

Re: SSH or Telnet?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-03/8714.html>

From: N. J. Cash (ncash@pei.eastlink.ca)

Date: 03/30/02

From: "N. J. Cash" <ncash@pei.eastlink.ca>

To: "Fernando Gleiser" <fgleiser@cactus.fi.uba.ar>, "Jesper Wallin" <z313zt@phucking.kicks-ass.or>

Date: Sat, 30 Mar 2002 11:36:20 -0400

I would also recomend that you restrict access to ssh using /etc/hosts.allow if you would like some added security to just who all can ssh to your box.

Also, if you're going with ssh *which you should* I would only enable protocol 2 and restrict user access to ssh using /etc/ssh/sshd_config as well.

AllowUsers user1 user2 user3 etc...

DenyUsers root nobody etc...

At least if you're really parioned about sshd those steps will let you sleep a little better at night! :)

N. J. Cash

ncash@pei.eastlink.ca

----- Original Message -----

From: Fernando Gleiser

To: Jesper Wallin

Cc: security@FreeBSD.ORG

Sent: Thursday, March 28, 2002 7:42 PM

Subject: Re: SSH or Telnet?

On Thu, 28 Mar 2002, Jesper Wallin wrote:

> *Hey!*

>

>

> *I've heard and seen alot of security problems related to SSH (OpenSSH) and*

> *many of my friends have been playing with alot of Oday exploits for it..*

> *Right now I'm running the latest port version of it on a non-standard port*

> *and hope to be secured with it.. I don't accualy see the reason to not use*

> *Telnet.. All I know tells me it's old and recommend me running OpenSSH*

> *instead..*

Telnet also had some remote root vulnerabilities.

Every program has bugs. You need to keep them up to date and apply all the security fixes.

FreeBSD-Security: Re: SSH or Telnet?

Also, having sshd running in a non standard port doesn't buy you much. There are scanners which try to verify which service is which port and they will find out it's ssh even if it is listening in port 31337. =0)

>
> *What is the best solution? Ofcourse peoples are able to attack me with*
> *brute-force attacks and it's not encrypted.. well, all the peoples who've*
> *shell/ssh access are trusted and I think they know what they do..*

The people may be trusted, but are you sure you can trust the networks they are logging in from?

Besides sniffing, ssh protects you against other threats:

1. ssh has some protection against IP spoofing.
2. ssh has stronger authentication methods.
3. ssh protects you against session hijacking.
4. ssh lets you authenticate the server to the client.
5. ssh lets you tunnel an insecure protocol (POP, IMAP) through an encrypted connection

You can use an SSL enabled telnet or IPsec for the first four, but I find ssh easier to set up if all you need is remote login/shell/file transfer.

Fer

>
>
> *Anyone have any idea/suggestion?*
>
> *//Jesper aka Z3l3zT*
>
>
>
> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> *with "unsubscribe freebsd-security" in the body of the message*
>

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message