Course Title: **Network Security**
Course No.: ICT. Ed 468
Level: Bachelor
Semester: Sixth

Program: **BICTE**
Nature of course: Theoretical + Practical
Credit Hour: 3 (2+1)
Teaching Hour: 64(32+32)

1. Course Description

The course, Network Security, is a major course for students studying towards acquiring the Bachelor in Information Communication Technology Education (BICTE). This course aims to provide fundamental skills needed to understand the internal and external security threats against a network, and to implement security policies that will protect an organization's information. The course objective is to impart fundamental understanding of every facet of information security, security policies, cryptography, authentication, security of network, system, user and program, identifying malware, perform vulnerability analysis, auditing and attacks and responses to those attacks.

2. General Objectives

The general objectives of this course are as follows:

- Develop an understanding of computer security and its mechanism.
- Gain familiarity with prevalent network and system attacks, defenses against them, and forensics to investigate the aftermath.
- Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

3. Course Outlines:

Specific Objectives	Contents	Hours (Th+Pr)
• Explain the concept of Computer Security. • Understand the basic terminologies related to security.	**1. Introduction** 1.1 The Basic Components 1.2 Threats 1.3 Policy and Mechanism 1.4 Assumptions and Trust 1.5 Assurance 1.6 Operational and Human Issues	3
• Explain Security policies and its types • Develop confidentiality, integrity, and availability policies	**2. Policies** **2.1 Security Policies** 2.1.1 The Nature of Security Policies 2.1.2 Types of Security Policies 2.1.3 The Role of Trust 2.1.4 Example: Academic Computer Security Policy	5+5

	2.2 Confidentiality Policies 2.2.1 The Bell-LaPudala Model **2.3 Integrity Policies** 2.3.1 The Biba Model **2.4 Availability Policies** 2.4.1 Goals of Availability Policies 2.4.2 Denial of Service Models 2.4.3 Example: Availability and Network Flooding **Practical Works** • Visit an organization in your local place and develop security policies and procedures for that organization. Present the prepared report in front of your classmates and the stakeholders of that organization.	
• Explain the Public-Key Encryption Structure. • Apply the Symmetric Cryptosystem. • Explain the requirements for digital signature. • Explain the key management strategies. • Develop cipher text • Identify and implement different types of authentication methods	**3. Cryptography** **3.1 Basic Cryptography** 3.1.1 Symmetric Cryptosystems 3.1.2 Public Key Cryptography 3.1.3 Cryptographic Checksums 3.1.4 Digital Signature 3.1.5 Hashing **3.2 Key Management** 3.2.1 Session and Interchange Keys 3.2.2 Key Exchange and Generation 3.2.3 Cryptographic Key Infrastructures 3.2.4 Storing and Revoking Keys **3.3 Cipher Techniques** 3.3.1 Stream and Block Ciphers 3.3.2 Authenticated Encryption **3.4 Authentication** 3.4.1 Authentication Basics 3.4.2 Passwords 3.4.3 Password Selection 3.4.4 Attacking Passwords 3.4.5 Password Aging 3.4.6 Biometrics 3.4.7 Multifactor Authentication **Practical Works** • Write program to create cipher text • Write program to validate strong password	7+5
• Analyze the network infrastructure.	**4. Security and Protection** **4.1 Network Security**	8+10

• Configure Network devices to enhance security. • Explain the different types of encryption and decryption techniques in network. • Identify and discuss the different strategies used to secure wired and wireless network. • Explain the mechanism of System, User, Program, Email, Web and Database Security. • Install and configure the firewall to achieve its benefits. • Make use of VPN to secure electronic communication.	4.1.1 Network Infrastructure Analysis 4.1.2 Encryption and Decryption in Network 4.1.3 Firewall and its types 4.1.4 Wired and Wireless Security 4.1.5 Virtual Private Network **4.2 System Security** **4.3 Email, Web and Database Security** **4.4 User Security** 4.4.1 Access 4.4.2 Files and Devices 4.4.3 Electronic Communications **4.5 Program Security** 4.5.1 Common Security-Related Programming Problems **Practical Works** • Configure routers, switches, and other network devices to enhance security. • Assess and secure web applications against common security threats. Use tools like OWASP ZAP or Burp Suite for web application security testing. • Configure firewalls to control and monitor network traffic.	
• Explain the different methods of intrusion detection. • Perform vulnerability analysis. • Conduct penetration testing. • Know different types of Malicious Software. • Design an auditing system. • Engage in simulated attacks and develop response techniques to overcome the attacks.	**5. Threats, Assessment and Solutions** **5.1 Malware** 5.1.1 Introduction 5.1.2 Trojan Horses 5.1.3 Computer Viruses 5.1.4 Computer Worms 5.1.5 Bots and Botnets 5.1.6 Other Malware 5.1.7 Theory of Computer Viruses 5.1.8 Defenses **5.2 Vulnerability Analysis** 5.2.1 Penetration Studies 5.2.2 Vulnerability Classification **5.3 Auditing** 5.3.1 Definition 5.3.2 Designing an Auditing System 5.3.3 Examples: Auditing File Systems **5.4 Intrusion Detection** 5.4.1 Principles 5.4.2 Basic Intrusion Detection 5.4.3 Organization of Intrusion Detection Systems **5.5 Attacks and Responses** 5.5.1 Attacks	9+12

	5.5.2 Representing Attacks 5.5.3 Intrusion Response 5.5.4 Digital Forensics **<u>Practical Works</u>** • Conduct vulnerability assessments on systems and networks using tools such as Nessus or OpenVAS. • Conduct security audits to assess the overall security posture of an organization. • Develop and deliver security awareness training programs for naive users. • Engage in simulated attacks on systems to identify vulnerabilities. Use tools like Metasploit or Wireshark to analyze network traffic and find potential security weaknesses.	

4. Instructional Techniques

The instructional techniques for this course are divided into two groups. First group consists of general instructional techniques applicable to most of the units. The second group consists of specific instructional techniques applicable to specific units.

4.1 General Techniques

- Providing the reading materials to the students to familiarize the units.
- Lecture, question-answer, discussion, brainstorming, practical, and buzz session.

4.2 Specific Instructional Techniques

Unit	Activity and instructional techniques	Teaching Hours(64)
1 to 5	Use network security tools to implement the algorithm	

5. Evaluation (Internal Assessment and External Assessment):

Nature of course	Internal Assessment	External Practical Exam/Viva	Semester Examination	Total Marks
Theory	40%	20%	40%	100%

***Note**: Students must pass separately in internal assessment, external practical exam / viva and or semester examination.*

5.1 Evaluation for Part I (Theory)

5.1.1 Internal Evaluation 40%

Internal evaluation will be conducted by course teacher based on following activities: