

**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: 9<sup>th</sup> 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.

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

## **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.

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

## **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**

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

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

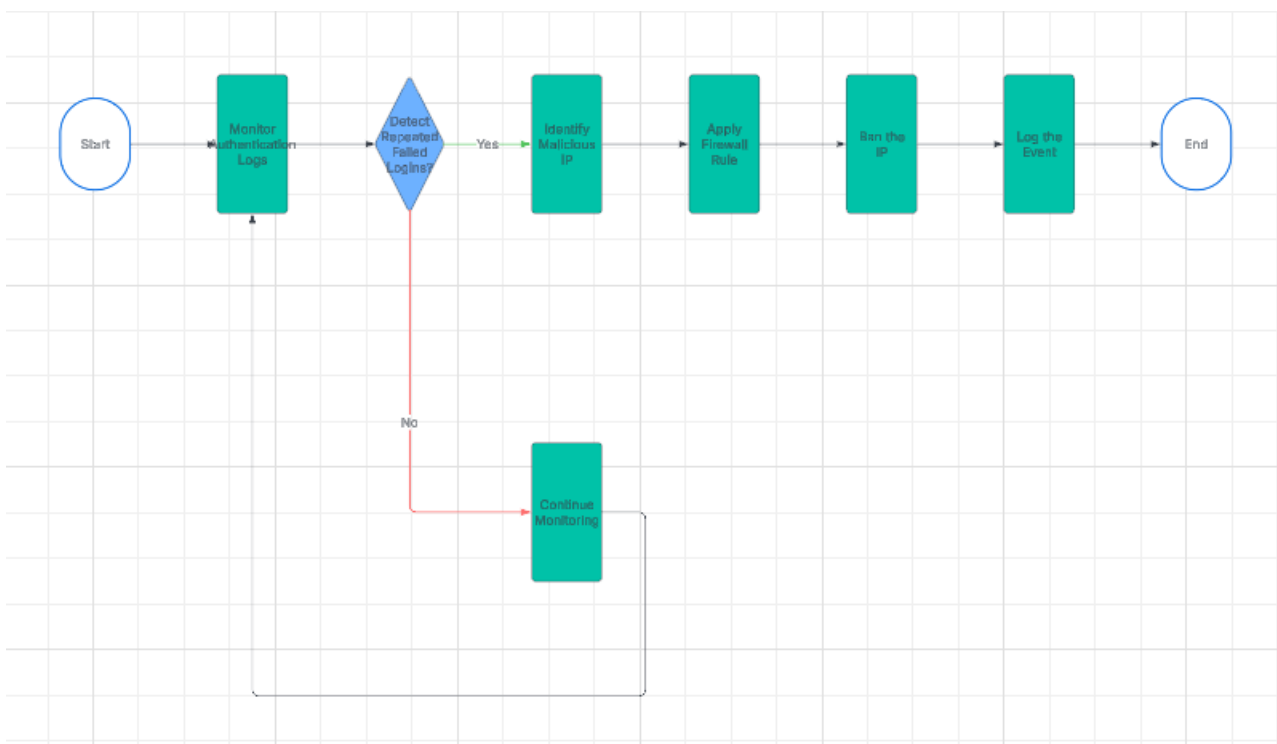
**sudo fail2ban-client set sshd unbanip your-ip-address**

