[轉]Centos使用DenyHosts阻止SSH暴力攻击

作者是 Administrator
週二, 22 十月 2013 15:15 - 最近更新 週二, 22 十月 2013 15:45

轉自: http://www.centoscn.com/CentosSecurity/CentosSafe/2013/0724/473.html

錯誤參考:http://free.yes81.net/yes81/view-11072.html

現在的互聯網非常不安全，很多人沒事就拿一些掃描機掃描ssh端口，然後試圖連接ssh端口進行暴力破解（窮舉掃描），所以建議vps主機的空間,盡量設置複雜的s sh登錄密碼，雖然在前段時間曾經介紹過Linux VPS禁止某個IP訪問使用hosts.deny禁止某些IP訪問，但是功能方面欠缺，如：不能自動屏蔽，那麼有什麼更好的辦法嗎，就可以使用denyhosts這款軟件了，它會分析/var/log/secure（redhat，Fedora Core）等日誌文件，當發現同一IP在進行多次SSH密碼嘗試時就會記錄IP到/etc/hosts.deny文件，從而達到自動屏蔽該IP的目的。

DenyHosts官方網站為：http://denyhosts.sourceforge.net/

1、下載DenyHosts 並解壓

wget http://www.centoscn.com/tool /DenyHosts-2.6.tar.gz

tar zxvf DenyHosts-2.6.tar.gz

1 / 8

cd DenyHosts-2.6

2、□□、□□□□□

python setup.py install

□□□□□□/usr/share/denyhosts/□□□,□□□□□□□□□□□□□□

cd /usr/share/denyhosts/

cp denyhosts.cfg-dist denyhosts.cfg

cp daemon-control-dist daemon-control

centos vi denyhosts.cfg daemon-control

denyhosts

chown root daemon-control

chmod 700 daemon-control

./daemon-control start

DenyHosts

cd /etc/init.d

ln -s /usr/share/denyhosts/daemon-control denyhosts

chkconfig --add denyhosts

chkconfig --level 2345 denyhosts on

/etc/rc.local

echo "/usr/share/denyhosts/daemon-control start" >> /etc/rc.local

DenyHosts denyhosts.cfg

SECURE_LOG = /var/log/secure

#sshd 。

HOSTS_DENY = /etc/hosts.deny

#

PURGE_DENY = 5m

#

BLOCK_SERVICE = sshd

#

BLOCK_SERVICE = ALL

DENY_THRESHOLD_INVALID = 1

#

DENY_THRESHOLD_VALID = 10

#

DENY_THRESHOLD_ROOT = 5

root

HOSTNAME_LOOKUP=NO

#

DAEMON_LOG = /var/log/denyhosts

README VPS VPSer
VPS。

#service denyhost start

starting DenyHosts: /usr/bin/env python /usr/bin/denyhosts.py --daemon
--config=/usr/share/denyhosts/denyhosts.cfg

python: can't open file '/usr/bin/denyhosts.py': [Errno 2] No such file or directory

PYTHON_BIN = "/usr/bin/env python" -> PYTHON_BIN = "/usr/local/bin/python2.7"
(python)