

Re: SSH scans vs connection ratelimiting

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2006-08/msg00041.html>

- *From:* Joerg Pulz <Joerg.Pulz@xxxxxxxxxxxx>
 - *Date:* Sat, 19 Aug 2006 23:30:50 +0200 (CEST)
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Sat, 19 Aug 2006, Pieter de Boer wrote:

Gang,

For months now, we're all seeing repeated bruteforce attempts on SSH. I've configured my pf install to ratelimit TCP connections to port 22 and to automatically add IP-addresses that connect too fast to a table that's filtered:

```
table <lamers> { }
```

```
block quick from <lamers> to any
```

```
pass in quick on $ext_if inet proto tcp from any to ($ext_if) port 22 modulate state  
(source-track rule max-src-nodes 8 max-src-conn 8 max-src-conn-rate 3/60 overload  
<lamers> flush global)
```

This works as expected, IP-addresses are added to the 'lamers'-table every once in a while.

However, there apparently are SSH bruteforcers that simply use one connection to perform a brute-force attack:

```
Aug 18 00:00:01 aberdeen sshd[87989]: Invalid user serwis from 83.19.113.122  
Aug 18 00:00:03 aberdeen sshd[88010]: Invalid user serwis from 83.19.113.122  
Aug 18 00:00:05 aberdeen sshd[88012]: Invalid user serwis from 83.19.113.122  
Aug 18 00:00:10 aberdeen sshd[88014]: Invalid user serwis from 83.19.113.122  
Aug 18 00:00:13 aberdeen sshd[88019]: Invalid user serwis from 83.19.113.122  
Aug 18 00:00:14 aberdeen sshd[88021]: Invalid user serwis from 83.19.113.122
```

My theory was/is that this particular scanner simply multiplexes multiple authentication attempts over a single connection. I 'used the source luke' of OpenSSH to find support for this theory, but found the source a bit too wealthy for my brain to find such support.

Re: SSH scans vs connection ratelimiting

So, my question is: Does anyone know how this particular attack works and if there's a way to stop this? If my theory is sound and OpenSSH does not have provisions to limit the authentication requests per TCP session, I'd find that an inadequacy in OpenSSH, but I'm probably missing something here :)

Isn't it the "MaxAuthTries" option for sshd which provides such functionality?
Please look for "MaxAuthTries" in the sshd_config(5) manpage for details.

regards
Joerg

--- The beginning is the most important part of the work.

-Plato

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.5 (FreeBSD)

iD8DBQFE54MNSPOsGF+KA+MRAh0GAJ45v4C9+xJ5vy+4BPItXwBxpKzzIwCePWa8

o/XSdoB2tFdMXQv1Yo1rwFU=

=dHjL

-----END PGP SIGNATURE-----

frebsd-security@xxxxxxxxxxx mailing list