

Enhancement req.: run script on event

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2001-12/0381.html>

From: Steve Snyder (swsnyder@home.com)

Date: 12/30/01

From: Steve Snyder <swsnyder@home.com>

Date: Sun, 30 Dec 2001 16:38:24 GMT

I would like to suggest an enhancement to a future release of OpenSSH: the ability to run an external program/script on a given event.

My rationale: I want to block firewall access (I use iptables on a Linux v2.4.x box) on apparent attempts to crack my system. Or perhaps on any failed authentication, depending on how mean I'm feeling. :-)

I get a lot of logged messages in this format:

```
sshd[26526]: Did not receive identification string from 000.111.222.333.
```

This is different from the "authentication failed" msg I get when my fat finger fail to type in my name/pass correctly. I'm told that this sort of message indicates an attempt to exploit old security flaws on my current version of OpenSSH. What I would like to do is block all IP traffic from the source address causing the message to be generated (in the example above, 000.111.222.333).

Yes, I'm aware that I can periodically scan the system logs to extract the addresses from the messages, but that leaves a gap between scans, allowing further break-in attempts. I want the blocking to occur when the first attempt is detected, not an hour later.

Please, please, please add the ability to run a program/script (passing the IP addr as a parameter) to OpenSSH.

Thank you.

- **Next message:** [Richard E. Silverman: "Re: service ssh-connection method none <?>"](#)
- **Previous message:** [Joonas Saarinen: "Re: SSH doesn't work without a user logged in?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)