MAIN CONCEPTS & SCOPE

CONTENT

NETWORK SECURITY

Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. It consists of the policies, processes, and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.No matter the specific method or enterprise security strategy, security is usually framed as everyone's responsibility because every user on the network represents a possible vulnerability in that network.

Access Control and Authentication:

Network Monitoring and Logging

Perimeter Security
Firewalls
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Data Encryption:
secure sockets layer (SSL)/transport layer security (TLS) protocols, virtual private networks (VPNs), or secure file transfer protocols (SFTP)

NETWORK SCANNER

The objective of the project is to create a network scanner that can efficiently discover active IP addresses within a specified range, perform ICMP ping to validate their reachability and conduct port scanning on the active IP addresses to identify open ports. The project aims to provide a tool that aids in network management and security assessment.

MAIN CONCEPTS

01

TCP/IP: Transmission Control Protocol/Internet Protocol is a set of protocols used for communication between devices on the internet or a private network..

02

IPort: is a logical endpoint for communication. It is identified by a numerical value and allows different services or applications to listen for incoming connections or send data to specific destinations. Ports are categorized as either well-known ports (0-1023), registered ports (1024-49151), or dynamic or private ports (49152-65535)

03

TCP (Transmission Control Protocol): is a connection-oriented protocol that provides reliable, ordered, and error-checked data transmission between devices over a network. Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins.

04

IP address: is a unique address that identifies a device on the internet or a local network. Computers use IP addresses to communicate with each other both over the Internet and on other networks.

05

ICMP (Internet Control Message Protocol): network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. ICMP is crucial for error reporting and testing.

06

Ping: is a network utility that sends an Internet Control Message Protocol (ICMP) echo request from a source device to a destination device to determine reachability and measure the round-trip time (RTT) for the ICMP echo reply. It is used for network diagnostics, troubleshooting, and assessing network responsiveness by examining the availability and latency between hosts in a TCP/IP network.

07

Ping sweeping is a network scanning technique that involves systematically sending ICMP echo requests (pings) to a range of IP addresses to identify active hosts on a network. It allows for the rapid discovery of multiple live hosts within a given IP address range by sequentially pinging each IP address and recording the responsive ones.

SCOPE

1. **Host Reachability Check:**
   - Validate the user-provided IP address to ensure it is a valid format.
   - Send ICMP echo requests (ping) to the specified IP address to check its reachability.
   - Display the list of active IP addresses that respond to the ping requests.
2. **Port Scanning:**
   - Allow the user to specify the number of ports to scan.
   - Implement multi-threading to improve scanning efficiency.
   - Perform TCP port scanning on each active IP address discovered during the host reachability check.
   - Identify open ports and report them as "up" to the user.
3. **User Interface:**
   - Provide a command-line interface for user interaction.
   - Display appropriate messages and instructions to guide the user.

SCOPE

4. Performance and Execution Time:

- Measure the execution time of the scanning process.
- Display the total execution time at the end of the scan.

5. Platform Compatibility:

- Ensure compatibility with both Windows and Linux operating systems.
- Adapt the ping command and other system-related functionalities based on the operating system.