Quick Guide to Securing a Lamp Server

By *felosi*
Created *03/08/2006 - 3:32am*
Submitted by felosi on Thursday 3rd of August 2006 03:32:37 AM Filed under Howtos [1]

In the last few years on the Internet the price of dedicated servers have went down and more people are beginning to use them for their sites, game servers, or small hosting companies. With this comes as I was talking about in my last article inexperienced admins. Lots of people I spoke too are too intimated by the linux shell and try to administer their server completely from the control panel.
This short guide will show you a few copy and paste walkthroughs you can use to help secure your server, these should work with any control panel, the mod security update script however is only for apache2. Using these tools and using basic security procedures will help you keep your server secure and free of hackers, spammers, and other annoyances.

Using linux as a personal desktop helps a lot as well as it gets you used to using the command line. The other extremely valuable tool is google. I would probably be nowhere without google. You can look stuff up as you go and find about any answer to any question you may have, Plus there is lots of walkthroughs just like this one I am just putting all the basic ones together.

OK this is not a complete guide but those who are less experienced should be able to follow these walkthroughs and make their server more secure then it was before.
First thing, install apf, bfd, and dos deflate. Complete walkthrough **HERE** [2]
Note: Dos deflate will not work with debian unless you disable ipv6.

Next install modsecurity using the simple guide from eth0.us, guide can be found **HERE** [3]

After you install mod security make a directory in /etc called modsecurity. Use my update script found **HERE** [4] (apache2 only)
This will get all the latest rules from gotroot.com when you have them at the bottom of the mod security configuration in httpd.conf put
Include /etc/modsecurity/apache2/rulename.conf
I suggest using them all besides rules.conf as it gives lots of false positives.

Now if you have shell users or are running redhat, fedora, or debian you most likely need to update your kernel. Now this isn't as hard as you would think, with this copy and paste guide I made that is all you have to do is copy and paste, same as these other tutorials.
The guide can be found **HERE** [5]. I will be making one for debian soon but you just use any basic debian kernel how to and patch the kernel the same way as you do in this one.

Once you have modsecurity installed keep an eye on the audit log to make sure it is not giving any false positives or

blocking legitimate web apps. With the ruleset and rules you have included it should not unless someone is using some oddball web app.
None of these will make your server totally secure, it takes basic security practices such as using strong passwords, not using the same password for everything, and keeping up with all the latest exploitrs and hacking methods.

If you ever get hacked don't go ranting about how you are gonna prosecute so and so, go find out how they done it, how they got in, and what you can do to prevent it again. You will most likely never track down the hackers and the FBI most likely will not care so secure your system and make sure it does not happen again. As I have explained before defacers can actually be helpful to admins. That's about it, good luck and stay on your toes.

Howtos

Links:
[1] http://www.tuxmachines.org/taxonomy/term/58
[2] http://www.evolution-security.com/modules.php?name=News&file=article&sid=167
[3] http://www.eth0.us/mod_security
[4] http://www.evolution-security.com/modules.php?name=News&file=article&sid=248
[5] http://www.evolution-security.com/modules.php?name=News&file=article&sid=245