Internship Project Report

Task 2: Basic Firewall Configuration with UFW

Name: Sibiraj B

Company: Oasis infobyte

Duration: [15 july 2025 – 15 augest 2025]

Submitted as part of the internship program

1. Objective

The objective of this project is to set up a basic firewall using UFW (Uncomplicated Firewall) on a Linux system, configure rules to allow SSH and deny HTTP traffic, and verify the firewall status.

2. Tools & Technologies

- Tool: UFW (Uncomplicated Firewall)

- Operating System: Ubuntu / Debian-based Linux system

3. Implementation Steps

Step 1: Install UFW on your system

Command:

```
sudo apt update && sudo apt install ufw -y
```

Step 2: Allow SSH Traffic

Command:

```
sudo ufw allow ssh
```

Step 3: Deny HTTP Traffic

Command:

```
sudo ufw deny http
```

Step 4: Enable UFW

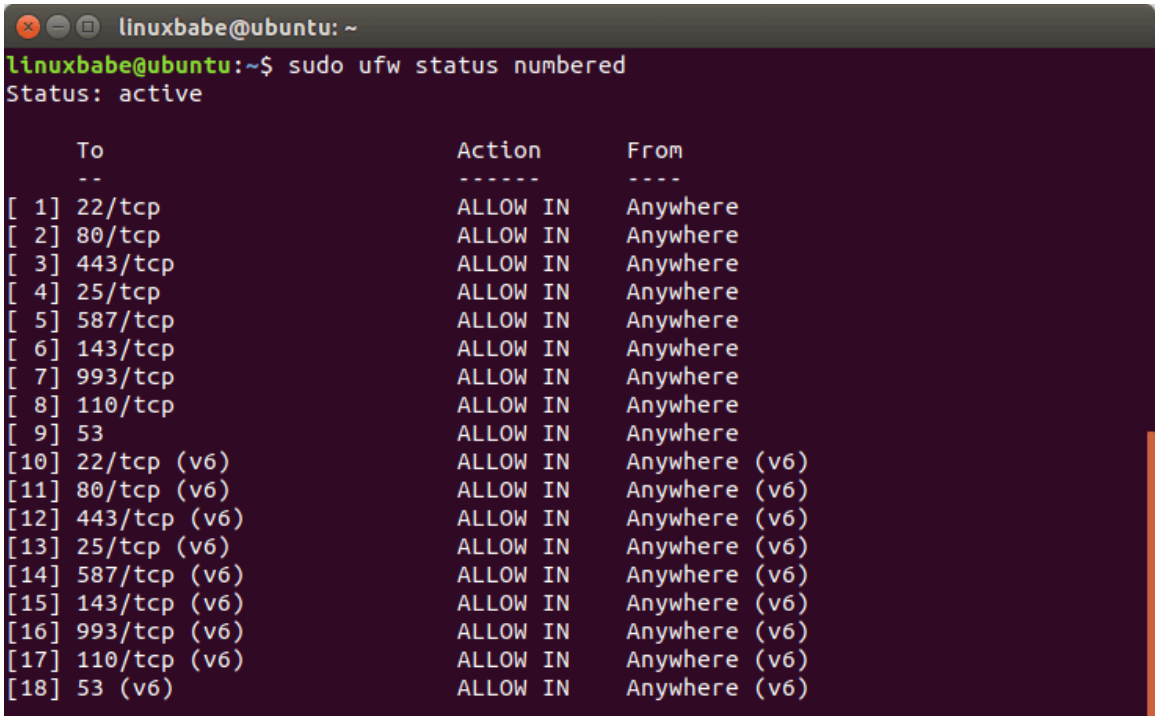
Command:

```
sudo ufw enable
```

Step 5: Check UFW Status and Rules

Command:

```
sudo ufw status verbose
```



4. GitHub Deliverables

1. ufw_configuration.sh – Shell script containing UFW configuration commands.

2. Screenshot of 'ufw status' showing active rules.

3. README.md – Documentation explaining the configuration.

5. Demo Video Idea

Create a short video demonstrating the configuration process:
1. Installing UFW
2. Allowing SSH and Denying HTTP
3. Showing 'ufw status' output with active rules

6. Conclusion

This project demonstrates how to configure a basic firewall on a Linux system using UFW. The configuration ensures secure remote access via SSH while blocking HTTP traffic, showing the importance of proper firewall rule management.