

Re: [SLE] Security, ssh/vpn into a network

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2006-07/msg01959.html>

- *From:* rouvas <rouvas@xxxxxxxxxx>
 - *Date:* Thu, 27 Jul 2006 16:44:17 +0300
-

HI,

What do you think of port-knocking?

Sorry if this has already been suggested, I didn't quite follow the discussion from the start.

–Stathis

On Thursday 27 July 2006 17:46, Cody Nelson wrote:

You are completely miss-understanding me and are calling me an idiot. How many times do I have to say: "I am forwarding ssh/22 and http/80 from my firewall to my server. Everything else is tunneled through ssh. (yes that means encrypted)"

Want me to cut and paste every time I have said that? Here is one from my previous message:

"My server is running several services, the only ones accesable outside are http and ssh. ssh is how I connect into my network remotely, and I use things like VNC, Squid, etc through that."

Again, ports 5900 is not open to the outside, neither is any of the other ports/services. Only http/ssh is open from outside my network. I will secure up Apache as much as I can. But that will be a later topic, but then most likely not here.

Yes, I know every bit is encrypted, but it is possible to brute force / get lucky and get into my box. I don't think I'll get hacked because of an exploit from ssh. Or that someone will sniff my traffic. I want to add another level.

There is nothing enlightening in the post other than the fact you keep calling me an idiot indirectly. I know that I can use putty to ssh in, and create tunnels so if I connect to localhost I can get inside my network. I do this for a lot of things, such as my squid, vnc, etc. This is nothing new.

Re: [SLE] Security, ssh/vpn into a network

Right now if someone got lucky and got into ssh they would automatically have access to my server. If I move it to vmware or find some way to chroot it, no ports have been opened, I only put in a layer.

Or if I add WebVPN so you would have a ssl into my network. And I would have port 22 closed from the outside.

I am surprised there have been no one to come forward who is a security Nazi and could help me. Instead I get attacks from people miss understanding what I have stated.

So let me state again. I am forwarding port 80 and 22 through my firewall. I ssh to my server and VNC, proxy and all other things are not being forwarded on the firewall but through the ssh tunnel.

Am I still unclear on this? I appreciate the effort used to reply to me, but you are grossly misunderstanding what I am stating/asking. I have stated it many times.

I do not want to open more ports. I want to put in another level of protection. (vmware, chroot, webvpn/closing prots)

On 7/27/06, John Andersen <jsa@xxxxxxxxxxxxxxxx> wrote:

On Wednesday 26 July 2006 13:16, Cody Nelson wrote:

Currently I ssh to my network, I VNC and everything I need to through that SSH tunnel. I don't like this because I am forwarding ports from outside to this box.

That's what I don't understand.

You are "forwarding these ports" thru the ssh tunnel. Don't you see that that is the MOST SECURE setup you could possibly have? Anything else you do will be less secure than what you already are doing.

Are you SURE you understand what it means to tunnel other traffic thru ssh?

You DO KNOW, don't you, that every bit of ssh traffic is encrypted? Even login?

You do know that all the tunneled traffic (forwarded ports) is also encrypted and hidden from the world, and CAN'T be accessed from any where else?

Re: [SLE] Security, ssh/vpn into a network

Re: [SLE] Security, ssh/vpn into a network

You DO know that you can have VNC on the server to listen only to 127.0.0.1 and these then can ONLY be accessed from an ssh connection into the server?

Any other "layer" you add will be worse than what you already have. You will open MORE ports with LESS secure software.

I think you need to to read up on the capabilities of SSH.

The mere fact that you can forward a port from your home workstation to your server thru the ssh tunnel does NOT make that a security risk. Those ports are not available to anyone else.

--

John Andersen

--

Check the headers for your unsubscribe address
For additional commands send e-mail to suse-linux-e-help@xxxxxxxx
Also check the archives at <http://lists.suse.com>
Please read the FAQs: suse-linux-e-faq@xxxxxxxx