Monitoring ssh login attempts

Waikato Linux Users Group
22nd June 2020
Ian Stewart

/var/log/ files wtmp and btmp, btmp.1

Files in recently install Linux system.

```
$ ls -l /var/log/wtmp*
-rw-rw-r-- 1 root utmp 92544 Jun 22 07:50 /var/log/wtmp

$ ls -l /var/log/btmp*
-rw-rw---- 1 root utmp 384 Jun 14 08:43 /var/log/btmp
```

Files in Linux internet firewall system.

```
$ ls -l /var/log/wtmp*
-rw-rw-r-- 1 root utmp 30720 Jun 22 08:43 /var/log/wtmp
-rw-rw-r-- 1 root utmp  8832 Mar  4 16:57 /var/log/wtmp.1

$ ls -l /var/log/btmp*
-rw-rw---- 1 root utmp  77097216 Jun 22 08:43 /var/log/btmp
-rw-rw-r-- 1 root utmp 220089216 Jun  1 00:00 /var/log/btmp.1
```

$ sudo chmod +664 /var/log/btmp.1

“last” utility

- “last” is part of the util-linux package.
- Available from Linux Kernel Archive.
- Author: Miquel van Smoorenburg ⟨miquels@cistron.nl⟩
- DESCRIPTION

last searches back through the /var/log/wtmp file (or the file designated by the -f option) and displays a list of all users logged in (and out) since that file was created. One or more usernames and/or ttys can be given, in which case last will show only the entries matching those arguments. Names of ttys can be abbreviated, thus last 0 is the same as last tty0.

```
$ last --hostlast --fullnames --time-format iso /var/log/wtmp
wtmp begins 2020-06-05T17:23:44+12:00

$ last --hostlast --fullnames --time-format iso /var/log/btmp
wtmp begins 2020-06-05T17:23:44+12:00
```

Need to be able to ssh in to get wtmp and btmp files before using “last” utility

- Trying to ssh into my Laptop and then into a remote server...

```
$ ssh ian@192.168.1.16
ssh: connect to host 192.168.1.16 port 22: Connection refused

$ ssh aroha@111.222.222.111
aroha@111.222.222.111's password:
Linux firewall 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1
(2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free
software; the exact distribution terms for each program are
described in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 22 08:43:04 2020 from 111.222.222.111
```

Retrieving wtmp / btmp files ~ Pythons paramiko

```
import paramiko

def copy_from_remote_server(server, port, user, pass, remote, local):
    ssh = paramiko.SSHClient()
    ssh.load_host_keys(os.path.expanduser(os.path.join("~", ".ssh",
                                                       "known_hosts")))
    try:
        ssh.connect(server, port, user, pass)
    except Exception as e:
        print("Error: {}".format(e))

    sftp = ssh.open_sftp()
    sftp.get(remote, "remote_server_wtmp")
    sftp.close()
    ssh.close()

copy_from_remote_server("111.222.222.111", 22, "aroha", "my_password",
        "/var/log/wtmp", "servers_wtmp")
```

paramiko.ssh_exception.AuthenticationException:
Authentication failed

For Debian. Don’t use root:
$ nano /etc/ssh/sshd_config
PermitRootLogin no

Retrieving wtmp / btmp files ~ Pythons paramiko

```
$ python login_attempt_ip_addresses.py -h

This program is designed to use the paramiko modules ssh to copy
wtmp or btmp files from a remote Linux server so they may be locally
analysed.

A prerequisite to using this program is to have previously performed
a ssh connection so that the ~/.ssh/known_hosts file contains an
entry for the remote server. E.g. $ ssh root@111.222.222.111 -p 22

The first time this is done you are prompted to save the ssh-rsa in
~/.ssh/known_hosts.

Note that a wtmp / btmp file from a previous month may have a path
and file name of /var/log/btmp.1 and have r access for root and
group, but not world. Thus you may need to log in via ssh and set $
sudo chmod +664 /var/log/btmp.1 before using this program, so that
the file may be accessed in order to be copied.
```

Retrieving wtmp / btmp files ~ Pythons paramiko

```
$ python login_attempt_ip_addresses.py -h   (...continued...)

usage: login_attempt_ip_addresses.py [-h] [-s SERVER] [-p PORT]
                                     [-u USERNAME]
                                     [-f FILE]

optional arguments:
  -h, --help            show this help message and exit
  -s SERVER, --server SERVER
                        Internet name or ip address of remote server.
  -p PORT, --port PORT  Secure Shell port number used on remote
                        server. E.g. 22
  -u USERNAME, --username USERNAME
                        Account username to login to remote server.
  -f FILE, --file FILE  Path and File name for remote servers. E.g.
                        /var/log/wtmp
```

