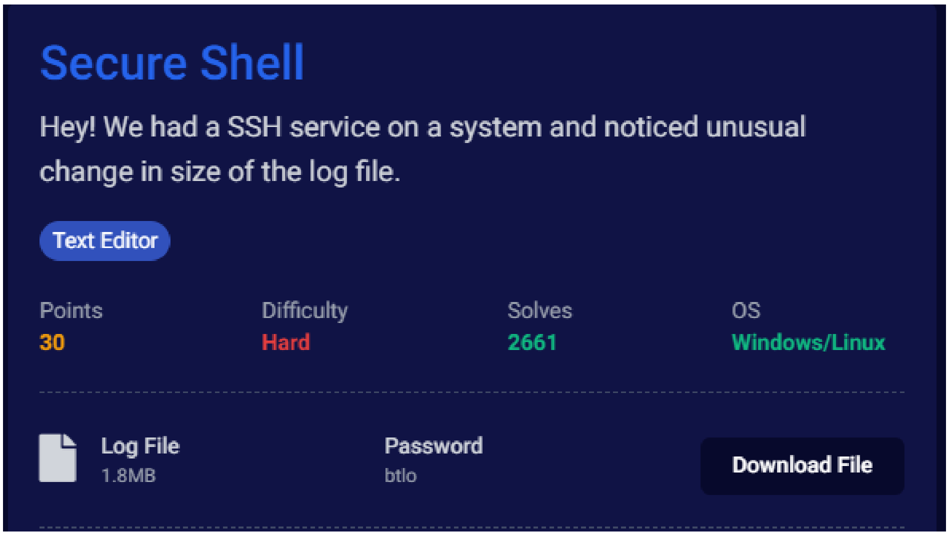
Reference: https://blueteamlabs.online/home/challenge/secure-shell-1aecac55c3

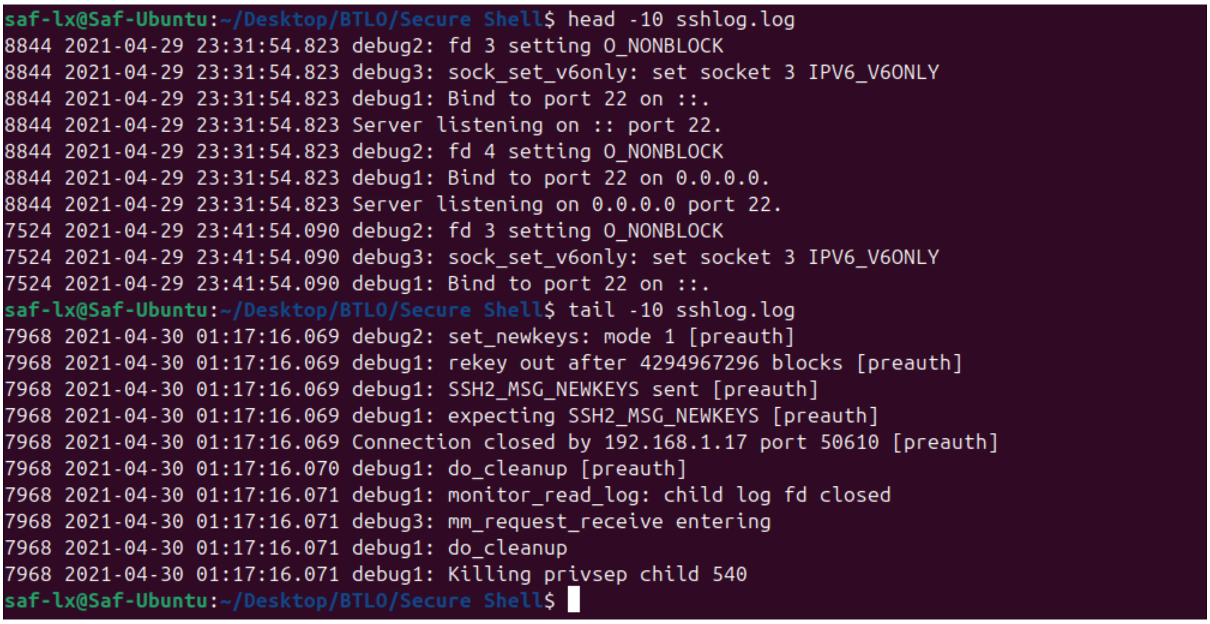


Secure Shell

Hey! We had a SSH service on a system and noticed unusual change in size of the log file.

