

Task 10: Firewall Configuration & Testing

System Used

- OS: WSL (Ubuntu / Kali)
- Firewall Tool: UFW (Uncomplicated Firewall)

Step 1: Check Firewall Status

Open terminal and check whether firewall is installed and its current status.

```
sudo ufw status
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status
[sudo] password for vikas_stark:
Status: active

To                         Action      From
--                         ----       ---
22/tcp                      ALLOW      Anywhere
22/tcp (v6)                 ALLOW      Anywhere (v6)

vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 2: Enable Firewall

Enable the firewall to start filtering traffic.

```
sudo ufw enable
```

Verify status again:

```
sudo ufw status verbose
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw enable
Firewall is active and enabled on system startup
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ----       ---
22/tcp                      ALLOW IN   Anywhere
22/tcp (v6)                 ALLOW IN   Anywhere (v6)
```

Step 3: Allow Required Ports

Allow only necessary services.

Allow SSH (Port 22)

```
sudo ufw allow 22
```

Allow HTTP (Port 80)

```
sudo ufw allow 80
```

Allow HTTPS (Port 443)

```
sudo ufw allow 443
```

Check rules:

```
sudo ufw status numbered
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw allow 22
Rule added
Rule added (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw allow 80
Rule added
Rule added (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw allow 443
Rule added
Rule added (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status numbered
Status: active

      To          Action    From
      --          ----
[ 1] 22/tcp     ALLOW IN  Anywhere
[ 2] 22          ALLOW IN  Anywhere
[ 3] 80          ALLOW IN  Anywhere
[ 4] 443         ALLOW IN  Anywhere
[ 5] 22/tcp (v6) ALLOW IN  Anywhere (v6)
[ 6] 22 (v6)    ALLOW IN  Anywhere (v6)
[ 7] 80 (v6)    ALLOW IN  Anywhere (v6)
[ 8] 443 (v6)   ALLOW IN  Anywhere (v6)
```

Step 4: Deny Unused / Risky Ports

Block a port that is not required (example: Port 23 – Telnet).

```
sudo ufw deny 23
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw deny 23
Rule added
Rule added (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 5: Configure Inbound & Outbound Rules

Block Outbound Traffic on a Port (Example)

```
sudo ufw deny out 25
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw deny out 25
Rule added
Rule added (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Allow Inbound Traffic from Specific IP (Optional)

```
sudo ufw allow from 192.168.1.10
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw allow from 192.168.1.10
Rule added
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 6: Block a Malicious IP Address

Block a known malicious IP (example IP used for testing).

```
sudo ufw deny from 192.168.1.100
```

Verify:

```
sudo ufw status numbered
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw deny from 192.168.1.100
Rule added
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status numbered
Status: active

          To          Action    From
          --          ----
[ 1] 22/tcp      ALLOW IN   Anywhere
[ 2] 22          ALLOW IN   Anywhere
[ 3] 80          ALLOW IN   Anywhere
[ 4] 443         ALLOW IN   Anywhere
[ 5] 23          DENY IN    Anywhere
[ 6] 25          DENY OUT   Anywhere
[ 7] Anywhere    ALLOW IN   192.168.1.10
[ 8] Anywhere    DENY IN    192.168.1.100
[ 9] 22/tcp (v6) ALLOW IN   Anywhere (v6)
[10] 22 (v6)     ALLOW IN   Anywhere (v6)
[11] 80 (v6)     ALLOW IN   Anywhere (v6)
[12] 443 (v6)   ALLOW IN   Anywhere (v6)
[13] 23 (v6)     DENY IN    Anywhere (v6)
[14] 25 (v6)     DENY OUT   Anywhere (v6)
```

Step 7: Enable Firewall Logging

Enable logging to monitor traffic.

```
sudo ufw logging on
```

Check logs:

```
sudo tail -f /var/log/ufw.log
```

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw logging on
Logging enabled
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo tail -f /var/log/ufw.log

^C
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo tail -f /var/log/ufw.log
```

Step 8: Test Firewall Rules

Test Allowed Port

ping google.com

```
vikas_stark@LAPTOP-AOQBLKHF:~$ ping google.com
PING google.com (142.250.194.238) 56(84) bytes of data.
64 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=1 ttl=117 time=22.5 ms
64 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=2 ttl=117 time=3.87 ms
64 bytes from del12s08-in-f14.1e100.net (142.250.194.238): icmp_seq=3 ttl=117 time=4.37 ms
```

Test Blocked Port

telnet localhost 23

```
vikas_stark@LAPTOP-AOQBLKHF:~$ telnet localhost 23
Command 'telnet' not found, but can be installed with:
sudo apt install inetutils-telnet  # version 2:2.4-3ubuntu1, or
sudo apt install telnet-ssl      # version 0.17.41+really0.17-4
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo apt install inetutils-telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  inetutils-telnet
0 upgraded, 1 newly installed, 0 to remove and 70 not upgraded.
Need to get 100 kB of archives.
After this operation, 247 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/amd64 inetutils-telnet amd64 2:2.5-3ubuntu4 [100 kB]
Fetched 100 kB in 1s (67.6 kB/s)
Selecting previously unselected package inetutils-telnet.
(Reading database ... 122095 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.5-3ubuntu4_amd64.deb ...
Unpacking inetutils-telnet (2:2.5-3ubuntu4) ...
Setting up inetutils-telnet (2:2.5-3ubuntu4) ...
update-alternatives: using /usr/bin/inetutils-telnet to provide /usr/bin/telnet (telnet) in auto mode
Processing triggers for man-db (2.12.0-4build2) ...
vikas_stark@LAPTOP-AOQBLKHF:~$ telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 9: Document Firewall Rules

List rules with numbering:

sudo ufw status numbered

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status numbered
Status: active

To                         Action      From
--                         --          --
[ 1] 22/tcp                  ALLOW IN   Anywhere
[ 2] 22                      ALLOW IN   Anywhere
[ 3] 80                      ALLOW IN   Anywhere
[ 4] 443                     ALLOW IN   Anywhere
[ 5] 23                      DENY IN    Anywhere
[ 6] 25                      DENY OUT   Anywhere
[ 7] Anywhere                ALLOW IN   192.168.1.10
[ 8] Anywhere                DENY IN    192.168.1.100
[ 9] 22/tcp (v6)              ALLOW IN   Anywhere (v6)
[10] 22 (v6)                 ALLOW IN   Anywhere (v6)
[11] 80 (v6)                 ALLOW IN   Anywhere (v6)
[12] 443 (v6)                ALLOW IN   Anywhere (v6)
[13] 23 (v6)                 DENY IN    Anywhere (v6)
[14] 25 (v6)                 DENY OUT   Anywhere (v6)

(vout)
```

Step 10: Analyze Impact

- Unauthorized ports blocked
- Only required services accessible
- Malicious IP denied
- Logs help monitor suspicious traffic

Final Outcome

- ✓ Firewall successfully configured
- ✓ Ports allowed and denied correctly
- ✓ Malicious IP blocked
- ✓ Connectivity tested and verified
- ✓ Firewall management skills achieved

