SOMAIYA VIDYAVIHAR UNIVERSITY

Somaiya TRUST

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Roll Numbers: 16010122203, 16010122205, 16010122214, 16010122232 Group No: 18
Name of the students: Anish Talari, Krish Telang , Arya Torne, Mansi Sharma
Div: B1, B2
Branch:Computer Engineering IA No: IA1
Date: 9th February, 2025

Subject: Information Security

TITLE: Implementation of Fail2Ban for Server Security

AIM: To install, configure, and test Fail2Ban to protect servers from brute-force attacks.

Introduction

Fail2Ban is a security tool that protects servers from brute-force attacks by automatically banning suspicious IPs. This guide walks through the installation, configuration, and testing of Fail2Ban.

Features/Characteristics

Fail2Ban offers a range of features that enhance server security:

- Automatic IP Banning: Identifies and blocks malicious IP addresses after multiple failed login attempts.
- Configurable Jails: Uses custom jails to define security rules for different services (SSH, HTTP, FTP, etc.).
- Flexible Ban Timing: Allows setting temporary or permanent bans based on attack severity.
- Email Alerts: Sends notifications when an IP is banned.
- Firewall Compatibility: Works with iptables, firewalld, and other firewall solutions.
- Log Monitoring: Continuously scans system logs to detect brute-force attempts.
- Whitelisting & Blacklisting: Allows administrators to manually specify trusted or banned IP addresses.

Methodology

The implementation of Fail2Ban follows these steps:

1. Server Connection: Securely access the server via SSH.
2. Installation: Install Fail2Ban using the package manager.
3. Service Management: Enable and start the Fail2Ban service.
4. Configuration: Modify jail settings to enforce SSH security.
5. Testing: Simulate brute-force login attempts to verify automatic banning.
6. Log Analysis: Review Fail2Ban logs to confirm blocked IPs.
7. Customization: Fine-tune settings for enhanced security.

Literature survey/Theory:

Fail2Ban is a security tool that helps protect servers from brute-force attacks by monitoring authentication logs and banning IPs that repeatedly fail login attempts.
It is commonly used to secure SSH, FTP, and web services by automatically updating firewall rules to block malicious traffic.

Key Concepts:

- **Brute-force Attack Prevention:** Detects multiple failed login attempts and bans the offending IP address.
- **IP Blacklisting:** Temporarily or permanently blocks suspicious IP addresses.
- **Firewall Integration:** Works with iptables, firewalld, and other firewall solutions.
- **Custom Filters and Jails:** Allows configuration for various services beyond SSH.
- **Automated Security Enforcement:** Reduces server vulnerabilities with minimal manual intervention.

Flowchart/Implementations/Screenshots with steps:

Implementation Steps:

Step 1: Connecting to the Server **ssh**

root@your-server-ip

Step 2: Installing Fail2Ban

sudo apt-get update
sudo apt-get install fail2ban

Step 3: Enabling the Fail2Ban Service

sudo systemctl enable fail2ban.service
sudo systemctl start fail2ban.service

Step 4: Configuring Fail2Ban
Navigate to the configuration directory:

cd /etc/fail2ban/
ls -sl

Edit jail configuration:

sudo vi jail.d/defaults-debian.conf

Add the following settings:

[sshd]
enabled = true
port = ssh
filter = sshd
maxretry = 3
bantime = 600

Step 5: Restarting the Fail2Ban Service

sudo systemctl restart fail2ban

Step 6: Checking Fail2Ban Status

sudo fail2ban-client status
sudo fail2ban-client status sshd

Step 7: Simulating a Brute-Force Attack
Attempt multiple failed logins:

ssh user@your-server-ip
(Enter incorrect password multiple times)

Check if the IP is banned:

sudo fail2ban-client status sshd
sudo tail -n 50 /var/log/fail2ban.log

Step 8: Unbanning an IP

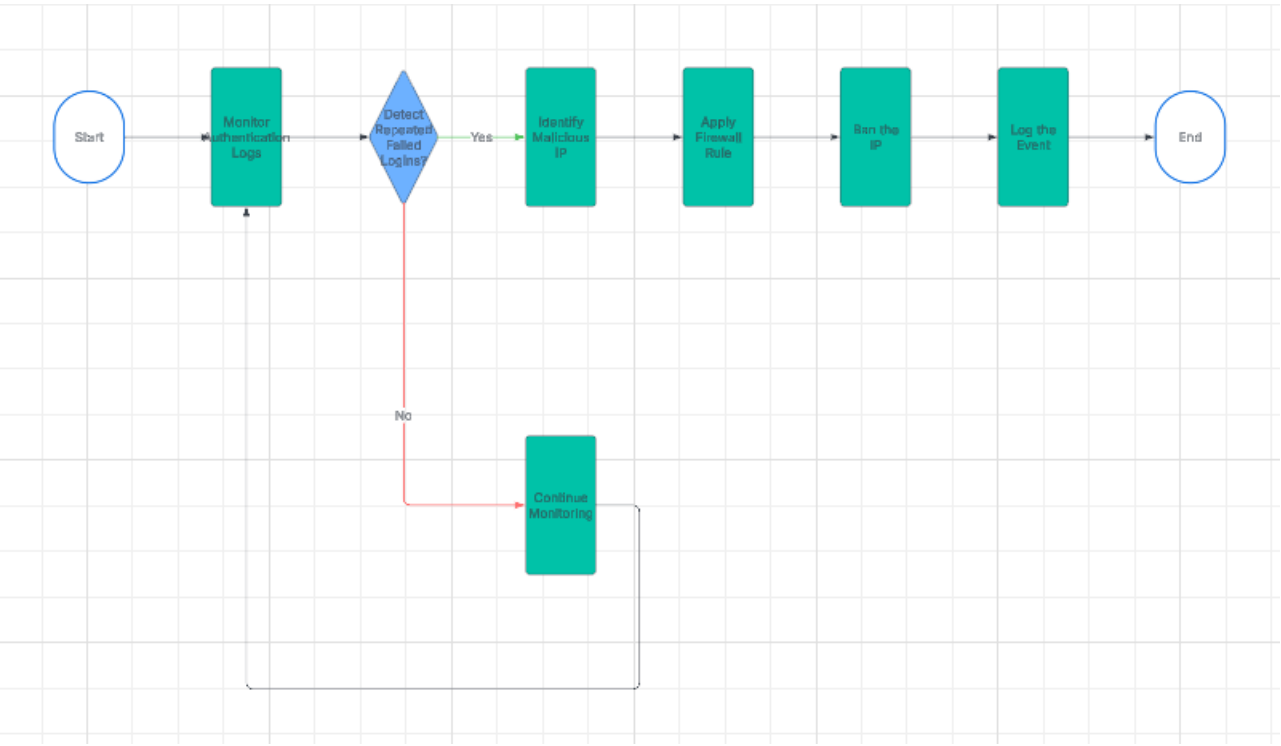
sudo fail2ban-client set sshd unbanip your-ip-address

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

FLOWCHART :

