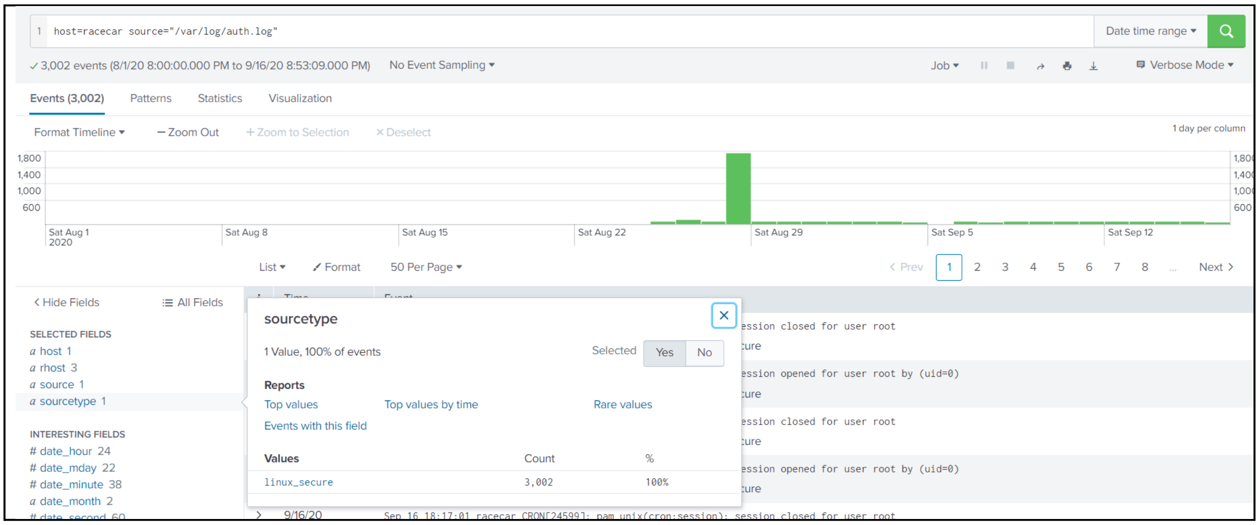
Virtual Lab 6 – Log Analysis
MGS 650 Information Assurance
Submitted by: Akhilesh Anand Undralla

1. What is the sourcetype of the /var/log/auth.log?

A: `linux_secure`



```
host=racecar source="/var/log/auth.log"
```

✓ 3,002 events (8/1/20 8:00:00.000 PM to 9/16/20 8:53:09.000 PM)

SELECTED FIELDS
- a host 1
- a rhost 3
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 24
- # date_mday 22
- # date_minute 38
- a date_month 2
- # date_second 60

sourcetype

1 Value, 100% of events

Selected: Yes No

Reports: Top values, Top values by time, Rare values, Events with this field

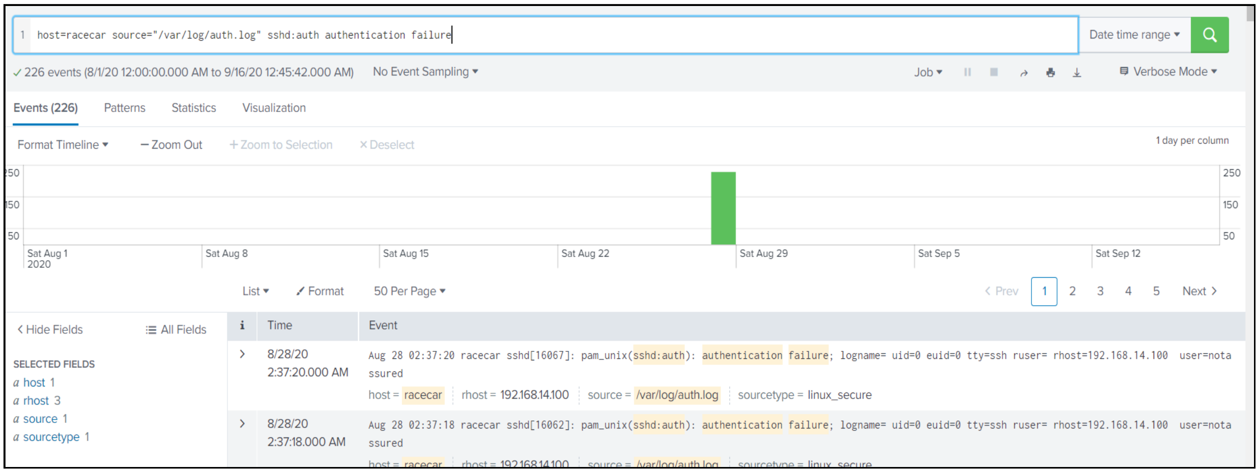
Values	Count	%
linux_secure	3,002	100%

```
ession closed for user root
ure
ession opened for user root by (uid=0)
ure
ession closed for user root
ure
ession opened for user root by (uid=0)
ure
9/16/20   Sep 16 18:17:01 racecar CRON[24599]: pam_unix(cron:session): session closed for user root
```

