

Re: Secured Linux box for Windows access

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-02/0202.html>

From: N407ER (n407er_at_myrealbox.com)

Date: 02/12/04

Date: Wed, 11 Feb 2004 20:34:41 -0500

To: jbloggs000@yahoo.com

Matthew White wrote:

- > *Firstly I'd like to thank those people who responded to my questions*
- > *(both on and off the list – particularly Richard's :)*
- >
- > *Briefly the responses I received centred around the following:*
- > ** Remote admin via OpenSSH*
- > ** Client access via WinSCP, sftp etc...*
- >
- > *Having done some research into them since, they do look good, however I do have*
- > *one other requirement I didn't mention that may change things.*
- >
- > *Because some of the client machines are similar to public kiosks, and*
- > *some of the data on the server is important to some users I'd really like to*
- > *avoid the necessity for users to drag and drop / copy / ftp to the local*
- > *machine. On the client side, I can automatically remove temp files, harden up*
- > *Word (as much as is possible of course) and generally look after the security*
- > *of the client box but all of that is moot if the user forgets to copy the file*
- > *back, or to delete it after copying it back. Therefore if possible I'd like to*
- > *have the windows system access it directly via a UNC share (hence the question*
- > *about samba and OpenVPN) where it saves it back to the server each time. Is*
- > *this possible? What do I need to do to achieve this objective?*
- >
- >
- >
- > *One last thing. Since the suggestions came in about which version of Linux to*
- > *use, I've downloaded (much to my network admins' chagrin) and setup a*
- > *few different versions already. I admit that I'm fine with the concepts but am*
- > *struggling with the Linux side and its configuration. Where would you guys*
- > *suggest I look for information on setting up a Linux server – preferably*
- > *starting with an overview then moving to more detail (eg "First you need to*
- > *secure your network connection, passwords, updates, etc. To harden the*
- > *password use MD5 --> To do that go to /etc/..."). Are there any good websites*
- > *or newsgroups you'd suggest?*

So first, it is possible to use a VPN to secure your shares as they go across the Internet. The two major VPN implementations for Linux are FreeS/WAN (recommended for 2.4 kernels) and the kernel implementation

SecurityFocus BASICS: Re: Secured Linux box for Windows access

itself, available in 2.6 by default and as a patch for 2.4. I've got little experience between the two, but my reading seems to imply that the 2.6 code is far superior (I've heard many complaints about the code quality in FreeS/WAN). That said, FreeS/WAN is clearly production–usable, and the documentation is far more complete than that for the new kernel implementation.

Your options are probably to either set up a VPN client on each of the client Windows machines, or to set up a VPN tunnel between the router the Windows clients are behind and your server. The latter is more efficient and easier to set up, but only if you have a router capable of this (VPN–capable hardware routers are available for as little as USD\$300).

Once you have this set up, on the server you will see a different interface representing the IPSec tunnel. If you set Samba to only listen on that interface, only people over the tunnel will be able to access it. You are essentially done (you probably want to secure the Samba users, still, so that not just anybody behind the VPN gateway on the other end can access the share); the Samba traffic going over the Internet will (assuming you have chosen ESP in your IPSec tunnel) now be encrypted so nobody can tamper with it or read it.

As for securing Linux, there are many good Linux howtos in general at tldp.org; linuxsecurity.org and similar websites, and many vendors have distribution–specific guides to security. There are also some good scripts to help secure an install, like BastilleLinux, which changes settings to make it more secure by default. There are also many books on the subject, and it's really far too complex a topic to discuss here.

Good luck.

Free trial: Astaro Security Linux — firewall with Spam/Virus Protection

Protect your network with the comprehensive security solution that integrates six applications for ease of use and lower TCO.

Firewall – Virus protection – Spam protection – URL blocking – VPN
– Wireless security.

Download 30–day evaluation at:

<http://www.astaro.com/php/contact/securityfocus.php>
