Task 4: Setup and Use a Firewall on Linux (UFW)

Intern Name: Rishika Singh  
Department: Computer Science & IT  
Training Organization: Steel Authority of India Limited (SAIL), RDCIS  
Project Guide: Archana Sharan  
Task Date: 27th June 2025

# Objective:

To configure and test basic firewall rules using UFW (Uncomplicated Firewall) in Linux and understand how firewalls filter network traffic.

# Tools Used:

- Linux Terminal (Ubuntu 20.04)  
- UFW (Uncomplicated Firewall)

# Steps Performed:

* Check UFW Status:  
  sudo ufw status verbose
* Enable the Firewall:  
  sudo ufw enable
* Block Incoming Traffic on Port 23 (Telnet):  
  sudo ufw deny 23
* Verify the Rule:  
  sudo ufw status numbered
* Allow SSH on Port 22:  
  sudo ufw allow 22
* Delete the Telnet Block Rule:  
  sudo ufw delete deny 23
* Disable the Firewall (Optional):  
  sudo ufw disable

# Screenshots:

All screenshots of the above commands have been saved and added to the GitHub repository.

# Outcome:

- Understood how UFW is used to control network traffic.  
- Successfully configured rules to allow or block specific ports.  
- Gained basic skills in Linux firewall management.

# Key Concepts Learned:

- Firewall rules (Allow/Deny)  
- Importance of securing unused ports  
- Basic terminal commands for UFW  
- Inbound vs. Outbound traffic control

# GitHub Repository:

[Paste your GitHub repository link here]

# Interview Questions & Answers:

* Q: What is a firewall?

A: A firewall is a security device that monitors and controls incoming/outgoing traffic based on security rules.

* Q: Difference between stateful and stateless firewall?

A: Stateful: Tracks the state of active connections. Stateless: Evaluates each packet independently.

* Q: What are inbound and outbound rules?

A: Inbound: Controls traffic coming into the system. Outbound: Controls traffic leaving the system.

* Q: How does UFW simplify firewall management?

A: UFW provides a simplified command-line interface for managing iptables rules in Linux.

* Q: Why block port 23 (Telnet)?

A: Telnet is insecure and transmits data in plaintext. Blocking it prevents potential security risks.

* Q: What are common firewall mistakes?

A: Leaving unnecessary ports open, not testing rules, misconfiguring SSH rules (getting locked out).

* Q: How does a firewall improve network security?

A: It acts as a barrier between trusted and untrusted networks, filtering malicious or unnecessary traffic.

* Q: What is NAT in firewalls?

A: NAT (Network Address Translation) allows multiple devices to share a single public IP address.

# Final Submission:

Paste your GitHub repository link above and submit the task using this link:  
https://forms.gle/8Gm83s53KbyXs3Ne9