Figure 1.1: sourcetype of the /var/log/auth.log

2. How many sshd:auth events have occurred in the given time range?

A: 226



```
host=racecar source="/var/log/auth.log" sshd:auth authentication failure
```

✓ 226 events (8/1/20 12:00:00.000 AM to 9/16/20 12:45:42.000 AM)

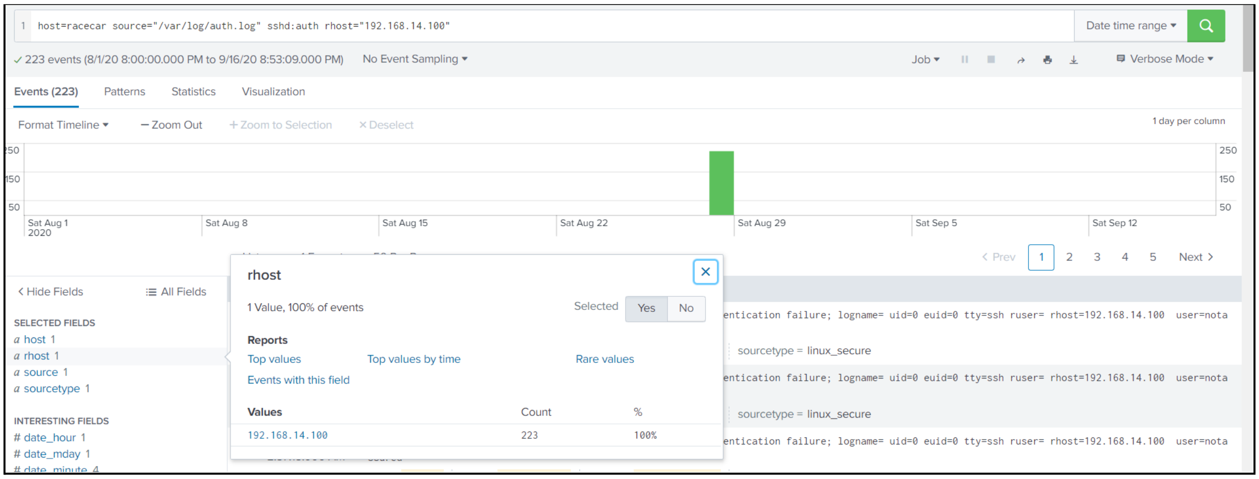
SELECTED FIELDS
- a host 1
- a rhost 3
- a source 1
- a sourcetype 1

```
i  Time                   Event
>  8/28/20 2:37:20.000 AM Aug 28 02:37:20 racecar sshd[16067]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=notassured
                          host = racecar | rhost = 192.168.14.100 | source = /var/log/auth.log | sourcetype = linux_secure
>  8/28/20 2:37:18.000 AM Aug 28 02:37:18 racecar sshd[16062]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=notassured
                          host = racecar | rhost = 192.168.14.100 | source = /var/log/auth.log | sourcetype = linux_secure
```

Figure 1.2: sshd:auth log events (refer search bar)

