Name :- Abhijeet A. Basant
Roll No:- 9689
Branch :- AI & DS
Sub:- Cybersecurity (Sem V)

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Assignment 1

1) What are the core components of the TCP/IP protocol stack & how do they contribute to the functioning of computer networks

Ans The TCP/IP protocol stack is the fundamental framework that governs how data is transmitted & received over computer networks. The core components are:

1) Application Layer

This is the topmost layer & deals with the communication between application running on different devices. It provides protocols that allow application to exchange data over the network. Some common protocol are HTTP, FTP, SMTP & DNS.

2) Transport layer

The transport layer is responsible for end-to-end communication & data segmentation. It shields the upper layer application from the complexities of data. The two main protocols in this layer are:

a) Transmission Control Protocol (TCP)

It provides reliable, connection-oriented communication. It fixes errors, orders the segment & establishes the connections.

b) User Diagram Protocol (UDP)

It is connection-less, lightweight protocol. It is used when speed & low overhead are more important than reliability.

3) Internet layer
This layer is responsible for addressing, routing & packet forwarding. It deals with IP address, which uniquely identify devices on the network & routing protocols that determine the best path for transmission.

4) Link Layer
It also known as Network Interface or Data Link layer This layer deals with physical connection to the network medium like Ethernet, Wi-Fi, etc It is responsible for data packaging into frames, error detection & medium access control.

→ Each layer of TCP/IP protocol contributes different function-ing.

i) Application layer: Establish communication between devices, facilitating data exchange.

ii) Transport layer: Ensure reliable data transfer (TCP) or speed (UDP)

iii) Internet layer :- Routes data with IP addresses, ensuring proper delivery.

iv) Link layer : Handles physical connection, data framing & low level communication.

Q) Explain the process of IP addressing & routing in a computer network. How does routing protocol help in efficient data transmission?

Ans: IP addressing:

1) Unique Identification:
IP addresses uniquely identify devices on a network.

2) IPv4 & IPv6:
Two main versions: IPv4 (32 bit) & IPv6 (128-bit).

3) Subnetting:
Dividing a network into smaller subnets for efficient address allocation.

4) Private & Public Addresses:
Private addresses for local networks, public addresses for internet communication.

5) DHCP: Dynamic Host Configuration Protocols assigns IP addresses dynamically.

Routing:

1) Definition: Process of directing data packets from source to destination.
2) Router Roles: Routers determine optimal paths for data transmissions.

iv) Routing Tables: Store network topology & paths to diff destinations.

iv) Static vs Dynamic Routing:
Static routes manually configured; dynamic routes updated using routing protocols.

v) Routing algorithms:
Determine best path based on metrics like distance, cost or speed.

-> Routing Protocol's Role in Effivient Data Transmission

i) Path Determinations
ii) Dynamic Adaptation
iii) Redundancy
iv) Load Balancing
v) Fast Convergence
vi) Scalability

3) Outline the key steps involved in ethical hacking & describe how these steps contribute to securing computer system.

i) Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a traget using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, etc.

ii) Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be ~~expo~~ exploited. The tools used in this process are Nessus, NMAP, Nexpose.

iii) Gaining Access

In this process, the vulnerability is located and ~~the~~ hacker attempt to exploit it in order to enter into the system. The primary tool used is Metasploit.

iv) Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker install some backdoors in order ~~into~~ to enter into the system when he needs access in this owned system in future.

v) Clearing Tracks
This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during hacking process.

vi) Reporting
Reporting is the last step of finishing the ethical hacking process. Here hackers compiles a report with his/her finding of the job that was done such as the tool used, the success rate, vulnerabilities found & the exploit processes.

How Ethical hacking Secures Systems
i) Weakness detection :- Reveals vulnerabilities before attackers do.
ii) Risk Reduction :- Proactively minimizes attack potential.
iii) Testing Defenses :- Assesses security measure's effectiveness.
iv) Incident Response :- Improves response strategies.
v) Compliance :- Helps meet industry regulations
vi) Continuous Improvement :- Adapts to evolving threats.

4) Compare and contrast the OSI model and TCP/IP model, highlighting their significance in understanding network communication.

