensics, traditional security, business continuity and disaster recovery.

UNIT - III

Cloud Service providers: Cloud Service Provider Companies, Amazon EC2, AWS vs Azure vs GCP. Different Clouds - Mobile Cloud Computing, Fog Computing, Green cloud, Sensor Cloud Computing, IoT cloud.

UNIT - IV

Data security tools and techniques for the cloud: Understanding the cloud architecture, Governance and enterprise risk management, design of customized cloud security measures,

application security, targets of cybercrime.

Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues,

References / Textbooks:

1. Jim Smith, Ravi Nair, and Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005.
2. John Rittinghouse and James F.Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press Taylor and Francis Group, 2010.
3. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010.
4. John R. Vacca, Cloud Computing Security, CRC Press, 2016.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3113
PROACTIVE SECURITY TOOLS AND TECHNOLOGY

Course Outcomes:

CO1: Learn about the security policies and strategies

CO2: Gain the knowledge about various tools to be used in the implementation of penetration testing

CO3: Learn various commands used in the implementation of proactive security

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3113
PROACTIVE SECURITY TOOLS AND TECHNOLOGY

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Network Security tool taxonomy: Reconnaissance tools, attack and penetration tools, defensive tools, Security planning, Security Strategies, Security threats.

UNIT - II

High interaction honeypots, Medium interaction honeypots, Low interactions honeypots and Virtual honeypots, Netcat (Sniff army knife), NMAP (Active scanning), Nessus (Penetration testing), TCPDUMP, Wireshark (passive traffic sniffing)

UNIT - III

NSLOOKUP, DIG (DNS information retrieval), Firewalling (iptables), Reverse firewalling, securing honeypots, sebek, Argos, Honeywall, Network traffic visualization.

UNIT - IV

Hybrid systems, client honeypots, Botnets, tracking botnets, analysing malware, Hacking channel jargon and interpretation.

References / Textbooks:

1. Niels Provos, Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison-Wesley, 2007.
2. The Honeynet Project, Know Your Enemy: Learning about Security Threats, Addison-Wesley Professional, 2004.

3. Mike Schiffman, Building Open Source Network Security Tools: Components and Techniques, Wiley, 2002.
4. Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, Network Security: The Complete Reference, McGraw Hill Education, 2017.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3114
PENETRATION TESTING AND AUDITING

Course Outcomes:

CO1: Learn about the risk analysis

CO2: Student can achieve the knowledge about the planning and scheduling of penetration testing

CO3: Achieve the knowledge about different platforms of testing

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3114
PENETRATION TESTING AND AUDITING

Examination Time: 3 Hrs **Max. Marks: 100**

Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT – I

Identify Risk, Manage Risk, Risk mitigation, Customers and legal agreements, Penetration testing planning and scheduling, Information gathering.

UNIT – II

External and internal network penetration testing. Router penetration testing, Firewalls penetration testing, Intrusion detection system penetration testing

UNIT – III

Wireless networks penetration testing, Password cracking penetration testing, social engineering penetration testing.

UNIT – IV

Application penetration testing, Policies and controls testing. Penetration testing report and documentation writing

References / Textbooks:

1. T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Hack I.T.: Security Through Penetration Testing, Addison-Wesley, 2002.
2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, Metasploit: The Penetration Tester's Guide, No Starch Press, 2011.
3. Thomas Wilhelm, Professional Penetration Testing: Creating and Learning in a Hacking Lab, Syngress, 2013.

4. William Chuck Easttom II, Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, Pearson, 2018.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3115
CRYPTOGRAPHY AND NETWORK SECURITY

Course Outcomes:

CO1: Learning of classifying the symmetric encryption techniques

CO2: Illustrate various public key cryptographic techniques

CO3: Evaluate the authentication and hash algorithms

CO4: Learn basic concepts of system level security.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINL - 3115
CRYPTOGRAPHY AND NETWORK SECURITY

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction to cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play fair Cipher, Block Cipher. Data Encryption Standard (DES), DES (Contd.), Triple DES, Modes of Operation, Stream Cipher, Pseudorandom Sequence. LFSR based Stream Cipher, Abstract algebra, Number Theory.

UNIT - II

Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Eular Phi-Function, Eular's theorem, Quadratic Residue, Polynomial Arithmetic. Advanced Encrypton Standard (AES), Introduction to Public Key Cryptosystem, Dife-eellman KeyExchange, Knapsack Cryptosystem, RSA Cryptos ystem. Primarily Testing, Ellamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curveModulo a Prime.

UNIT - III

Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function, Universal hashing, Cryptographic hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), More on Key Exchange Protocol.

