

PRINCIPLES OF CYBER SECURITY

I Year B. Tech. I Semester
(Common to CSC, CSF)

Course Code:

L T P C

Prerequisites:

3 0 2 4

COURSE OUTCOMES (COS)

At the end of the course, students will be able to:

CO1: Understand the network security model and security principles. (L2)

CO2: Classify the cryptographic techniques and authentication mechanisms. (L2)

CO3: Understand the Email Security Mechanisms and IP security. (L2)

CO4: Use different techniques to create passwords and understand SNMP versions. (L3)

CO5: Explain types of malicious soft wares and firewalls. (L2)

UNIT I

(8 Lectures)

INTRODUCTION:

Computer Security Concepts, Security Goals, Attack Surface, Model of Network Security.

SECURITY PRINCIPLES: Security Trends, The OSI Security Architecture Security Attacks, Security Mechanisms and Services; Security Controls: Authentication, Authorization and Access Control.

Learning Outcomes: At the end of the unit, student will be able to

1. Define security concepts and attack surface. (L1)
2. Understand the network security model. (L2)
3. Explain OSI security architecture, and security controls. (L2)

UNIT II

(12 Lectures)

CRYPTOGRAPHIC FOUNDATIONS: Cryptography Concepts, Symmetric Key Encryption, Asymmetric Key Encryption, Cryptographic Hash Functions, Digital Signatures, Digital Certificates, Public Key Infrastructure (PKI).

AUTHENTICATION APPLICATIONS: Kerberos, X.509 Authentication Service, Federated Identity Management -SSO

Learning Outcomes: At the end of the unit, student will be able to

1. Understand the basic cryptographic concepts. (L2)
2. Explain authentication Mechanisms. (L2)
3. Compare Kerberos and X.509 authentication mechanisms. (L2)

UNIT III

(12 Lectures)

NETWORK SECURITY: E-MAIL, Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (SMIME)

IP SECURITY: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload.

Learning Outcomes: At the end of the unit, student will be able to

1. Understand the E-mail security Mechanisms. (L2)
2. Explain IPsec architecture. (L2)
3. Understand authentication header and, payload encapsulation of IP. (L2)

UNIT IV

(10 Lectures)

NETWORK MANAGEMENT SECURITY: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3.

INTRUDERS: Intruders, Intrusion Detection, Password Management

Learning Outcomes: At the end of the unit, student will be able to

1. Explain the basic concepts and versions of SNMP protocol. (L2)
2. Identify and analyse different types of intruders and intrusion detection techniques.(L1)
3. Demonstrate different mechanisms to create and protect passwords.(L3)

UNIT V

(8 Lectures)

MALICIOUS SOFTWARE: Viruses and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks.

FIREWALLS: The Need for Firewall, Characteristics and Access Policy 412 12.3 Types of Firewalls

Learning Outcomes: At the end of the unit, student will be able to

1. Explain different types of malicious soft wares and countermeasures.(L2)
2. Understand Distributed Denial-of-Service (DDoS) attacks.(L2)
3. Explain the role of firewalls and types.(L2)

TEXT BOOKS:

1. William Stallings, “*Network Security Essentials: Applications and Standards*”, 6th Edition, Pearson Education, 2017

REFERENCE BOOKS:

1. William Stallings, “*Cryptography and Network Security: Principles and Practice*”, 8th Edition, Pearson Education, 2023
2. Behrouz A. Forouzan, “*Cryptography and Network Security*”, 3rd Edition, McGraw Hill, 2015

WEB REFERENCES:

1. <https://www.verizon.com/business/resources/articles/s/understanding-essential-cyber-security-principles/>

COURSE OUTCOMES

CO1: Analyse and filter network packets using Wireshark. (L4)

CO2: Examine HTTP, HTTPS/TLS, DNS, and email protocols traffic. (L4)

CO3: Examine TCP, UDP, and DHCP communication processes. (L4)

CO4: Demonstrate network connectivity and address resolution using ICMP and ARP. (L3)

CO5: Analyse IEEE 802.11 frames and basic wireless security mechanisms. (L4)

Note: Students have to use open source tool Wireshark to do the following:

- Wireshark is a free and open-source packet analyser.
- It is used for network trouble shooting, analysis, software and communication protocol development and education.

- It captures network traffic and allows the user to see the data flow across the network.

Any 12 Programs must be completed

LIST OF EXPERIMENTS:

1. **Introduction to Wireshark:** Capture network packets using Wireshark and explore its basic interface, packet details, and filtering features.
2. **HTTP Traffic Analysis:** Capture and analyse HTTP traffic to examine request methods and server response messages.
3. **HTTPS and TLS Analysis:** investigate HTTPS connections by capturing packets and analysing the TLS handshake process.
4. **DNS Traffic Analysis:** Capture and analyse DNS queries and responses to understand the domain name resolution process.
5. **TCP Three-Way Handshake:** Examine TCP packets to understand the three-way handshake, sequence numbers, and acknowledgment mechanisms.
6. **TCP Flow and Congestion Control:** Observe TCP traffic to analyse flow control and congestion control mechanisms during data transmission.
7. **TCP and UDP Comparison:** Capture and compare TCP and UDP traffic to understand the differences between connection-oriented and connectionless communication.
8. **ICMP Analysis using Ping and Traceroute:** Use Ping and Traceroute to capture and analyse ICMP packets, including echo requests and replies.
9. **ARP Packet Analysis:** Capture and examine ARP packets to understand the process of resolving IP addresses to MAC addresses.
10. **DHCP Process Analysis:** Capture and analyse DHCP packets to understand the Discover, Offer, Request, and Acknowledgment (DORA) process.
11. **Email Protocol Analysis:** Capture and examine SMTP, POP, and IMAP traffic to understand electronic mail communication protocols.
12. **Wireless Frame Analysis:** Capture and analyse wireless frames to understand IEEE 802.11 standards and basic wireless security mechanisms.
13. **Password Cracking & Strength Analysis:** Perform password cracking using sample password hashes and analyse password strength using John the Hashcat.
14. **Packet Capture & Replay:** Capture and replay network packets in a controlled environment and analyse replay attack detection techniques using Wireshark and Scapy.
15. **MITM Demonstration:** Simulate a MITM attack in a controlled network and analyse intercepted traffic using Wireshark and Ettercap.
16. **Network Scanning & Vulnerability Assessment:** Perform network scanning to identify open ports, running services, and potential vulnerabilities using Nmap and OpenVAS.

