FACULTY OF ENGINEERING & TECHNOLOGY

SYLLABUS

FOR

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

SESSION: 2019–20

GURU NANAK DEV UNIVERSITY
AMRITSAR

Note: (i) Copy rights are reserved.
   Nobody is allowed to print it in any form.
   Defaulters will be prosecuted.

(ii) Subject to change in the syllabi at any time.
    Please visit the University website time to time.
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
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

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

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:
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
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.

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
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:
2. Forouzan, TCP–IP, Protocol Suit, TMH.
5. SNMP, Stallings, Pearson.
6. TCP–IP Network Administration, Hunt Craig.
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.


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


Section–D

Case & Comparative Studies: Windows 2003 Server & Linux Server


References:

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:

Lab on NOS: Installation & Configuration of NOS (Windows 2003, Linux) and their Administration. User account creation, group creation, DHCP settings, Backup & Recovery plan.
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:
Paper–II: N/W Security Practices

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:
2. Introduction to Modern Cryptography by J. Katz and Y. Lindell.
M.Sc. Information & Network Security (Semester – II)

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


Section–B


Section–C


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:
Paper–IV: Secure Code Development

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

Recommended Books:
M.Sc. Information & Network Security (Semester – II)

Paper–V: Lab on N/W Security Practice

Time: 3 Hrs.                                          Max. Marks: 100

Lab on N/W Security Practice
M.Sc. Information & Network Security (Semester – III)

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


Section B


Section C


Section D

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

Recommended Books:

2. The Effective Incident Response Team, Julie Lucas, Brian Moeller, Addison-Wesley Professional.
Paper-II: Cloud Computing & Its Security

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

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

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.

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

Recommended Books:
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


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

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.

Section D

Penetration testing report and documentation writing

Recommended Books

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

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:
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

Section C

Section D

Recommended Books:

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


Recommended Books:

2. Ethical Hacking, Thomas Mathew, OSB Publisher, 28-Nov-2003.
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.