

Re: Block IP

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2006-08/msg04224.html>

- *From:* James Wilkinson <fedora@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 31 Aug 2006 13:43:12 +0100
-

Kaushal Shriyan wrote:

w command showed me suspicious IP.

w shows who's got past your defences and actually logged in. So "suspicious" is worrying.

Is there any chance that it could be legitimate --- say, someone you know SSHing in from an unusual IP address?

Can you run
host 10.10.10.10
(where 10.10.10.10 is the IP address) to see if there's a name associated with it, and
whois 10.10.10.10
to see who "owns" that IP block?

Unless you can verify that whoever it was had permission to be on your computer, you should worry, try to find out how they got in (are any of your passwords guessable? How many usernames are allowed to SSH in? Are you running any other server programs?) *re-install your system from scratch*, and do your best to close the holes.

If you want any further explanation, please ask this list.

Thanks,

James.

E-mail: james@ | ... more holes in Internet Explorer than
aprilcottage.co.uk | Blackburn, Lancashire...
| --- <http://theinquirer.net/?article=17235>

fedora-list mailing list
fedora-list@xxxxxxxxxx
To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>