Subject: Re: VPS can not be entered
Posted by leobrown on Wed, 06 Jan 2010 21:48:51 GMT
View Forum Message <> Reply to Message

Right....

Nothing for that time. Just the VPS restart messages when I restarted it...

And then... grepped ALL host logs for that VPS. Nothing.

And THEN, grepped all VPS logs, and got this:

Jan 5 11:32:25 my-hostname xinetd[3780]: Started working: 0 available services
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: Found user 'avahi' (UID 70) and group 'avahi' (GID 70).
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: Successfully dropped root privileges.
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: avahi-daemon 0.6.16 starting up.
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: WARNING: No NSS support for mDNS detected, consider installing nss-mdns!
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: dbus_bus_get(): Failed to connect to socket /var/run/dbus/system_bus_socket: No such file or directory
Jan 5 11:32:28 my-hostname avahi-daemon[3957]: WARNING: Failed to contact D-Bus daemon.
Jan 5 11:32:28 my-hostname init: no more processes left in this runlevel

Avahi was new to me, but I see it is a service discovery layer. This is clearly malicious and possibly the result of a rootkit. What do you think?!?

If so, manual exploit attempt, or automated? I am not seeing high numbers of reports on this approach.

After restart, I am not seeing any unusual open ports, just 22 and 80.

I am presuming you believe like me this is non-OpenVZ, so happy to close this up, but if you have any useful feedback I'd obviously be keen to hear it.

Best regards
Leo