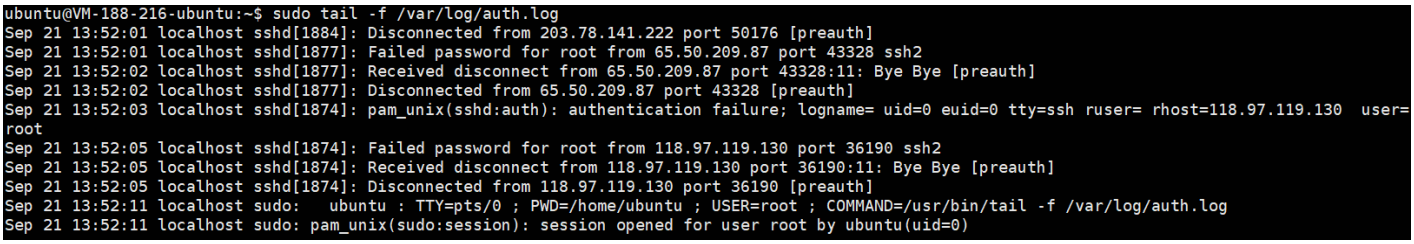
ubuntu SSH

> “ IP SSH IP

```
sudo tail -f /var/log/auth.log
```



root

```
sudo grep "Failed password for root" /var/log/auth.log | awk '{print $11}' | sort | uniq -c |
sort -nr | more
   3579 111.198.159.85
   1185 111.229.204.86
    457 121.89.198.64
    109 112.85.236.98
    106 36.94.17.242
     99 45.141.84.126
     89 129.28.163.90
     83 111.231.87.10
     77 64.225.53.232
     77 122.155.202.93
     72 64.225.126.22
     72 113.57.170.50
     72 103.117.120.47
     71 45.232.244.5
     71 138.197.149.97
     70 134.175.154.93
     67 159.65.100.44
     67 120.131.13.186
     67 104.248.205.67
     64 152.32.222.192
     61 150.136.40.83
```

```
     59 188.170.13.225
     59 178.128.14.102
```

`root`

```
sudo grep "Failed password for invalid user" /var/log/auth.log | awk '{print $13}' | sort |
uniq -c | sort -nr | more
   1812 111.198.159.85
    645 111.229.204.86
    275 45.141.84.126
     85 36.94.17.242
     85 112.85.236.98
     56 111.231.87.10
     55 172.103.3.143
     52 211.253.26.117
     51 129.28.163.90
     50 134.175.154.93
```

1. `SSH` `root`

`/etc/ssh/sshd_config`

```
sudo vim /etc/ssh/sshd_config

Port 1234 #
PermitRootLogin no

sudo service sshd restart
```

2. `RSA`

`SSH`

```
#
ssh-keygen -t rsa

#
ssh-copy-id -i .ssh/id_rsa.pub server
```

```
#      .shh/id_rsa.pub          .ssh
# $ scp .shh/id_rsa.pub server:~/.ssh

#
cd ./.ssh/

mv id_rsa.pub authorized_keys

chmod 400 authorized_keys

vim /etc/ssh/sshd_config

RSAAuthentication yes #RSA
PubkeyAuthentication yes #
AuthorizedKeysFile .ssh/authorized_keys #
PasswordAuthentication no #
PermitEmptyPasswords no #
UsePAM no #  PAM



#
sudo service sshd restart
```

3. `denyhosts`

`denyhosts` `Python` `sshd` `IP` `/etc/hosts.deny` `IP` `denyhosts`

`ubuntu 16.04` `SSH` `RESET_ON_SUCCESS = yes #` `ip5` `iptables` `iptables` `IP` `RESET_ON_SUCCESS` `denyhosts` `Shell`

`ubuntu 16.04` ,

```
#
touch ~/install.sh

#       ,                        SSH
#     denyhosts                  iptables
echo "sudo apt-get install denyhosts" >> ~/install.sh

#
echo "sudo sed -i 's/^#RESET_ON_SUCCESS/RESET_ON_SUCCESS/g'  /etc/denyhosts.conf" >>
```

```
~/install.sh

#
echo "sudo service denyhosts restart" >> ~/install.sh

#
sudo bash ~/install.sh
```

`/etc/denyhosts.conf`

```
sudo vim /etc/denyhosts.conf

SECURE_LOG = /var/log/auth.log #ssh
HOSTS_DENY = /etc/hosts.deny #
PURGE_DENY = #
BLOCK_SERVICE = sshd #
DENY_THRESHOLD_INVALID = 5 #
DENY_THRESHOLD_VALID = 10 #
DENY_THRESHOLD_ROOT = 1 #  root
DENY_THRESHOLD_RESTRICTED = 1
WORK_DIR = /var/lib/denyhosts #
SUSPICIOUS_LOGIN_REPORT_ALLOWED_HOSTS=YES
HOSTNAME_LOOKUP=YES #
LOCK_FILE = /var/run/denyhosts.pid #    ID
ADMIN_EMAIL = root@localhost #      ,
SMTP_HOST = localhost
SMTP_PORT = 25
SMTP_FROM = DenyHosts <nobody@localhost>
SMTP_SUBJECT = DenyHosts Report
AGE_RESET_VALID=5d #               0 (h    d    m    w    y  )
AGE_RESET_ROOT=25d
AGE_RESET_RESTRICTED=25d
AGE_RESET_INVALID=10d
RESET_ON_SUCCESS = yes #   ip               0
DAEMON_LOG = /var/log/denyhosts #
DAEMON_SLEEP = 30s #
DAEMON_PURGE = 1h #             HOSTS_DENY          ,     PURGE_DENY
```

`/etc/hosts.deny` `3`

```

```

```
sudo cat /etc/hosts.deny |  wc -l
3
```

`ubuntu 16.04` `denyhosts` `BUG` `iptables` Iptables not persistent

- VPS SSH
- Meaning of “Connection closed by xxx [preauth]” in sshd logs
- denyhosts keeps adding back my IP
- fail2ban SSH

Revision #1
Created 21 September 2020 05:50:35 by
Updated 21 September 2020 06:01:45 by