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

Objective: Configure and test basic firewall rules to allow or block traffic.

Introduction:

Uncomplicated Firewall, a tool designed to simplify the process of managing a firewall on Linux systems, particularly those based on Ubuntu and Debian.

Purpose of UFW

UFW provides a **user-friendly interface** for configuring firewall rules, acting as a front-end to the more complex ip tables system built into the Linux kernel. It allows administrators to allow or block network traffic based on ports, IP addresses, or specific services, thereby helping to protect servers from unauthorized access and cyber threats.

Using UFW (Uncomplicated Firewall)

1. Install UFW:
   - sudo apt-get update
   - sudo apt-get install ufw

```
┌──(root㉿Punk)-[~]
└─# apt-get install ufw
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
ufw is already the newest version (0.36.2-9).
The following packages were automatically installed and are no longer required:
  libgdal36 libogdi4.1
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

2. Check firewall status:
   - sudo ufw status

```
┌──(root㉿Punk)-[~]
└─# ufw status
Status: active

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

i. Enable UFW:

- sudo ufw enable

```
┌──(root㉿Punk)-[~]
└─# ufw enable
Firewall is active and enabled on system startup
```

ii. Set default policies:

a. Deny all incoming traffic:

- sudo ufw default deny incoming

```
┌──(root㉿Punk)-[~]
└─# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

b. Allow all outgoing traffic:

- sudo ufw default allow outgoing

```
┌──(root㉿Punk)-[~]
└─# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

3. Allow specific services or ports:

- sudo ufw allow ssh

```
┌──(root㉿Punk)-[~]
└─# ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
```

4. Deny specific IP addresses:

- sudo ufw deny from 192.168.1.100

```
┌──(root㉿Punk)-[~]
└─# ufw deny from 192.168.1.100
Rule added
```

5. Check firewall status with detailed info:
   - sudo ufw status verbose

```
┌──(root㉿Punk)-[~]
└─# 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
80/tcp                     DENY IN     Anywhere
Anywhere                   DENY IN     192.168.1.100
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                DENY IN     Anywhere (v6)
```

6. Disable UFW (if needed):
   - sudo ufw disable

```
┌──(root㉿Punk)-[~]
└─# ufw disable
Firewall stopped and disabled on system startup

┌──(root㉿Punk)-[~]
└─# ufw status
Status: inactive
```