Network Security: Basics, Threats, and Troubleshooting"

Asst.Lec. Tiba Hussein Shamman

Lec1

Introduction:

- Importance of Networks in the Information Age
- Networks have become the backbone of communication and data transfer.
- Networks are used in organizations, companies, and both government and private services.
- Network security is important to protect information and safeguard systems.

1. Definition of a Network

Network: A network is a group of devices connected to each other to exchange data and information.

- **Devices in a network:** Computers, printers, servers, phones.
- **Purpose:** To share resources (files, printers, Internet), improve communication, and provide services centrally.

2. Types of Networks

1. Based on Geographical Area:

- **LAN (Local Area Network):** A local network that covers a limited area, such as a building or office.
- **WAN (Wide Area Network):** A wide network that covers large geographical areas, such as the Internet.
- **MAN (Metropolitan Area Network):** A medium-sized network that covers a city or urban area.
- **PAN (Personal Area Network):** A personal network connecting devices of a single person, such as a phone and a computer.

2. Based on Connection Method:

- **Wired Network:** Uses cables (e.g., Ethernet).
- **Wireless Network:** Uses radio waves or Wi-Fi.

3. Basic Network Components

- **Endpoints:** Computers, phones, printers.
- **Servers:** Provide services such as email, storage, and applications.
- **Networking Devices:**
  - **Switches:** Connect devices within a local network.
  - **Routers:** Connect different networks and direct data traffic.
  - **Access Points:** Provide Wi-Fi connectivity.
- **Network Software:** Network operating systems, monitoring tools, security programs.
- **Transmission Media:** Cables, fiber optics, radio waves.

4. Basics of Network Security

Network security refers to the policies, technologies, and practices used to protect networks, devices, and data from unauthorized access, misuse, or attacks.

1. Core Principles:

- Confidentiality: Ensuring that information is accessible only to authorized users.

  Example: Password protection, Encryption

- Integrity: Ensuring data is not altered without authorization.

  Example: Hashing, Digital signatures

- Availability: Ensuring systems and data are available when needed.

  Example: Backup systems, Protection against DoS attacks

Why is Network Security Important?

1. Protect sensitive information
2. Prevent data theft
3. Maintain system availability
4. Protect organizational reputation
5. Avoid financial loss

Security Tools and Techniques:

- **Firewalls**
- **Antivirus and anti-malware software**
- **Encryption:** Protecting data during transmission
- **Intrusion Detection Systems (IDS):** Detects suspicious activity.
- **Intrusion Prevention System IPS:** Detects and blocks attacks automatically.
- **Authentication Methods:** Passwords, Biometrics ,Two-Factor Authentication (2FA)

5. Network Threats

Any activity that attempts to damage, disrupt, or gain unauthorized access to a network.

- **Internal Threats:** User errors, misuse of privileges.
- **External Threats:** Hacker attacks, malware.
- **Common Examples:** Data theft, eavesdropping on communications.

6. Network Troubleshooting

1. Troubleshooting Steps:

- Identify the problem accurately (e.g., Internet outage, slow network).
- Check endpoints, cables, and wireless connections.
- Use network commands

2. Troubleshooting Methods:

- Restart devices.
- Adjust settings .
- Replace damaged cables or devices.
- Update software and operating systems.
- Scan the network for malware.

How to Protect Against Threats

1. Use strong passwords
2. Enable firewalls
3. Update software regularly
4. Install antivirus software
5. Use encryption
6. Perform regular backups