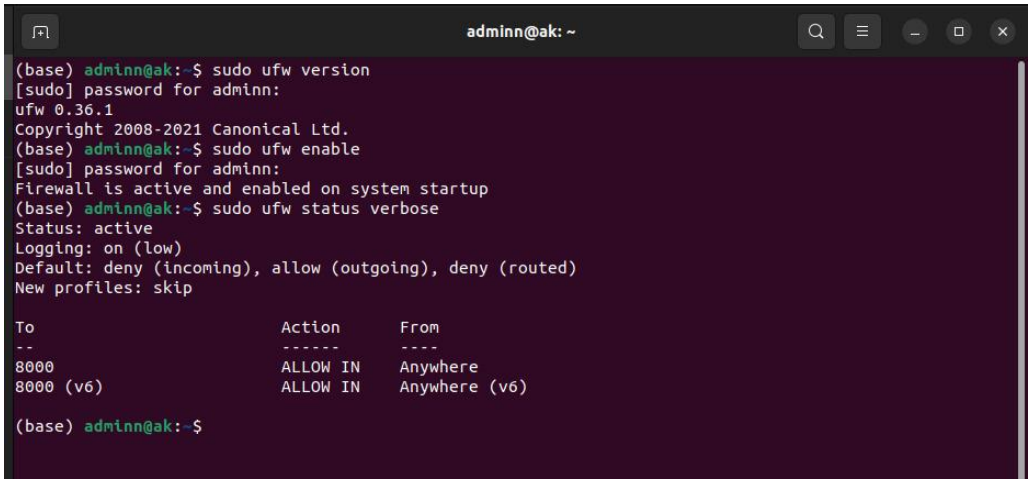
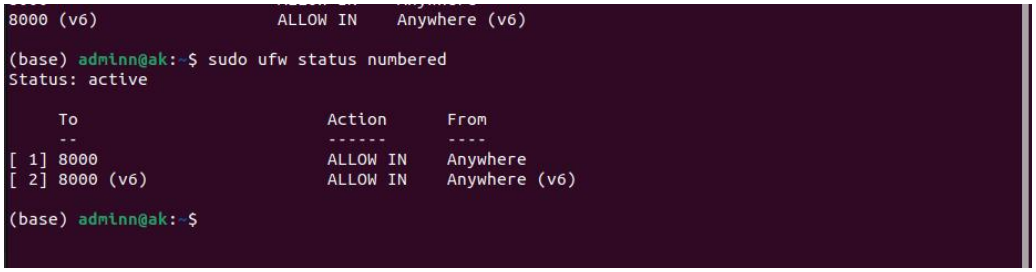
Task -4: Setup and Use a Firewall on Windows/Linux

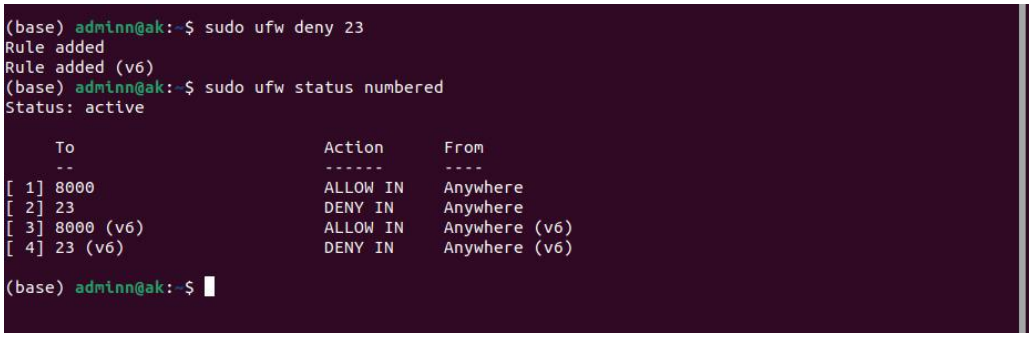
Step 1: Check UFW installed and enable UFW



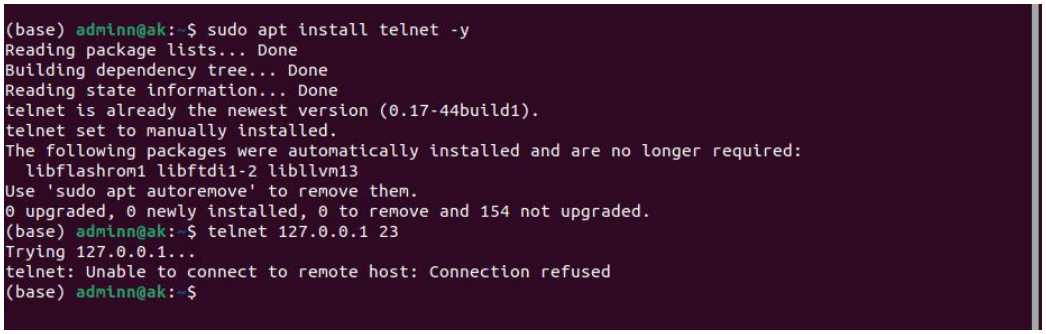
Step 2: View current Firewall rules



Step 3: Block telnet (port 23)