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

**FLOWCHART :**

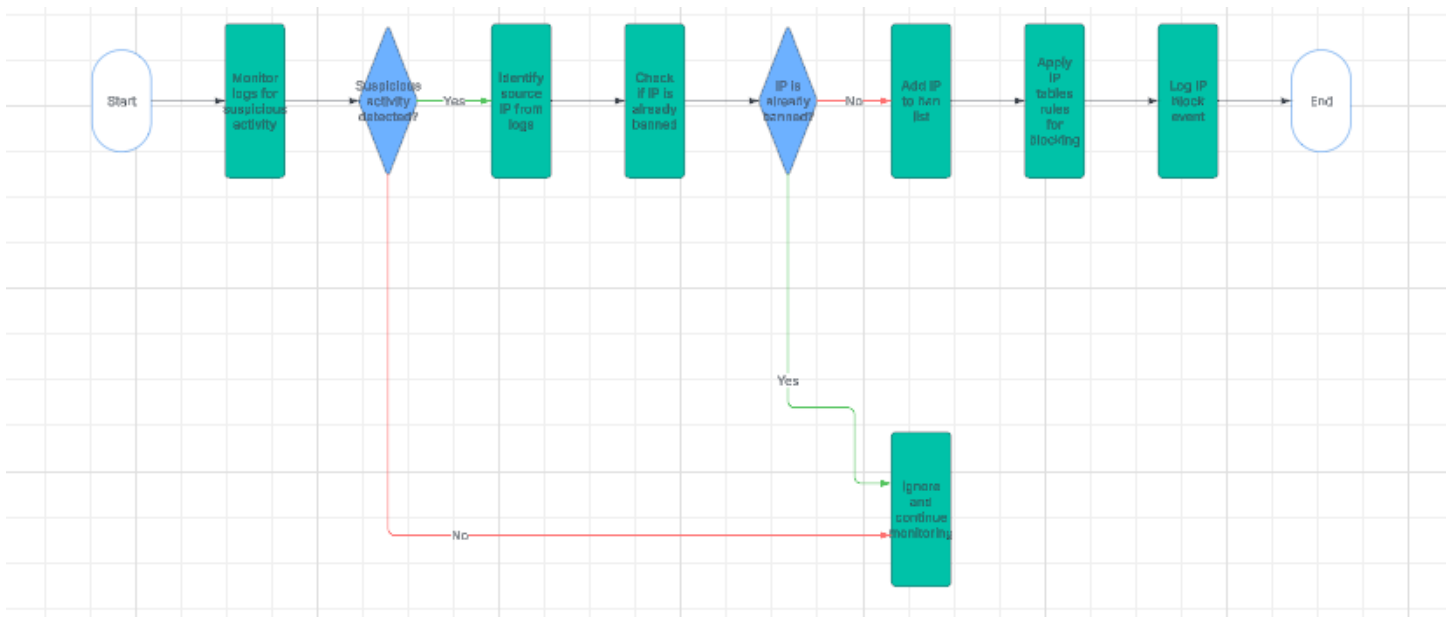
**Fail2Ban Working Process :**



**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:**

```
Select krish@DESKTOP-T68173U: ~
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/krish/.hushlogin file.
krish@DESKTOP-T68173U:~$ ssh root@45.79.30.118
The authenticity of host '45.79.30.118 (45.79.30.118)' can't be established.
ED25519 key fingerprint is SHA256:HqBMAHnOzfymHakc1K0D1L8b+ZISLR0ZVWkaudPF84.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '45.79.30.118' (ED25519) to the list of known hosts.
root@45.79.30.118: Permission denied (publickey).
krish@DESKTOP-T68173U:~$ sudo apt-get update
[sudo] password for krish:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
krish@DESKTOP-T68173U:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fail2ban is already the newest version (0.11.3-6).
0 upgraded, 0 newly installed, 0 to remove and 143 not upgraded.
krish@DESKTOP-T68173U:~$ sudo systemctl enable fail2ban.service
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
krish@DESKTOP-T68173U:~$ ls -sl /etc/fail2ban/
total 48
-rwxr-xr-x 1 root root 512 Feb  8 23:40 action.d
-rw-r--r-- 1 root root 2816 Nov 24 2020 fail2ban.conf
-rwxr-xr-x 1 root root 512 Mar 11 2022 fail2ban.d
-rwxr-xr-x 1 root root 512 Feb  8 23:40 filter.d
-rw-r--r-- 1 root root 25071 Mar 11 2022 jail.conf
-rwxr-xr-x 1 root root 512 Feb  8 23:40 jail.d
-rw-r--r-- 1 root root 645 Nov 24 2020 paths-arch.conf
-rw-r--r-- 1 root root 2827 Nov 24 2020 paths-common.conf
-rw-r--r-- 1 root root 650 Mar 11 2022 paths-debian.conf
-rw-r--r-- 1 root root 758 Nov 24 2020 paths-opensuse.conf
krish@DESKTOP-T68173U:~$
```

