# INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal, Hyderabad - 500 043

## COMPUTER SCIENCE ENGINEERING

## DEFINITION AND TERMINOLGY

| | | | | | |
|---|---|---|---|---|---|
| Department | **CYBER SECURITY** | | | | |
| Course Title | **NETWORK SECURITY** | | | | |
| Course Code | ACCC03 | | | | |
| Program | B.Tech | | | | |
| Semester | V | | | | |
| Course Type | Core | | | | |
| Regulation | UG-20 | | | | |
| Course Structure | Theory | | | Practical | |
| | Lecture | Tutorials | Credits | Laboratory | Credits |
| | 3 | 1 | 4 | 3 | 1.5 |
| Course Coordinator | Y.Manohar Reddy,Asst.Professor | | | | |

## COURSE OBJECTIVES:

**The students will try to learn:**

| | |
|---|---|
| I | The Fundamental practices, policies, technologies and standards in providing security on network |
| II | The TCP/IP networking mechanism to diagnose the security problems in network. |
| III | The different network and communication protocols presence in the network to apply some security factors. |

## COURSE OUTCOMES:

**After successful completion of the course, students should be able to:**

| | | |
|---|---|---|
| CO 1 | **Demonstrate** various security problems that implemented in Tcp/ip protocol suite. | Understand |
| CO 2 | **Recall** Denial of Service(DoS) attcks can cause the problems in network. | Remember |
| CO 3 | **Compare** different practices,policies and standards that provides security on network. | Understand |
| CO 4 | **Analyze** Internet Control Message Protocol(ICMP) utilities that helps to monitor the networking mechanism. | Analyze |

| | | |
|---|---|---|
| CO 5 | **Utilize** the different Pretty Good Privacy(PGP) services that offered on Email Security. | Apply |
| CO 6 | **Summarize** the Concept of Transport Layer Security(TLS) provides security against on web threats . | Understand |

## DEFINITION AND TERMINOLOGY:

| S.No | DEFINITION | CO's |
|---|---|---|
| | **MODULE I** | |
| | **INTRODUCTION ON NETWORKING AND SECURITY** | |
| 1 | **Recall the term security in Networking?** | CO 1 |
| | This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects. | |
| 2 | **State the term Access Control?** | CO 1 |
| | Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources | |
| 3 | **List the Components of Access Control?** | CO 1 |
| | Authentication,Authorization,Access,Manage,Audit are the Components of Access Control. | |
| 4 | **Is there Difference Between Authentication and Authorization?** | CO 1 |
| | Authentication and authorization are crucial to access control in security. Authentication is the process of logging in to a system, such as an email address, online banking service, or social media account. Authorization is the process of verifying the user's identity to provide an extra layer of security that the user is who they claim to be. | |
| 5 | **Recall the term website security?** | CO 1 |
| | Website security refers to the protection of personal and organizational public-facing websites from cyber attacks. | |
| 6 | **List some additional steps to protect against website attacks?** | CO 1 |
| | • Sanitize all user input. • Increase resource availability. • Implement cross-site scripting (XSS) and cross-site request forgery (XSRF) protections. • Implement a Content Security Policy (CSP). • Audit third-party code. • Implement additional security measures. | |
| 7 | **How does we refer LAN?** | CO 2 |
| | LAN is also referred to as a broadcast domain. This simply means in a situation when a user uses his/her LAN to broadcast any information. | |
| 8 | **List out Some Security Services?** | CO 2 |

| | | |
|---|---|---|
| | •Confidentiality (privacy) •Authentication (who created or sent the data) •Integrity (has not been altered) •Non-repudiation (the order is final) •Access control (prevent misuse of resources) •Availability (permanence, non-erasure) •Denial of Service Attacks •Virus that deletes files | |
| 9 | **State the name of Routing Information Protocol (RIP) ?** | CO 2 |
| | Routing Information Protocol (RIP) is a routing protocol used in TCP/IP suite to route packets based on hop count. Before making a routing decision RIP counts the number of hops on every path available and dispatches the packet on the path with minimum hops to the destination. | |
| 10 | **What is the difference between a DDoS attack and a DOS attack?** | CO 2 |
| | difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as "low and slow" attacks like Slowloris, derive their power in the simplicity and minimal requirements needed to them be effective. | |
| **MODULE II** | | |
| **REAL-TIME COMMUNICATION SECURITY** | | |
| 1 | **State the term of TCP/IP protocol importance?** | CO 3 |
| | TCP/IP includes several higher level protocols that facilitate common applications such as electronic mail, terminal emulation, and file transfer. | |
| 2 | **Recall the function of Application Level Gateways?** | CO 3 |
| | An application-level gateway intercepts the incoming and outgoing packets, runs a proxy to copy and forward information across the gateway, and functions as a proxy server, thereby preventing any direct connection between a trusted server or client and an untrusted host. | |
| 3 | **Define Internet Protocol Security ?** | CO 3 |
| | Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs). | |
| 4 | **Formulate the Term IPSecurity?** | CO 3 |
| | IP Sec= Aunthenticate Header(AH)+Encapsulating Security Payload(ESP)+Internet Key Exchange (IKE) | |
| 5 | **Frame the Format of Authenticate Header in Transport Mode?** | CO 3 |
| | Original IP,Authenticate Header,TCP header,Data | |
| 6 | **Recall the Protocol IKE?** | CO 3 |

