Fall2ban Setup

Fail2ban watches your system logs for repeated failed login attempts. When it sees too many failures from the same IP, it automatically bans that IP using your firewall.

It protects services like:

- SSH
- Nginx / Apache
- FTP
- Postfix / Dovecot

It’s basically an automated bouncer for your server.

Configure Fall2ban

1. Install Fall2ban

```
sudo apt update
sudo apt install fail2ban
```

2. Enable SSH jail

```
sudo nano /etc/fail2ban/jail.local
```

Add

```
[sshd]
enabled = true
port = 42
logpath = /var/log/auth.log
maxretry = 5
```

Save and Exit

3. Restart Fall2ban

```
sudo systemctl restart fail2ban
```

4. Check status

```
sudo fail2ban-client status
```

```
sudo fail2ban-client status sshd
```

Revision #2
Created 2026-01-15 18:12:03 UTC by lumxux
Updated 2026-01-15 18:18:38 UTC by lumxux