3. How many failed login events are from host 192.168.14.100?

A: 223



```
host=racecar source="/var/log/auth.log" sshd:auth rhost="192.168.14.100"
```

✓ 223 events (8/1/20 8:00:00.000 PM to 9/16/20 8:53:09.000 PM)

rhost

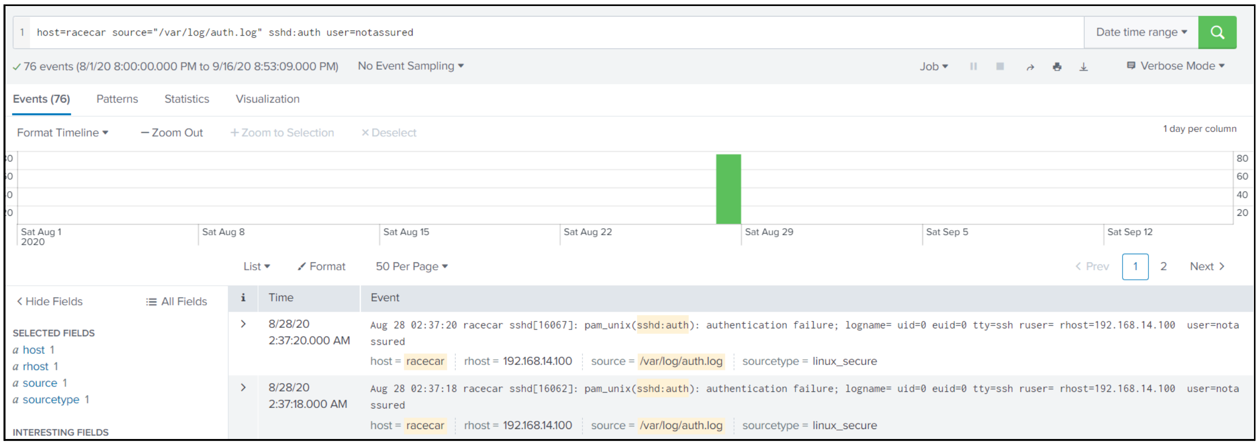
1 Value, 100% of events

Values	Count	%
192.168.14.100	223	100%

```
entication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
sourcetype = linux_secure
entication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
sourcetype = linux_secure
entication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
```

Figure 1.3: logs showing failed login events from host 192.168.14.100

4. How many failed login attempts are for user "notassured"?
A: 76



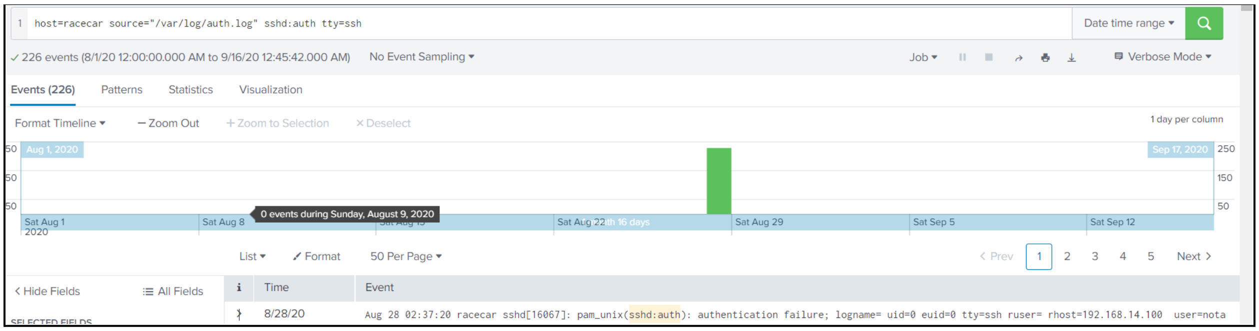
```
host=racecar source="/var/log/auth.log" sshd:auth user=notassured
```

