Table Of Contents

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

Debian Linux Stop SSH User Hacking / Cracking Attacks with DenyHosts Software

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

I've noticed lots of failed login attempt for my Debian Linux VPS root server account. How do I stop automated bot based SSH attacks on my server?

You can use DenyHosts - a Python based script that analyzes the sshd server log messages to determine what hosts are attempting to hack into your system. It is an utility to help sys admins thwart ssh crackers. It also determines what user accounts are being targeted. It keeps track of the frequency of attempts from each host. It will automatically blocks ssh attacks by adding entries to /etc/hosts.deny. DenyHosts will also inform Linux administrators about offending hosts, attacked users and suspicious logins.

Step # 1: Make Sure Python is installed

First, make sure python is installed under Debian / Ubuntu Linux:

```
# dpkg --list | grep python2
```

Find out version (DenyHosts requires 2.3 or above version)

```
$ python -V
```

Output:

```
Python 2.5.1
```

Step # 2: Download DenyHosts

Visit official project home page to grab latest source code or packages [2]. Use apt-get command under Debian / Ubuntu Linux, enter

```
$ sudo apt-get install denyhosts
```

DenyHosts configuration - /etc/denyhosts.conf

1. The default configuration file is **/etc/denyhosts.conf**.
2. You also need to create / update a whitelist in **/etc/hosts.allow**. For example, if you have static IP assigned by ISP, enter in this file. You can add all the important hosts that you never want blocked.

Step # 1: Setup a whitelist

Open /etc/hosts.allow:

```
# vi /etc/hosts.allow
```

Allow sshd from 202.54.1.2 i.e. you never want to block yourself

```
sshd: 202.54.1.2
```

Save and close the file. Verify and examines your tcp wrapper configuration file and reports all potential and real problems:

```
# tcpdchk -v
```

Step # 1: Configure DenyHosts

Open default configuration file - /etc/denyhosts.conf, enter:

```
# vi /etc/denyhosts.conf
```

Setup your email ID so you would receive emails regarding newly restricted hosts and suspicious logins, set this address to match your email address.

```
ADMIN_EMAIL = vivek@nixcraft.com
```

Save and close the file. Here is my own sample configuration file for Debian Linux 4.0 server (config file is documented very well, just open and read it):

```
############## THESE SETTINGS ARE REQUIRED #############
SECURE_LOG = /var/log/auth.log
HOSTS_DENY = /etc/hosts.deny
PURGE_DENY =
BLOCK_SERVICE  = sshd
DENY_THRESHOLD_INVALID = 5
DENY_THRESHOLD_VALID = 10
DENY_THRESHOLD_ROOT = 1
DENY_THRESHOLD_RESTRICTED = 1
WORK_DIR = /var/lib/denyhosts
SUSPICIOUS_LOGIN_REPORT_ALLOWED_HOSTS=YES
HOSTNAME_LOOKUP=YES
LOCK_FILE = /var/run/denyhosts.pid
############## THESE SETTINGS ARE OPTIONAL #############
ADMIN_EMAIL = vivek@nixcraft.com
SMTP_HOST = localhost
SMTP_PORT = 25
SMTP_FROM = DenyHosts <webmaster@cyberciti.biz>
SMTP_SUBJECT = DenyHosts Report
AGE_RESET_VALID=5d
AGE_RESET_ROOT=25d
AGE_RESET_RESTRICTED=25d
AGE_RESET_INVALID=10d
########## THESE SETTINGS ARE SPECIFIC TO DAEMON MODE  ###########
DAEMON_LOG = /var/log/denyhosts
DAEMON_SLEEP = 30s
DAEMON_PURGE = 1h
```

Restart the daemon:

```
# /etc/init.d/denyhosts restart
```

See Also:

- How can I remove an IP address that DenyHosts blocked? [3]

Further readings:

- Red Hat / Centos Install Denyhosts To Block SSH Attacks / Hacking [4]
- Top 20 OpenSSH Server Best Security Practices [5]
- denyhosts project [2]

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/bash-shell/**
[2] grab latest source code or packages: **http://denyhosts.sourceforge.net/**
[3] How can I remove an IP address that DenyHosts blocked?: **http://www.cyberciti.biz/faq/linux-unix-delete-remove-ip-address-that-denyhosts-blocked/**
[4] Red Hat / Centos Install Denyhosts To Block SSH Attacks / Hacking: **http://www.cyberciti.biz/faq/rhel-linux-block-ssh-dictionary-brute-force-attacks/**
[5] Top 20 OpenSSH Server Best Security Practices: **http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html**