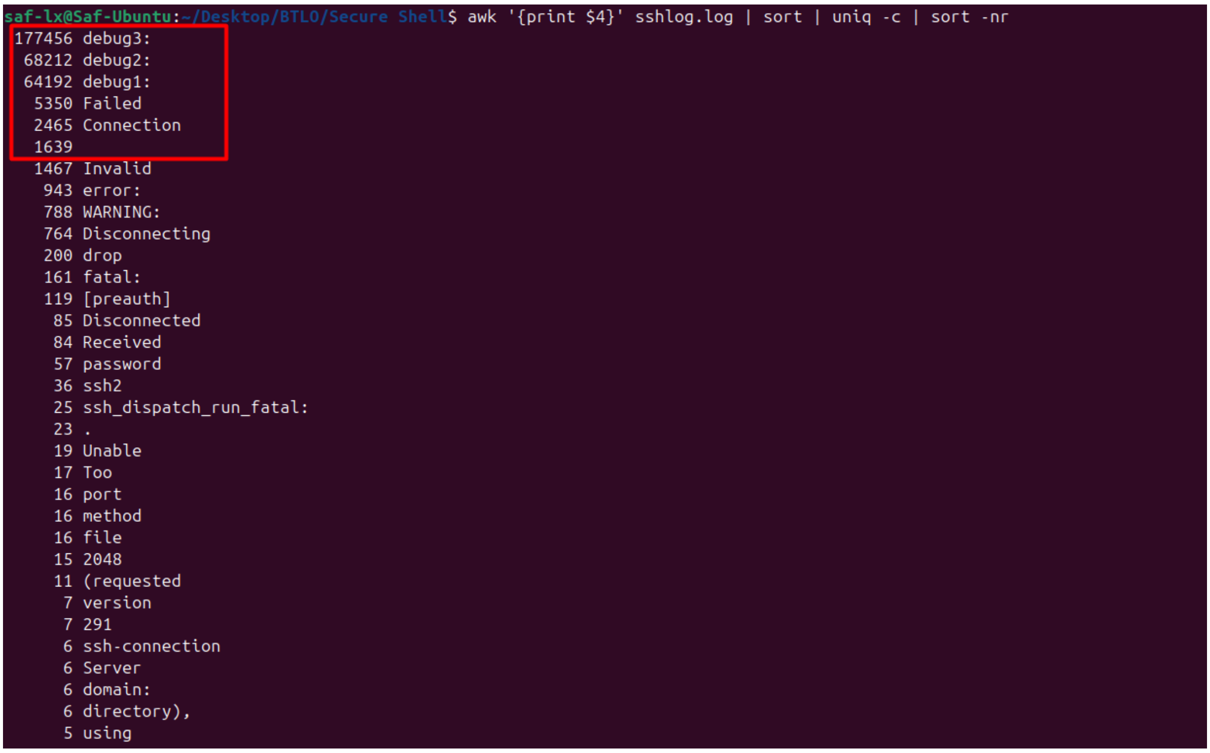
Download the log file of SSH sever log from here. Usually, the log file is located in **C:\ProgramData\ssh\logs\sshd.log on windows.**

Head and tail peek from the log file.