UNIT - IV

Cryptanalysis, Time-Memory Trade-of Attack, Differential Cryptanalysis, Linear Cryptanalysis. Cryptanalysis on Stream Cipher. Internetwork Security, SSL, PGP, Cloud Security, Introduction to Blockchain and Bitcoin.

References / Textbooks:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2003.
2. Behrouz A. Forouzan, Cryptography & Network Security, McGraw Hill Education, 2010.
3. S.Bose, P.Vijayakumar, Cryptography and Network Security, Pearson, 2016.
4. Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill, 2003.
5. Bruce Schneier, Applied Cryptography, John Wiley & Sons, 2015.

Note: The latest editions of the books should be followed.

Master of Science (Information and Network Security) Semester – III

(Session 2020-21)
COURSE CODE: MINP - 3116
LAB ON PENETRATION TRSTING AND VIRTUALIZATION

Examination Time: 3 Hrs **Max. Marks: 100**
Practical: 80
CA:20

Lab on Penetration Testing and Virtualization using Vmware etc.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4111
INTRUSION DETECTION SYSTEM

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend the importance of intrusion detection.

CO2: Identify various Intrusion Detection systems and methodologies associated with them.

CO3: Evaluate the impact of Intrusion Detection Systems.

CO4: Identify the integration of multiple IDS.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4111
INTRUSION DETECTION SYSTEM

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction and an Overview of Intrusion Detection Systems: Introduction about intrusion detection systems, Purpose and Scope of intrusion detection systems, Need of intrusion detection systems, applications of intrusion detection systems, Firewalls and intrusion detection systems.

UNIT - II

Intrusion Detection Systems and Associated Methodologies: Uses of Intrusion detection technologies, Key Functions of Intrusion detection systems, Common Detection Methodologies, Signature-Based Detection, Anomaly-Based Detection, stateful protocol analysis, Types of Intrusion detection technologies

UNIT - III

Intrusion detection Technologies and Components: Components and Architecture, Typical Components Network Architectures, Security capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities Prevention Capabilities and its implementation, Deploying IDS.

UNIT - IV

Using and Integrating Multiple Intrusion Detection Systems Technologies The Need for Multiple IDS technologies, Integrating Different IDS Technologies, Direct IDS Integration Indirect IDS Integration, Other Technologies with IDS Capabilities, Network Forensic Analysis Anti-Malware Technologies, Honeypots

References / Textbooks:

1. Tim Crothers, Implementing Intrusion Detection Systems: A Hands–On Guide for Securing the Network, John Wiley and Sons.
2. Christopher Kruegel, Fedrick Valeur, Intrusion Detection and Correlation: Challenges and Solutions, Springer.
3. Chris Sanders, Intrusion Detection Honeypots: Detection through Deception (2020).

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4112
REVERSE ENGINEERING AND MALWARE

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend complete taxonomy of malware.

CO2: Comprehend the Reverse Engineering Malware Methodology.

CO3: Examine the presence and impact of malware.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4112
REVERSE ENGINEERING AND MALWARE

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Malware, Analysis, and Trends, Malware taxonomy and characteristics: Understanding Malware Threats: Malware indicators, Malware Classification, Examining Clam AV Signatures , Creating Custom Clam AV Databases.

UNIT - II

Malware Analysis (MA): Reverse Engineering Malware (REM) Methodology, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis.

UNIT - III

Resources for Reverse-Engineering Malware (REM): Initial Infection Vectors and Malware Discovery, Sandboxing Executables and Gathering Information From Runtime Analysis, The Portable Executable (PE32) File Format, Identifying Executable Metadata, Executable Packers and Compression, and Obfuscation, Techniques.

UNIT - IV

Utilizing Software Debuggers to Examine Malware, Analyzing Malicious Microsoft Office and Adobe PDF Documents, Analyzing Malicious Browser-based Exploits, Automating the Reverse Engineering Process.

References / Textbooks:

1. Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard “Malware Analyst’s Cookbook and DVD: Tools and Techniques for Fighting Malic ious Code”, First Edition (2010), Wiley Publications.
2. Ed Skoudis and Lenny Zeltser, “Malware: Fighting Malicious Code” (2003). Prentice Hall Publications.
3. Cameron H. Malin, Eoghan Casey, and James M. Aquilina “Malware Forensics: Investigating and Analyzing Malicious Code” (2008), Syngress Publications.
4. EldadEilam , “Reversing: Secrets of Reverse Engineering” (2005), Wiley.
5. Blokdyk, Gerardus, “Reverse Engineering Malware: The Ultimate Step-By-Step Guide” (2018).