Retrieving wtmp / btmp files ~ Pythons paramiko

```
$ python login_attempt_ip_addresses.py \
         --server 111.222.222.111 \
         --port 22 \
         --username aroha \
         --file /var/log/wtmp

A connection and file transfer will be attempted to...
Server: 111.222.222.111  Port: 22  Username: aroha  File: /var/log/wtm

Do you wish to proceed with connect and transfer? [Y/n]: y

Enter account password for remote server:

Connecting to remote server and copying file...
Using 'last' to convert file to text...
Analysis of wtmp output to wtmp.txt.
Analyzing the text data...
```

Retrieving wtmp / btmp files ~ Pythons paramiko

```
$ python login_attempt_ip_addresses.py \
         --server 111.222.222.111 \
         --port 22 \
         --username aroha \
         --file /var/log/wtmp

A connection and file transfer will be attempted to...
Server: 111.222.222.111  Port: 22  Username: aroha  File: /var/log/wtm

Do you wish to proceed with connect and transfer? [Y/n]: y

Enter account password for remote server:

Connecting to remote server and copying file...
Using 'last' to convert file to text...
Analysis of wtmp output to wtmp.txt.
Analyzing the text data...
```

“last” output of remote server wtmp

```
$ last -f wtmp
aroha    pts/0        111.222.222.000  Tue Jun 16 21:17 - 21:17  (00:00)
root     tty1                          Tue Jun 16 16:05 - 16:05  (00:00)
reboot   system boot 4.19.0-9-amd64    Tue Jun 16 15:52   still running
root     tty1                          Tue Jun 16 15:45 - down   (00:00)
reboot   system boot 4.19.0-9-amd64    Tue Jun 16 15:44 - 15:45  (00:00)
aroha    pts/0        111.222.222.000  Tue Jun 16 09:19 - 15:44  (06:24)
aroha    pts/0        111.222.222.000  Mon Jun 15 18:55 - 22:06  (03:11)
aroha    pts/0        111.222.222.000  Mon Jun 15 11:16 - 11:59  (00:43)
aroha    pts/0        111.222.222.000  Mon Jun 15 10:33 - 11:16  (00:42)
root     pts/0        111.222.222.000  Mon Jun 15 10:15 - 10:17  (00:01)
aroha    pts/1        111.222.222.000  Mon Jun 15 10:14 - 10:33  (00:18)
root     pts/0        111.222.222.000  Mon Jun 15 10:09 - 10:15  (00:05)
root     pts/0        111.222.222.000  Sun Jun 14 15:50 - 18:20  (02:29)
aroha    pts/0        111.222.222.000  Thu Jun  4 17:58 - 22:41  (04:43)
aroha    pts/0        111.222.222.000  We          13 16:30 - 16:31  (00:01)
root                  .000                                   09:51  (02:33)
root                  .000                                   00:45  (12:05)
aroha                 .000  Tue Apr 14 12:39 -               12:39  (00:00)
```

Login from console

Before setting
$ nano /etc/ssh/sshd_config
PermitRootLogin no

My laptop logging in
from home

“last” output of remote server btmp

```
$ last -f btmp.1
sawmill  ssh:notty    37.187.122.195   Mon Jun  1 00:00    gone - no logout
stylofre ssh:notty    111.229.58.117   Sun May 31 23:59 - 00:00  (00:00)
stylofre ssh:notty    111.229.58.117   Sun May 31 23:59 - 23:59  (00:00)
root     ssh:notty    93.170.36.5      Sun May 31 23:59 - 23:59  (00:00)
technico ssh:notty    129.211.146.50   Sun May 31 23:59 - 23:59  (00:00)
technico ssh:notty    129.211.146.50   Sun May 31 23:59 - 23:59  (00:00)
root     ssh:notty    180.76.147.105   Sun May 31 23:59 - 23:59  (00:00)
root     ssh:notty    134.209.236.191  Sun May 31 23:59 - 23:59  (00:00)
root     ssh:notty    190.171.240.51   Sun May 31 23:58 - 23:59  (00:00)
localhos ssh:notty    109.86.194.177   Sun May 31 23:58 - 23:58  (00:00)
localhos ssh:notty    109.86.194.177   Sun May 31 23:58 - 23:58  (00:00)
tara     ssh:notty    51.178.24.61     Sun May 31 23:58 - 23:58  (00:00)
tara     s            [illegible]      Sun May 31 23:58 - 23:58  (00:00)
root     ssh:notty    121.229.2.136    Sun May 31 23:58 - 23:58  (00:00)
root     ssh:notty    198.199.124.109  Sun May 31 23:58 - 23:58  (00:00)
vboxuser ssh:notty    114.118.7.75     Sun May 31 23:58 - 23:58  (00:00)
vboxuser ssh:notty    114.118.7.75     Sun May 31 23:58 - 23:58  (00:00)
root     ssh:notty    106.53.20.179    Sun May 31 23:58 - 23:58  (00:00)
zz       ssh:notty    46.101.33.198    Sun May 31 23:58 - 23:58  (00:00)
```