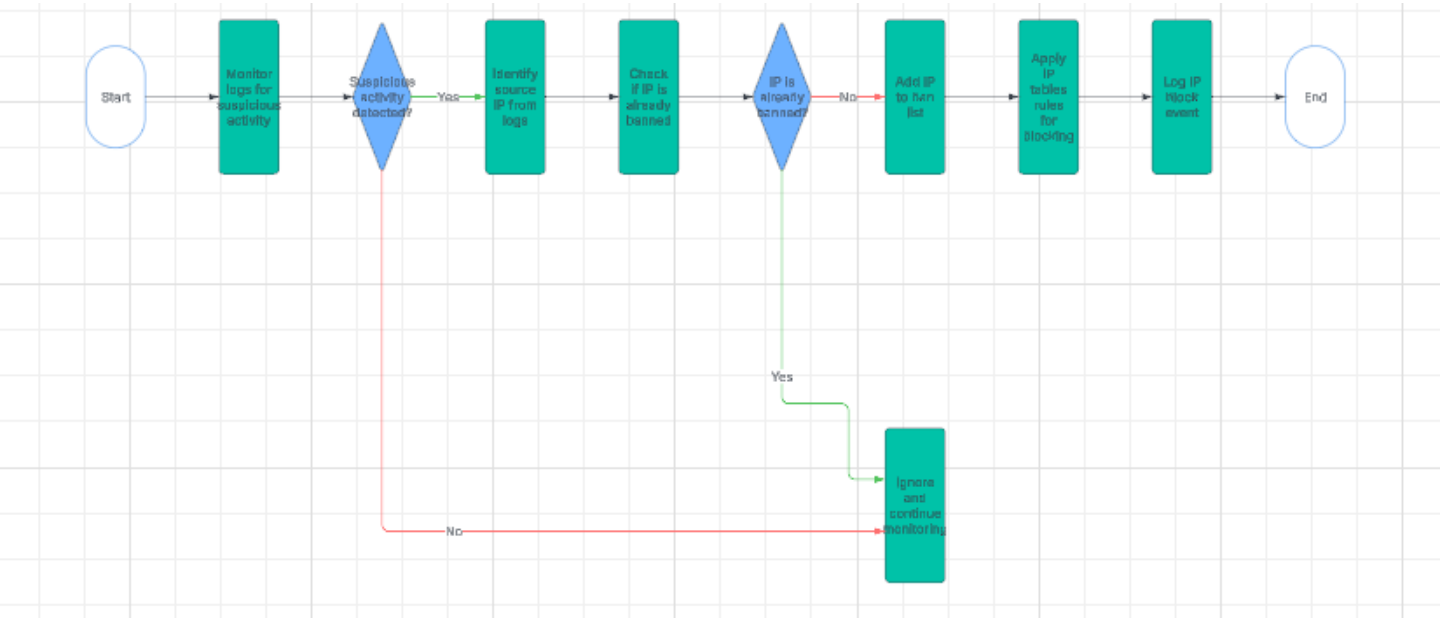
Fail2Ban Working Process :



K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Fail2Ban IP Blocking Process :

