Assignment No: 01

Q] What are the core components of the TCP/IP protocol stack & how do they contribute to the functioning of computer net?

Ans: The core components of TCP/IP protocol stack:

- Application Layer: It includes programs and services that let you do things like sending emails (SMTP), websites (HTTP), and chatting (FTP).

- Transport Layer: It manages the actual sending and receiving of data between your computer and the other device. There are 2 popular 'waiters': TCP & UDP.

- Internet Layer: It uses IP addresses to locate your computer and the one you want to talk to. Just like your home address helps the delivery person find you, IP addresses help data find its way across the internet.

- Link Layer: It deals with physical connections, like wifi or ethernet cables. It make sure that the data packets travel safely across these connections.

network. How does routing protocol help in efficient data transmission?

Ans:

- IP Addressing: Assigns unique numerical labels (IP addresses) to devices on a network. Identifies and locates devices for communication.

- Routing: Selects paths for data to travel from source to destination. Data is divided into packets with destination IP addresses.

- Routers: Specialized network devices for routing data.

- Routing Tables: Stores information about network destinations and paths

- Routing Protocols: Used by routers to exchange destination info. Dynamically updates routing tables based on network changes.

- Efficient Data Transmission: Routing protocols help routers choose optimal paths. Adjust routing based on changing network conditions. Ensures quick and efficient data transmission.

Q7. Outline the key steps involved in the ethical hacking and describe how these steps contribute to securing computer systems.

Ans: i) Planning & reconnaissance.

- understanding the target system and its computers.
- Gather information about potential vulnerabilities and weaknesses.

ii) Scanning.

- use various tools to actively scan the target for vulnerabilities.
- Identify open ports, services and potential attacks vector.

iii) Gaining Access.

- Attempt to exploit vulnerabilities to gain access.
- Mimic real-world attacks to uncover weaknesses.

iv) Maintaining Access.

- once access is achieved, maintain control to analyse the extent of compromise.

v) Analysis and reporting:

- Evaluate the results of the ethical hacking tests.
- Provides recommendations to fix and strengthen security measures.

Ans:

Aspects	OSI Model	TCP/IP model
Layers	7 layers	4 layers
Layer Names	Physical, Data-link, network, Transport, session, Presentation & Application	Network, Transport linked, Application.
Granularity	More detailed, each layer has specific functions	Less detailed, layers encompasses broader functions
Origin	Developed by the ISO	evolved from the ARPANET
Adoption	less commonly referenced in practice	widely used as the basis for internet architecture.

Q]. Explain the process of information gathering and reconnaissance in the context of network security?

Ans: i] Info gathering & Recon in security Assessment.

- Essential in security checks, exposing vulnerabilities.
- Ethical hacking's recon phase collects data for attack paths.

ii] Footprinting: Passive & Active.

- Passive → Gather public data
- Active → Intrusive methods

iii] Recon objectives

- Attackers choose vulnerable targets, explore exploits.
- Any org member can be the initial target.

iv] Exploiting Recon Data.

- Data used for targeted attacks, social engineering.
- Vulnerabilities found exploited for unauthorized access.

v] Preventing Recon Attacks.

- Strong security policies, controls needed.
- Regular network monitoring is crucial.

Ans:

Aspect	Vulnerability Assessment	Penetration Testing
Purpose	Identifies vulnerabilities in a system.	Simulates real-world attack to exploit vulnerabilities
Focus	Scans & identifies potential weakness.	Actively exploits vulnerabilities to assess real-world
Depth	Less intrusive	More aggressive.
Ex. Tools	Nessus, OpenVAS.	Metasploit, Burp.
Outcome	Provides a list of vulnerabilities.	Evaluates the system defense & response mechanisms

Q] Describe the key characteristics of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks.

Ans: i] Manipulation of Human Psychology

- Social engineering attacks exploit human emotions and behaviors, such as trust, fear, authority.

ii] Pretexting

- Attackers create fabricated scenarios or pretexts to deceive victims into divulging sensitive info.

iii] Impersonation

- Attackers impersonate legitimate individuals or entities, often using fake emails, phone calls.

iv] Urgency.

- Attackers create a sense of urgency to pressure victims into making hasty decisions

v] Scarcity:

- By creating a perception of limited availability, attackers entice victims to act quickly without careful consideration

Q] Investigate the different types of malware threats, such as viruses, worms and Trojans & explain their impact on network security.

Ans; i] Viruses: Replicates by modifying other programs & inserting its own code. Successful replication results in infection of the affected areas.

ii] Worms: Independent malware program that self-replicates to spread to other computers.

iii] Trojan Horses: Misleads users about its true intent. Named after the deceptive Trojan Horse from Greek mythology.

Impact & Risks:

Malware can steal sensitive data, disrupt networks, and damage or destroy data.