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4113
ETHICAL HACKING

Course Outcomes:

After passing this course the student will be able to:

CO1: Articulate the concept of security and phases involved in hacking.

CO2: Comprehend various hacking techniques Sniffing Traffic, DNS and IP Sniffing, HTTPS Sniffing, WLAN Sniffers, etc.

CO3: Comprehend session hijacking along with its types and phases.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4113
ETHICAL HACKING

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Introduction: Understanding the importance of security, Concept of ethical hacking and essential Terminologies-Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking

UNIT - II

Foot Printing: Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase.

System Hacking: Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing.

UNIT - III

Session Hijacking: Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools.

UNIT - IV

Hacking Wireless Networks: IEEE 802.11a and IEEE 802.11b standards, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.

References / Textbooks:

1. Network Security and Ethical Hacking, Rajat Khare, Luniver Press,(2006).
2. Ethical Hacking, Thomas Mathew, OSB Publisher, (2003).
3. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, (2005).
4. Ethical Hacking and Network defense, Simpson, Cengage Learning, (2009).

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4114
BLOCKCHAIN FOR ENTERPRISE APPLICATIONS

Course Outcomes:

After passing this course the student will be able to:

CO1: Comprehend elements and working of Blockchain.

CO2: Identify the role of Blockchain in Decentralization.

CO3: Apply payment process in Bitcoin and Ethereum.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MINL-4114
BLOCKCHAIN FOR ENTERPRISE APPLICATIONS

Examination Time: 3 Hrs **Max. Marks: 100**
Theory: 80
CA:20

Instructions for Paper Setter -

Eight questions of equal marks (16 marks each) are to set, two in each of the four sections (A-D). Questions of Sections A-D should be set from Units I-IV of the syllabus respectively. Questions may be divided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each section. The fifth question may be attempted from any section.

UNIT - I

Blockchain : Introduction, History, Elements of Blockchain, Working of a blockchain, tiers, features, Types, Benefits and Limitations, Consensus.

Decentralization: Use of Blockchain in Decentralization, Methods of Decentralization, Routes, Smart Contracts, Decentralized Organizations, Requirements of Decentralized Application, Platforms for Decentralization, Symmetric Cryptography, Private Key Cryptography

UNIT - II

BitCoin: Introduction, Digital Key and address, Transaction, Blockchain Structure, Mining

Bitcoin Network Wallets, Bitcoin Payments

UNIT - III

Bitcoin Clients and APIs: Bitcoin Installation, Type of Clients, setting up a bitcoin node

Bitcoin Limitations, Development of altcoins, Namecoin, Primecoin, Zcash

UNIT - IV

Ethereum: Introduction, Ethereum network, Components, Development Environment, Alternative Blockchains – Kadena, Ripple, Stellar, Rootstack, Quorum, BigchainDB

References / Textbooks:

1. Ambadas Tulajadas Choudhari, MR Sharn, Blockchain for Enterprise Applications, Wiley (2020)
2. Tiana Laurence, Blockchain for Dummies, Wiley (2017)
3. Daniel Drescher, Blockchain Basics, Apress (2017), 1st Edition
4. David Shrier, Basic Blockchain: What it is and How it will transform the way we work and live, Robinson Publishers (2020)

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MIND-4115
MAJOT PROJECT / DISSERTATION

Course Outcomes:

After passing course the student will be able to:

CO1: Apply the tools and techniques learnt to frame problems and their corresponding solutions.

CO2: Develop skills necessary to structure, manage and execute projects.

CO3: Learn to work as a member of a cohesive unit.

CO4: Develop presentation skills.

CO5: Perform documentation related to development of the project.

Master of Science (Information and Network Security) Semester – IV

(Session 2020-21)
COURSE CODE: MIND-4115
MAJOT PROJECT / DISSERTATION

Examination Time: 6 Hrs **Max. Marks: 200**
Practical: 160
CA:40

1. Candidates have to submit only one hard copy and CD of documentation which shall be kept with the course supervisor/guide in the college only. Further, supervisor/guide OR principal of college shall forward two copies of DVD (Digital Versatile Disk) containing all the documentation files of the students (file name to be saved as Rollno_of_the_student .pdf) to the concerned branch of the University. Covering letter (duly signed by the principal/Head of the college/institute) should contain the following information. Candidate name, Candidate Roll no, Project Title of the student and .pdf file name of his project documentation.
2. The assignment shall be evaluated by a board of three examiner (two (02) External examiners and one (01) internal examiner) as approved by the BOS.
3. The Project is to be submitted as per the common ordinances for P.G. courses under semester system.