

RE: SSH break-in attempts

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2008-09/msg01136.html>

- *From:* "Peter Weaver" <info-vax@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 26 Sep 2008 09:25:59 -0400
-

...
Another thing to note when using this procedure (as I have learned in the last two days) is that the script kiddies will fire off five or ten simultaneous SSH threads. Thus, you will have five or ten log files with no records in them yet. Given that each one gives them three attempts to guess the password, you will get a lot of alarms before the rate limiting kicks in. But when those log files are closed/flushed, boy do they hit a brick wall! :-)

My original goal was to tie the hacker's machine up waiting for the prompt rather than stopping them. I have logged over 63,000 break-in attempts but they only hit a valid username 165 times so I am not worried about one of these idiots getting in. When I first created this I was disappointed to see that the attackers give up so early in the attack. But if you want them to go away faster you can try adding a "SET OUTPUT_RATE=00:00:02" to the LOGIN.COM and see if that helps.

...
Now I just wish for a similar one for FTP.
...

I very seldom see FTP attacks. POP attacks were more common when I had the POP port opened on the firewall, but I had to close that because of the huge security whole JF keeps mentioning but HP keeps ignoring. I use HG_FTP because it plays with Windows user better than HP's FTP so I don't know if a similar technique would work with HP's FTP.

Peter Weaver
www.weaverconsulting.ca www.openvmsvirtualization.com
www.vaxvirtualization.com www.alphavirtualization.com
Winner of the 2007 OpenVMS.org Readers' Choice Award for System Management/Performance