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ head -10 sshlog.log
8844 2021-04-29 23:31:54.823 debug2: fd 3 setting O_NONBLOCK
8844 2021-04-29 23:31:54.823 debug3: sock_set_v6only: set socket 3 IPV6_V6ONLY
8844 2021-04-29 23:31:54.823 debug1: Bind to port 22 on ::.
8844 2021-04-29 23:31:54.823 Server listening on :: port 22.
8844 2021-04-29 23:31:54.823 debug2: fd 4 setting O_NONBLOCK
8844 2021-04-29 23:31:54.823 debug1: Bind to port 22 on 0.0.0.0.
8844 2021-04-29 23:31:54.823 Server listening on 0.0.0.0 port 22.
7524 2021-04-29 23:41:54.090 debug2: fd 3 setting O_NONBLOCK
7524 2021-04-29 23:41:54.090 debug3: sock_set_v6only: set socket 3 IPV6_V6ONLY
7524 2021-04-29 23:41:54.090 debug1: Bind to port 22 on ::.
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ tail -10 sshlog.log
7968 2021-04-30 01:17:16.069 debug2: set_newkeys: mode 1 [preauth]
7968 2021-04-30 01:17:16.069 debug1: rekey out after 4294967296 blocks [preauth]
7968 2021-04-30 01:17:16.069 debug1: SSH2_MSG_NEWKEYS sent [preauth]
7968 2021-04-30 01:17:16.069 debug1: expecting SSH2_MSG_NEWKEYS [preauth]
7968 2021-04-30 01:17:16.069 Connection closed by 192.168.1.17 port 50610 [preauth]
7968 2021-04-30 01:17:16.070 debug1: do_cleanup [preauth]
7968 2021-04-30 01:17:16.071 debug1: monitor_read_log: child log fd closed
7968 2021-04-30 01:17:16.071 debug3: mm_request_receive entering
7968 2021-04-30 01:17:16.071 debug1: do_cleanup
7968 2021-04-30 01:17:16.071 debug1: Killing privsep child 540
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ 
```

Let’s parse the 4th field, what we can extract.



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ awk '{print $4}' sshlog.log | sort | uniq -c | sort -nr
 177456 debug3:
  68212 debug2:
  64192 debug1:
   5350 Failed
   2465 Connection
   1639 
   1467 Invalid
    943 error:
    788 WARNING:
    764 Disconnecting
    200 drop
    161 fatal:
    119 [preauth]
     85 Disconnected
     84 Received
     57 password
     36 ssh2
     25 ssh_dispatch_run_fatal:
     23 .
     19 Unable
     17 Too
     16 port
     16 method
     16 file
     15 2048
     11 (requested
      7 version
      7 291
      6 ssh-connection
      6 Server
      6 domain:
      6 directory),
      5 using
```

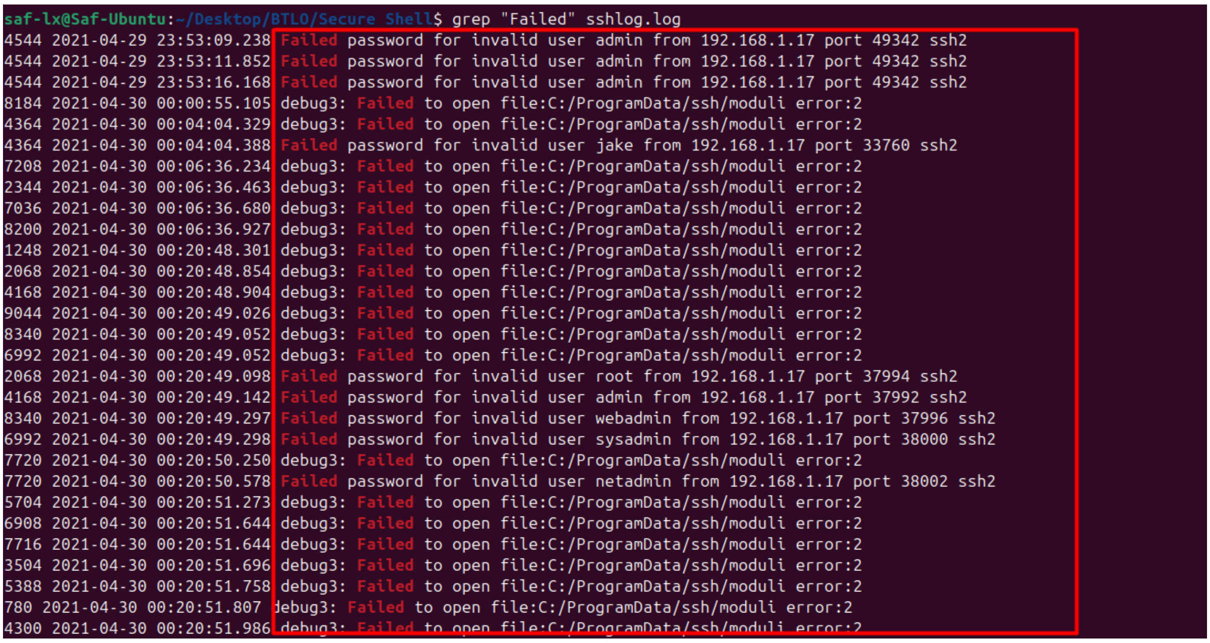
We can see debug3, debug2 and debug1 from 4th filed. We can conclude that the log file is **debug level log**. We have level of log as:

Level 0 – emerg (emergency)
Level 1 – alert
Level 2 – crit (critical)
Level 3 – err/error
Level 4 – warning/warn
Level 5 – notice
Level 6 – info
Level 7 – debug ->> Detailed technical info for debugging.

