NETWORKING PROJECT 2

EID: 291226 Name: J Prashanth

Title: Network Design with Firewall and Open Ports (SSH, HTTP, HTTPS)

Purpose:

- Network design with firewalls and open ports is crucial for securing network communication while enabling necessary services.
- A firewall acts as a barrier between trusted internal networks and untrusted external networks (like the internet), controlling incoming and outgoing traffic based on predefined security rules.
- Open ports are specific points of access on a device (like a server) that allow communication with other devices, typically for services like SSH, HTTP, and HTTPS.

How it Works:

- **Firewall:** A network security system that monitors and controls incoming and outgoing traffic based on security rules. It can be hardware-based or software-based.
    - **Types of Firewalls:**
        - **Packet Filtering Firewall:** Inspects packets and allows or blocks them based on predefined rules.
        - **Stateful Inspection Firewall:** Tracks the state of active connections and makes decisions based on both the rules and the state of the connection.
        - **Proxy Firewall:** Acts as an intermediary between users and the services they are accessing, filtering content.
- **Open Ports:** Network ports are used for communication between devices. When you open a port on a device, you're allowing traffic to flow through that port, enabling specific services.
    - **SSH (Secure Shell):** Typically uses port **22** for secure remote access to servers.
    - **HTTP (Hypertext Transfer Protocol):** Uses port **80** for web traffic.
    - **HTTPS (Hypertext Transfer Protocol Secure):** Uses port **443** for secure web traffic (encrypted communication).
- **Firewall Configuration:** By configuring a firewall to allow or deny traffic to specific open ports, administrators can control access to these services. For example:
    - Allow traffic on port 22 for SSH (to enable remote server management).
    - Allow traffic on port 80 for HTTP (to serve unencrypted web pages).
    - Allow traffic on port 443 for HTTPS (to serve secure, encrypted web pages).

Common Results:

- **Open Ports:** When the firewall is correctly configured to allow traffic on specific ports, the corresponding services (SSH, HTTP, HTTPS) become accessible.
    - **SSH (Port 22):** Used for secure remote command-line access to a server.
    - **HTTP (Port 80):** Used to deliver standard, unencrypted web pages.
    - **HTTPS (Port 443):** Used to deliver secure, encrypted web pages.
- **Firewall Blocking:** If the firewall is configured to block traffic on specific ports, communication on those ports will not be allowed, and services associated with those ports will be inaccessible.
    - For instance, blocking port **22** will prevent SSH connections, blocking **80** will prevent unencrypted web browsing, and blocking **443** will prevent secure web browsing.

Practical: Steps to Configure Open Ports on a Firewall (for SSH, HTTP, HTTPS):

1. **Step 1:** Access the firewall configuration settings (via a web interface or command line).

2. **Step 2:** Open the specific ports required for your services.
    - **For SSH (Port 22):**
        - Allow inbound connections on **Port 22** to enable secure remote management.
    - **For HTTP (Port 80):**
        - Allow inbound connections on **Port 80** to serve unencrypted web traffic.
    - **For HTTPS (Port 443):**
        - Allow inbound connections on **Port 443** to serve encrypted web traffic.
3. **Step 3:** Set up rules for outbound traffic (if necessary), ensuring that your device can also initiate connections as needed.
4. **Step 4:** Apply and save the firewall configuration.
5. **Step 5:** Test the configuration by attempting to access the services (SSH, HTTP, HTTPS) from an external device.

Diagram Representation