Step 4: Test telnet



Step 5: Allow SSH (port 22)

```
telnet: Unable to connect to remote host: Connection refused
(base) adminn@ak:~$ sudo ufw allow 22
Rule added
Rule added (v6)
(base) adminn@ak:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 8000                       ALLOW IN    Anywhere
[ 2] 23                         DENY IN     Anywhere
[ 3] 22                         ALLOW IN    Anywhere
[ 4] 8000 (v6)                  ALLOW IN    Anywhere (v6)
[ 5] 23 (v6)                    DENY IN     Anywhere (v6)
[ 6] 22 (v6)                    ALLOW IN    Anywhere (v6)

(base) adminn@ak:~$
```

Step 6: Test SSH

```
(base) adminn@ak:~$ ssh localhost
ssh: connect to host localhost port 22: Connection refused
(base) adminn@ak:~$
```

Step 7: Solution to the issue faced

```
adminn@ak: ~                                    adminn@ak: ~
(base) adminn@ak:~$ sudo systemctl status ssh
[sudo] password for adminn:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-09-26 18:31:23 IST; 47min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 21118 (sshd)
      Tasks: 1 (limit: 18299)
     Memory: 1.7M
        CPU: 17ms
     CGroup: /system.slice/ssh.service
             └─21118 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 26 18:31:23 ak systemd[1]: Starting OpenBSD Secure Shell server...
Sep 26 18:31:23 ak sshd[21118]: Server listening on 0.0.0.0 port 3435.
Sep 26 18:31:23 ak sshd[21118]: Server listening on :: port 3435.
Sep 26 18:31:23 ak systemd[1]: Started OpenBSD Secure Shell server.
(base) adminn@ak:~$
```

Step 8: Allow SSH

```
(base) adminn@ak:~$ sudo ufw allow 3435
Rule added
Rule added (v6)
(base) adminn@ak:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 8000                       ALLOW IN    Anywhere
[ 2] 23                         DENY IN     Anywhere
[ 3] 22                         ALLOW IN    Anywhere
[ 4] 3435                       ALLOW IN    Anywhere
[ 5] 8000 (v6)                  ALLOW IN    Anywhere (v6)
[ 6] 23 (v6)                    DENY IN     Anywhere (v6)
[ 7] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 8] 3435 (v6)                  ALLOW IN    Anywhere (v6)

(base) adminn@ak:~$ ssh -p 3435 localhost
The authenticity of host '[localhost]:3435 ([127.0.0.1]:3435)' can't be established.
ED25519 key fingerprint is SHA256:5CgvmbxEdUP2W+7VdcQI5ApobwIfzDCB4DAnVJp0Lpw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:3435' (ED25519) to the list of known hosts.
adminn@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

156 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

19 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Wed Feb 21 23:17:06 2024 from 172.20.10.12
(base) adminn@ak:~$
```

Step 9: Clean Up

```
(base) adminn@ak:~$ sudo ufw status numbered
[sudo] password for adminn:
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 8000                       ALLOW IN    Anywhere
[ 2] 23                         DENY IN     Anywhere
[ 3] 22                         ALLOW IN    Anywhere
[ 4] 3435                       ALLOW IN    Anywhere
[ 5] 8000 (v6)                  ALLOW IN    Anywhere (v6)
[ 6] 23 (v6)                    DENY IN     Anywhere (v6)
[ 7] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 8] 3435 (v6)                  ALLOW IN    Anywhere (v6)

(base) adminn@ak:~$ sudo ufw delete 8
Deleting:
 allow 3435
Proceed with operation (y|n)? y
Rule deleted (v6)
(base) adminn@ak:~$ sudo ufw delete 7
Deleting:
 allow 22
Proceed with operation (y|n)? y
Rule deleted (v6)
(base) adminn@ak:~$ sudo ufw delete 6
Deleting:
 deny 23
Proceed with operation (y|n)? y
Rule deleted (v6)
(base) adminn@ak:~$ sudo ufw delete 4
Deleting:
 allow 3435
Proceed with operation (y|n)? y
Rule deleted
(base) adminn@ak:~$ sudo ufw delete 3
Deleting:
 allow 22
Proceed with operation (y|n)? y
Rule deleted
(base) adminn@ak:~$ sudo ufw delete 2
Deleting:
 deny 23
Proceed with operation (y|n)? y
Rule deleted
(base) adminn@ak:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 8000                       ALLOW IN    Anywhere
[ 2] 8000 (v6)                  ALLOW IN    Anywhere (v6)
```