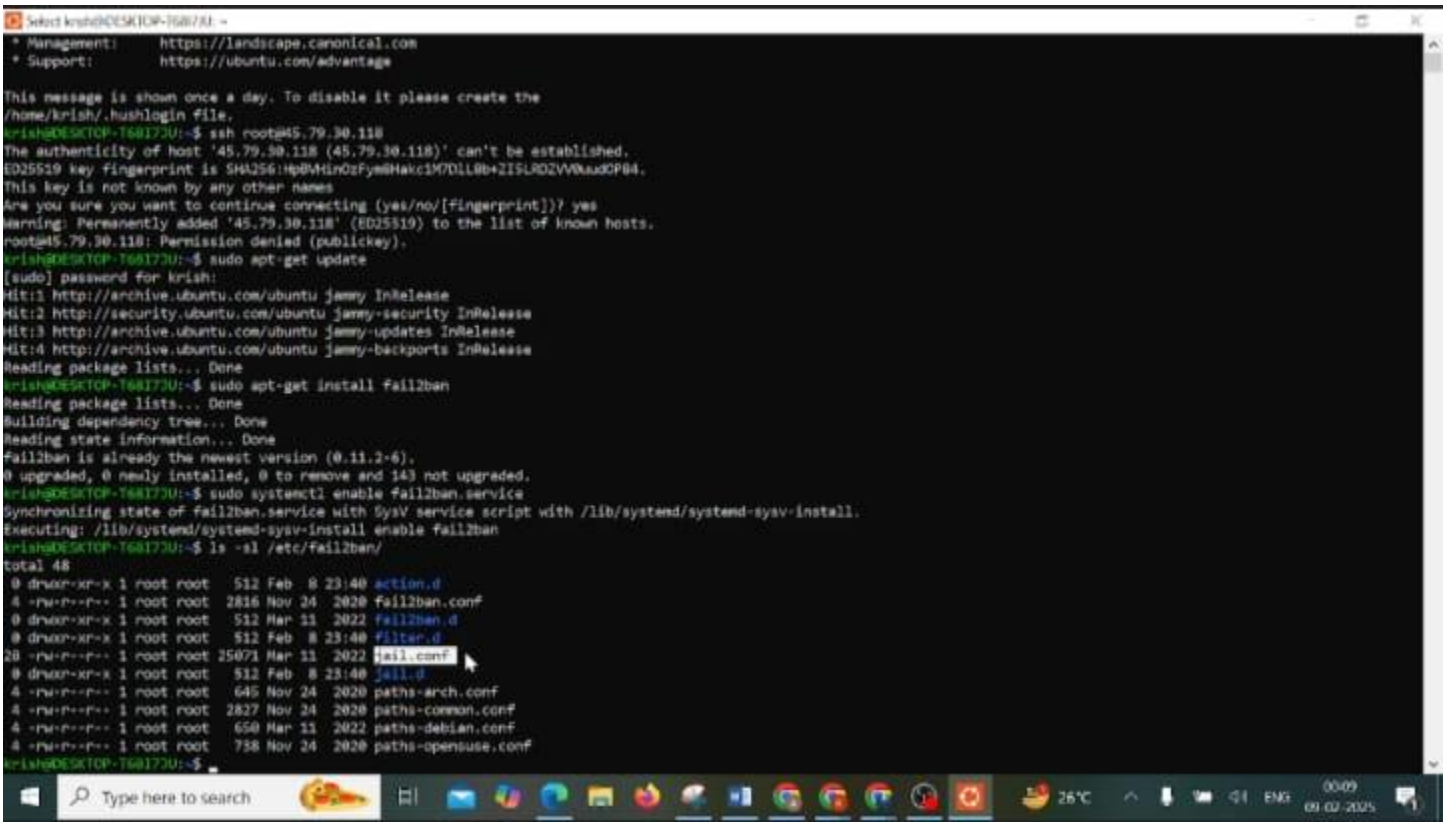


K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

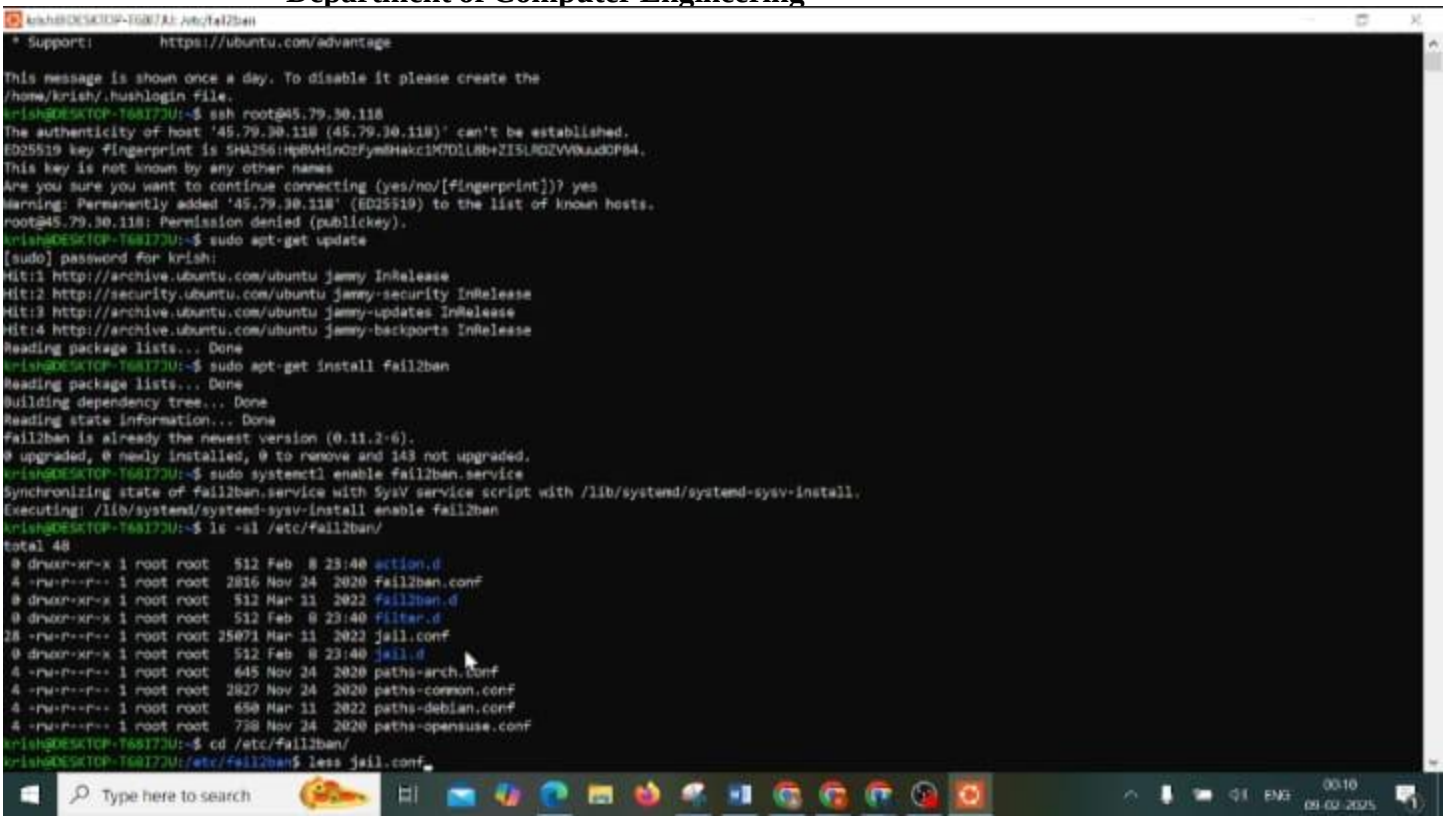
GitHub Repository Link: https://github.com/krishtel15/Implementation-of-Fail2ban-Security-Tool.git

Output:



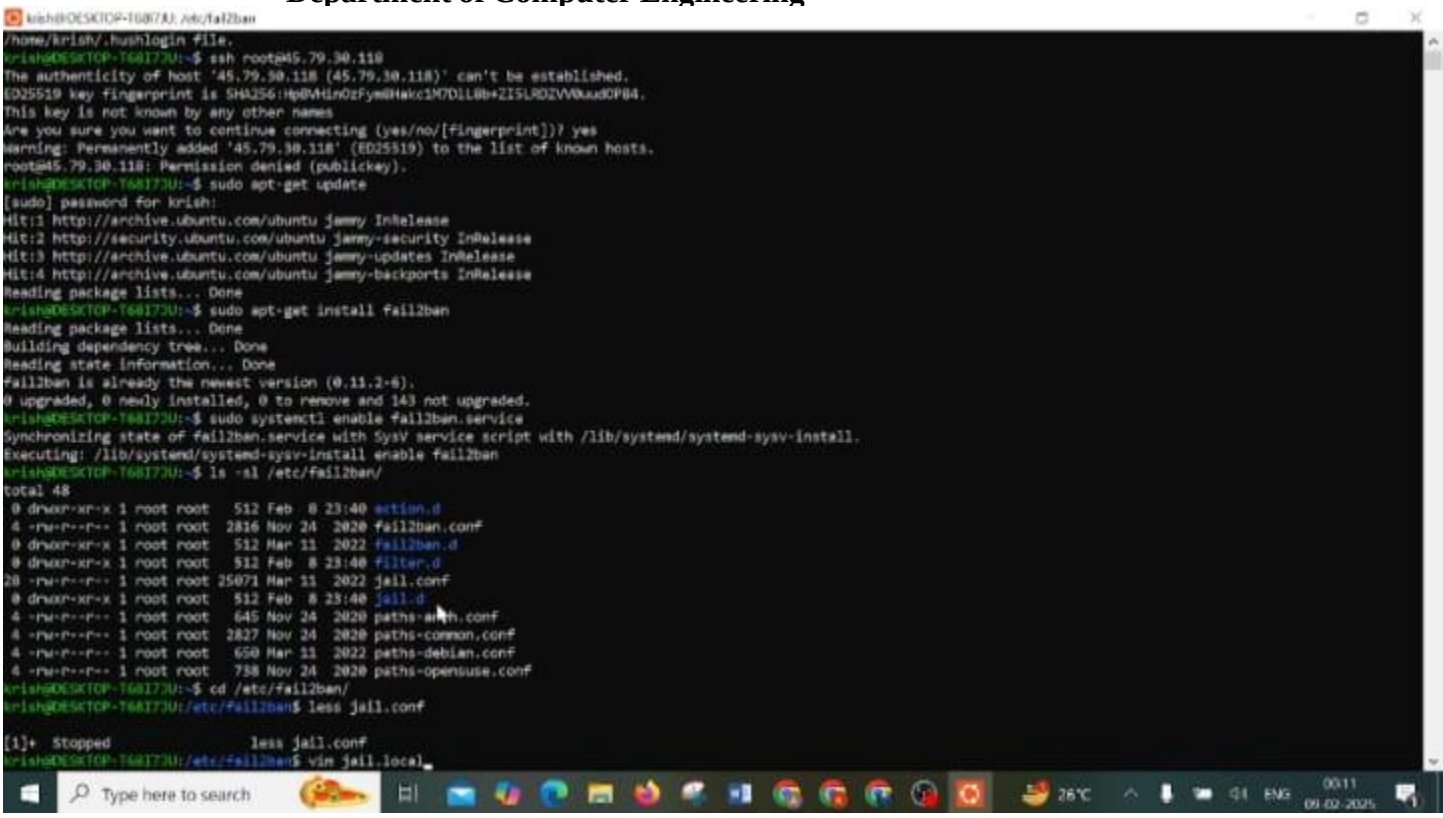
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