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

```
krish@DESKTOP-T68172U: ~$ sudo apt-get install fail2ban
* Support: https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/krish/.hushlogin file.
krish@DESKTOP-T68172U:~$ ssh root@45.79.30.118
The authenticity of host '45.79.30.118 (45.79.30.118)' can't be established.
ED25519 key fingerprint is SHA256:HpbM4InozfymHakc1K7D1L8b+ZISJROZVVAudOP84.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '45.79.30.118' (ED25519) to the list of known hosts.
root@45.79.30.118: Permission denied (publickey).
krish@DESKTOP-T68172U:~$ sudo apt-get update
[sudo] password for krish:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
krish@DESKTOP-T68172U:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fail2ban is already the newest version (0.11.2-6).
0 upgraded, 0 newly installed, 0 to remove and 143 not upgraded.
krish@DESKTOP-T68172U:~$ sudo systemctl enable fail2ban.service
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
krish@DESKTOP-T68172U:~$ ls -sl /etc/fail2ban/
total 48
-rwxr-xr-x 1 root root 512 Feb  8 23:40 action.d
-rw-r--r-- 1 root root 2816 Nov 24 2020 fail2ban.conf
-rwxr-xr-x 1 root root 512 Mar 11 2022 fail2ban.d
-rwxr-xr-x 1 root root 512 Feb  8 23:40 filter.d
-rw-r--r-- 1 root root 25071 Mar 11 2022 jail.conf
-rwxr-xr-x 1 root root 512 Feb  8 23:40 jail.d
-rw-r--r-- 1 root root 645 Nov 24 2020 paths-arch.conf
-rw-r--r-- 1 root root 2827 Nov 24 2020 paths-common.conf
-rw-r--r-- 1 root root 650 Mar 11 2022 paths-debian.conf
-rw-r--r-- 1 root root 720 Nov 24 2020 paths-opensuse.conf
krish@DESKTOP-T68172U:~$ cd /etc/fail2ban/
krish@DESKTOP-T68172U:/etc/fail2ban$ less jail.conf
```



## K J Somaiya College of Engineering, Mumbai-400077

### Department of Computer Engineering

```

krish@DESKTOP-T68173U: /etc/fail2ban
/home/krish/.hushlogin file.
krish@DESKTOP-T68173U:~$ ssh root@45.79.30.118
The authenticity of host '45.79.30.118 (45.79.30.118)' can't be established.
ED25519 key fingerprint is SHA256:HqBv4HnO2FymHake1MOD1L8b+Zi5LROZVWkaadQP84.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '45.79.30.118' (ED25519) to the list of known hosts.
root@45.79.30.118: Permission denied (publickey).
krish@DESKTOP-T68173U:~$ sudo apt-get update
[sudo] password for krish:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
krish@DESKTOP-T68173U:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fail2ban is already the newest version (0.11.2-4).
0 upgraded, 0 newly installed, 0 to remove and 143 not upgraded.
krish@DESKTOP-T68173U:~$ sudo systemctl enable fail2ban.service
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
krish@DESKTOP-T68173U:~$ ls -ls /etc/fail2ban/
total 48
0 drwxr-xr-x 1 root root 512 Feb  8 23:40 action.d
4 -rwxr-xr-x 1 root root 2816 Nov 24 2020 fail2ban.conf
0 drwxr-xr-x 1 root root 512 Mar 11 2022 fail2ban.d
0 drwxr-xr-x 1 root root 512 Feb  8 23:40 filter.d
20 -rwxr-xr-x 1 root root 25071 Mar 11 2022 jail.conf
0 drwxr-xr-x 1 root root 512 Feb  8 23:40 jail.d
4 -rwxr-xr-x 1 root root 645 Nov 24 2020 paths-ssh.conf
4 -rwxr-xr-x 1 root root 2827 Nov 24 2020 paths-common.conf
4 -rwxr-xr-x 1 root root 650 Mar 11 2022 paths-debian.conf
4 -rwxr-xr-x 1 root root 738 Nov 24 2020 paths-opensuse.conf
krish@DESKTOP-T68173U:~$ cd /etc/fail2ban/
krish@DESKTOP-T68173U:/etc/fail2ban$ less jail.conf
[1]+  Stopped                  less jail.conf
krish@DESKTOP-T68173U:/etc/fail2ban$ vim jail.local
  