✓ 76 events (8/1/20 8:00:00.000 PM to 9/16/20 8:53:09.000 PM)

i	Time	Event
>	8/28/20 2:37:20.000 AM	Aug 28 02:37:20 racecar sshd[16067]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=notassured host = racecar rhost = 192.168.14.100 source = /var/log/auth.log sourcetype = linux_secure
>	8/28/20 2:37:18.000 AM	Aug 28 02:37:18 racecar sshd[16062]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=notassured host = racecar rhost = 192.168.14.100 source = /var/log/auth.log sourcetype = linux_secure

Figure 1.4: logs showing failed login events for user “notassured”

5. What network protocol are these attempts happening over?
A: ssh



```
host=racecar source="/var/log/auth.log" sshd:auth tty=ssh
```

✓ 226 events (8/1/20 12:00:00.000 AM to 9/16/20 12:45:42.000 AM)

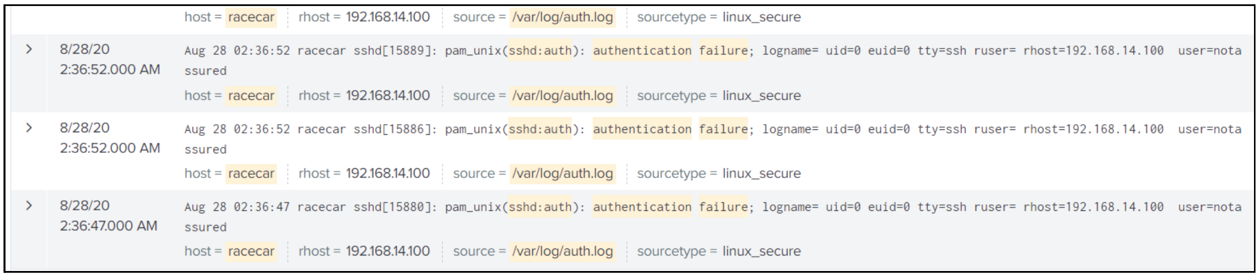
i	Time	Event
>	8/28/20	Aug 28 02:37:20 racecar sshd[16067]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=nota

Figure 1.5: ssh in the search bar lists 226 fail event logs

6. What are the time and date of the first and last events when someone tried to login as "notassured", but failed?

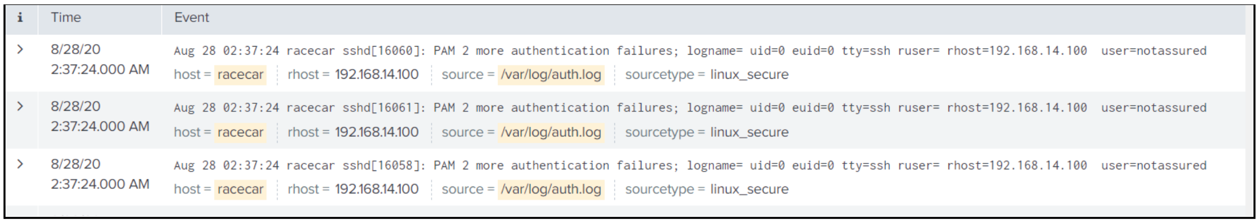
A: First event - 8/28/20 2:36:47.000 AM

Last event - 8/28/20 2:37:24.000 AM



```
                host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20      Aug 28 02:36:52 racecar sshd[15889]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
   2:36:52.000 AM ssured
                host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20      Aug 28 02:36:52 racecar sshd[15886]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
   2:36:52.000 AM ssured
                host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20      Aug 28 02:36:47 racecar sshd[15880]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=nota
   2:36:47.000 AM ssured
                host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
```

Figure 1.6: First event showing login fail by “notassured” (check the last line)



```
i  Time           Event
>  8/28/20        Aug 28 02:37:24 racecar sshd[16060]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=notassured
   2:37:24.000 AM host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20        Aug 28 02:37:24 racecar sshd[16061]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=notassured
   2:37:24.000 AM host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20        Aug 28 02:37:24 racecar sshd[16058]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100  user=notassured
   2:37:24.000 AM host = racecar   rhost = 192.168.14.100   source = /var/log/auth.log   sourcetype = linux_secure
```