For SSH (sshd), log levels determine how much detail you see in /var/log/auth.log or /var/log/secure:

- info → successful/failed logins, connection attempts
- notice → reconfiguration messages
- debug or debug2, debug3 → extremely detailed connection tracing

Also, we have Failed and the count of Failed looks a lot, lets investigate that.

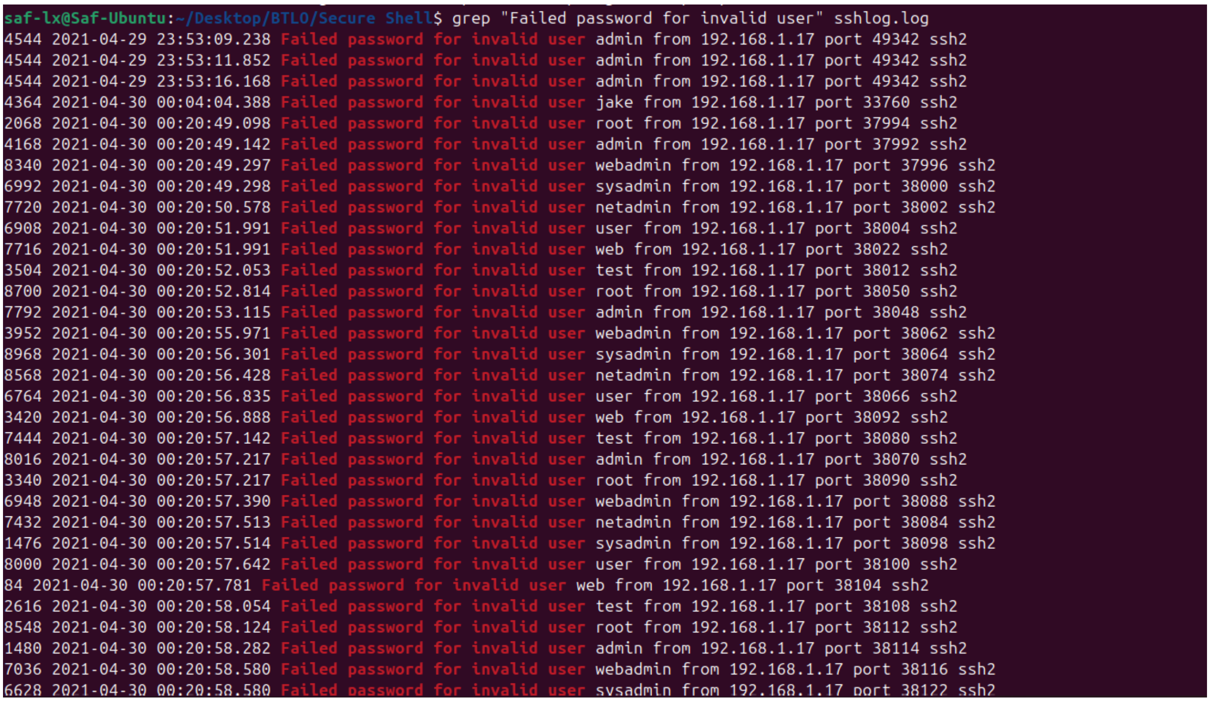


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Failed" sshlog.log
4544 2021-04-29 23:53:09.238 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:11.852 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:16.168 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
8184 2021-04-30 00:00:55.105 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
4364 2021-04-30 00:04:04.329 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
4364 2021-04-30 00:04:04.388 Failed password for invalid user jake from 192.168.1.17 port 33760 ssh2
7208 2021-04-30 00:06:36.234 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
2344 2021-04-30 00:06:36.463 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
7036 2021-04-30 00:06:36.680 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
8200 2021-04-30 00:06:36.927 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
1248 2021-04-30 00:20:48.301 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
2068 2021-04-30 00:20:48.854 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
4168 2021-04-30 00:20:48.904 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
9044 2021-04-30 00:20:49.026 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
8340 2021-04-30 00:20:49.052 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
6992 2021-04-30 00:20:49.052 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
2068 2021-04-30 00:20:49.098 Failed password for invalid user root from 192.168.1.17 port 37994 ssh2
4168 2021-04-30 00:20:49.142 Failed password for invalid user admin from 192.168.1.17 port 37992 ssh2
8340 2021-04-30 00:20:49.297 Failed password for invalid user webadmin from 192.168.1.17 port 37996 ssh2
6992 2021-04-30 00:20:49.298 Failed password for invalid user sysadmin from 192.168.1.17 port 38000 ssh2
7720 2021-04-30 00:20:50.250 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
7720 2021-04-30 00:20:50.578 Failed password for invalid user netadmin from 192.168.1.17 port 38002 ssh2