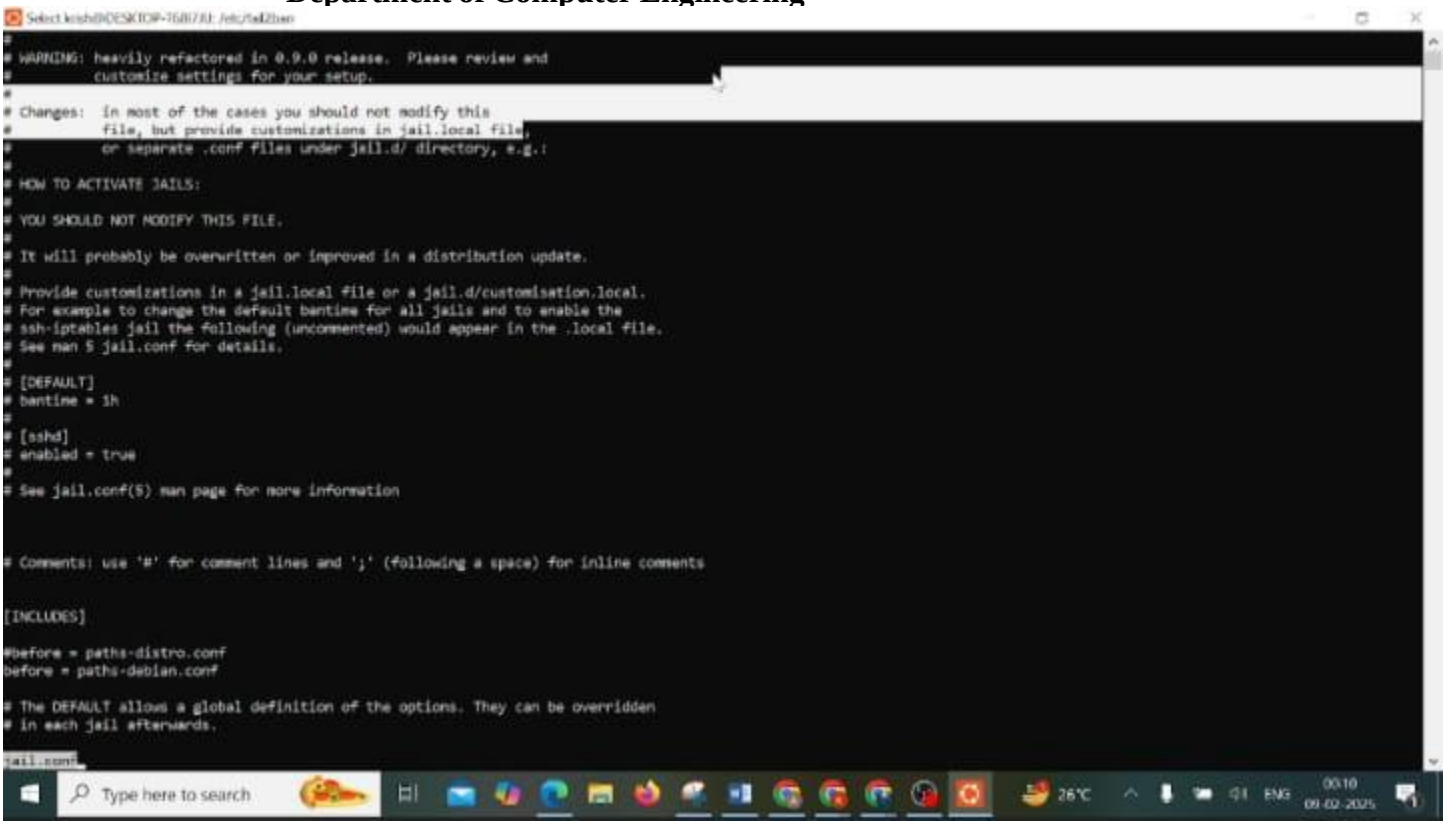
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



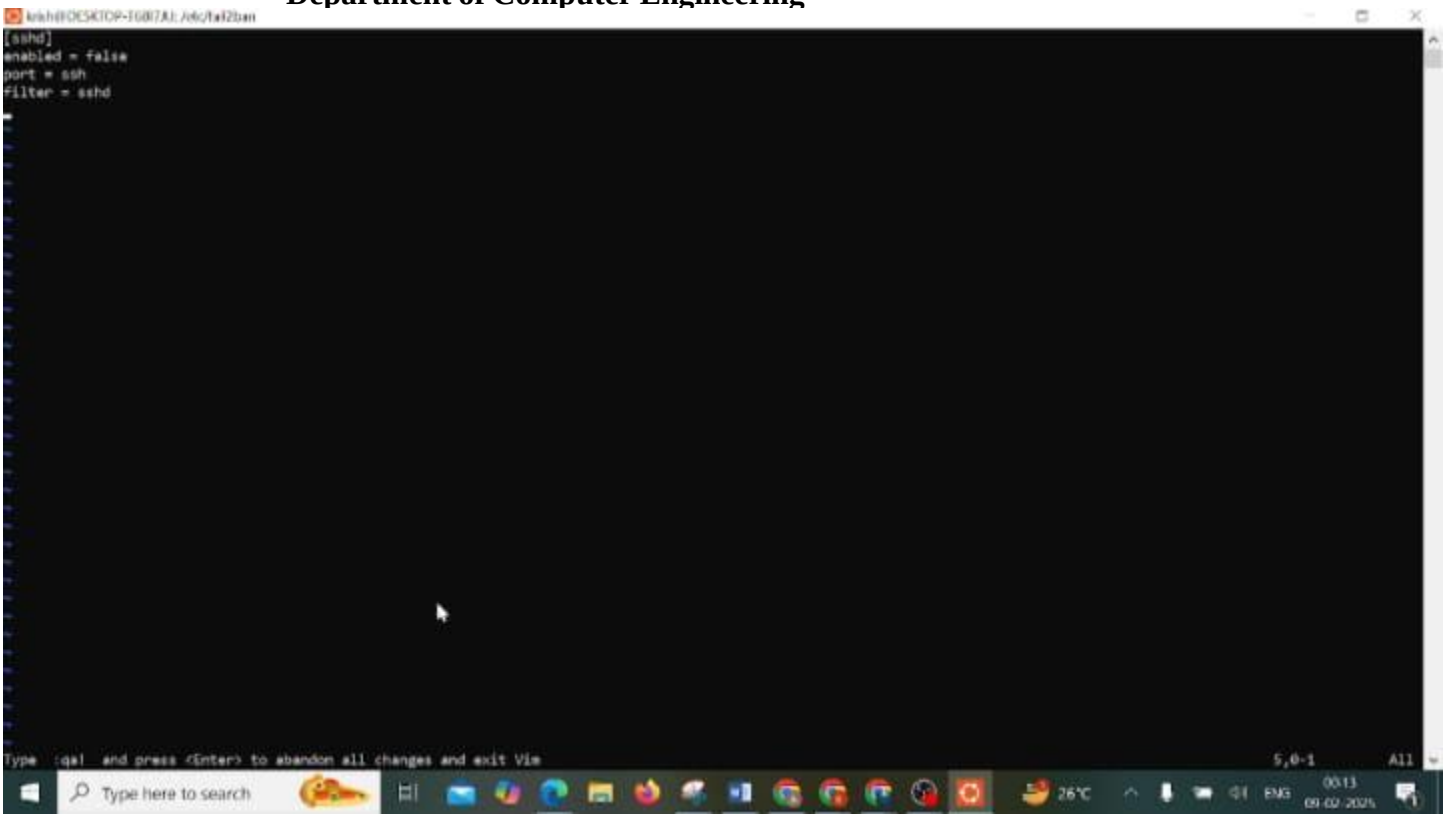
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



