Subject: *BUG REPORTED* support for grsecurity-patched kernels?
Posted by eliast on Sat, 26 May 2007 19:22:11 GMT
View Forum Message <> Reply to Message

Hy all. Is there a possibility of official support for grsecurity (http://grsecurity.net) patched kerenls in openvz's patch? I'm usually manually modifying the patches to fit grsec based kernels, but sometimes I have kernel panics on the test system (eg.: when I turn on pax features). I'm pretty sure, that it is because I do semantic correction only on the patches to make it work with grsecurity enabled kernel.

Subject: Re: support for grsecurity-patched kernels?
Posted by Vasily Tarasov on Sat, 26 May 2007 21:20:30 GMT
View Forum Message <> Reply to Message

Hello,

I suppose we will not work on it. Please, use forum's search (there was a thread about grsecurity patches) to find out why.

Thanks,
Vasily

Subject: Re: support for grsecurity-patched kernels?
Posted by eliast on Sun, 27 May 2007 12:27:00 GMT
View Forum Message <> Reply to Message

It's written in Russian, I don't understand it.

Subject: Re: support for grsecurity-patched kernels?
Posted by Vasily Tarasov on Mon, 28 May 2007 05:58:13 GMT
View Forum Message <> Reply to Message

Well, shortly, we have no reasons at the moment to support grsecurity. Can you tell us, please, why do you need grsecurity on OpenVZ? What exact features of grsecurity do you use?

Thanks,
Vasily

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.

Subject: Re: support for grsecurity-patched kernels?
Posted by Vasily Tarasov on Mon, 28 May 2007 11:40:26 GMT
View Forum Message <> Reply to Message

Thank you for the answer! I think you should post an enhancament bug in our bugzill1a with enhancement severity. Then sometime we'll probably introduce support of grsecurity....

As concerns PAX: In RH kernels there is ExecShield feature, that does approximately the same that PAX does. So, OpenVZ kernels, that are based on RH kernels, also have this feature.

HTH,
Vasily.

Subject: Re: support for grsecurity-patched kernels?
Posted by eliast on Tue, 29 May 2007 09:01:34 GMT
View Forum Message <> Reply to Message

okay, I'll do that. PAX is a more mature and offering more protection than ExecShield I belive, and I do not use RH kernels, since I use debian.

Hope, grsecurity support will be implemented in a timely manner, since there are quite lot of forum topics on grsecurity's forum, on the same topic, and there are already various successfull implementations for older kernels.

But these unrelieable hacks cannot be applied in real environments. I would be happy with an official support. It will greatly improve openvz's security on many ways, I'm extremely sure. (Lot of ppl waiting this development...)