Sr.	Aspect	OSI model	TCP/IP model
i)	Layers	Divided into 7 distinct layers.	Comprises 4 layers with less granularity.
ii)	Standardization	A comprehensive & theoretical framework.	A practical, widely used model in networking.
iii)	Layer function.	Each layer has specific function & responsibilities.	Some layer function overlap or are combined.
iv)	Flexibility	Offers a more modular & theoretical approach.	More streamlined for real world implementation.
v)	Widespread Adoption	Less directly used in practice but offers a conceptual foundation.	Widely used as the basis for the internet's architecture.
vi)	Communication	Each layer communicates with its corresponding layer on another device.	Not always a strict one-to-one correspondence.
vii)	Header format	Encapsulation involves headers, trailers & data	Header contain necessary information for communication.
viii)	Networking Devices	Networking devices can be mapped to OSI layer for conceptual understanding	TCP/IP layers are less rigidly tied to specific devices.

5) Explain the process of information gathering & recon-sance in the context of network security. How can attackers exploit this phase?

Ans Information gathering and reconnaissance are initial phase of an attack where attackers gather intelligence about a target network to identify vulnerabilities and potential entry points. This phase involves:

a) Passive Information Gathering:

i) Collecting publicly available data from source like social media, websites and online directories.

ii) Gathering information about the target's domain names, IP addresses and network infrastructure.

b) Active Information Gathering.

i) Employing network scanning tools to discover active devices, open ports & services.

ii) Identifying potential weakness & vulnerabilities.

c) Footprinting:

i) Assembling information to create a "footprint" of the target network's architecture.

ii) Understanding the network's structure, identifying key assets & potential attack vectors.

d) Network Mapping

i) Utilizes tools for topology & device relationship understanding.

ii) Aids attackers in planning intrusion part

Exploit Exploitation by Attackers

i) Target Identification:
Identifying valueable targets, like sensitive data.

ii) Vulnerability Discovery:
Finding weaknesses for effective attack approaches.

iii) Social Engineering
Exploiting personal data for manipulative attacks

iv) Attack Surface Expansion
Using gathered data to explore more potential vulnerabilities.

6) Differentiate between vulnerability assessment & penetr... Provide e.g. of tools used for each processes.

Aspect	Vulnerability Assessment	Penetration Testing
Purpose	Identifies & quantifies vulner-abilities in a system	Simulates real-world attacks to test system security
Depth of Testing	Generally automated, scans for a wide range of vulnera-bilities.	Manual & automated testing, delves deeper into attacks
Testing Approach	Focuses on identifying vulner-abilities for remediation.	Explores vulnerabilities to assess their real impact
Level of Realism	Less realistic, doesn't exploit vulnerabilities actively.	Highly realistic, mimics attacker's methods & tools.
Tools	Nessus, OpenVAS, BurpSuite	Metasploit, Nmap, Wireshark
Frequency	Regularly performed as part of continuous monitoring.	Often conducted periodically or before major changes.

7) Describe the key characteristic of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks.

Ans Characteristic

1) Manipulation of Human Psychology
Exploits human emotions & behaviour to deceive victims.

2) Deceptive Techniques
Involves methods like phishing, pretexting, tailgating.

3) Human-Centric Targeting
Focuses on tricking individuals to reveal information or take actions.

4) Psychological, Not Technical
Relies on psychological manipulation, not technical vulnerabilities.

5) Varied Attack Channels :
Can occur via emails, calls, in-person interactions or online ~~for~~ platforms.

Educating Employees

1) Awareness Programs
→ To Regular training sessions on social engineering risk
→ Emphasize skepticism & cautions.

iii) Recognizing Suspicious Activities
Identifying unusual emails, calls or access attempts & promptly report such activities.

iii) Phishing Simulations:
→ Conduct simulated phishing campaigns.
→ Offer instant feedback on responses.

iv) Strong Password Practices!
Create strong, unique passwords and avoid sharing.

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

Ans
i) Viruses!
→ Definition: Malicious code that attaches to legitimate programs & spreads when the infected program is executed.

→ Impact: Can corrupt or delete files, slow down system performance & spread over a network

→ Network Impact: Spread via infected files, attachments & removable media, affecting multiple devices.

ii) Worms
→ Definition: Self-replicating malware that spreads across networks without user interaction.

→ Impact: Consumes network resources, overloads servers & can deliver payloads like ransomware or spyware

→ Network impact: Rapidly spreads through vulnerable network points, causing congestion & potential service disruptions

iii) Trojans (Trojan Horses):

Definition :- Malware disguised as legitimate software, often granting attackers unauthorized access.

Impact :- Enables remote control, data theft or other malicious actions.

Network Impact :- Allows attackers to infiltrate a network & gain control over systems