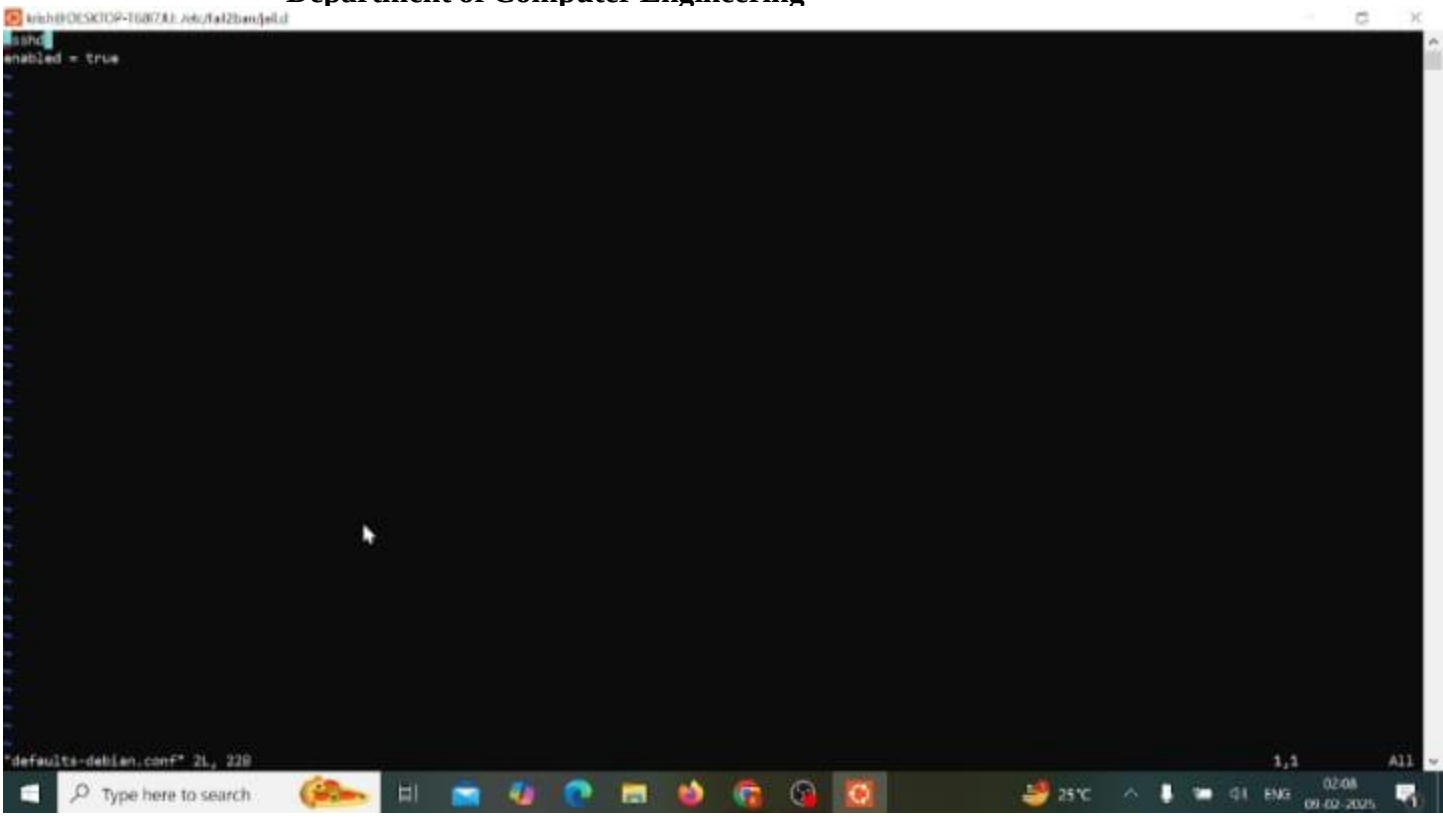
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



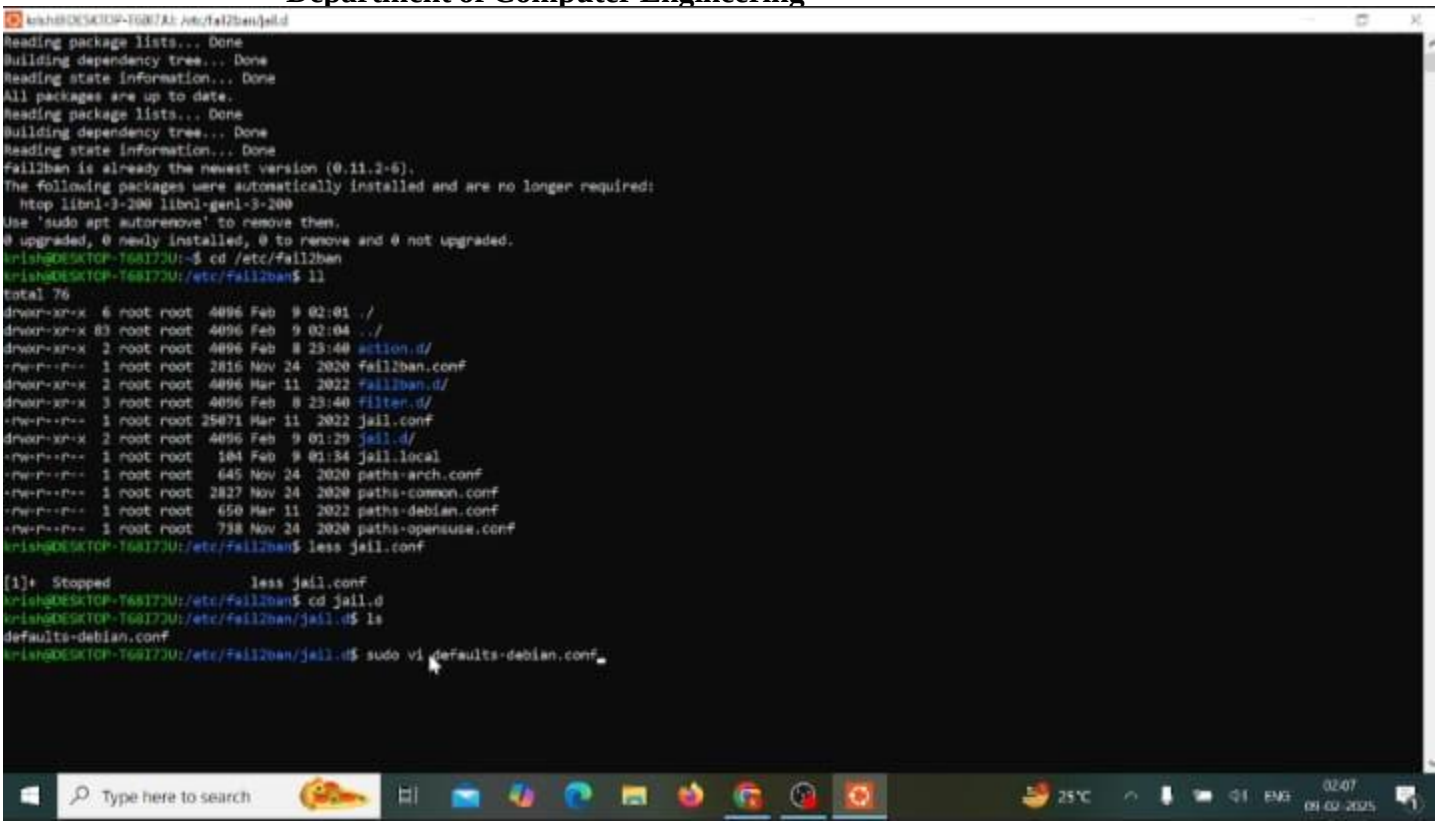
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



