FACULTY OF ENGINEERING & TECHNOLOGY

SYLLABUS

FOR

M.Sc. (Information and Network Security)
(Semester: I – IV)

SESSION: 2019–20

GURU NANAK DEV UNIVERSITY
AMRITSAR

APPENDICES TO ACADEMIC COUNCIL (SYLLABI FOR THE SESSION 2019-20)
(FACULTY OF ENGINEERING & TECHNOLOGY)

Eligibility:
B.C.A/B. Sc. (IT) with 50% marks in aggregate

OR

Graduation with Computer Science / Computer Application / IT / Computer Maintenance as one of the elective subjects with 50% marks in aggregate.

The rest ordinances will be as per common ordinance for undergraduate courses w.e.f. 2012–2013 and postgraduate courses under semester system w.e.f. 2011–2012 for affiliated colleges /distance education/ private candidates.

SEMESTER – I:

1)	Computer Networks	100 Marks
2)	Network Protocols	100 Marks
3)	Network Operating System	100 Marks
4)	Information Security & Threats	100 Marks
5)	Lab on NOS	100 Marks

SEMESTER – II:

1)	N/W Planning, Analysis & Performance	100 Marks
2)	N/W Security Practices	100 Marks
3)	Computer Forensic Fundamentals	100 Marks
4)	Secure Code Development	100 Marks
5)	Lab on N/W Security Practice	100 Marks

SEMESTER – III:

1)	Cyber Incident Handling & Reporting	100 Marks
2)	Cloud Computing and Its Security	100 Marks
3)	Proactive Security Tools & Technology	100 Marks
4)	Penetration Testing & Auditing	100 Marks
5)	Lab on Penetration Testing & Virtualization	100 Marks

SEMESTER – IV:

1)	Intrusion Detection System & Analysis	100 Marks
2)	Reverse Engineering & Malware	100 Marks
3)	Ethical Hacking	100 Marks
4)	Major Project/ Dissertation	300 Marks

Paper–I: Computer Networks

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

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

Section–B

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)

Section–C

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

Section–D

Quality of Service in Routing & Signalling: 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:

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 Frozen: Computer Network.

Paper–II: Network Protocols

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

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.

Section–B

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. Routing in an internet, direct and indirect delivery, table driven IP routing, next Hop Routing, default routes, host specific routes, The

Section–C

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.

Section–D

User Datagram Peotocol (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:

1. Douglas E.Comer, Internetworking with TCP/IP: Principles, Protocols.
2. Forouzan, TCP–IP, Protocol Suit, TMH.
3. Comer, Internetworking with TCP–IP, Vol. 3.
4. Unix Network Programming, W. Richard Stevens.
5. SNMP, Stallings, Pearson.
6. TCP–IP Network Administration, Hunt Craig.

M.Sc. Information & Network Security (Semester – I)

Paper–III: Network Operating System

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

Instructions for the Paper Setters:-

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.

The student can use only Non-programmable & Non-storage type calculator.

Section–A

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

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

Section–B

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.

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

Section–C

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.
Jobs, Disaster Recovery Plan, Assessing Threats, Restoring Data using Backup

Section–D

Case & Comparative Studies: Windows 2003 Server & Linux Server

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

References:

1. Redhat Linux(10) Bible : Christopher Negus, 2003.
2. Linux Unleashed : Tim Parker, 2006.
3. Linux Administration Tools : Charles Fisher, 2007.
4. Window 2003 4 in 1: Dream Tech.

Paper–IV: Information Security & Threats

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

Essential terminology, Hardware, Software, Malware, Defining security, Need for security

Cyber crime vs Computer based crime, Information Security statistics, Three pillars of Security

Section–B

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.

Section–C

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

Section–D

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 tcpdump and wireshark, generating digital certificates, understanding CAs.

Recommended Books:

1. Cryptography and Network Security, Atul Kahate, Second Edition, McGraw Hill, 2010.
2. Information Security Principles and Practices, Mark Merkow. Jim Briethaupt, Pearson, 2006.
3. Principles of Information Security, Michael E Whitman, Herbert J Mattord, Cengage Learning, 2010.

Paper–V: Lab on NOS

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

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

Paper–I: N/W Planning, Analysis and Performance

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

Traffic Engineering and Capacity Planning: Throughout calculation traffic characteristics & source models, traditional traffic engineering, queued data & packet switched traffic modeling, designing for peaks, delay or latency

Section–B

Requirements, Planning & Choosing Technology: Business requirements, technical requirement user requirements, traffic sizing characteristics time & delay consideration
Network Performance Modeling and Analysis: creating traffic matrix, design tools, components of design tools, types of design projects

Section–C

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.

Section–D

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:

1. James D McCabe, Network Analysis, Architecture and Design, 2nd Edition, Morgan Kaufman Series in Networking, 2007.
2. Youeu Zheng, Shakil Akhtar, Network for Computer Scientists and Engineers, Oxford University Press, 2007.
3. Foruzan, Data Communications & Networking, Tata–Megraw Gill 2006.
4. Darren L. Spohn, Co–Authors: Tina L. Brawn and Scott G Rau.

Paper–II: N/W Security Practices

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

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

Section–B

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

Section–C

Public Key Encryption Methods: Principles, RSA Algorithm, Key management, Diffie–Hellman key exchange, Elliptic curve cryptography
Authentication: Requirements, functions, Authentication codes, Hash functions

Section–D

Digital Signatures: Basics, Digital signature standard, Authentication Protocols
Other Securities:
IP Security: overview and architecture, Authentication Header; Electronic Mail security: Pretty Good Privacy; Web security: overview.

