Table Of Contents

Table Of Contents 1
Suggested readings: 2

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Debian / Ubuntu Linux Public key Blacklisted (see ssh-vulnkey(1)) Error and Solution

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. When ever I try to login to my remote Debian Linux server called in013.example.com, I get the following error message in /var/log/auth.log file:

```
Jul 1 17:04:36 in013 sshd[14447]: Public key 48:de:55:22:xx:yy:zz:yy:xx:yy:zz:yy::88:e8:87:47
blacklisted (see ssh-vulnkey(1))
Jul 1 17:04:36 in013 sshd[14447]: Public key 48:de:55:22:xx:yy:zz:yy:xx:yy:zz:yy::88:e8:87:47 blacklisted
(see ssh-vulnkey(1))
```

I'm using Ubuntu Linux as desktop operating system. How do I fix this error?

A. This is well known security flow in Debian / Ubuntu Linux OpenSSL package. First, you need to update your Ubuntu Linux desktop software, by typing following commands:

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

This will update openssl, openssh server and client packages for you. This will also regenerate COMPROMISED keys stored /etc/ssh/ directory. However, this will update your personal COMPROMISED keys stored at $HOME/.ssh. Type the following command to list all COMPROMISED keys:

```
$ sudo ssh-vulnkey -a
```

ssh-vulnkey checks a key against a blacklist of compromised keys. You must remove all COMPROMISED keys and regenerate them again using ssh-keygen command.

```
$ cd ~/.ssh
$ rm id_*
$ ssh-keygen -t rsa [2]
```

OR

```
ssh-keygen -t dsa [3]
```

Upload new id_rsa.pub or id_dsa.pub file to remote host and overwrite existing authorized_keys2 file, enter:

```
$ scp ~/.ssh/id_rsa.pub user@in013.example.com:.ssh/authorized_keys2
```

If you have multiple keys, then copy ~/.ssh/id_rsa.pub to $HOME and manually delete / update authorized_keys2 file:

```
$ scp ~/.ssh/id_rsa.pub user@in013.example.com:~/
```

Find out line number, enter:

```
$ grep 'your-desktop-name' ~/.ssh/authorized_keys2
```

Use vi to open COMPROMISED key, enter (replace N with actual line number):

```
$ vi +N ~/.ssh/authorized_keys2
```

Delete file pressing dd once. Save and close the file. Append new public key, enter:

```
$ cat ~/id_rsa.pub >> ~/.ssh/authorized_keys2
```

Suggested readings:

Suggested readings:

- Impact of the Debian OpenSSL Vulnerability On other Linux Distribution [4]
- Ubuntu / Debian Linux Regenerate OpenSSH Host Keys [5]
- man pages ssh-keygen, ssh-vulnkey,scp, and ssh

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-publickey-blacklisted-see-ssh-vulnkey1-error/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/debian-ubuntu/**
[2] ssh-keygen -t rsa: **http://www.cyberciti.biz/tips/ssh-public-key-based-authentication-how-to.html**
[3] ssh-keygen -t dsa: **http://www.cyberciti.biz/tips/linux-multiple-ssh-key-based-authentication.html**
[4] Impact of the Debian OpenSSL Vulnerability On other Linux Distribution : **http://www.cyberciti.biz/tips/impact-of-debian-openssl-vulnerability.html**
[5] Ubuntu / Debian Linux Regenerate OpenSSH Host Keys: **http://www.cyberciti.biz/faq/howto-regenerate-openssh-host-keys/**