| | | |
|---|---|---|
| | Internet Key Exchange (IKE) is a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN). | |
| 7 | **Write various Improvements in IKEv2 over IKEv1 ?** | CO 3 |
| | Various methods of holding the grain in the case are Cartridge loaded grain and case bonded grains | |
| 8 | **Write the importance of Packet Firewall in Network Security?** | CO 5 |
| | A packet filtering firewall is a network security feature that controls the flow of incoming and outgoing network data. The firewall examines each packet, which comprises user data and control information, and tests them according to a set of pre-established rules. | |
| 9 | **recall the concept of Anonymity?** | CO 3 |
| | An anonymity network enables users to access the Web while blocking any tracking or tracing of their identity on the Internet. This type of online anonymity moves Internet traffic through a worldwide network of volunteer servers. | |
| 10 | **How do we Understand Message Integrity?** | CO 3 |
| | Message integrity means that a message has not been tampered with or altered. The most common approach is to use a hash function that combines all the bytes in the message with a secret key and produces a message digest that is difficult to reverse. | |
| **MODULE III** | | |
| **INTERNET CONTROL MESSAGE PROTOCOL** | | |
| 1 | **State the Protocol Internet Control Message Protocol (ICMP)?** | CO 4 |
| | The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. | |
| 2 | **Write the attacks available with ICMP?** | CO 4 |
| | ICMP flood attack,Ping of death attack, Smurf attack ICMP is not the only network layer protocol used in layer 3 DDoS attacks. Attackers have also used GRE packets in the past, for instance. | |
| 3 | **List the Parameters that ICMP contains?** | CO 4 |
| | 1.Type. 2.Code. 3.Checksum. | |
| 4 | **state the term reconnaissance technique?** | CO 4 |
| | Reconnaissance is a set of processes and techniques (Footprinting, Scanning , Enumeration) used to covertly discover and collect information about a target system. | |
| 5 | **List different Scanning and reconnaissance tools ?** | CO 4 |
| | 1. Nmap 2. Wireshark 3. Google Hacking 4.AngryIPScanner etc.. | |
| 6 | **Recall the term ping sweep (ICMP sweep)?** | CO 4 |

| | | |
|---|---|---|
| | A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers). | |
| 7 | **State the Importance of IP Host Network Monitor?** | CO 4 |
| | IP Host Network Monitor is a powerful ping tool with a significant cost benefit. This software runs as a Windows service and offers basic ping monitoring functionalities, including automatic scheduling of ICMP ping requests, with response, errors, and response time logged and reported on. | |
| 8 | **What Is the Difference Between Ping and Traceroute?** | CO 4 |
| | The primary difference between ping and traceroute is that while ping simply tells you if a server is reachable and the time it takes to transmit and receive data, traceroute details the precise route info, router by router, as well as the time it took for each hop. | |
| 9 | **refer the use of ICMP Router Discovery in Networking?** | CO 4 |
| | The IP address of surrounding routers is discovered via the ICMP router discovery protocol. "Router Advertisements" or "Router Solicitations" are the ICMP router discovery messages. | |
| 10 | **List different types of attacks and utilities of ICMP?** | CO 4 |
| | •ICMP Tunneling •ICMP Router Discovery •Smurf attack •Fraggle Attack •ICMP flood attack •Ping of death attack •Information Gathering •Trace Route •Port Scan •OS fingerprinting •Teardrop | |
| **MODULE IV** | | |
| **ELECTRONIC MAIL SECURITY** | | |
| 1 | **State the Term PGP in Electronic Mail Security?** | CO 5 |
| | Pretty Good Privacy (PGP) provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. | |
| 2 | **What are the various services offered by PGP?** | CO 5 |
| | 1. Authentication 2. Confidentiality 3. Compression 4. E-mail compatibility 5. Segmentation | |
| 3 | **List various Cryptographic Keys and Key Rings offered by PGP?** | CO 5 |
| | PGP makes use of four types of keys:<br>1. One-time session symmetric keys 2. Public keys 3. Private keys 4. Passphrase based symmetric keys | |
| 4 | **List the Parameters in structure of private and public-key rings?** | CO 5 |
| | • Timestamp: • Key ID: • Public Key: • Private key: • User ID: | |
| 5 | **Write the steps that to perform Message Transmission?** | CO 5 |
| | 1.Signing the message: 2. Encrypting the message: 3. Decrypting the message: 4. Authenticating the message: | |

