Network Architectures

Network architecture refers to the design and structure of a network, encompassing its physical and logical layout, including the devices, connections, protocols, and services involved. Understanding network architecture is fundamental for managing, securing, and troubleshooting networks.

Types of Network Architectures

1. **Local Area Network (LAN):**
    - **Description:** Covers a small geographic area, like an office or a building.
    - **Example:** A corporate office network with computers, printers, and servers connected through Ethernet or Wi-Fi.
2. **Wide Area Network (WAN):**
    - **Description:** Spans a large geographic area, connecting multiple LANs.
    - **Example:** The internet, or a company's global network connecting offices in different cities or countries.
3. **Metropolitan Area Network (MAN):**
    - **Description:** Covers a city or a large campus.
    - **Example:** A city-wide Wi-Fi network or a university campus network.
4. **Personal Area Network (PAN):**
    - **Description:** Network for personal devices within a range of a few meters.
    - **Example:** Bluetooth connections between a smartphone, smartwatch, and wireless earbuds.
5. **Enterprise Private Network:**
    - **Description:** Large network built by an organization to connect various parts of its operations.
    - **Example:** A multinational corporation's internal network connecting its headquarters, branch offices, and data centers.

Real-Life Scenario

Scenario: A multinational company, TechCorp, operates in five countries. Each office has its own LAN, and these are interconnected through a WAN. The headquarters in New York hosts the main data center.

- **LAN:** Each office has a local network for internal communication and resource sharing.
- **WAN:** The offices are connected through leased lines and VPNs to ensure secure communication.
- **Data Center:** The New York headquarters hosts the main servers, databases, and applications, accessible by all offices through the WAN.

Network Mapping

Network mapping involves creating a visual representation of a network's structure, showing how devices and segments are connected. This process is crucial for network management, troubleshooting, and security.

Techniques for Network Mapping

1. **Manual Mapping:**
    - Using network diagrams and documentation to manually record the network layout.
    - Tools: Microsoft Visio, draw.io.
2. **Automated Mapping:**
    - Using software tools to automatically discover and map the network.
    - Tools: Nmap, SolarWinds Network Topology Mapper, Cisco Network Assistant.

Steps in Network Mapping

1. **Discovery:**
    - Identify all devices on the network using tools like Nmap or SNMP.
    - Example: Running an Nmap scan to discover all devices and open ports in a network.
2. **Documentation:**
    - Record device details, IP addresses, MAC addresses, and connections.
    - Example: Using a network documentation tool to log details of discovered devices.
3. **Visualization:**
    - Create a visual map showing devices and their connections.
    - Example: Using SolarWinds to generate a network topology map.

Real-Life Scenario

Scenario: An IT manager at a medium-sized enterprise needs to troubleshoot intermittent network outages.

- **Discovery:** Runs Nmap to identify all devices and open ports.
- **Documentation:** Logs the details using a network documentation tool.
- **Visualization:** Uses SolarWinds to create a topology map, highlighting potential bottlenecks or misconfigurations.

Target Identification

Target identification involves identifying specific devices or systems on a network for security assessments or penetration testing. It's a crucial step in ethical hacking to pinpoint vulnerable systems.

Techniques for Target Identification

1. **Network Scanning:**
    - Use tools to scan the network and identify active devices and open ports.
    - Tools: Nmap, Angry IP Scanner.
2. **Service Detection:**
    - Identify the services running on open ports.
    - Tools: Nmap service/version detection (`-sV` option).

3. **Vulnerability Scanning:**
    - Scan devices for known vulnerabilities.
    - Tools: Nessus, OpenVAS.

Steps in Target Identification

1. **Ping Sweep:**
    - Determine which IP addresses in a subnet are active.
    - Example: Using Nmap (`nmap -sn 192.168.1.0/24`) to find live hosts.
2. **Port Scanning:**
    - Identify open ports and the services running on them.
    - Example: Using Nmap (`nmap -p 1-65535 192.168.1.100`) to scan all ports on a specific IP.
3. **Service Detection:**
    - Determine the software versions of services on open ports.
    - Example: Using Nmap (`nmap -sV 192.168.1.100`) to detect service versions.
4. **Vulnerability Scanning:**
    - Identify vulnerabilities in services.
    - Example: Running Nessus against a target IP to find known vulnerabilities.

Real-Life Scenario

Scenario: A cybersecurity team at a financial institution is conducting a penetration test to identify vulnerabilities.

- **Ping Sweep:** Uses Nmap to identify live hosts in the subnet.
- **Port Scanning:** Scans identified hosts to find open ports and services.
- **Service Detection:** Detects versions of services running on open ports.
- **Vulnerability Scanning:** Runs Nessus to find vulnerabilities in detected services.

Conclusion

Understanding network architectures, mapping, and target identification is essential for effective network management, security, and troubleshooting. Real-life scenarios illustrate how these concepts are applied in practical situations, providing a clear understanding of their importance and usage.

- **Network Architectures:** Provide the blueprint of a network's structure and design.
- **Network Mapping:** Offers a visual representation of the network, aiding in management and troubleshooting.
- **Target Identification:** Focuses on pinpointing specific devices or systems for security assessments.

By mastering these concepts, network administrators and cybersecurity professionals can ensure robust, secure, and efficient network operations.