```

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

```
Select krishna@DESKTOP-76B7JL: /etc/jail2/
#
# WARNING: heavily refactored in 0.9.0 release. Please review and
#          customize settings for your setup.
#
# Changes: in most of the cases you should not modify this
#          file, but provide customizations in jail.local file,
#          or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information
#
# Comments: use '#' for comment lines and ';' (following a space) for inline comments

[INCLUDES]

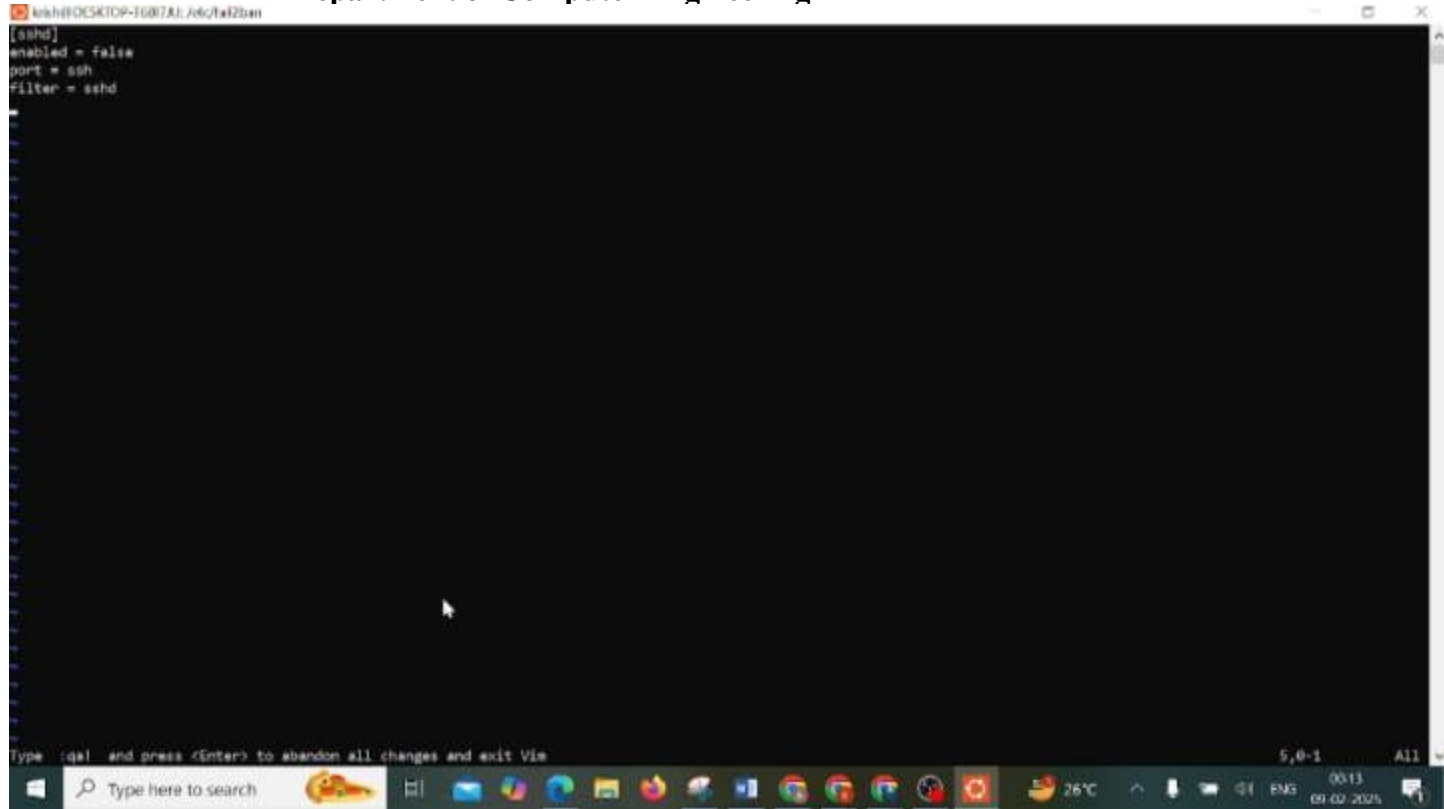
#before = paths-distro.conf
before = paths-debian.conf

# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.

jail.conf
```

