Course Title: Network Security **Credit: 3**
Course No: CSIT.423.3 **Number of period per week: 3+3**
Nature of the Course: Theory + Lab **Total hours: 45+45**
Year: Fourth, Semester: Eight
Level: B. Sc. CSIT

1. Course Introduction

This course introduces key concepts of network security. The topics include the basic concepts of network security including application, transport, IP and data link layer security mechanisms and protocols. The course covers the wireless security principles as well as the use of firewalls to secure networks.

2. Objectives

The objective of the course is to introduce basics of network security principles so that students will be able to use network and internet security techniques including transport and IP security approaches together with the use of firewall to secure the public and private networks.

3. Specific Objectives and Contents

Specific Objectives	**Contents**
• Understand basics of network security • Understand security in OSI • Discuss attacks on network • Understand and explore about NAC, EAP	**Unit I: Introduction (7 Hrs)** 1.1. Overview of network security, Goals of Network Security, Methods to achieve network security 1.2. Security Architecture of OSI Reference Model 1.3. Security Services and Layering: Link to Link Encryption, End-to-End Encryption 1.4. Threats and Attacks in Network, Denial of Service Attacks, Repudiation Attacks 1.5. Network Access Control (NAC), NAC enforcement methods, Extensible Authentication Protocol (EAP)
• Understand basic security mechanisms at application layer • Discuss Email Security Protocols • Explore about DNS Security, Secured HTTP and security in ecommerce using SET.	**Unit II: Application Level Security(8 hr)** 2.1. Security issues at application layer 2.2. Email-Security, Email Security Services, Pretty Good Privacy (PGP), Services of PGP, Privacy Enhancement Mail (PEM), Secure Multipurpose Internet Mail Extension (S/MIME), Domain Keys Identified Mail (DKIM) 2.3. DNS Security, Domain Name System Security Extension (DNSSEC) 2.4. S-HTTP, Secure Electronic Transaction (SET)
• Explore details of SSL and TLS. • Understand the differences	**Unit III: Transport Level Security (6 hr)** 3.1. Security issues at transport layer 3.2. Secured Socket Layer (SSL), Features of SSL,

between SSL and TLS • Understand an overview of HTTPS (HTTP over SSL). • Understand an overview of Secure Shell (SSH).	Architecture of SSL 3.3. Transport Layer Security (TLS), Features of TLS, Architecture of TLS, Comparison of SSL and TLS 3.4. HTTPS, SSH, SSH Services
• Present an overview of IP security (IPsec). • Explain the difference between transport mode and tunnel mode. • Understand the concept of security association. in IPSec • Summarize use of IPsec in VPN	**Unit IV: IP Security (5 hr)** 4.1. Overview of IP Security 4.2. IPSec Protocol, Architecture of IPSec Protocol: IPSec Policy AH Protocol, ESP Protocol, Transport and Tunnel Mode of IPSec, Key Management in IPSec 4.3. Applications of IPSec 4.4. Virtual Private Network(VPN), Ensuring VPN using IPSec
• Understand the security attacks at data link layer • Discuss different Ethernet security approaches	**Unit V: Data Link Layer Security (5 Hrs)** 5.1. Attacks at Data Link Layer: ARP Spoofing, MAC Flooding, Port Stealing 5.2. Securing Ethernet LANs: Port Security, Preventing ARP Spoofing, Spanning Tree Protocols, Preventing Attacks on STP, 5.3. Securing VLANs
• Understand the essential elements of the IEEE 802.11 wireless LAN standard. • Explore the various components of the IEEE 802.11i wireless LAN security architecture.	**Unit VI: Wireless Network Security(6 Hrs)** 6.1. IEEE 802.11 Wireless LAN Overview 6.2. IEEE 802.11i Wireless LAN Security 6.3. Wireless Application Protocol Overview 6.4. Wireless Transport Layer Security 6.5. WAP End-to-End Security
• Understand concepts of firewalls • Explore types of firewalls • Explain the use of firewalls in secured networks	**Unit VII: Firewalls (4 Hrs)** 7.1. Introduction of firewalls, Need for Firewalls 7.2. Types of Firewalls: Packet Filtering, Stateful Inspection, Application Level Gateways, Circuit Level Gateways, Host Based Firewalls, 7.3. Securing Networks by configuring Firewalls
• Understand the concepts of network security management • Understand the use of SNMP • Explore the concepts of USM and VACM	**Unit VIII: Network Management Security (4 Hrs)** 8.1. Basic Concepts of SNMP, Protocol Context of SNMP 8.2. SNMP V1, V2, V3 8.3. User Security Model (USM) 8.4. View Based Access Control Model (VACM)

