

Firewall-Wizards: Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-07/0163.html>

From: InHisGrip (*servie_platon_at_yahoo.com*)

Date: 07/22/04

To: Chuck Swiger <chuck@codefab.com>

Date: Wed, 21 Jul 2004 20:36:21 -0700 (PDT)

Hi Chuck,

Thanks for the tips. Sorry, I forgot to mention about the distro which is Fedora Core 2.

Incidentally, you mentioned about nfslock, since I don't use nfs or network file system in my small home network would it be advisable for me to comment this out from xinetd, disable this service or just leave it as it is?

Same goes with port 111, sunrpc port and port 773, notify service, shall I leave these alone too?

The only services I have enabled are web service and mail service plus kernel compile and development options. I hope what I have selected has nothing to do with the ports that are under question here?

Sorry for the incorectness about my question on shielding DMZ host on my linksys as it is known to everyone that putting it on a DMZ zone isolates it from the local LAN segement which sort of protect your other PC's from getting compromised. The question should have been, based on the listening port above, would my other PC's get compromised or be subjected to attack?

And finally, you mentioned this:

I think that means you've got a stateful NAT

- > *firewall going. It's certainly*
- > *useful and functional, but offers no protection for*
- > *the DMZ host. Use*
- > *specific port forwarding rules instead of the DMZ if*

Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

Firewall-Wizards: Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

- > *you want to improve your*
- > *security, and/or lockdown unneeded services on your*
- > *Linux box.*

On this assumption, I have configured my linksys router to do port forwarding which works fine. If I remove the apache from the DMZ port and include in my home LAN would other people from the Internet be able to access my home site?

Well, I just thought of putting the web server in a DMZ host and port to protect my other PC's. Since this is a bastion host which will be accessible for everyone, the only safeguard I was thinking of is tcp wrappers, along side with the firewall rules of the linux box, plus limited permissions on certain directories.

What would you suggest? I am just an intermediate linux user and would love some feedback from you or anyone else who are advanced users to linux gurus.

Thanks in advance and hope to hear from you guys soon.

Regards,
Servie

- Chuck Swiger <chuck@codefab.com> wrote:
- > *InHisGrip wrote:*
 - > *[...]*
 - >
 - > *To answer the subject, rumor has it that port 37628*
 - > *is used by the nfslock*
 - > *service on some common Linux platforms (ie, Redhat).*
 - > *It's probably that or*
 - > *some other RPC-based service, considering that port*
 - > *111 also open.*
 - >
 - > *Although it is possible something bad is using that*
 - > *port, I'd start by*
 - > *checking which services you have enabled. It would*
 - > *have helped if you had*
 - > *mentioned which version and distribution of Linux*
 - > *you are running, BTW.*
 - >
 - >> *Oh, by the way, just wanted to make sure because I*
 - >> *have placed the web server in a DMZ port and zone*
 - >> *from my linksys router and I think but not sure*
 - > *that*
 - >> *I am being shielded and protected atleast?*
 - >

Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

Firewall-Wizards: Re: [fw-wiz] Port 37628....Is it just another port or out of the extra ordinary???

- > *Probably not, actually: a machine in the DMZ does*
- > *not have the firewall rules*
- > *protecting it, the router just forwards traffic to*
- > *the DMZ host as-is.*
- >
- > *There are plenty of tools which will do a port scan*
- > *of your network from*
- > *outside: try using one.*
- >
- > *Likewise, I have enabled advanced firewall*
- > *protection on my*
- > *linksys router.*
- >
- > *I think that means you've got a stateful NAT*
- > *firewall going. It's certainly*
- > *useful and functional, but offers no protection for*
- > *the DMZ host. Use*
- > *specific port forwarding rules instead of the DMZ if*
- > *you want to improve your*
- > *security, and/or lockdown unneeded services on your*
- > *Linux box.*
- >
- > --
- > -Chuck
- >

Do you Yahoo!?

Vote for the stars of Yahoo!'s next ad campaign!

<http://advison.webevents.yahoo.com/yahoo/votelifeengine/>

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>