| | | |
|---|---|---|
| 6 | **How do we understood PGP is safe ?** | CO 5 |
| | PGP is extremely safe, if used correctly and securely by individuals and organizations' employees. The encryption method uses algorithms that are considered unbreakable and is one of the most secure ways to protect data and cloud systems. Protecting data with PGP makes it effectively impossible to be intercepted by hackers | |
| 7 | **Understand the process of Digital Signature Verification?** | CO 5 |
| | A digital signature works through algorithms that combine a sender's key with the data they try to send in an email message. This creates a hash function, which is an algorithm that converts the email message into a fixed-size block of data. That data is then encrypted using the email sender's private key, and the recipient can decrypt the message using the sender's public key. | |
| 8 | **What are the public key versions of PGP?** | CO 5 |
| | •Rivest-Shamir-Adleman (RSA): RSA is one of the first public-key cryptosystems, which encrypts a short key created using the International Data Encryption Algorithm (IDEA). •Diffie-Hellman: The Diffie-Hellman version enables two users to generate shared private keys through which they can exchange data on insecure channels. It encrypts the message with a short key using the CAST algorithm and the Secure Hash Algorithm (SHA-1) to create a hash code. | |
| 9 | **list the steps for How Does PGP Encryption Work** | CO 5 |
| | PGP follows a three-step process:<br>Step 1: PGP generates a huge, one-time-use public encryption algorithm that cannot be guessed, which becomes the random session key. Step 2: The session key is then encrypted using the recipient's public key, which protects the message while being transmitted. The recipient shares that key with anyone they want to receive messages from. Step 3: The message sender submits their session key, then the recipient can decrypt the message using their private key. | |
| 10 | **Refer the uses of PGP Encryption** | CO 5 |
| | •authenticate messages and for integrity checking •Encrypting Emails•Digital Signature Verification•Encrypting Files | |
| **MODULE V** | | |
| **WEB SECURITY** | | |
| 1 | **List various Protocols that implemented on Web?** | CO 6 |
| | •Hypertext Transfer Protocol (HTTP) •File Transfer Protocol (FTP) •Simple Mail Transfer Protocol (SMTP) •Simple Network Management Protocol (SNMP) | |
| 2 | **List various higher-layer protocols are defined as part of TLS?** | CO 6 |
| | •the Handshake Protocol. •the Change Cipher Spec Protocol. •the Alert Protocol. | |

| | | |
|---|---|---|
| 3 | **Understand different states associated with sessions in Web?** | CO 6 |
| | •Session identifier •Peer certificate: •Compression method: •Cipher spec: •Master secret: | |
| 4 | **What are TLS Record Protocol provides services for TLS connections?** | CO 6 |
| | •Confidentiality •Message Integrity | |
| 5 | **State the importance of Handshake Protocol?** | CO 6 |
| | The most complex part of TLS is the Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in a TLS record. The Handshake Protocol is used before any application data is transmitted. | |
| 6 | **What are the different TLS Handshake Protocol Message Types?** | CO 6 |
| | •Hello-request •client-hello •Server-hello •Certificate-verify | |
| 7 | **State the importance of SSL?** | CO 6 |
| | SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. SSL encrypts data that is transmitted across the web. | |
| 8 | **What is an SSL certificate?** | CO 6 |
| | SSL can only be implemented by websites that have an SSL certificate (technically a "TLS certificate"). An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server. | |
| 9 | **Write the types of SSL certificates?** | CO 6 |
| | • Single-domain • Wildcard: • Multi-domain: | |
| 10 | **How do we understand SSL/TLS working?** | CO 6 |
| | • SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be. • SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient. | |

**Course Coordinator:**
**Mr Y.Manohar reddy**

**HOD CSE(CS)**