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

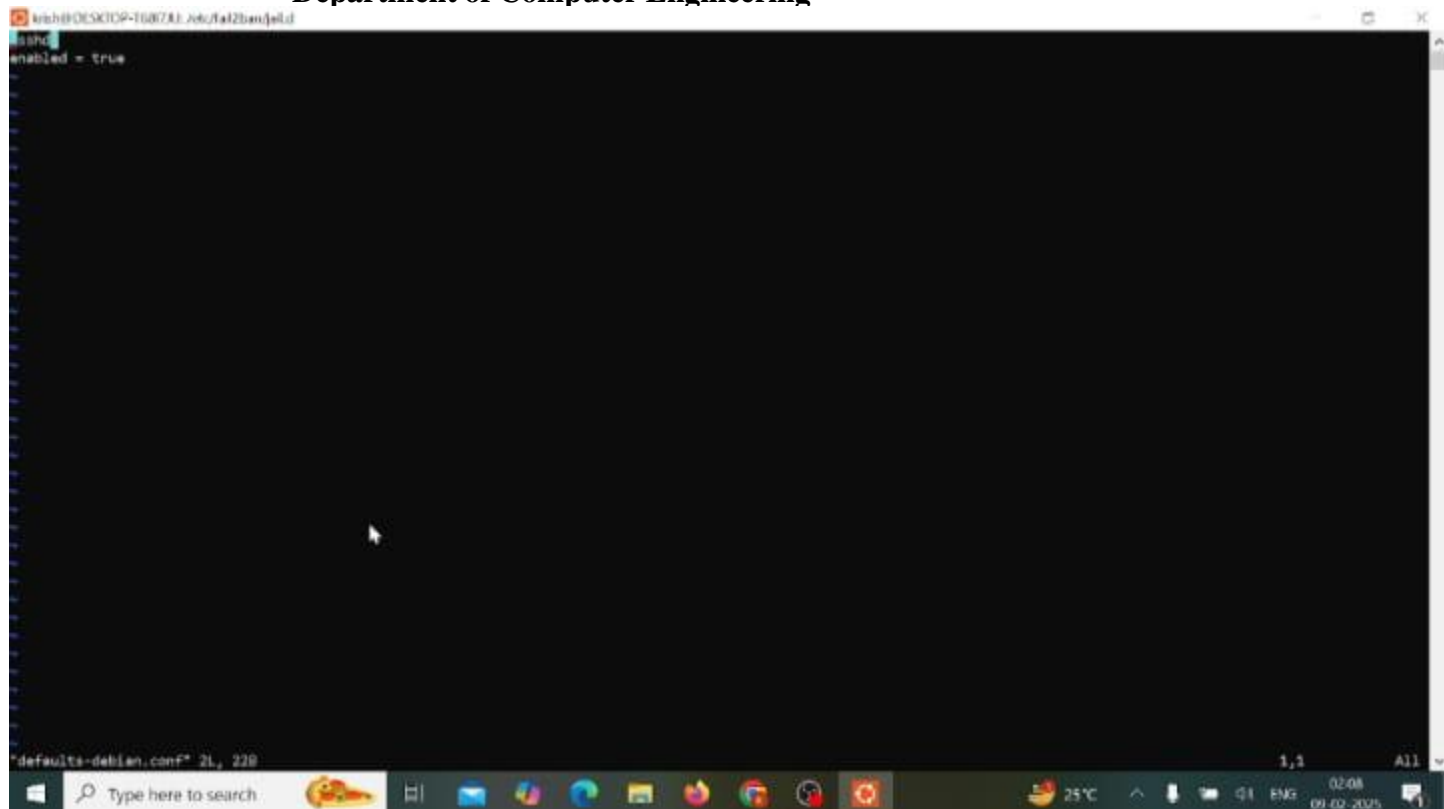


```
kskh@POCSKTCP-168B7A1: /etc/tail2ban
[sshd]
enabled = false
port = ssh
filter = sshd

Type :q! and press <Enter> to abandon all changes and exit Vim
```

