

RE: Security warning with sshd

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-08/0034.html>

From: Stephen Major (*smajor_at_gmail.com*)

Date: 08/22/05

To: <remko@FreeBSD.org>, "'Pat Maddox'" <pergesu@gmail.com>

Date: Sun, 21 Aug 2005 23:03:28 -0700

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

Hash: SHA512

This is due to a mis-configured firewall. If you are using IPFW there are many tutorials out there that tell you to do the wrong thing. And almost all of them contradict each other. Below is a basic script that only allows in and out SSH sessions and blocks all the garbage. Of course you must add any other services you need. The key here is that you allow connections from any to any established. Then on all outgoing tcp connections be sure to use the setup keep-state flags. The keep-state flag puts the rule into the dynamic rules table. Then the allow connections from any to any established allows already established connections to flow without going through the ruleset again. When I did this the error messages you are now experiencing went away.

```
#!/bin/sh
```

```
#IPFW script by Salvia
```

```
ipfwcmd="/sbin/ipfw"
```

```
flags="-q"
```

```
#int
```

```
oif="rl0"
```

```
logall="log"
```

```
### Flush the rules
```

```
    $ipfwcmd $flags -f flush
```

```
### Allow loopback and deny loopback spoofs
```

```
    $ipfwcmd $flags add 00100 allow all from any to any via lo0
```

```
    $ipfwcmd $flags add 00110 deny $logall ip from any to 127.0.0.0/8  
via $oif
```

```
    $ipfwcmd $flags add 00120 deny $logall ip from 127.0.0.0/8 to any  
via $oif
```

FreeBSD–Security: RE: Security warning with sshd

Stop PNAs from connecting

\$ipfwcmd \$flags add 00130 deny \$logall ip from 192.168.0.0/16 to any
via \$oif

\$ipfwcmd \$flags add 00140 deny \$logall ip from 172.16.0.0/12 to any
via \$oif

\$ipfwcmd \$flags add 00150 deny \$logall ip from 10.0.0.0/8 to any via
\$oif

\$ipfwcmd \$flags add 00160 deny \$logall ip from any to 192.168.0.0/16
via \$oif

\$ipfwcmd \$flags add 00170 deny \$logall ip from any to 172.16.0.0/12
via \$oif

\$ipfwcmd \$flags add 00180 deny \$logall ip from any to 10.0.0.0/8 via
\$oif

Deny XMAS tree, Null scan, SYN Flood, Stealth FIN, and forced packer
routing

\$ipfwcmd \$flags add 00200 deny log tcp from any to any in tcpflags
fin,psh,urg recv \$oif

\$ipfwcmd \$flags add 00210 deny log tcp from any to any in tcpflags
!fin,!syn,!rst,!psh,!ack,!urg recv \$oif

\$ipfwcmd \$flags add 00220 deny log tcp from any to any in tcpflags
syn,fin recv \$oif

\$ipfwcmd \$flags add 00230 deny log tcp from any to any in tcpflags
fin,rst recv \$oif

\$ipfwcmd \$flags add 00240 deny log ip from any to any in ipoptions
ssrr,lsrr,rr,ts recv \$oif

Deny late, redirect, and spoofing attacks

\$ipfwcmd \$flags add 00250 deny \$logall all from any to any frag

\$ipfwcmd \$flags add 00270 deny \$logall icmp from any to any icmptype

5

\$ipfwcmd \$flags add 00280 deny \$logall ip from me to me in via \$oif

inbound section

check the traffic's state

\$ipfwcmd \$flags add 00500 check-state

\$ipfwcmd \$flags add 00501 allow tcp from any to any established

Allow in ssh

\$ipfwcmd \$flags add 00620 allow tcp from any to me 22 in via \$oif
setup keep-state

Deny & Log all incoming that fall through to here
#####

\$ipfwcmd \$flags add 01000 deny \$logall logamount 500 all from any to
any in via \$oif

FreeBSD–Security: RE: Security warning with sshd

```
#####  
#####
```

```
##### outbound section #####
```

```
### Allow out ssh
```

```
    $ipfwcmd $flags add 02150 allow tcp from me 22 to any out via $oif  
setup keep–state
```

```
##### Everything Else #####
```

```
### deny and log everything else that is trying to get out.
```

```
    $ipfwcmd $flags add 03000 deny $logall logamount 500 all from any to  
any out via $oif
```

```
##### deny and log all packets that fell through to see what they  
are #####
```

```
    $ipfwcmd $flags add 04000 deny $logall logamount 500 all from any to  
any
```

– -----Original Message-----

From: owner–freebsd–security@freebsd.org
[mailto:owner–freebsd–security@freebsd.org] On Behalf Of Remko Lodder
Sent: Sunday, August 21, 2005 2:36 AM
To: Pat Maddox
Cc: freebsd–security@freebsd.org; FreeBSD Questions
Subject: Re: Security warning with sshd

Pat Maddox wrote:

```
> In my recent security email, I got the following errors:  
> cantona.dnswatchdog.com login failures:  
> Aug 20 02:37:19 cantona sshd[9444]: fatal: Write failed: Operation not  
permitted  
> Aug 20 04:30:42 cantona sshd[16142]: fatal: Write failed: Operation  
> not permitted  
> Aug 20 21:21:51 cantona sshd[45716]: fatal: Write failed: Operation  
> not permitted  
>  
> So three questions: What is it? Should I be worried? How can I fix it?  
>  
> Thanks,  
> Pat
```

A couple of messages that i read when searching through google appear to indicate that it might rely on your firewall, bad packets that are not in state anymore and such and then gets blocked by your firewall.

Could you provide some more details of events happening around the same time of the messages you posted here? Perhaps something

RE: Security warning with sshd

FreeBSD-Security: RE: Security warning with sshd

else precedes the message which gives more information on what might have happened...

Url with some information:

<http://lists.freebsd.org/pipermail/freebsd-pf/2005-August/001337.html>
(and related messages)

Cheers,
Remko

--

Kind regards,

Remko Lodder ** remko@elvandar.org
FreeBSD ** remko@FreeBSD.org
Reporter DSINET ** remko@DSINet.org

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"

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

Version: PGP Desktop 9.0.1 (Build 2185)

iQEVAwUBQwlqtKKXvLS903/FAQqVxQf+K3+E/dEYVrN2znbBnSyNRCOspyhrsG1t
2pJnEkyldzc8wKE0dIRv1GZA1OFvyOwsQ8Bt2V5Hz/I3w0liXN5y2JRzl5VB2mPF
wCtT01Y9gFyvuf16yzlv2YkS8sr1AcChAlttOYq/b8xUTSOynyLVaVe90un9CQE/
EmiKkafaJOOlqMle1GyluOKlnsHRfVdENFAqXjm9Q5yEhedjUduHQF4RHp8v+COz
i8AFpTyO3m/M/tgRYo5fhBoPzFkm8P70TMJhvDnF26xRzrcWCQtJqAhVzzGsgSZ
Eo/z1W2xOsLIZL/DuaS4SIXZtR7Yk0DYxzw1qn31JuI2kM55kKnsCQ==
=40+R

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

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"