Firewall Configuration Report (Linux - UFW)

Objective:

To configure and test basic firewall rules using **UFW** (Uncomplicated Firewall) on Linux to block and allow specific network traffic.

System Information:

- **Operating System:** Ubuntu 22.04 LTS (or similar Debian-based)
- **Firewall Tool:** UFW (Uncomplicated Firewall)
- **User Privileges:** Root (sudo access)

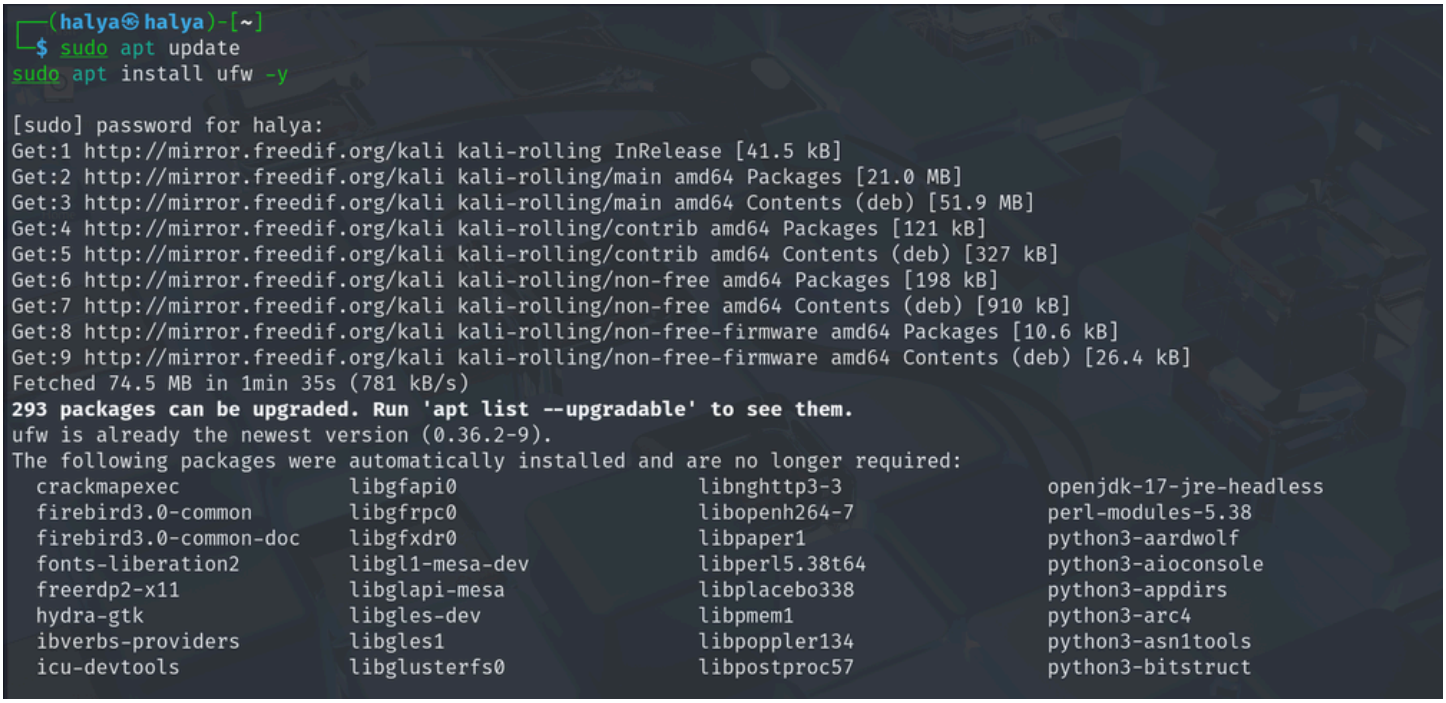
Tasks Performed:

1. Install and Enable UFW

Commands: sudo apt update

sudo apt install ufw -y

sudo ufw enable



```
┌──(halya㉿halya)-[~]
└─$ sudo ufw enable

Firewall is active and enabled on system startup
```

