Redmine - Defect #18055

Wiki page "HowTo Configure Fail2ban For Redmine" contains incomplete/misleading instructions

2014-10-10 06:08 - Gilles Léonard

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Documentation	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	2.5.0

Description

HowTo_Configure_Fail2ban_For_Redmine
I am running Redmine with the following versions:
Environment:
Redmine version 2.5.1.stable.13174
Ruby version 2.0.0-p481 (2014-05-08) [x86_64-linux]
Rails version 3.2.18
Environment production
Database adapter Mysql2
SCM:
Subversion 1.8.8
Git 1.9.1

Redmine is installed on Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-24-generic x86_64)

In **Configure** section of the howto, in the box following the text that says "add following lines somewhere in your /etc/fail2ban/jail.conf...", the action line (action = iptables-allports[name=redmine]) is a bit heavy handed as it bans all ports, not only http and https.

This is a problem, especially in view of the fact that the rest of the howto fails to inform you that Redmine doesn't prepends logged lines with a time stamp in "production.log" with the result that "when you're banned, you're banned forever ever ever ever... on all ports, including SSH which might be your only possible access to a cloud server. I got locked out ! Fortunately, DigitalOcean VMs have a remote console access that I could use to get out of trouble.

Here are the changes that propose based on my production setup that has successfully tested in the above mentioned environment:

1. No changes should me made to /etc/fail2ban/jail.conf as this file gets overwritten every time fail2ban gets updated. Instead, it is recommended to create or add to a file named /etc/fail2ban/jail.local;
2. The content of the Redmine section in /etc/fail2ban/jail.local should read as follow:

   ```
   [redmine]
   enabled  = true
   filter   = redmine
   port     = http,https
   logpath  = /srv/redmine/log/production.log
   maxretry = 5
   findtime = 600
   bantime = 600
   ```

   This would have the effect of banning the IP address of a client trying to connect on ports HTTP and HTTPS for 10 minutes, after it has seen 5 failed login reties within the last 10 minutes.
3. The howto contains some explanation about findtime and bantime that is not in line with fail2ban's documentation and the result of using the large numbers that are proposed in the howto would not yeld good results.
4. Note that on my production setup the default location of Redmine's production log is in /srv/redmine/production.log
5. A section should be added to explain how to get redmine to add a timestamp in front of each line production.log, and it should read as follow "Add the following to /srv/redmine/config/environment.rb :"

   ```
   class Logger
   def format_message(severity, timestamp, progname, msg)
   "#{timestamp} (#{$$}) #{msg}\n"
   end
   end
   ```

History

#1 - 2014-10-10 07:29 - Toshi MARUYAMA

- Description updated

- Category changed from Wiki to Documents

#2 - 2014-10-10 07:32 - Toshi MARUYAMA

You are free to edit wiki.

#3 - 2015-04-06 16:18 - Go MAEDA

- Category changed from Documents to Documentation

#4 - 2016-04-22 03:06 - Kirill Kirillenko

It`s work!

Very thx!