Table Of Contents

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

Red Hat / Centos Install Denyhosts To Block SSH Attacks / Hacking

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

How do I block and stop attacks on ssh server under CentOS Linux or Red Hat Enterprise Linux server 5.x?

You can easily thwart SSH server attacks including dictionary based attacks and brute force attacks using denyhosts software.


[2]

It is a Python based script that analyzes the sshd server log messages to determine what hosts are attempting to hack into your system.

Step #1: Enable Rpmforge Repo

First, enable rpoforge repo. For 32bit CentOS / RHEL Linux enter:

```
# rpm -Uhv http://apt.sw.be/packages/rpmforge-release/rpmforge-release-0.3.6-
1.el5.rf.i386.rpm
```

For 64 bit CentOS / RHEL 5 Linux, enter:

```
# rpm -Uhv http://apt.sw.be/packages/rpmforge-release/rpmforge-release-0.3.6-
1.el5.rf.x86_64.rpm
```

Step #2: Install Denyhosts

Type the following command:

```
# yum -y install denyhosts
```

Step #3: Configure Denyhosts

The default configuration file is located at /etc/denyhosts/denyhosts.cfg.

Allow Your Computer To Access sshd

You need to setup a whitelist so that you never want to block yourself using this script. Edit /etc/hosts.allow, enter:

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

Allow sshd from 202.54.1.2 and 203.51.2.3:

```
sshd: 202.54.1.2 203.51.2.3
```

Save and close the file.

Setup Alert Email ID

Edit /etc/denyhosts/denyhosts.cfg, enter:

```
# vi /etc/denyhosts/denyhosts.cfg
```

If you would like to receive emails regarding newly restricted hosts and suspicious logins, set this address to match your email address. If you do not want to receive these reports # leave this field blank (or run with the --noemail option). Multiple email addresses can be delimited by a comma, eg:
ADMIN_EMAIL = vivek@nixcraft.co.in, vivek@nixcraft.net.in

```
ADMIN_EMAIL = vivek@dsl.nixcraft.net.in
```

Save and close the file. Here is my own sample configuration file for RHEL / CentOS 5.x server / vps box - config file is documented very well, just open and read it:

```
       ############ THESE SETTINGS ARE REQUIRED ############
SECURE_LOG = /var/log/secure
HOSTS_DENY = /etc/hosts.deny
PURGE_DENY = 7d
BLOCK_SERVICE  = sshd
DENY_THRESHOLD_INVALID = 5
DENY_THRESHOLD_VALID = 10
DENY_THRESHOLD_ROOT = 1
DENY_THRESHOLD_RESTRICTED = 1
WORK_DIR = /usr/share/denyhosts/data
SUSPICIOUS_LOGIN_REPORT_ALLOWED_HOSTS=YES
HOSTNAME_LOOKUP=YES
LOCK_FILE = /var/lock/subsys/denyhosts
       ############ THESE SETTINGS ARE OPTIONAL ############
ADMIN_EMAIL = vivek@dsl.nixcraft.net.in
SMTP_HOST = localhost
SMTP_PORT = 25
SMTP_FROM = DenyHosts <nobody@localhost>
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
   #########   THESE SETTINGS ARE SPECIFIC TO     ##########
   #########        DAEMON SYNCHRONIZATION         ##########
```

Turn On Denyhosts

Type the following commands:

```
# chkconfig denyhosts on
# service denyhosts start
```

How do I view Denyhosts Log?

Type the command:

```
# tail -f /var/log/denyhosts
# tail -f /var/log/secure
```

See Also:

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

Recommend Readings:

1. Debian Linux Stop SSH User Hacking / Cracking Attacks with DenyHosts Software [4]
2. Top 20 OpenSSH Server Best Security Practices [5]
3. Denyhosts project [6]

you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

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

URL to article: **http://www.cyberciti.biz/faq/rhel-linux-block-ssh-dictionary-brute-force-attacks/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/centos/**
[2] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[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] Debian Linux Stop SSH User Hacking / Cracking Attacks with DenyHosts Software: **http://www.cyberciti.biz/faq/block-ssh-attacks-with-denyhosts/**
[5] Top 20 OpenSSH Server Best Security Practices: **http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html**
[6] Denyhosts project: **http://denyhosts.sourceforge.net/**
