# Fail2Ban Implementation Code and Steps on Ubuntu

## 1. Update System & Install Fail2Ban

sudo apt-get update

sudo apt-get install fail2ban

This installs Fail2Ban, which monitors log files for repeated failed login attempts and bans malicious IPs.

## 2. Enable Fail2Ban Service

sudo systemctl enable fail2ban.service

Ensures Fail2Ban runs automatically on system startup.

## 3. Access Fail2Ban Configuration

cd /etc/fail2ban/

ls -sl

Configuration files are stored in /etc/fail2ban/.

## 4. Modify Jail Configuration

less jail.conf

cd jail.d

ls

sudo vi defaults-debian.conf

Instead of editing jail.conf, configurations should be modified inside jail.d/. The SSH jail must be enabled.

## 5. Restart Fail2Ban

sudo systemctl restart fail2ban

Applies configuration changes.

## 6. Check Fail2Ban Status

sudo fail2ban-client status

sudo fail2ban-client status sshd

Verifies that Fail2Ban is running and monitoring SSH login attempts.

## 7. Simulate Failed SSH Logins (Testing Fail2Ban using different terminal)

ssh anish@172.22.18.222

ssh arya@172.22.18.222

ssh mansi@172.22.18.222

Multiple failed login attempts trigger Fail2Ban.

## 8. Check Banned IPs

sudo fail2ban-client status sshd

sudo tail -n 50 /var/log/fail2ban.log

Displays the banned IPs and logs.

## 9. Unban an IP (If Needed)

sudo fail2ban-client set sshd unbanip 172.22.16.1

Removes a mistakenly banned IP.

### **Conclusion:**

Fail2Ban enhances server security by automatically banning suspicious IPs after repeated failed logins. This setup ensures protection against brute-force attacks.