Truncated account names

“last” output of remote server btmp.1 ~ different layout

```
$ cat btmp.1.txt
sawmill  ssh:notty    2020-06-01T00:00:15+12:00   gone - no logout                                  37.187.122.195
stylofrete ssh:notty    2020-05-31T23:59:51+12:00 - 2020-06-01T00:00:15+12:00  (00:00)     111.229.58.117
stylofrete ssh:notty    2020-05-31T23:59:48+12:00 - 2020-05-31T23:59:51+12:00  (00:00)     111.229.58.117
root     ssh:notty    2020-05-31T23:59:32+12:00 - 2020-05-31T23:59:48+12:00  (00:00)     93.170.36.5
technicom ssh:notty    2020-05-31T23:59:31+12:00 - 2020-05-31T23:59:32+12:00  (00:00)     129.211.146.50
technicom ssh:notty    2020-05-31T23:59:29+12:00 - 2020-05-31T23:59:31+12:00  (00:00)     129.211.146.50
root     ssh:notty    2020-05-31T23:59:21+12:00 - 2020-05-31T23:59:29+12:00  (00:00)     180.76.147.105
root     ssh:notty    2020-05-31T23:59:21+12:00 - 2020-05-31T23:59:21+12:00  (00:00)     134.209.236.191
root     ssh:notty    2020-05-31T23:58:56+12:00 - 2020-05-31T23:59:21+12:00  (00:00)     190.171.240.51
localhost ssh:notty    2020-05-31T23:58:44+12:00 - 2020-05-31T23:58:56+12:00  (00:00)     109.86.194.177
localhost ssh:notty    2020-05-31T23:58:42+12:00 - 2020-05-31T23:58:44+12:00  (00:00)     109.86.194.177
tara     ssh:notty    2020-05-31T23:58:38+12:00 - 2020-05-31T23:58:42+12:00  (00:00)     51.178.24.61
tara     ssh:notty    2020-05-31T23:58:36+12:00 - 2020-05-31T23:58:38+12:00  (00:00)     51.178.24.61
root     ssh:notty    2020-05-31T23:58:28+12:00 - 2020-05-31T23:58:36+12:00  (00:00)     121.229.2.136
root     ssh:notty    2020-05-31T23:58:28+12:00 - 2020-05-31T23:58:28+12:00  (00:00)     198.199.124.109
vboxuser ssh:notty    2020-05-31T23:58:24+12:00 - 2020-05-31T23:58:28+12:00  (00:00)     114.118.7.75
vboxuser ssh:notty    2020-05-31T23:58:22+12:00 - 2020-05-31T23:58:24+12:00  (00:00)     114.118.7.75
root     ssh:notty    2020-05-31T23:58:15+12:00 - 2020-05-31T23:58:22+12:00  (00:00)     106.53.20.179
zz       ssh:notty    2020-05-31T23:58:06+12:00 - 2020-05-31T23:58:15+12:00  (00:00)     46.101.33.198
zz       ssh:notty    2020-05-31T23:58:04+12:00 - 2020-05-31T23:58:06+12:00  (00:00)     46.101.33.198
root     ssh:notty    2020-05-31T23:57:49+12:00 - 2020-05-31T23:58:04+12:00  (00:00)     111.229.58.117
root     ssh:notty    2020-05-31T23:57:48+12:00 - 2020-05-31T23:57:49+12:00  (00:00)     191.239.243.123
root     ssh:notty    2020-05-31T23:57:45+12:00 - 2020-05-31T23:57:48+12:00  (00:00)     223.197.175.91
angel                 2020-05-31T23:57:30+12:00 - 2020-05-31T23:57:45+12:00  (00:00)     37.139.1.197
angel                 2020-05-31T23:57:28+12:00 - 2020-05-31T23:57:30+12:00  (00:00)     37.139.1.197
root                  2020-05-31T23:56:58+12:00 - 2020-05-31T23:57:28+12:00  (00:00)     36.111.182.35
root                  2020-05-31T23:56:19+12:00 - 2020-05-31T23:56:58+12:00  (00:00)     46.101.249.232
root                  2020-05-31T23:55:59+12:00 - 2020-05-31T23:56:19+12:00  (00:00)     121.229.2.136
```

