How to install fail2ban on Ubuntu Server 18.04

by **Jack Wallen** in **Security** on November 21, 2018, 7:13 AM PST

Your Ubuntu Server might be vulnerable to attacks. To prevent unwanted logins, Jack Wallen shows you how to install intrusion detection system, fail2ban.

Image: Jack Wallen

If you're looking to secure your Ubuntu Server, one of the first things you should do is install the fail2ban (https://www.fail2ban.org/) intrusion detection system. What fail2ban does is monitor specific log files (in /var/log) for failed login attempts or automated attacks on your server. When an attempted compromise is discovered from an IP address, fail2ban then blocks the IP address (by adding a new chain to iptables) from gaining entry (or attempting to further attack) the server.

More about cybersecurity

Who has banned Zoom? Google, NASA, and more (https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/)

Upgrade your personal security with a password manager or security key (https://www.techrepublic.com/article/upgrade-your-personal-security-with-a-password-manager-or-security-key/)

How to become a cybersecurity pro: A cheat sheet (https://www.techrepublic.com/article/cheat-sheet-how-to-become-a-cybersecurity-pro/)

Kubernetes security guide (free PDF) (https://www.techrepublic.com/resource-library/downloads/kubernetes-security-guide-free-pdf/)

Believe it or not, fail2ban is so easy to install and use, it should be considered a no-brainer for all Linux servers.

I want to walk you through the process of installing fail2ban on Ubuntu Server 18.04. I'll then show you how to add a jail to monitor for failed SSH login attempts.

SEE: Intrusion detection policy (http://www.techproresearch.com/downloads/intrusion-detection-policy/) (Tech Pro Research)

Installation

Installing fail2ban is simple. Log into your Ubuntu Server and update/upgrade. Do note that should the kernel be upgraded in this process, the server will have to be rebooted (so run this at a time when a reboot is viable). To update and upgrade the server, issue the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

Once the above commands complete, reboot the server (if necessary).

Installing fail2ban can be done with a single command:

```
sudo apt-get install -y fail2ban
```

When that command finishes, fail2ban is ready to go. You'll want to start and enable the service with the commands:

```
sudo systemctl start fail2ban
sudo systemctl enable fail2ban
```

Configuring a jail

Next we're going to configure a jail for SSH login attempts. In the */etc/fail2ban* directory, you'll find the jail.conf file. Do not edit this file. Instead, we'll create a new file, jail.local, which will override any similar settings in jail.conf. Our new jail configuration will monitor */var/log/auth.log*, use the fail2ban sshd filter, set the SSH port to 22, and set the maximum retry to 3. To do this, issue the command:

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

In this new file, paste the following contents:

```
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Save and close that file. Restart fail2ban with the command:

```
sudo systemctl restart fail2ban
```

At this point, if anyone attempts to log into your Ubuntu Server via SSH, and fails three times, they will be prevented from entry, by way of iptables blocking their IP Address.

Testing and unbanning

You can test to make sure the new jail works by failing three attempts at logging into the server, via ssh. After the third failed attempt, the connection will hang. Hit [Ctrl]+[c] to escape and then attempt to SSH back into the server. You should no longer be able to SSH into that server from the IP address you were using.

You can then unban your test IP address with the following command:

```
sudo fail2ban-client set sshd unbanip IP_ADDRESS
```

where IP_ADDRESS is the banned IP Address.

You should now be able to log back into the server with SSH.

Scratching the surface

This barely scratches the surface as to what fail2ban can do. But now you have a good idea on how to use the system. To find out more, make sure to read the man page with the command:

```
man fail2ban
```

That manual page provides a good overview of what fail2ban can do.

Also see

- How to enable SSL and TLS 1.3 on NGINX (https://www.techrepublic.com/article/how-to-enable-ssl-and-tls-1-3-on-nginx/) (TechRepublic)
- Why you should use a password manager (https://www.techrepublic.com/article/why-you-should-use-a-password-manager/) (TechRepublic)

- How to create an encrypted vault with KDE Vaults (https://www.techrepublic.com/article/how-to-create-an-encrypted-vault-with-kde-vaults/) (TechRepublic)
- How to install and run the Maltrail detection system on Ubuntu Server 18.04 (https://www.techrepublic.com/article/how-to-install-and-run-the-maltrail-detection-system-on-ubuntu-server-18-04/) (TechRepublic)
- DerpTrolling game server DoS attacker pleads guilty (https://www.zdnet.com/article/derptroll-game-server-hacker-pleads-guilty/) (ZDNet)
- PGP encryption won't protect your data. But PURBs can (https://www.zdnet.com/article/plugging-leaks-in-pgp-encryption/) (ZDNet)

EDITOR'S PICKS

The Internet of Wild Things: Technology and the battle against biodiversity loss and climate change

Transgender employees in tech: Why this "progressive" industry has more work to do

Python is eating the world: How one developer's side project became the hottest programming language on the planet

How iRobot used data science, cloud, and DevOps to design its next-gen smart home robots

Beyond the PC: Lenovo's ambitious plan for the future of computing

Straight up: How the Kentucky bourbon industry is going high tech

By Jack Wallen

Jack Wallen is an award-winning writer for TechRepublic and Linux.com. He’s an avid promoter of open source and the voice of The Android Expert. For more news about Jack Wallen, visit his website jackwallen.com.

SECURITY OPEN SOURCE SOFTWARE CXO HARDWARE MOBILITY DATA CENTERS

SECURITY ON ZDNET

SHOW COMMENTS

EDITOR'S PICKS

The Internet of Wild Things: Technology and the battle against biodiversity loss and climate change

Transgender employees in tech: Why this "progressive" industry has more work to do

Python is eating the world: How one developer's side project became the hottest programming language on the planet

How iRobot used data science, cloud, and DevOps to design its next-gen smart home robots