Task 4 - Setup and Use a Firewall on Windows/Linux

Objective:

To gain hands-on experience in configuring and testing basic firewall rules on a Linux system using UFW (Uncomplicated Firewall), along with understanding how firewalls filter network traffic and secure remote access through SSH.

Environment Used:

- Operating System: Kali Linux (in VirtualBox)
- Firewall Tool: UFW (Uncomplicated Firewall)
- Remote Access Test: From Windows CMD via SSH

Step-by-Step Configuration:

1. Updating and Installing UFW:

sudo apt update
sudo apt install ufw

2. Checking UFW Status:

sudo ufw status verbose
Initially showed: Status: inactive

3. Enabling UFW:

sudo ufw enable
Now shows: Status: active

4. Allowing Port 22 for SSH:

sudo ufw allow 22

5. Blocking Port 23 (Telnet):

sudo ufw deny 23

6. Viewing Active Rules:

sudo ufw status numbered

6. Enabling SSH server:

sudo systemctl start ssh

7. Remote SSH Access Test from Windows CMD:

ssh Kali_username@<Kali-IP>

8. Removing Test Rule (Restore):

sudo ufw delete deny 23

Screenshot:

Screenshots are available in Github Repository.

Key Learnings:

- Understood how firewalls filter traffic based on port rules.
- Gained hands-on experience with UFW on Linux.
- Practiced remote SSH access to Kali Linux from Windows CMD.
- Learned about securing systems by blocking insecure services.

Commands Summary:

sudo apt update
sudo apt install ufw
sudo ufw enable
sudo ufw allow 22
sudo ufw deny 23
sudo ufw status numbered
sudo systemctl start ssh