Task Report: Setup and Use Firewall in Linux

Objective

Configure and manage a firewall on a Linux system to control network traffic and improve security.

Tools Used

- UFW (Uncomplicated Firewall) - beginner-friendly interface for iptables
- Linux Terminal - for executing commands

Steps Performed

1. Check Firewall Status:

```
sudo ufw status
```

If UFW is not installed:

```
sudo apt update && sudo apt install ufw -y   # For Ubuntu/Debian
```

2. Enable Firewall:

Before enabling, allow SSH:

```
sudo ufw allow ssh
```

Enable:

```
sudo ufw enable
```

3. Allow and Deny Specific Services/Ports:

Allow HTTP:

```
sudo ufw allow 80
```

Allow HTTPS:

```
sudo ufw allow 443
```

Deny Telnet:

```
sudo ufw deny 23
```

4. View Current Rules:

```
sudo ufw status verbose
```

5. Delete a Rule:

```
sudo ufw delete allow 80
```

6. Reset Firewall (Optional):

```
sudo ufw reset
```

Verification

1. List open ports:

```
sudo ss -tuln
```

2. Test blocked ports from another system using nmap:

```
nmap -p 23 <target_IP>
```

   Expected: port 23 should be filtered/closed.

Conclusion

We successfully installed and configured a firewall using UFW on Linux. The firewall now allows essential services (SSH, HTTP, HTTPS), blocks insecure ports (Telnet), and runs automatically at startup. This improves system security by restricting unauthorized access.