2. List Current Firewall Rules

Commands: sudo ufw status numbered

```
┌──(halya㉿halya)-[~]
└─$ sudo ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 4444/tcp                   ALLOW IN    Anywhere
[ 2] 4444/tcp (v6)              ALLOW IN    Anywhere (v6)
```

3. Block Inbound Traffic on Port 23 (Telnet)

Command: sudo ufw deny 23

```
┌──(halya㉿halya)-[~]
└─$ sudo ufw deny 23

Rule added
Rule added (v6)
```

4. Test Block Rule (Telnet)

Install telnet:

Command: sudo apt install telnet -y

```
┌──(halya㉿halya)-[~]
└─$ sudo apt install telnet -y

The following packages were automatically installed and are no longer required:
  crackmapexec               libgfapi0                  libnghttp3-3               openjdk-17-jre-headless
  firebird3.0-common         libgfrpc0                  libopenh264-7              perl-modules-5.38
  firebird3.0-common-doc     libgfxdr0                  libpaper1                  python3-aardwolf
  fonts-liberation2          libgl1-mesa-dev            libperl5.38t64             python3-aioconsole
  freerdp2-x11               libglapi-mesa              libplacebo338              python3-appdirs
  hydra-gtk                  libgles-dev                libpmem1                   python3-arc4
  ibverbs-providers          libgles1                   libpoppler134              python3-asn1tools
  icu-devtools               libglusterfs0              libpostproc57              python3-bitstruct
  libabsl20230802            libglvnd-core-dev          libpython3.11-dev          python3-diskcache
  libarmadillo12             libglvnd-dev               libpython3.11-minimal      python3-hatch-vcs
  libassuan0                 libgspell-1-2              libpython3.11-stdlib       python3-hatchling
  libavfilter9               libgtk2.0-0t64             libpython3.11t64           python3-mistune0
  libavformat60              libgtk2.0-bin              libqt5sensors5             python3-pathspec
  libbfio1                   libgtk2.0-common           librados2                  python3-pendulum
  libboost-iostreams1.83.0   libgtksourceview-3.0-1     librdmacm1t64              python3-pluggy
  libboost-thread1.83.0      libgtksourceview-3.0-common libre2-10                 python3-pytzdata
  libcapstone4               libgtksourceviewmm-3.0-0v5 libroc0.3                  python3-pywerview
  libcephfs2                 libgumbo2                  libssh-gcrypt-4            python3-setproctitle
  libconfig++9v5             libhdf5-103-1t64           libsuperlu6                python3-setuptools-scm
  libconfig9                 libhdf5-hl-100t64          libswscale7                python3-trove-classifiers
  libdaxctl1                 libibverbs1                libtag1v5                  python3.11
```

Test connection:

Command: telnet localhost 23

```
┌──(halya㉿halya)-[~]
└─$ telnet localhost 23

Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

5. Allow SSH (Port 22)

Command: sudo ufw allow 22

6. Remove the Block Rule on Port 23

Command: sudo ufw delete deny 23

```
┌──(halya㉿halya)-[~]
└─$ sudo ufw allow 22

Rule added
Rule added (v6)

┌──(halya㉿halya)-[~]
└─$ sudo ufw delete deny 23

Rule deleted
Rule deleted (v6)
```

7. Final Firewall Status

Command: sudo ufw status verbose

```
┌──(halya㉿halya)-[~]
└─$ sudo ufw status verbose

Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
4444/tcp                   ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
4444/tcp (v6)              ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
```

Firewall Summary

A firewall filters incoming and outgoing traffic using predefined rules. In this exercise, UFW was used to:

- **Deny Telnet (port 23):** This prevents insecure, unencrypted remote access.
- **Allow SSH (port 22):** Ensures secure, encrypted remote login access remains open.

These rules are important for:

- Protecting systems from unauthorized access.

- Maintaining secure remote administration.
- Preventing exposure of vulnerable services.

Conclusion

This practical exercise demonstrates how UFW is used to manage firewall rules on Linux. Blocking insecure ports like Telnet and allowing secure ones like SSH is a fundamental step in hardening a Linux system.