VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
B.E: Electronics & Communication Engineering / B.E: Electronics & Telecommunication Engineering
NEP, Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
(Effective from the academic year 2021 – 22)

VII Semester

Network Security			
Course Code	**21EC742**	CIE Marks	50
Teaching Hours/Week (L:T:P:S)	3:0:0:1	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	3	Exam Hours	3

Course objectives:

- **Preparation**: To prepare students with fundamental knowledge/ overview in the field of Network Security with knowledge of security mechanisms and services.
- **Core Competence**: To equip students with a basic foundation of Network Security by delivering the basics of Transport Level Security, Secure Socket Layer, Internet Protocol security, Intruders, Intrusion detection and Malicious Software, Firewalls, Firewall characteristics, Biasing and Configuration.

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teacher can use to accelerate the attainment of the various course outcomes.

1. Lecture method (L) does not mean only traditional lecture method, but different type of teaching methods may be adopted to develop the outcomes.
2. Show Video/animation films to explain the different Network Security Techniques / Algorithms
3. Encourage collaborative (Group) Learning in the class
4. Ask at least three HOTS (Higher order Thinking) questions in the class, which promotes critical thinking
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyze information rather than simply recall it.
6. Topics will be introduced in a multiple representation.
7. Show the different ways to solve the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.
9. Adopt Flipped class technique by sharing the materials / Sample Videos prior to the class and have discussions on the that topic in the succeeding classes
10. Give Programming Assignments

Module-1

Attacks on Computers and Computer Security: Need for Security, Security Approaches, Principles of Security Types of Attacks. **(Text2: Chapter1)**
Security Mechanisms, Services and Attacks, A model for Network security **(Text1: Chapter1: 3, 4, 5, 6)**
Network Access Control, Extensible Authentication Protocol **(Text1: Chapter 16: Section 1,2)**

Teaching-Learning Process	Chalk and talk method, YouTube videos, Flipped Class Technique **RBT Level:** L1, L2, L3

Module-2

Transport Level Security: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, Secure Shell (SSH) **(Text1: Chapter15)**

Teaching-Learning Process	Chalk and talk method YouTube videos, Flipped Class Technique and PPTs. Self-study topics: Block cipher modes, Cryptographic Hash functions and MAC codes **RBT Level:** L1, L2, L3

Module-3	
IP Security: Overview of IP Security (IPSec), IP Security Architecture, Modes of Operation, Security Associations (SA), Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange. **(Text1: Chapter19)**	
Teaching-Learning Process	Chalk and talk method, YouTube videos, Flipped Class Technique and PPTs. Self-study topics: OSI Model **RBT Level:** L1, L2, L3
Module-4	
Intruders: Intruders, Intrusion Detection, Password Management. **(Chapter20-Text1)** **MALICIOUS SOFTWARE:** Viruses and Related Threats, Virus Countermeasures, **(Chapter21-Text1)**	
Teaching-Learning Process	Chalk and talk method, YouTube videos, Flipped Class Technique and PPTs. **RBT Level:** L1, L2, L3
Module-5	
Firewalls: The Need for firewalls, Firewall Characteristics, Types of Firewalls, Firewall Biasing, Firewall location and configuration **(Chapter 22-Text 1)**	
Teaching-Learning Process	Chalk and talk method, YouTube videos, Flipped Class Technique and PPTs. **RBT Level:** L1, L2, L3

Course outcomes (Course Skill Set)

At the end of the course the student will be able to:

1. Explain network security services and mechanisms and explain security concepts
2. Understand the concept of Transport Level Security and Secure Socket Layer.
3. Explain Security concerns in Internet Protocol security
4. Explain Intruders, Intrusion detection and Malicious Software
5. Describe Firewalls, Firewall Characteristics, Biasing and Configuration

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 35% (18 Marks out of 50) in the semester-end examination (SEE), and a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

Three Unit Tests each of **20 Marks (duration 01 hour**)

1. First test at the end of 5th week of the semester
2. Second test at the end of the 10th week of the semester
3. Third test at the end of the 15th week of the semester

Two assignments each of **10 Marks**

4. First assignment at the end of 4th week of the semester
5. Second assignment at the end of 9th week of the semester

Group discussion/Seminar/quiz any one of three suitably planned to attain the COs and POs for **20 Marks** (**duration 01 hours**)

6. At the end of the 13th week of the semester

The sum of three tests, two assignments, and quiz/seminar/group discussion will be out of 100 marks and will be **scaled down to 50 marks**

(to have less stressed CIE, the portion of the syllabus should not be common /repeated for any of the methods of the CIE. Each method of CIE should have a different syllabus portion of the course).

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per

the outcome defined for the course.

Semester End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the subject (**duration 03 hours)**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.

The students have to answer 5 full questions, selecting one full question from each module. Marks scored out of 100 shall be reduced proportionally to 50 marks

Suggested Learning Resources:

Text Books:

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 5th Edition, 2014, ISBN: 978-81-317- 6166-3
2. Atul Kahate, "Cryptography and Network Security", TMH, 2003.

Reference Books:

1. Cryptography and Network Security, Behrouz A Forouzan, TMH, 2007.
2. Introduction to Computer Security, Matt Bishop, Sathyanarayana S V, Pearson Education, 2006, ISBN 81-7758-425/1.

Web links and Video Lectures (e-Resources)

https://nptel.ac.in/courses/106105031
https://nptel.ac.in/courses/128106006

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Programming Assignments / Mini Projects can be given to improve programming skills.