pfSense - Bug #8864

SSH Guard Sensitivity/Whitelist on 2.4.4

08/31/2018 04:58 PM - Zachary McGibbon

Status:	Resolved	**Start date:**	08/31/2018
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2.4.4_1		
Affected Version:	2.4.4	**Affected Architecture:**	All

Description

I am running 2.4.4.a.20180831.0830 and noticed that my Icinga monitoring started to show issues with SSH. When I looked in the logs I saw the following:

Aug 31 17:04:09 sshguard 39986 Attack from "192.168.0.2" on service 100 with danger 10.

Is this a new feature and if so how do I tune it to allow my Icinga server to check SSH?

Associated revisions

Revision ef4a242c - 10/31/2018 07:19 AM - Renato Botelho

Fix #8864: Let users modify sshguard parameters and whitelist

Revision 087a1f6b - 10/31/2018 07:19 AM - Renato Botelho

Fix #8864: Let users modify sshguard parameters and whitelist

History

#1 - 08/31/2018 04:59 PM - Zachary McGibbon

Sorry I meant to put 2.4.4.a.20180831.0830 in the topic after 'SSH Guard on 2.4.4.a.20180831.0830'

#2 - 08/31/2018 06:56 PM - James Dekker

- Subject changed from SSH Guard on to SSH Guard on 2.4.4.a.20180831.0830

#3 - 09/25/2018 03:11 PM - Nicki Messerschmidt

I just want to chime in on this. I just updated my pfsense to 2.4.4 and very soon after I got notifications from my nagios system. Is there any way to whitelist IPs?

#4 - 09/25/2018 03:42 PM - Jim Pingle

- Subject changed from SSH Guard on 2.4.4.a.20180831.0830 to SSH Guard Sensitivity/Whitelist on 2.4.4

- Target version set to 2.4.4-GS

- Affected Architecture set to All

There isn't a way to set a whitelist currently. But if your monitoring system relies on a probe that is triggering an alert, that sounds more like a problem in the monitoring system.

I sent maybe 100 probes immediately to a 2.4.4 box with that only tested the TCP port and it never triggered sshguard. I then sent a handful that caused a login failure and it tripped after only three attempts.

If your ssh test is actually causing a login failure, try changing it to one that does a simple TCP handshake instead of checking the banner or whatever else it's doing.

#5 - 09/26/2018 04:35 AM - Nicki Messerschmidt

Well... I'm using the default check_ssh plugin of nagios. This plugin connects to the ssh server and checks before authentication if there really is a ssh server responding and what version number is reported. That in intself should not trigger an alarm. The corresponding logfile on the pfsense looks like this:

```
pfsense sshd[xxxxx]: Connection closed by xxx.xxx.xxx.xxx port 45345 [preauth]
```

According to the sshguard website whitelisting is possible using single IPs or using a whitelist file.

At least give the option of restarting/disabling sshguard via the interface. Right now it is a process that interferes with normal operations in a way pfsense did not before and there is no way to control this behaviour.

#6 - 09/26/2018 05:39 AM - Alexander Müller

I found following workaround:

- create whitelist file for sshguard following sshguards file format (https://www.sshguard.net/docs/whitelist/). put the file somewhere in the filesystem
- adjust /etc/inc/system.inc / line 1062:

```
auth.info;authpriv.info  |exec /usr/local/sbin/sshguard -w $fullPathToYourWhitelist
```

- Navigate to Status > System Logs > Manage Logs and save without any changes

Would be really cool to have a proper configuration function in the webConfigurator. My monitoring systems (icinga2) gets blocked during ssh probes

#7 - 09/26/2018 09:15 AM - Michael Reardon

Alexander Müller wrote:

> I found following workaround:
>
> - create whitelist file for sshguard following sshguards file format (https://www.sshguard.net/docs/whitelist/). put the file somewhere in the filesystem
> - adjust /etc/inc/system.inc / line 1062:
> [...]
> - Navigate to Status > System Logs > Manage Logs and save without any changes
>
> Would be really cool to have a proper configuration function in the webConfigurator. My monitoring systems (icinga2) gets blocked during ssh probes

Thanks! This seems to be working well enough for me for the time being.

#8 - 09/28/2018 08:59 AM - Renato Botelho

- Status changed from New to This Sprint

#9 - 09/28/2018 08:59 AM - Renato Botelho

- Assignee set to Renato Botelho

#10 - 09/30/2018 09:05 PM - dean hamstead

Is it possible to simply disable sshguard?

#11 - 10/03/2018 08:47 AM - Steve Beaver

- Target version changed from 2.4.4-GS to 2.4.4_1

#12 - 10/31/2018 07:25 AM - Renato Botelho

- Status changed from This Sprint to Feedback

- % Done changed from 0 to 100

Applied in changeset ef4a242c0df1b69b3348997165afc8555471202c.

#13 - 11/02/2018 03:04 PM - James Dekker

On 2.4.5.a.20181102.0213, works as expected. Address(es) added to the whitelist are not subject to SSH Guard detection.

#14 - 11/02/2018 03:05 PM - James Dekker

- Status changed from Feedback to Resolved