Task 10: Firewall Configuration & Testing

1. Learn firewall concepts.

A firewall is a network security mechanism that monitors incoming and outgoing traffic and allows or blocks it based on predefined rules.
It works as a barrier between a trusted internal network and untrusted external networks (like the internet).
Firewalls help reduce unauthorized access, malware communication, and network-based attacks.

2. Configure rules.

Firewall rules define **what traffic is allowed or blocked**.
Rules are created based on:

- Port number
- Protocol (TCP/UDP)
- IP address
- Direction (inbound/outbound)

Example:

```
sudo ufw enable
```

This activates the firewall so rules can be enforced.

3. Allow/deny ports.

Ports are communication endpoints used by services.

- Allow required services (SSH, HTTP)
- Deny unused or risky ports (Telnet, FTP)

Example:

```
sudo ufw allow 22

sudo ufw allow 80

sudo ufw deny 23
```

This allows SSH & web traffic and blocks Telnet.

4. Test connectivity.

After configuring rules, connectivity must be tested to confirm expected behavior.

- Allowed ports → connection should succeed
- Blocked ports → connection should fail

Example:

```
telnet localhost 80

telnet localhost 23
```

5. Observe logs.

- Firewall logs record allowed and blocked traffic.
- Logs help detect suspicious activity.
- They assist in troubleshooting and security monitoring.

6. Block malicious IP.

ALL SCREENSHOTS ARE ATTACHED TO GITHUB REPO

7. Document rules

- All firewall rules must be properly documented.
- Documentation includes allowed ports, blocked ports, and blocked IPs.
- It helps in auditing and future maintenance.

8. Explain impact

- Firewalls improve security by controlling network access.
- They reduce unauthorized access and attacks.
- Incorrect rules may block legitimate traffic, so careful management is required.