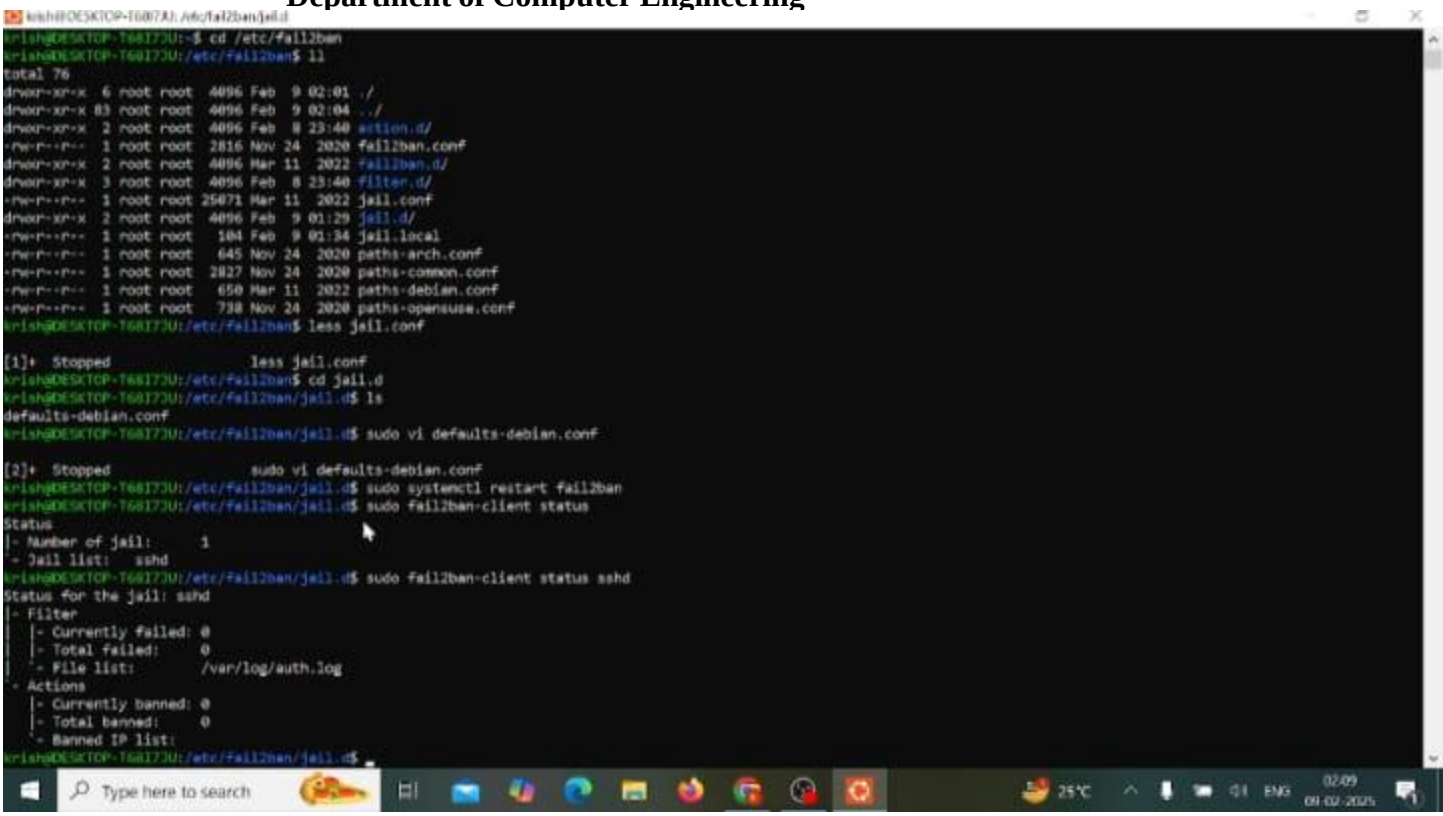
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



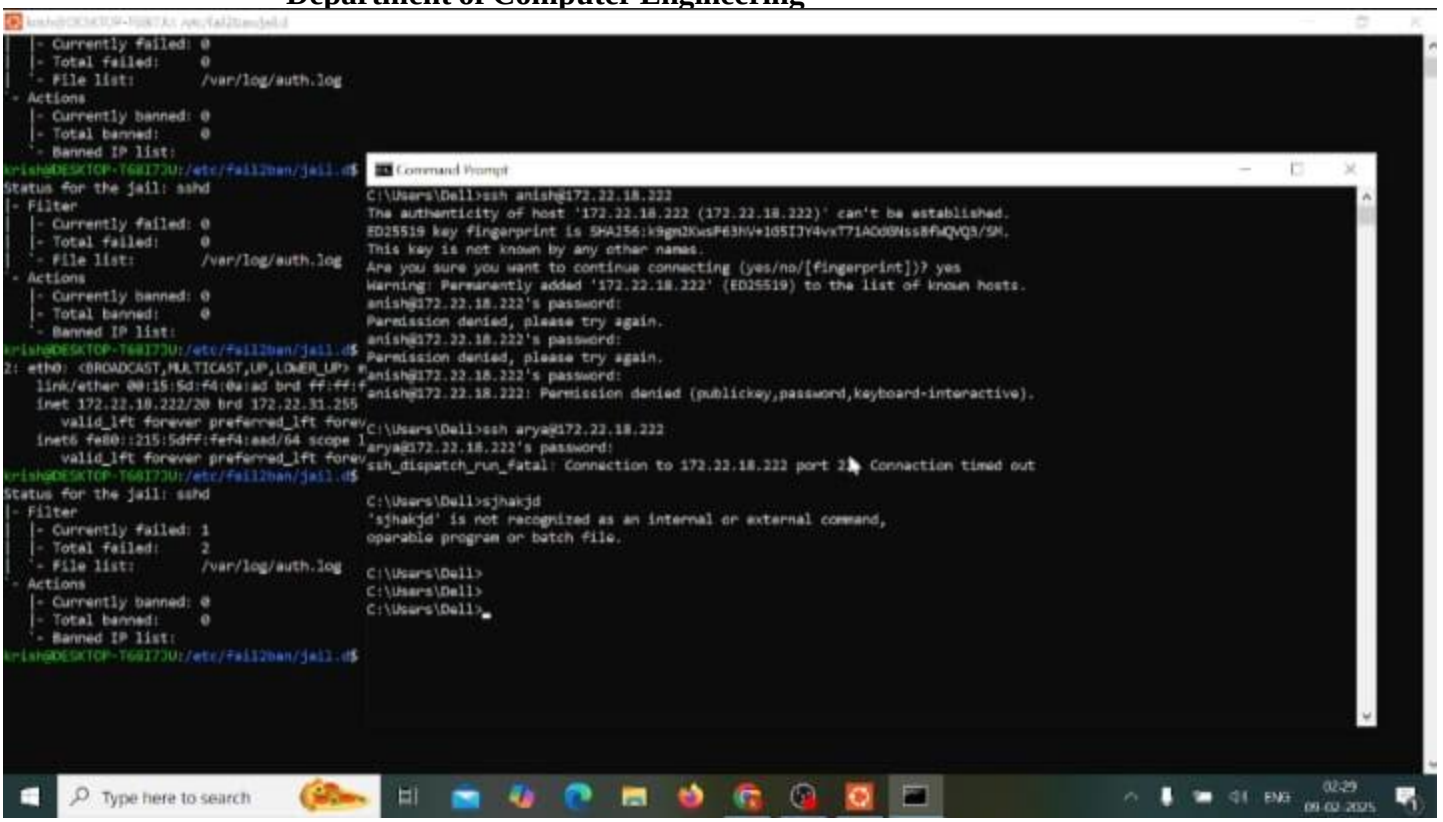
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