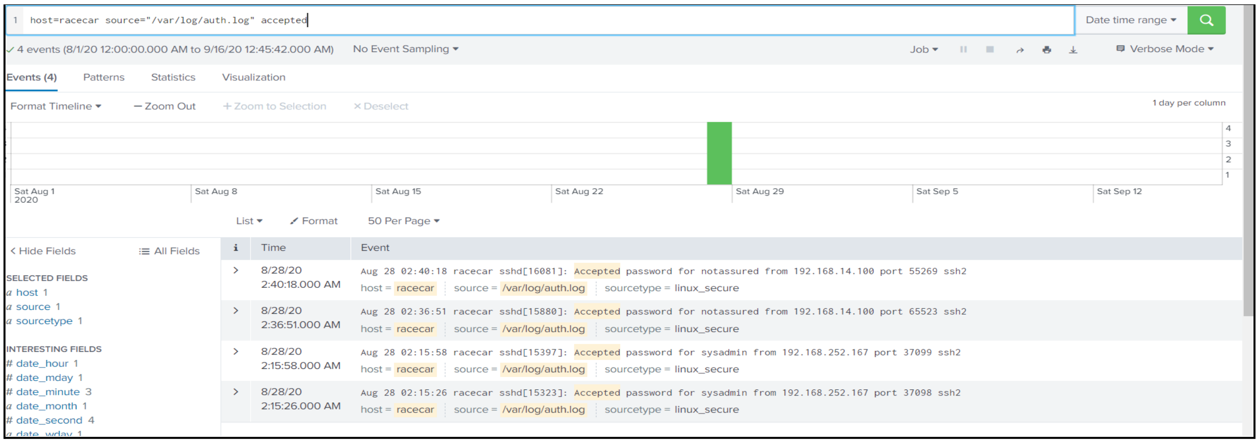
Figure 1.7: Last event showing login fail by “notassured” (check the first line)

7. Considering the number of attempts, is it feasible for a human being to login that many times given the time range?

A: No, a human being can not login since the difference between login attempts is merely millisecond. It could have been an automated script running.

8. How many total successful authentications events?

A: 4



```
1  host=racecar source="/var/log/auth.log" accepted
```

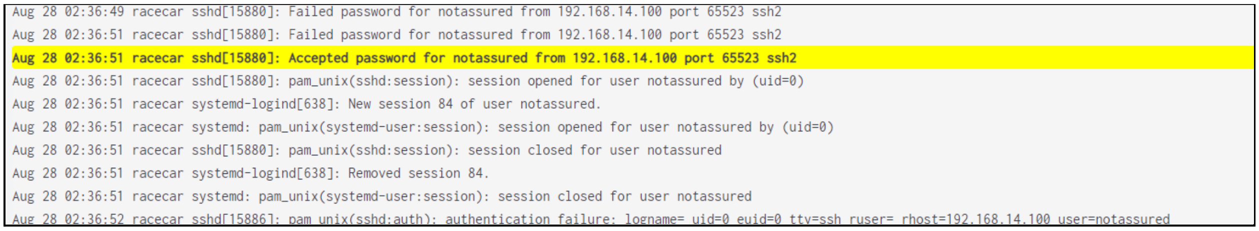
✓ 4 events (8/1/20 12:00:00.000 AM to 9/16/20 12:45:42.000 AM)

```
i  Time           Event
>  8/28/20        Aug 28 02:40:18 racecar sshd[16081]: Accepted password for notassured from 192.168.14.100 port 55269 ssh2
   2:40:18.000 AM host = racecar   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20        Aug 28 02:36:51 racecar sshd[15880]: Accepted password for notassured from 192.168.14.100 port 65523 ssh2
   2:36:51.000 AM host = racecar   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20        Aug 28 02:15:58 racecar sshd[15397]: Accepted password for sysadmin from 192.168.252.167 port 37099 ssh2
   2:15:58.000 AM host = racecar   source = /var/log/auth.log   sourcetype = linux_secure
>  8/28/20        Aug 28 02:15:26 racecar sshd[15323]: Accepted password for sysadmin from 192.168.252.167 port 37098 ssh2
   2:15:26.000 AM host = racecar   source = /var/log/auth.log   sourcetype = linux_secure
```

Figure 1.8: Total number of logs with successful logon events from all the users

9. What user did 192.168.14.100 login as?

A: The user `notassured` from 192.168.14.100 logged in successfully.

