Subject: Re: support for grsecurity-patched kernels?
Posted by eliast on Mon, 28 May 2007 11:33:47 GMT
View Forum Message <> Reply to Message

Simply, I use all the features that grsecurity offers, and I also think that building secure linux servers without the PAX protection is closely impossible.

I use trusted path execution, kernel process hiding, and all features of chroot jail restriction, also /proc restrictions, dmesg restrictions and executables resource limits. Also when using chroot restrictions I always setup the executables with chpax, so denying processes to load shared segments and other stuff if they do not need to. (For example preventing apache to load modules I do not want to...). Also using socket restrictions, for example for running apache, and client sockets are denied for apache, it makes it impossible to use for example in php to cnnect to remote smtp servers and using spam activity.

I belive, all PAX features, like Adress Space Randomization and sanitizing all freed memory makes it even harder to compromise the server. Especially when you have dosens of shell accounts. (For this I'm using chrooted shell accounts, and I'm planning to move to openvz, (XEN needs a modular kernel and some other things that it is not yet useable for me...) but I really miss grsec features and pax.)

Also I could patch openvz patched 2.6.20 kernel with grsec, and successfully using most features, since the patch needed only semantic correction (the line numbers did not match), but in case of PAX the memory protection stuff needs to be revised by a developer, since when I check it, the kernel would not compile, or if it is, it is segfaulting.