

Re: Newbie questions about security

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2007-02/msg04965.html>

- *From:* Andrew Sackville-West <andrew@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 28 Feb 2007 08:06:51 -0800
-

On Wed, Feb 28, 2007 at 05:38:27AM -0800, Jordi wrote:

Hello,

I just managed to configure my server and router and ips yesterday and now I have questions about security. I did a scan of ports and saw the only open are the ones I opened. I also set my router firewall to "standard".

1) Must I CLOSE the ports that I don't use? Or just let them not forwarded? (they appeared as STEALTH in the ports scan)

in linux, the only ports that are a danger are the ones that have a process listening on them. For example, if you only have and http server running (apache) then the only port that is open is 80 and that is the only port that is a concern. The other ports are effectively "closed" because there is no process listening to them...

2) Should I use an extra firewall in my server plus the one that my router has ? What about Firestarter? Any other good GPL firewall?

shorewall. check the excellent website for help.

3) Should I adjust the firewall in my router to something custom, not standard, and what do you recommend me?

a good hardware firewall is a great tool. And its easy to use -- only forward those ports that you want, and the rest will be blocked. done.

4) I fear intruders and specially ddos. I saw a IDS called Snort that many people use. What do you think? Any other good GPL IDS?

Re: Newie questions about security

You should fear intruders— install tiger and learn about it so that if you do get compromised, you'll know. Also learn to read your logs. there are log filtering programs that can help with this. Not sure why someone would want to go to the trouble of ddos'ing you those theres always a possibility. What is your concern there? DDOS would be a problem if you had some mission critical online app that you needed to have up. BUt if you're just running a little home server and you happen to get randomly hit by some attack, ust take it offline for a bit. but I don't really know.

5) Now that I have the server running, y suppose I must stop using gksudo and use only sudo. Not?

doesn't matter.

A

Attachment: signature.asc

Description: Digital signature