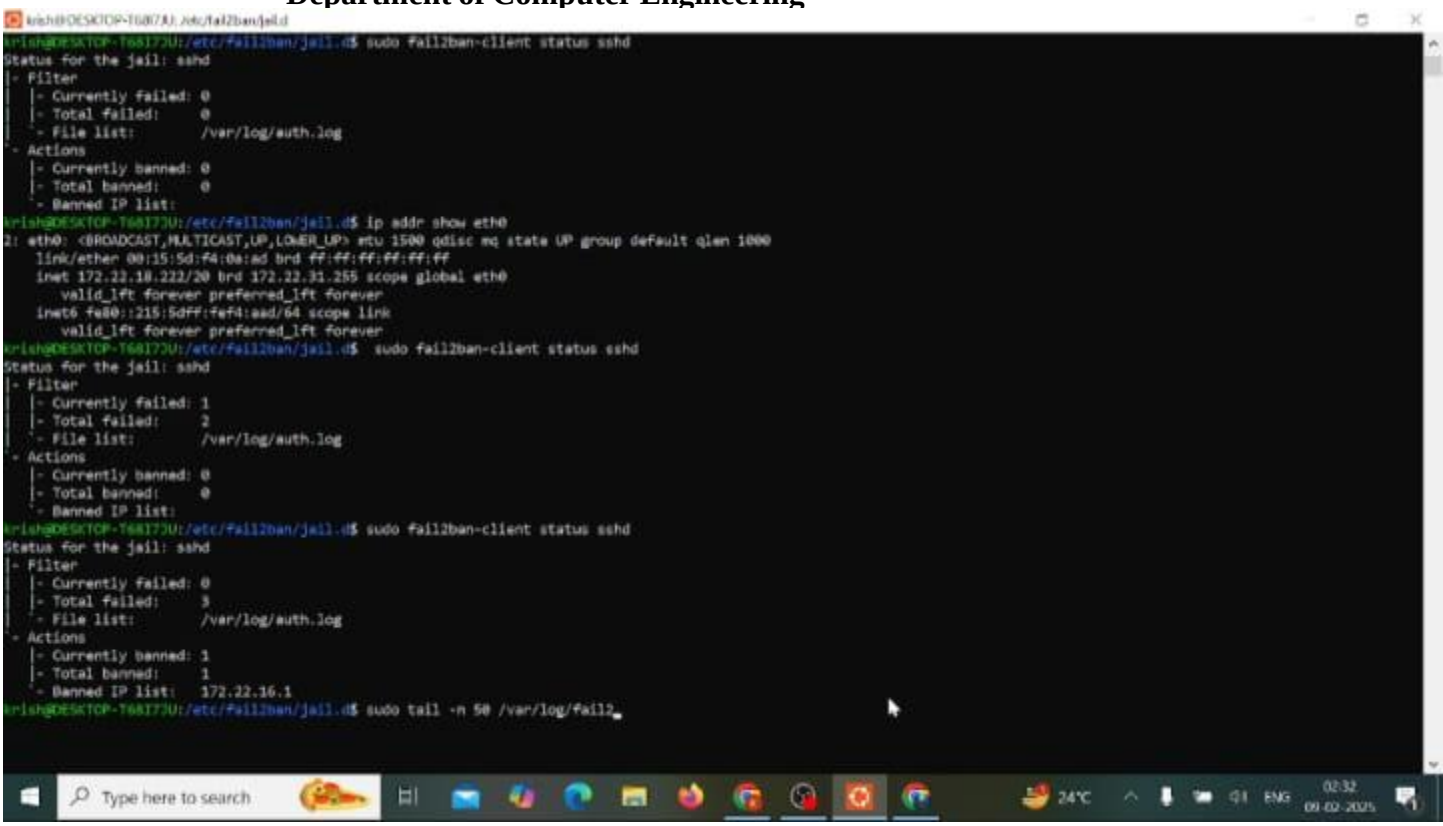
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



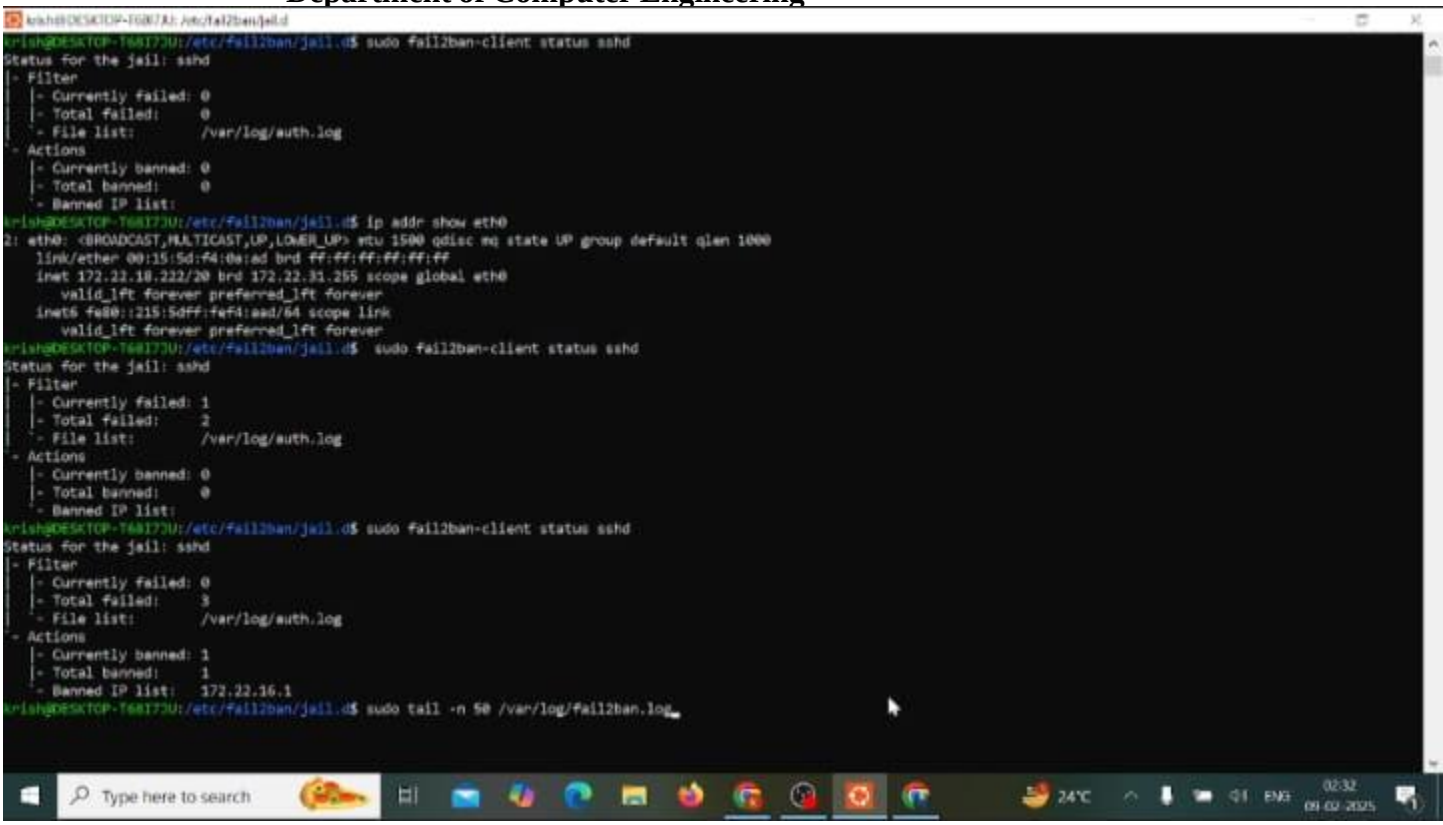
K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