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**



**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

```
krish@DESKTOP-T68I72U: /etc/fail2ban$ ll
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fail2ban is already the newest version (0.11.2-6).
The following packages were automatically installed and are no longer required:
  http libnl-3-200 libnl-genl-3-200
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
krish@DESKTOP-T68I72U:~$ cd /etc/fail2ban
krish@DESKTOP-T68I72U:/etc/fail2ban$ ll
total 76
drwxr-xr-x 6 root root 4096 Feb  9 02:01 ./
drwxr-xr-x 83 root root 4096 Feb  9 02:04 ../
drwxr-xr-x 2 root root 4096 Feb  8 23:40 action.d/
-rw-r--r-- 1 root root 2816 Nov 24 2020 fail2ban.conf
drwxr-xr-x 2 root root 4096 Mar 11 2022 fail2ban.d/
drwxr-xr-x 3 root root 4096 Feb  8 23:40 filter.d/
-rw-r--r-- 1 root root 25071 Mar 11 2022 jail.conf
drwxr-xr-x 2 root root 4096 Feb  9 01:29 jail.d/
-rw-r--r-- 1 root root 104 Feb  9 01:34 jail.local
-rw-r--r-- 1 root root 645 Nov 24 2020 paths-arch.conf
-rw-r--r-- 1 root root 2827 Nov 24 2020 paths-common.conf
-rw-r--r-- 1 root root 650 Mar 11 2022 paths-debian.conf
-rw-r--r-- 1 root root 738 Nov 24 2020 paths-opensuse.conf
krish@DESKTOP-T68I72U:/etc/fail2ban$ less jail.conf

[1]+  Stopped                  less jail.conf
krish@DESKTOP-T68I72U:/etc/fail2ban$ cd jail.d
krish@DESKTOP-T68I72U:/etc/fail2ban/jail.d$ ls
defaults-debian.conf
krish@DESKTOP-T68I72U:/etc/fail2ban/jail.d$ sudo vi defaults-debian.conf
```

**K J Somaiya College of Engineering, Mumbai-400077**

## Department of Computer Engineering

```

krish@DESKTOP-T66I73U: /etc/fail2ban/jail.d
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban
total 76
drwxr-xr-x 6 root root 4096 Feb 9 02:01 ./
drwxr-xr-x 83 root root 4096 Feb 9 02:04 ../
drwxr-xr-x 2 root root 4096 Feb 8 23:40 action.d/
-rw-r--r-- 1 root root 2616 Nov 24 2020 fail2ban.conf
drwxr-xr-x 2 root root 4096 Mar 11 2022 fail2ban.d/
drwxr-xr-x 3 root root 4096 Feb 8 23:40 filter.d/
-rw-r--r-- 1 root root 25071 Mar 11 2022 jail.conf
drwxr-xr-x 2 root root 4096 Feb 9 01:29 jail.d/
-rw-r--r-- 1 root root 184 Feb 9 01:34 jail.local
-rw-r--r-- 1 root root 645 Nov 24 2020 paths-arch.conf
-rw-r--r-- 1 root root 2827 Nov 24 2020 paths-common.conf
-rw-r--r-- 1 root root 650 Mar 11 2022 paths-debian.conf
-rw-r--r-- 1 root root 738 Nov 24 2020 paths-opensuse.conf
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban
krish@DESKTOP-T66I73U:~$ less jail.conf
[1]+  Stopped                  less jail.conf
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban/jail.d
krish@DESKTOP-T66I73U:~$ ls
defaults-debian.conf
krish@DESKTOP-T66I73U:~$ sudo vi defaults-debian.conf
[2]+  Stopped                  sudo vi defaults-debian.conf
krish@DESKTOP-T66I73U:~$ sudo systemctl restart fail2ban
krish@DESKTOP-T66I73U:~$ sudo fail2ban-client status
Status
|- Number of jail: 1
- Jail list: sshd
krish@DESKTOP-T66I73U:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|- Currently failed: 0
|- Total failed: 0
- File list: /var/log/auth.log
- Actions
|- Currently banned: 0
|- Total banned: 0
- Banned IP list:
krish@DESKTOP-T66I73U:~$ cd /etc/fail2ban/jail.d

```

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

[illegible]

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

```
krish@DESKTOP-T68172U: /etc/fail2ban/jail$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 0
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 0
  - Total banned: 0
  - Banned IP list:
krish@DESKTOP-T68172U: /etc/fail2ban/jail$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:f4:0a:ad brd ff:ff:ff:ff:ff:ff
    inet 172.22.18.222/20 brd 172.22.31.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe4:aa/64 scope link
        valid_lft forever preferred_lft forever
krish@DESKTOP-T68172U: /etc/fail2ban/jail$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 1
  - Total failed: 2
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 0
  - Total banned: 0
  - Banned IP list:
krish@DESKTOP-T68172U: /etc/fail2ban/jail$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 3
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 1
  - Total banned: 1
  - Banned IP list: 172.22.16.1
krish@DESKTOP-T68172U: /etc/fail2ban/jail$ sudo tail -n 50 /var/log/fail2ban.log
```



