

Re: securing a network with nfs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2001-08/0049.html>

From: Mogens Valentin (monz@danbbs.dk)

Date: 08/10/01

Message-ID: <3B739DEF.7B594CED@danbbs.dk>
Date: Fri, 10 Aug 2001 10:40:15 +0200
From: Mogens Valentin <monz@danbbs.dk>
To: focus-linux@securityfocus.org
Subject: Re: securing a network with nfs

David Johnson wrote:

> As my small isp expands, we need to move to a centralized file storage
> point (easier backups; also, if the mail server goes down, I want to be
> able to toss on another box quick without having to grab the files from
> the old server or backups of it; this can also lead to multiple
> mailservers receiving at different priorities). The obvious solution is
> NFS. But to run an NFS box out open on the net, not in a dmz, is rather
> dangerous IMO. And setting up one firewall to hide all boxes behind is
> hard to do (especially with ftp), and it's a choke point.

It's not that hard to explicitly portforward ftp. And since you do not seem to have lots of interfaces in each server, which would require separate rules, you don't need 80+ rules, thus choking shouldn't be a problem, at least that's my experience with Linux ipchains firewalling.

As for NFS, yes, it's generally considered a major security hole, but it's possible to prevent the outside world from having any clue to NFS services running on the inside. Setup NFS to only be accessible from certain known internal IP#'s. It's shown in the man pages, IMMSMR.

If I was using Linux in a setup like yours, I'd implement an deny-all, allow-specific based ipchains/ipfilter firewall on all computers, and deny (not reject) any traffic to ident/auth, sun-rpc and the like. I'd use masquerading to hide my internal RFC-private addresses.

> So, I had my idea of how to set up this kind of network, where I have a
> centralized file point accessible by only my servers (web, mail, ftp,
> db, etc.), but where these servers (except the NFS box) are public as
> well. Bit of ascii art:

```
>
> -----
> || NFS box
> private || private
> -----||-----
> /-----/
```

SecurityFocus Linux: Re: securing a network with nfs

```

> ||private |
> |||
>
-----/-----/-----/-----/-----
> |||
> -----
> ||MAIL ||OTHER ||WEB
> |||||
> |||||
> -----
> |||||
> ||public |public | |public
>
> NOTE: perhaps the dotted line should be between the public/private
> interfaces to show that the outer boxes bridge the gap between
> public/private networks.

```

Which is exactly what's achieved with a masquerading firewall/router setup.

Remember to setup egress filtering and the like in /proc (if Linux). Implementing egress filtering in a Cisco router is a one line statement.

```

> Obviously, if one of the outside facing boxes gets cracked, that's it
> for the nfs box. But that's a risk that always has to be taken at some
> point. What I'm trying to do is guard against my fileserver files going
> across a public net.
>
> Further precautions would need to be taken, like disabling packet
> forwarding for the outside facing boxes. No packets from the outside
> would be allowed to enter the internal net.
>
> SO, how does this sound? How penetrable would this be??

```

Generally speaking, Un*x boxes setup while observing sound security measures can be quite safe. While working for an online business, we had 12 linux servers hosted in the usa, no firewalls, but most everything updated and secured, using ssh, hostallow/deny and measures against spoofed IP#'s and the like setup in the /proc filesystem. We passed a security test by Vigilante, only thing they didn't like was a too publicly accessible snmp, which we had little control over, since the hosting business had done that setup.

--
 Regards,
 Mr Dev - Mogens Valentin
<http://www.mrdev.com> - mrdev@danbbs.dk
 OpenSource Security - Networking - Programming

• *Previous message:* [Daniel Santana: "RE: Apache hack attempts"](#)

SecurityFocus Linux: Re: securing a network with nfs

- ***In reply to:*** David Johnson: "securing a network with nfs"
- ***Next in thread:*** Derek D. Martin: "Re: securing a network with nfs"
- ***Next in thread:*** Dave Vehrs: "FW: securing a network with nfs"
- ***Reply:*** Derek D. Martin: "Re: securing a network with nfs"
- ***Reply:*** Derek D. Martin: "Re: securing a network with nfs"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]