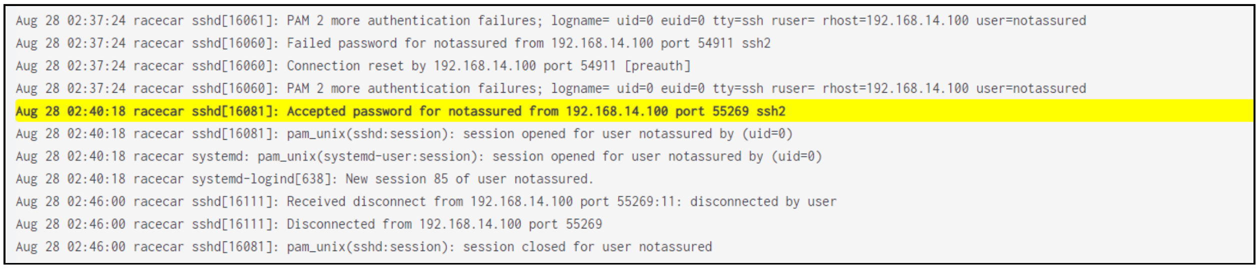


```
Aug 28 02:36:49 racecar sshd[15880]: Failed password for notassured from 192.168.14.100 port 65523 ssh2
Aug 28 02:36:51 racecar sshd[15880]: Failed password for notassured from 192.168.14.100 port 65523 ssh2
Aug 28 02:36:51 racecar sshd[15880]: Accepted password for notassured from 192.168.14.100 port 65523 ssh2
Aug 28 02:36:51 racecar sshd[15880]: pam_unix(sshd:session): session opened for user notassured by (uid=0)
Aug 28 02:36:51 racecar systemd-logind[638]: New session 84 of user notassured.
Aug 28 02:36:51 racecar systemd: pam_unix(systemd-user:session): session opened for user notassured by (uid=0)
Aug 28 02:36:51 racecar sshd[15880]: pam_unix(sshd:session): session closed for user notassured
Aug 28 02:36:51 racecar systemd-logind[638]: Removed session 84.
Aug 28 02:36:51 racecar systemd: pam_unix(systemd-user:session): session closed for user notassured
Aug 28 02:36:52 racecar sshd[15886]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=notassured
```

Figure 1.9: User details from seen from source details (Expand the event -> Change "Event Actions" to "Show Source")

10. What could be concluded from the data collected? Was there an attack performed on the target machine? If so, what attack, and was it successful?

A: It could be inferred that the network had a breach since there was no appropriate access restriction implementation. Here, brute force attack was performed and successfully able to crack the password.



```
Aug 28 02:37:24 racecar sshd[16061]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=notassured
Aug 28 02:37:24 racecar sshd[16060]: Failed password for notassured from 192.168.14.100 port 54911 ssh2
Aug 28 02:37:24 racecar sshd[16060]: Connection reset by 192.168.14.100 port 54911 [preauth]
Aug 28 02:37:24 racecar sshd[16060]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.14.100 user=notassured
Aug 28 02:40:18 racecar sshd[16081]: Accepted password for notassured from 192.168.14.100 port 55269 ssh2
Aug 28 02:40:18 racecar sshd[16081]: pam_unix(sshd:session): session opened for user notassured by (uid=0)
Aug 28 02:40:18 racecar systemd: pam_unix(systemd-user:session): session opened for user notassured by (uid=0)
Aug 28 02:40:18 racecar systemd-logind[638]: New session 85 of user notassured.
Aug 28 02:46:00 racecar sshd[16111]: Received disconnect from 192.168.14.100 port 55269:11: disconnected by user
Aug 28 02:46:00 racecar sshd[16111]: Disconnected from 192.168.14.100 port 55269
Aug 28 02:46:00 racecar sshd[16081]: pam_unix(sshd:session): session closed for user notassured
```

Figure 2.0: User details from seen from source details