Evaluation System

Undergraduate Programs							
External Evaluation	**Marks**	**Internal Evaluation**	**Weight age**	**Marks**	**Practical**	**Weight age**	**Mark**
End semester examination	60	Assignments	20%	20	Practical Report copy	25%	20
(Details are given in the separate table at the end)		Quizzes	10%		Viva	25%	
		Attendance	20%		Practical Exam	50%	
		Internal Exams	50%				
Total External	60	Total Internal	100%	20		100%	20
Full Marks 60+20+20 = 100							

External evaluation

1. **End semester examination:**
   It is a written examination at the end of the semester. The questions will be asked covering all the units of the course. The question model, full marks, time and others will be as per the following grid.

2. **External Practical Evaluation:**
   After completing the end semester theoretical examination, practical examination will be held. External examiner will conduct the practical examination according to the above mentioned evaluation. There will be an internal examiner to assist the external examiner. Three hours time will be given for the practical examination. In this examination Students must demonstrate the knowledge of the subject matter.

Full Marks: 100, Pass Marks: 45, Time: 3 Hrs

Nature of question	Total questions to be asked	Total questions to be answered	Total marks	Weightage
Group A: multiple choice*	20	20	20×1 = 20	60%
Group B: Short answer type questions	7	6	6×8 = 48	60%
Group C: Long answer type questions	3	2	2×16 =32	60%
			100	100%

Each student must secure at least 50% marks in internal evaluation in order to appear in the end semester examination. Failed student will not be eligible to appear in the end semester examinations.

Internal evaluation

Assignment: Each student must submit the assignment individually. The stipulated time for submission of the assignment will be seriously taken.

Quizzes: Unannounced and announced quizzes/tests will be taken by the respective subject teachers. Such quizzes/tests will be conducted twice per semester. The students will be evaluated accordingly.

Attendance in class: Students should regularly attend and participate in class discussion. Eighty percent class attendance is mandatory for the students to enable them to appear in the end semester examination. Below 80% attendance in the class will signify NOT QUALIFIED (NQ) to attend the end semester examination.

Presentation: Students will be divided into groups and each group will be provided with a topic for presentation. It will be evaluated individually as well as group-wise. Individual students have to make presentations on the given topics.

Mid-term examination: It is a written examination and the questions will be asked covering all the topics in the session of the course.

Discussion and participation: Students will be evaluated on the basis of their active participation in the classroom discussions.

Instructional Techniques: All topics are discussed with emphasis on real-world application. List of instructional techniques is as follows:

- Lecture and Discussion
- Group work and Individual work
- Assignments
- Presentation by Students
- Quizzes
- Guest Lecture

Students are advised to attend all the classes and complete all the assignments within the specified time period. If a student does not attend the class (es), it is his/her sole responsibility to cover the topic(s) taught during that period. If a student fails to attend a formal exam/quiz/test, there won’t be any provision for re-exam. Unless and until the student clears one semester he/she will not be allowed to study in the following semesters.

Laboratory Work

Student should write programs to simulate the network security protocols. The instructor should facilitate the appropriate use of security tools to simulate the security mechanisms in above mentioned chapters. Students should be able to configure the firewalls and other network security management tools. The lab work should be practiced for minimum of 3 lab hours per week.

Prescribed Text

1. William Stallings, “Network Security Essentials: *applications and standards”*, Prentice Hall

References

1. William Stallings, "Cryptography and Network Security: Principles and Practices", Pearson Education.
2. Michael T. Goodrich and Roberto Tamassia, “Introduction to Computer Security”, Pearson Education
3. Chris Brenton and Cameron Hunt, ‘Mastering Network Security”, SYBEX
4. Eric Maiwald , “Network Security A Beginner’s Guide”, McGraw-Hill
5. B. A. Forouzan, "Cryptography & Network Security", Tata Mc Graw Hill.