Elevate Labs

Interview Questions & Answers

1. What is a firewall?

A **firewall** is a security system that monitors and controls incoming and outgoing network traffic based on predefined rules. It acts as a barrier between a trusted network (like your internal system) and an untrusted network (like the internet) to block malicious or unauthorized access.

2. Difference between stateful and stateless firewall?

Feature	Stateful Firewall	Stateless Firewall
Memory	Keeps track of connection state	Does not keep track of connections
Security Level	More secure (context-aware)	Less secure (rule-based only)
Performance	Slightly slower due to tracking	Faster as no session tracking
Use Case	Enterprise networks, complex setups	Simple filtering, basic rules

3. What are inbound and outbound rules?

- **Inbound Rules**: Control traffic **coming into** your computer or network (e.g., blocking port 23 to prevent remote Telnet access).
- **Outbound Rules**: Control traffic **going out** from your computer or network (e.g., preventing apps from sending data outside).

4. How does UFW simplify firewall management?

UFW (Uncomplicated Firewall) is a **user-friendly command-line tool** for managing iptables in Linux. It simplifies tasks like:

- Enabling/disabling firewall
- Allowing or denying specific ports
- Viewing rules with simple commands like ufw status

5. Why block port 23 (Telnet)?

- **Telnet** is an old protocol that transmits data, including **passwords**, in **plain text**.
- Port 23 is commonly targeted by attackers for **unauthorized access**.
- Blocking it improves security by **disabling insecure remote access**.

6. What are common firewall mistakes?

- Forgetting to allow **SSH (port 22)** before enabling firewall (can lock yourself out).
- Misconfigured rules that block essential services (like DNS or HTTP).
- Leaving unused ports open.
- Not monitoring logs or updating rules based on new threats.

7. How does a firewall improve network security?

- Blocks **unauthorized access** to your system or network.
- Prevents **malware and attackers** from exploiting open ports.
- Controls which applications or services can communicate over the network.
- Helps enforce security policies and reduces **attack surface**.

8. What is NAT in firewalls?

NAT (Network Address Translation) is a method used in firewalls and routers to:

- Map **private IP addresses** to a **public IP address**.
- Allow multiple devices on a private network to access the internet using **one public IP**.
- Provide an additional **layer of security** by hiding internal IPs from external networks.