References:

1. Cryptography and Network Security: Principles and Practice – William Stallings.
2. Introduction to Modern Cryptography by J. Katz and Y. Lindell.
3. Handbook of Applied Cryptography by A. Menezes, P. Van Oorshot, S. Vanstone.

Paper–III: Computer Forensic Fundamentals

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

Computer Forensics Fundamentals: Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources, Employment Proceedings ,Computer Forensics Services ,Benefits of Professional Forensics Methodology ,Steps Taken by Computer Forensics Specialists ,Who Can Use Computer Forensic Evidence?

Section–B

Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised, Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls, Biometric Security Systems

Section–C

Vendor and Computer Forensics Services: Occurrence of Cyber Crime, Cyber Detectives, Fighting Cyber Crime with Risk–Management Techniques, Computer Forensics Investigative Services, Forensic Process Improvement

Data Recovery: Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data–Recovery Solution, Hiding and Recovering Hidden Data

Evidence Collection and Data Seizure: Why Collect Evidence?, Collection Options, Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure

Section–D

Computer Image Verification and Authentication: Special Needs of Evidential Authentication, Practical Considerations

Networks: Network Forensics Scenario, A Technical Approach, Destruction of Email, Damaging Computer Evidence, Tools Needed for Intrusion Response to the Destruction of Data, System Testing

Reference:

Computer Forensics: Computer Crime Scene Investigation, Second Edition, John R. Vacca.

Paper–IV: Secure Code Development

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section–A

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

Section–B

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

Section–C

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.

Section–D

Security Techniques, authentication, authorization, Buffer Overrun, Access control, least privilege, Input issues: database, web–specific, internationalization. Security testing, security code review, secure software installation, writing security documentation.

Recommended Books:

1. Writing Secure Code, Michael Howard and David LeBlanc, Microsoft Press, (2006).
2. Software Engineering – Security as A Process in the SDLC, Nithin Haridas, (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.

Paper–V: Lab on N/W Security Practice

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

Lab on N/W Security Practice

Paper-I: Cyber Incident Handling and Reporting

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

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.

Section B

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

Section C

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.

Section D

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

Recommended Books:

1. An Introduction to Computer Security: The NIST Handbook, Barbara Guttman, Edward Roback, NIST Special Publication 800-12.
2. The Effective Incident Response Team, Julie Lucas, Brian Moeller, Addison-Wesley Professional.
3. Principles of Incident Response and Disaster Recovery, Michael E. Whitman, Herbert J. Mattord, Thomson Course Technology, 2007.
4. Incident Response: A Strategic Guide to Handling System and Network Security Breaches, E. Eugene Schultz, Russell Shumway, New Rider Publishing-2002.
5. Incident Response & Computer Forensics, Mandia, Tata McGraw-Hill Education-2006.

Paper-II: Cloud Computing & Its Security

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

Introduction: Basics of the emerging cloud computing paradigm, Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Virtualization Technology and Cloud Computing.

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

Section B

Virtualization: concept and properties of virtualization, CPU virtualization, memory virtualization, I/O virtualization, Forms of CPU 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.

Section C

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 cyber crime.

SectionD

Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues, Virtual Machines and Security Issues.

Recommended Books:

1. Jim Smith, Ravi Nair, and Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005.
2. Cloud Computing: Implementation, Management, and Security, John Rittinghouse and James F.Ransome, CRC Press Taylor and Francis Group.

Paper-III: Proactive Security Tools and Technology

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

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

Section B

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).

Section C

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

Section D

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

Recommended Books

1. Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Niels Provos, Thorsten Holz.
2. Know Your Enemy: Learning about Security Threats (2nd Edition), Lance Spitzner.
3. Building Open Source Network Security Tools: Components and Techniques, Mike Schiffman.

Paper-IV: Penetration Testing and Auditing

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

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

Section B

Router penetration testing, Firewalls penetration testing, Intrusion detection system penetration testing

Section C

Wireless networks penetration testing, Password cracking penetration testing, Social engineering penetration testing, Application penetration testing, Policies and controls testing.

SectionD

Penetration testing report and documentation writing

Recommended Books

1. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8.
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, MatiAharoni.
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm.

Paper-V

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

Lab on Penetration Testing and Virtualization using Vmware etc.

Paper-I: Intrusion Detection System and Analysis

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

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.

Section B

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

Section C

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.

Section D

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

Recommended Books:

1. Tim Crothers, Implementing Intrusion Detection Systems: A Hands–On Guide for Securing the Network, John Wiley and Sons.
2. Christopher Kruegel, FedrickValeur, Intrusion Detection and Correlation: Challenges and Solutions, Springer.

Paper-II: Reverse Engineering & Malware

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

Introduction to Malware, Analysis, and Trends,Malware taxonomy and characteristics:
Understanding Malware Threats: Malware indicators, Malware Classification, Examining ClamAV Signatures ,Creating Custom ClamAV Databases.

Section B

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

Section C

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.

Section D

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

Recommended Books:

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.

Paper-III: Ethical Hacking

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

Instructions for the Paper Setters:-
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided 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.
The student can use only Non-programmable & Non-storage type calculator.

Section A

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

Section B

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.

Section C

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

Section D

Hacking Wireless Networks: Introduction to 802.11,Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLANScanners, WLANSniffers, Hacking Tools, Securing Wireless Networks.

Recommended Books:

1. Network Security and Ethical Hacking, Rajat Khare, Luniver Press, 30-Nov-2006.
2. Ethical Hacking, Thomas Mathew, OSB Publisher, 28-Nov-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.

Paper-IV: Major Project / Dissertation
(Based on Case Study of Live Cases etc.)

Time: 3 Hrs. **Max. Marks: 300**

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.