

---

Subject: Audit issues

Posted by [dagr](#) on Sat, 15 Sep 2007 14:04:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Lets say i put all users into vpss to secure HN.

How can i check for nonlegacy processes/open ports now ? The legacy processes inside vpss and in HN look identical .

```
[openvz@ws4-ca vps_dev]$ sudo lsof -ni :22
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
sshd 4309 root 3u IPv4 11706901 TCP *:ssh (LISTEN)
sshd 4875 root 3u IPv4 2540319 TCP *:ssh (LISTEN)
sshd 8888 root 3u IPv4 52596488 TCP *:ssh (LISTEN)
sshd 13142 root 3u IPv4 50829731 TCP *:ssh (LISTEN)
sshd 18998 root 3u IPv4 23048176 TCP *:ssh (LISTEN)
sshd 22560 root 3u IPv4 8446568 TCP *:ssh (LISTEN)
sshd 23212 root 3u IPv4 52624431 TCP *:ssh (LISTEN)
sshd 23231 root 3u IPv4 52624458 TCP 192.168.10.30:ssh->192.168.100
.113:4092 (ESTABLISHED)
sshd 23236 dagr 3u IPv4 52624458 TCP 192.168.10.30:ssh->192.168.100
.113:4092 (ESTABLISHED)
sshd 25431 root 3u IPv4 8451518 TCP *:ssh (LISTEN)
sshd 27287 root 3u IPv4 8453252 TCP *:ssh (LISTEN)
sshd 27417 root 3u IPv4 11736494 TCP *:ssh (LISTEN)
```

```
[openvz@ws4-ca vps_dev]$ netstat -ltn | grep 22
```

```
tcp 0 0.0.0.0:22 0.0.0.0:* LIST
EN
```

EN

Also all ports are shown like open on 0.0.0.0 , though they actually restricted to ips of vps.

So - the question - how can i distinguish vps and HN processes / ports / etc (looking from HN) ?

---