

Re: Securing Fedora Core 4

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2005-09/0012.html>

From: Syn Ack (*thin.hack_at_gmail.com*)

Date: 09/22/05

Date: Thu, 22 Sep 2005 11:07:05 +0200

To: AragonX <aragonx@dcsnow.com>

Hello AragonX,

I will add these steps to the list:

- Only allow ssh V.2
- Deny root ssh logins
- Allow only ssh login with pub/priv keys and secure your priv key on a encrypted filesystem on a USB key
- Turn off all unneeded services
- Remove all unneeded binaries
- If you need to access the server from outside your privatenet use ipsec, openvpn or something related.
- If data integrity is of interest use a journalized filesystem for both metadata AND data (by default ext3 put only metadata in the journal), LVM and RAID5 and pay attention to SMART

It's what I think at the moment. Some of these steps seems really obvious but peoples tend to forget obvious things sometime.

Take care,

Dodoche

On 9/21/05, AragonX <aragonx@dcsnow.com> wrote:

> *I am trying develop a method to secure my servers. I'll list the steps I
> am going to take. Can you please review and make any additional
> suggestions. Thank you.*

>

> *Install & configure Tripwire <http://sourceforge.net/projects/tripwire/>*

> *Install & configure Snort <http://www.snort.org/>*

> *Install & configure Bastille <http://www.bastille-linux.org/>*

> *Install & configure LIDS <http://www.lids.org/>*

> *Install & configure modsecurity <http://www.modsecurity.org/>*

> *Install & configure chkrootkit <http://www.chkrootkit.org/>*

> *install dansguardian <http://www.dansguardian.org>*

> *install squid <http://www.squid-cache.org/>*

> *Install & configure DCC <http://www.dcc-servers.net>*

> *Install & configure Pyzor <http://pyzor.sourceforge.net>*

> *Install & configure Razor <http://razor.sourceforge.net>*

> *install & configure Clamav <http://www.clamav.net>*

SecurityFocus Linux: Re: Securing Fedora Core 4

- > *Install & configure MailScanner <http://www.sng.ecs.soton.ac.uk/mailscanner/>*
- > *Install & configure Ntop <http://www.ntop.org/>*
- > *Install & configure Spamassassin <http://spamassassin.apache.org/>*
- > *install root access email command*
- > *create a seprate /tmp partition and mount noexec, nosuid*
- >
- > *Configure Apache*
- > *configure for php safe mode*
- > *configure /internal web directory w/ access from private network only*
- > *configure /external web directory w/ password authentication*
- >
- > *Configure SSH*
- > *respond on alternate port*
- > *only allow me to logon*
- >
- > *Configure Fireall:*
- > *only allow access to ssh from my domains*
- >
- >
- >
- >