

Re: Wanting To Try FreeBSD: Security Question.

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.bsd.freebsd.misc/2006-04/msg00086.html>

- *From:* Giorgos Keramidas <keramida@xxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 04 Apr 2006 14:58:28 +0300
-

Metal Head <MetalHead@xxxxxxxxxxxxxxxxxx> writes:

I've used Linux for a couple of years, the Linux that i've used have a point and click firewall. Suse, Mandriva Fedora.

How hard is it to secure FreeBSD for a desktop computer? I've been reading the handbook – the firewalls PF, IPFW & IPF look complicated.

That depends on what the first impression is, I guess. I find pf.conf many times more readable than an endless chain of iptables rule files (which is usually the case in Linux).

The relatively minimal pf.conf file for the firewall I run on my laptop, for example, is all in one file, one place, and includes only a short set of (somewhat strict) packet-filtering rules:

```
% $ cat /etc/pf.conf
% # $RCS: giorgos/firewall/pf/gothmog.pf.conf,v 1.2 2005/06/07 16:57:52 giorgos Exp $
%
% set block-policy return
% set require-order yes
% set skip on lo0
%
% scrub in all
%
% block in log all
% block out log all
%
% pass in proto icmp all
% pass out proto icmp all
% pass out proto { tcp, udp } all keep state
% pass in proto { tcp, udp } from any to any port = 22 keep state
```

Now, compare this to the byzantine chains of chains of chains of rules usually found on Linux installations, and you'll see that PF is not that hard to configure after all :)

Re: Wanting To Try FreeBSD: Security Question.

At least, not harder than your average Linux firewall of the week/month/whatever.

From what I've read: you can enable IPFW in the kernel and add `firewall_enable="YES"` to `rc.conf`. & `firewall_type="client"` for a standalone box. Will that be enough to secure a desktop?

No. A firewall is not the end of all your security needs. You will also need policies in place, and a security-aware mindset. This is not something provided by Linux or BSD though. You are the one who will study and get informed about security, instead.

With Fedora I have SELinux enabled. I may be wrong, from what I can tell: (MAC) or 'mandatory access control' does the same thing as SELinux. How difficult is it to set up (MAC) ?

Is there anything like this in FreeBSD?

Yes, MAC is similar to SELinux, in a way. It's also different in other ways.

Are you sure you need MAC, in the first place? Are you prepared to spend the time it takes to configure it properly? To what end?

=====

ExecShield can also randomize the location where programs are loaded into your computer's virtual memory. A hacker can exploit the knowledge of where a program is loaded into your computer's memory. Linux loads programs at fairly predictable locations, but ExecShield mostly fixes the problem.

Nice trick, but I don't really think this feature is available on FreeBSD.

Also, what about FreeBSD Jails... ? Do you have to jail all daemons? I'm reading up on jails now, this also looks complicated.

Yes and no. The answer depends on what you are trying to accomplish and how much time you are prepared to spend to secure this particular system.

No, jails are not complicated. You just have to let some of the information sink through. Also make sure you ask specific questions about the aspects of jails that seem confusing to you. Knowledgeable people are always available on this newsgroup and on the

Re: Wanting To Try FreeBSD: Security Question.

freebsd-questions mailing list to help you get started with jails.

Basically, I want to make sure I'm able to secure the system before I install.

'security' is not an easy thing to define. I say give it a try and ask about the specific things you want to 'secure' as you find them.

The BSDs are pretty well 'secured' from common bugs and mis-features of other systems, even in a clean, default installation. You can always tweak and configure and manage those parts of the general system security that you need to change later on.

Good luck with your installation, if you do decide that giving FreeBSD a try is worth your time.

It was definitely worth mine :)

– Giorgos

.