**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

```
krish@DESKTOP-T68177U:/etc/fail2ban/jail.d$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 0
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 0
  - Total banned: 0
  - Banned IP list:

krish@DESKTOP-T68177U:/etc/fail2ban/jail.d$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:f4:0a:ad brd ff:ff:ff:ff:ff:ff
    inet 172.22.18.222/20 brd 172.22.31.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe4d:aa/64 scope link
        valid_lft forever preferred_lft forever

krish@DESKTOP-T68177U:/etc/fail2ban/jail.d$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 1
  - Total failed: 2
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 0
  - Total banned: 0
  - Banned IP list:

krish@DESKTOP-T68177U:/etc/fail2ban/jail.d$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 3
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 1
  - Total banned: 1
  - Banned IP list: 172.22.16.1

krish@DESKTOP-T68177U:/etc/fail2ban/jail.d$ sudo tail -n 50 /var/log/fail2ban.log
```

**K J Somaiya College of Engineering, Mumbai-400077**

## Department of Computer Engineering

```
windows@DESKTOP-F6B7F81: /etc/fail2ban/jail$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 3
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 1
  - Total banned: 1
  - Banned IP list: 172.22.16.1

windows@DESKTOP-F6B7F81: /etc/fail2ban/jail$ sudo tail -n 50 /var/log/fail2ban.log
2025-02-09 02:01:48,891 fail2ban.jail [955]: INFO Jail 'sshd' uses pyinotify {}
2025-02-09 02:01:48,893 fail2ban.jail [955]: INFO Initiated 'pyinotify' backend
2025-02-09 02:01:48,894 fail2ban.filter [955]: INFO maxlines: 1
2025-02-09 02:01:48,900 fail2ban.filter [955]: INFO maxretry: 3
2025-02-09 02:01:48,900 fail2ban.filter [955]: INFO findtime: 600
2025-02-09 02:01:48,900 fail2ban.actions [955]: INFO banTime: 600
2025-02-09 02:01:48,900 fail2ban.filter [955]: INFO encoding: UTF-8
2025-02-09 02:01:48,910 fail2ban.filter [955]: INFO Added logfile: '/var/log/auth.log' (pos = 2459, hash = 2ab3345cdfd57dff68410cc7e6cd1bf90d7e1265)
2025-02-09 02:01:48,913 fail2ban.jail [955]: INFO Jail 'sshd' started
2025-02-09 02:04:26,429 fail2ban.server [219]: INFO -----
2025-02-09 02:04:26,433 fail2ban.server [219]: INFO Starting Fail2ban v0.11.2
2025-02-09 02:04:26,434 fail2ban.observer [219]: INFO Observer start...
2025-02-09 02:04:26,444 fail2ban.database [219]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-02-09 02:04:26,447 fail2ban.jail [219]: INFO Creating new jail 'sshd'
2025-02-09 02:04:26,460 fail2ban.jail [219]: INFO Jail 'sshd' uses pyinotify {}
2025-02-09 02:04:26,472 fail2ban.jail [219]: INFO Initiated 'pyinotify' backend
2025-02-09 02:04:26,477 fail2ban.filter [219]: INFO maxlines: 1
2025-02-09 02:04:26,513 fail2ban.filter [219]: INFO maxretry: 3
2025-02-09 02:04:26,514 fail2ban.filter [219]: INFO findtime: 600
2025-02-09 02:04:26,514 fail2ban.actions [219]: INFO banTime: 600
2025-02-09 02:04:26,514 fail2ban.filter [219]: INFO encoding: UTF-8
2025-02-09 02:04:26,518 fail2ban.filter [219]: INFO Added logfile: '/var/log/auth.log' (pos = 3885, hash = 2ab3345cdfd57dff68410cc7e6cd1bf90d7e1265)
2025-02-09 02:04:26,529 fail2ban.jail [219]: INFO Jail 'sshd' started
2025-02-09 02:08:43,884 fail2ban.server [219]: INFO Shutdown in progress...
2025-02-09 02:08:43,885 fail2ban.observer [219]: INFO Observer stop ... try to end queue 5 seconds
2025-02-09 02:08:43,905 fail2ban.observer [219]: INFO Observer stopped, 0 events remaining.
2025-02-09 02:08:43,945 fail2ban.server [219]: INFO Stopping all jails
2025-02-09 02:08:43,947 fail2ban.filter [219]: INFO Removed logfile: '/var/log/auth.log'
2025-02-09 02:08:44,292 fail2ban.actions [219]: NOTICE [sshd] Flush ticket(s) with iptables-multiport
2025-02-09 02:08:45,149 fail2ban.jail [219]: INFO Jail 'sshd' stopped
```

