Subject: Re: OpenVZ Web Panel & Sicherheit
Posted by shamu on Fri, 17 Dec 2010 12:08:03 GMT
View Forum Message <> Reply to Message

Hallo Forum,

hier noch ein kurzes Feedback, wie ich die Sache (für mich) gelöst habe:

Bei Libvirt gibt es verschiedene Möglichkeiten, die Übertragung zu verschlüsseln. Allerdings bin ich doch wieder zum OpenVZ Web Panel zurückgekehrt, weil dabei wesentlich weniger Pakete installieren werden müssen und mir (persönlich) die Darstellung besser gefällt, was natürlich Geschmackssache ist.

Auch habe ich ein paar Sachen getestet, die Thorsten vorgeschlagen hat. Also dann:

0. Feedback vom Entwickler: Benutzt für die Verbindung zwischen Panel und hw-daemon nur sicher Netze (LAN, Intranet, etc.). Daher sind keine Security Features für die Kommunikation zwischen panel und hw-daemon implementiert.

1. Der hw-daemon agiert nur dann richtig, wenn er als root läuft - leider Unter einem anderen Benutzer gestartet führt der Access vom Panel aus zu keinen Ergebnissen bzw. zu Fehlermeldungen.

2. Habe ich auf dem hw node sowie auf dem Panel Server einen dummy-User mit stark eingeschränkten Rechten angelegt, der sich ausschließlich per ssh key authentication am hw node anmelden kann.

3. Wird die Verbindung zwischen Panel und hw node nun über ssh getunnelt, d.h. es sind keine zusätzlichen offenen Ports erforderlich amd hw node. Den hw-daemon lasse ich nur noch auf Port 127.0.0.1 lauschen. Die (lokale) Umleitung besorgt netcat.

4. Die ssh-Session wird nur on demand aufgebaut, d.h. vom panel-server aus via xinetd.

5. Erlaube ich dem dummy-User auf dem hw-node mit netcat nur noch den Zugriff auf den hw-daemon.

6. Habe ich den timeout des hw-daemon relativ kurz angesetzt.

Das war's. Ich denke, wer sich mit ssh, (x)inetd und nc ein wenig auskennt, kommt mit der oben skizzierten Lösung zurecht.

Greetinx

shamu