Subject: OpenVZ web panel & security
Posted by shamu on Wed, 15 Dec 2010 09:20:00 GMT
View Forum Message <> Reply to Message

Hello everybody,

well, this is my first posting in this forum! I don't know if I'm right here, but I didn't find a special discussion forum which deals with OpenVZ web panel so far.

Sadly I didn't find a description how security issues are handled in the depth. So I'd like to ask my questions here in this forum. Maybe anyone is able to answer them.

So what's my config and what do I want to do/know?

Currently I'm running two servers with OpenVZ kernel (hw node), one in the internet and one in my dmz. On both I'm running debian lenny, but I tested squeeze successfully too.

On both OpenVZ hw nodes I'm running OpenVZ web panel's hw-daemon only. In my (more secure) intranet I'm running another server with the panel itself including sqlite database. All this works fine for me. I access the panel server from other computers in the intranet only and activated ssl for browser access.

Now my questions are:

1. Actually I don't need to use the root account on my OpenVZ servers (hw nodes) because of using sudo ... But, if I want to use web panel I need to give root a password. I think, web panel will store the root password for the OpenVZ servers (hw nodes) in its sqlite database. Right? But how is the access to this Database secured, i.e. is it possible for an intruder on the panel server to read the root passwords of my OpenVZ-Server form the sqlite database?

2. How is the connection between the web panel application in my intranet and my OpenVZ servers (hw nodes) in dmz and internet secured? Is it encrypted and how? Which type of protocol is used: http (hopefully not), https or an undocumented protocol? O.k., I'm able to change the port for hw-daemon from 7767 to another one, use a long cryptic key and set a short timeout. But, is the whole session encrypted or just the first packages until the session is established? Keep in m ind I'm sending my root password over this connection!

3. Is there a way to improve the security issues mentioned in 1.+2.? Let's say tunneling 2. over ssh or something else? And, how can I secure the access to the sqlite db?

Any hints, descriptions and experiences are very welcome!

Greetinx

shamu