## K J Somaiya College of Engineering, Mumbai-400077

### Department of Computer Engineering

```

krish@DESKTOP-T68172U: /etc/fail2ban/jail.d
2025-02-09 02:08:43.945 fail2ban.server [219]: INFO Stopping all jails
2025-02-09 02:08:43.947 fail2ban.filter [219]: INFO Removed logfile: '/var/log/auth.log'
2025-02-09 02:08:44.292 fail2ban.actions [219]: NOTICE [sshd] Flush ticket(s) with iptables-multiport
2025-02-09 02:08:45.149 fail2ban.jail [219]: INFO Jail 'sshd' stopped
2025-02-09 02:08:45.150 fail2ban.database [219]: INFO Connection to database closed.
2025-02-09 02:08:45.310 fail2ban.server [219]: INFO Exiting Fail2ban
2025-02-09 02:08:45.310 fail2ban.server [899]: INFO -----
2025-02-09 02:08:45.310 fail2ban.server [899]: INFO Starting Fail2ban v0.11.2
2025-02-09 02:08:45.311 fail2ban.observer [899]: INFO Observer start...
2025-02-09 02:08:45.314 fail2ban.database [899]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-02-09 02:08:45.315 fail2ban.jail [899]: INFO Creating new jail 'sshd'
2025-02-09 02:08:45.321 fail2ban.jail [899]: INFO Jail 'sshd' uses pyinotify {}
2025-02-09 02:08:45.323 fail2ban.jail [899]: INFO Initiated 'pyinotify' backend
2025-02-09 02:08:45.324 fail2ban.filter [899]: INFO maxLines: 1
2025-02-09 02:08:45.342 fail2ban.filter [899]: INFO maxRetry: 3
2025-02-09 02:08:45.343 fail2ban.filter [899]: INFO findTime: 600
2025-02-09 02:08:45.343 fail2ban.actions [899]: INFO banTime: 600
2025-02-09 02:08:45.343 fail2ban.filter [899]: INFO encoding: UTF-8
2025-02-09 02:08:45.343 fail2ban.filter [899]: INFO Added logfile: '/var/log/auth.log' (pos = 5366, hash = 2ab3345cdfd57dff08410cc7a6cd1bf98d7e1265)
2025-02-09 02:08:45.346 fail2ban.jail [899]: INFO Jail 'sshd' started
2025-02-09 02:26:32.763 fail2ban.filter [899]: INFO [sshd] Found 172.22.16.1 - 2025-02-09 02:26:32
2025-02-09 02:26:40.773 fail2ban.filter [899]: INFO [sshd] Found 172.22.16.1 - 2025-02-09 02:26:40
2025-02-09 02:28:55.884 fail2ban.filter [899]: INFO [sshd] Found 172.22.16.1 - 2025-02-09 02:28:55
2025-02-09 02:28:55.896 fail2ban.actions [899]: NOTICE [sshd] Ban 172.22.16.1
krish@DESKTOP-T68172U: /etc/fail2ban/jail.d$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 3
  - File list: /var/log/auth.log
- Actions
  - Currently banned: 1
  - Total banned: 1
  - Banned IP list: 172.22.16.1
krish@DESKTOP-T68172U: /etc/fail2ban/jail.d$ sudo fail2ban-client set sshd unbanip 172.22.16.1
1
krish@DESKTOP-T68172U: /etc/fail2ban/jail.d$
  
```

### 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.

**K J Somaiya College of Engineering, Mumbai-400077**

**Department of Computer Engineering**

**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.