Originating IP’s

Attempt to log into an account with this username

Used ISO timestamp to get the year

“last” output of remote server btmp.1

```
A connection and file transfer will be attempted to...
Server: 111.222.222.111  Port: 2022  Username: aroha  File: /var/log/btmp.1

$ Do you wish to proceed with connect and transfer? [Y/n]: y

Enter account password for remote server:

Connecting to remote server and copyong file...
Using 'last' to convert file to text...
Analysis of btmp.1 output to btmp.1.txt.
Analyzing the text data...

Total Usernames: 32597
Corrupted Usernames: 752
Total failed ssh logins for the month: 573147
Max attempts from one ip address: 8764
Total number of ip addresses performing attempts: 5903
Most popular Username: root with 85133 attempts.
```

Note that port forwarding is in place. Port 2022 forwards to Port 22 (default ssh port)

“corrupted” username contains a newline character

“last” output of remote server btmp.1

Attempts per day for May 2020

```
2020-05-01 Fri: 14339
2020-05-02 Sat: 10203
2020-05-03 Sun: 12339
2020-05-04 Mon: 18535
2020-05-05 Tue: 15410
2020-05-06 Wed: 16002
2020-05-07 Thu: 13095
2020-05-08 Fri: 14995
2020-05-09 Sat: 16443
2020-05-10 Sun: 16154
2020-05-11 Mon: 20062
2020-05-12 Tue: 19908
2020-05-13 Wed: 19462
2020-05-14 Thu: 14329
2020-05-15 Fri: 18156
2020-05-16 Sat: 46672
2020-05-17 Sun: 24427
2020-05-18 Mon: 10442
2020-05-19 Tue: 43873
2020-05-20 Wed: 26074
2020-05-20 Wed: 26074
2020-05-21 Thu: 37596
2020-05-22 Fri: 19505
2020-05-23 Sat: 11746
2020-05-24 Sun: 23856
2020-05-25 Mon: 10042
2020-05-26 Tue: 12714
2020-05-27 Wed: 10223
2020-05-28 Thu: 14819
2020-05-29 Fri: 15524
2020-05-30 Sat: 14135
2020-05-31 Sun: 12066
2020-06-01 Mon: 1
```

“last” output of remote server btmp

Attempts per day for June 2020

```
Analyzing the text data...

Total Usernames: 14744
Corrupted Usernames: 1602
Total failed ssh logins for the month: 200772
Max attempts from one ip address: 1026
Total number of ip addresses performing attempts: 3922
Most popular Username: root with 89106 attempts.
```

“last” output of remote server btmp

Attempts per day for June 2020

```
2020-06-01 Mon: 11436
2020-06-02 Tue: 10467
2020-06-03 Wed: 9964
2020-06-04 Thu: 7628
2020-06-05 Fri: 4973
2020-06-06 Sat: 6218
2020-06-07 Sun: 5733
2020-06-08 Mon: 8461
2020-06-09 Tue: 10698
2020-06-10 Wed: 12536
2020-06-11 Thu: 14351
2020-06-12 Fri: 9829
2020-06-13 Sat: 11688
2020-06-14 Sun: 8270
2020-06-15 Mon: 9639
2020-06-16 Tue: 15535
2020-06-17 Wed: 10471
2020-06-18 Thu: 13654
2020-05-16 Sat: 46672
2020-06-19 Fri: 6470
2020-06-20 Sat: 6271
2020-06-21 Sun: 5577
2020-06-22 Mon: 903
2020-06-23 Tue: 0
2020-06-24 Wed: 0
2020-06-25 Thu: 0
2020-06-26 Fri: 0
2020-06-27 Sat: 0
2020-06-28 Sun: 0
2020-06-29 Mon: 0
2020-06-30 Tue: 0
2020-07-01 Wed: 0
2020-07-02 Thu: 0
```

Add fail2ban application
No apparent effect

Questions

End