

# Re: Warning: Remote Host Identification

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-10/msg00246.html>

- *From:* "ajay raghuraj" <[ajay.raghuraj@xxxxxxxxxx](mailto:ajay.raghuraj@xxxxxxxxxx)>
- *Date:* Tue, 31 Oct 2006 06:49:57 -0800

delete the host abc entries from known\_hostsfile.

Regards,  
Ajay

On 10/31/06, A.Fadyushin@xxxxxxxxxxxxxx <A.Fadyushin@xxxxxxxxxxxxxx> wrote:

> -----Original Message-----

> From: redhat-list-bounces@xxxxxxxxxxxxxx [<mailto:redhat-list-bounces@xxxxxxxxxxxxxx>] On Behalf Of Budi Febrianto

> Sent: Tuesday, October 31, 2006 8:01 AM

> To: General Red Hat Linux discussion list

> Subject: WTA: Warning: Remote Host Identification

>  
> Dear All,

> I have 3 linux server, where 1 server (gateway server) the ssh port open

> for the public, while the other two is closed, only smtp port is open

> for public.

> This week I manage the servers from mobile with my notebook installed

> opensuse 10.

> First I login to gateway server, then after that I login to the other

> servers.

> But one day, after I successfully logged to the gateway server, and

> when

> trying to login to another server, I have this warning.

> >>>>>

> @@@@

> @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

> @@@@

## Re: Warning: Remote Host Identification

- > IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
- > Someone could be eavesdropping on you right now (man-in-the-middle attack)!
- > It is also possible that the RSA host key has just been changed.
- > The fingerprint for the RSA key sent by the remote host is
- > b4:10:fb:f9:3d:04:b8:86:44:f7:2e:ba:b7:41:82:7c.
- > Please contact your system administrator.
- > Add correct host key in /root/.ssh/known\_hosts to get rid of this message.
- > Offending key in /root/.ssh/known\_hosts:6
- > RSA host key for abc.xyz.com has changed and you have requested strict
- > checking.
- > Host key verification failed.
- > >>>>>
- >
- > This mean that my gateway server is under attack, or my others server
- > under attack?
- > While remote, the connection is bad, I had several drops connections.
- > Can this cause of the problem?
- >
- > The others server are smtp server, an only open smtp port for public.
- >
- > Best Regards

This means that the SSH server key which is kept on the server in one of the SSH configuration files has changed since the last time you accessed that server via SSH – i.e. somebody reinstalled SSH on the server or regenerated its key. It is hard to imagine the hacker who will change the server key on the hacked computer because this will lead to faster detection of attack.

In the other case it may be possible that you are actually connected not to the server you expected to connect to. It means that the host name abc.xyz.com is no longer point to the same computer as at the last time you accessed it. This may be due to changes in DNS or routing configuration. Generally, you should not enter your password to login into the server until you are absolutely sure that the changes which lead to connecting to the other computer instead of expected one are legitimate and not caused by hacked DNS or routing tables. If you are redirected to another computer as a result of a hacker's attack and enter the SSH password it could be retained by the hacker and later used by him to login into your server.

Alexey B. Fadyushin  
Brainbench MVP for Linux  
<http://www.brainbench.com>

--

redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

Re: Warning: Remote Host Identification

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>

<https://www.redhat.com/mailman/listinfo/redhat-list>