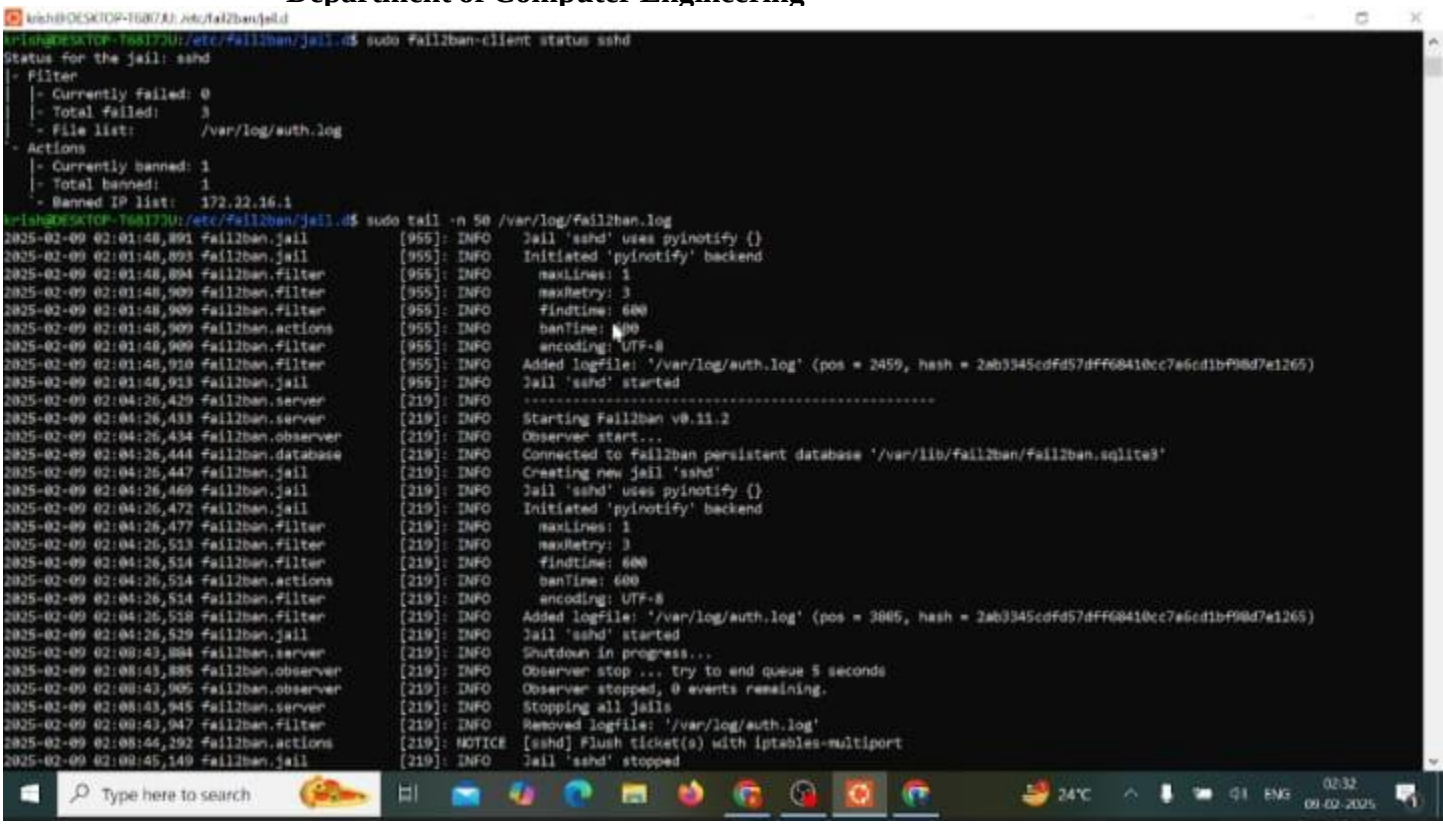
K J Somaiya College of Engineering, Mumbai-400077

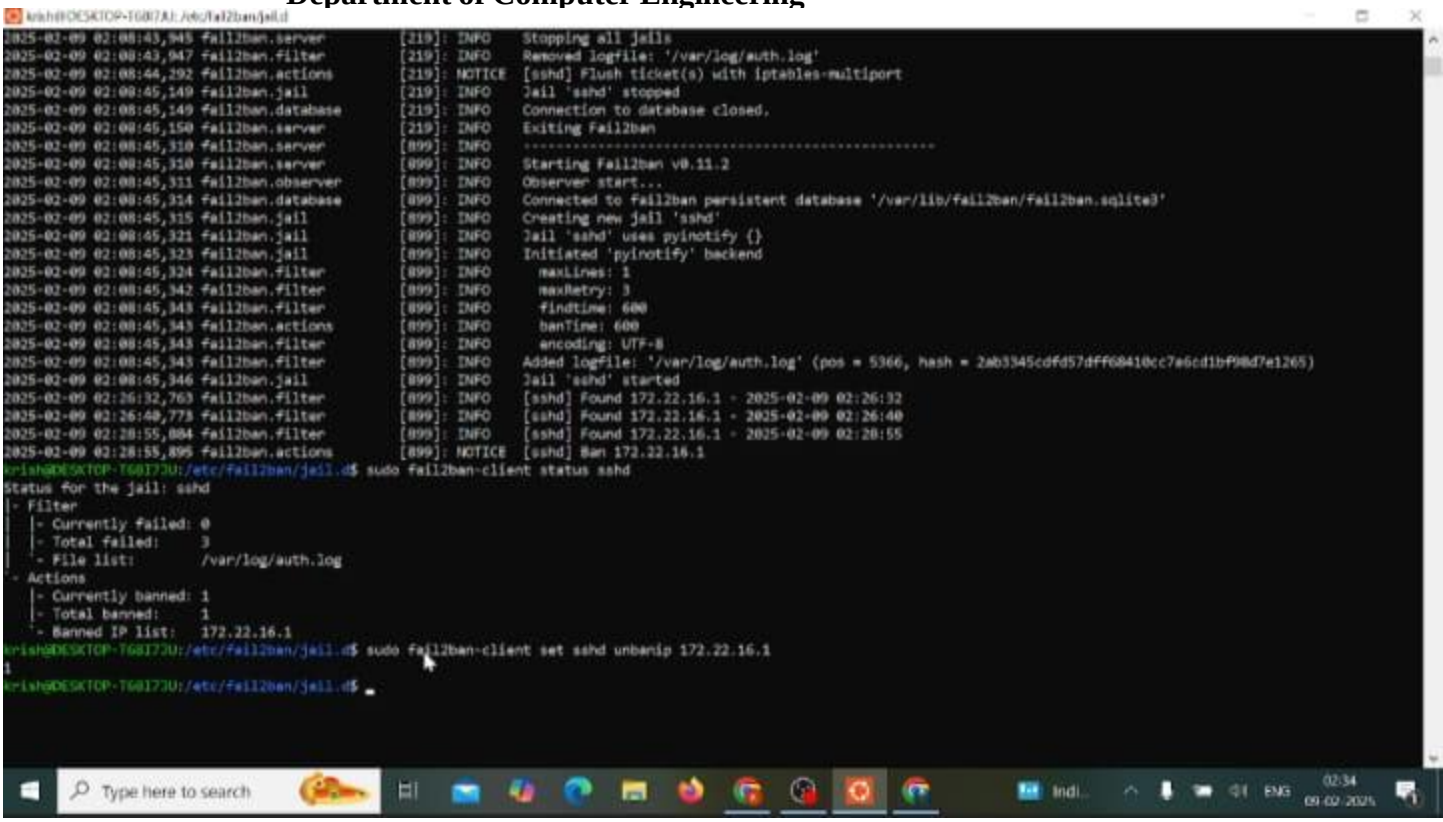
Department of Computer Engineering



K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering





Result/Discussion:

- Fail2Ban was successfully installed and configured to secure SSH.
- Repeated failed login attempts led to automatic banning of the attacker's IP.
- The service effectively prevented brute-force attacks without manual intervention.
- Log files confirmed that the firewall rules were dynamically updated.
- Unbanning commands were tested to ensure administrative control.

Limitations:

- Temporary bans may not deter sophisticated attackers using distributed IPs.
- Requires proper configuration to avoid accidentally banning legitimate users.
- Relies on log analysis, which can be bypassed by stealthy attackers.

Applications:

- Securing Remote Servers: Prevent unauthorized SSH access.
- Protecting Web Applications: Block repeated login failures on web-based services.
- Firewall Enhancement: Complement existing security mechanisms.
- Automated Security Policies: Reduce human intervention in access control**.**

References/Research Papers:

[1] J. Smith, "Enhancing Server Security with Fail2Ban," Journal of Cybersecurity, 2023.
[2] Linux Foundation, "Fail2Ban Documentation," https://www.fail2ban.org.

Conclusion:

Fail2Ban is an effective tool for securing servers against brute-force attacks by monitoring authentication logs and dynamically blocking malicious IPs. With proper configuration, it enhances server security with minimal manual intervention. While effective, it should be used alongside other security measures like strong passwords and multi-factor authentication.