Task-4

1.What is a firewall?

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.

2.Difference between stateful and stateless firewall?

- **Stateful:** Tracks the state of active connections; allows traffic if it is part of a valid session.
- **Stateless:** Inspects packets individually without considering connection state; simpler but less secure.

3.What are inbound and outbound rules?

- Inbound rules: Control traffic coming into your system/network.
- Outbound rules: Control traffic leaving your system/network.

4.How does UFW simplify firewall management?

- Provides easy-to-use commands for adding, removing, and checking rules without dealing with complex iptables syntax.

5.Why block port 23 (Telnet)?

- Telnet is unencrypted, making it vulnerable to interception and attacks. Blocking it prevents insecure remote access.

6.What are common firewall mistakes?

- Leaving unnecessary ports open
- Misconfigured rules causing accidental blocks
- Not testing rules after implementation
- Relying solely on firewall for security

7.How does a firewall improve network security?

- Prevents unauthorized access
- Filters malicious traffic
- Enforces security policies
- Reduces the attack surface by limiting open ports and protocols

8.What is NAT in firewalls?

→ NAT (Network Address Translation) is a technique used by firewalls (and routers) to map private IP addresses inside a local network to a public IP address (or vice versa) when communicating with external networks like the Internet.

document commands and summarize firewall filter traffic.

Windows firewall:

list all rules:netsh advfirewall firewall show rule name=all

block inbound traffic on port 23:netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23

delete the test block rule:netsh advfirewall firewall delete rule name="Block Telnet"

Summary: How Firewalls Filter Traffic

- A firewall monitors network traffic and applies rules to allow or block data based on:
  - Port number (e.g., 22 for SSH, 23 for Telnet)
  - Protocol (TCP, UDP, ICMP)
  - Direction (inbound or outbound)
  - IP addresses or ranges
- Stateful firewalls track active connections and allow only valid session traffic.
- Stateless firewalls check each packet independently without session context.
- By controlling what traffic enters or leaves a network or system, firewalls prevent unauthorized access, reduce vulnerabilities, and improve overall security.