5704 2021-04-30 00:20:51.273 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
6908 2021-04-30 00:20:51.644 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
7716 2021-04-30 00:20:51.644 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
3504 2021-04-30 00:20:51.696 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
5388 2021-04-30 00:20:51.758 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
780 2021-04-30 00:20:51.807 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
4300 2021-04-30 00:20:51.986 debug3: Failed to open file:C:/ProgramData/ssh/moduli error:2
```

We can clearly see that, this is the ssh brute force attack because, the attacker is trying to do ssh login via multiple users. Seems like an attacker guess the random username and doing the brute force attack. The ip address 192.168.1.17 is trying to ssh login in different port.

Let's dig deep.

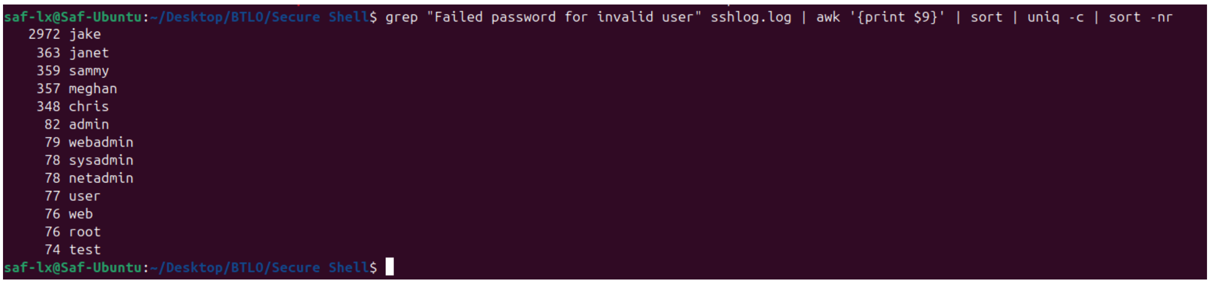
grep "Failed password for invalid user" sshlog.log



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Failed password for invalid user" sshlog.log
4544 2021-04-29 23:53:09.238 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:11.852 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:16.168 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4364 2021-04-30 00:04:04.388 Failed password for invalid user jake from 192.168.1.17 port 33760 ssh2
2068 2021-04-30 00:20:49.098 Failed password for invalid user root from 192.168.1.17 port 37994 ssh2
4168 2021-04-30 00:20:49.142 Failed password for invalid user admin from 192.168.1.17 port 37992 ssh2
8340 2021-04-30 00:20:49.297 Failed password for invalid user webadmin from 192.168.1.17 port 37996 ssh2
6992 2021-04-30 00:20:49.298 Failed password for invalid user sysadmin from 192.168.1.17 port 38000 ssh2
7720 2021-04-30 00:20:50.578 Failed password for invalid user netadmin from 192.168.1.17 port 38002 ssh2
6908 2021-04-30 00:20:51.991 Failed password for invalid user user from 192.168.1.17 port 38004 ssh2
7716 2021-04-30 00:20:51.991 Failed password for invalid user web from 192.168.1.17 port 38022 ssh2
3504 2021-04-30 00:20:52.053 Failed password for invalid user test from 192.168.1.17 port 38012 ssh2
8700 2021-04-30 00:20:52.814 Failed password for invalid user root from 192.168.1.17 port 38050 ssh2
7792 2021-04-30 00:20:53.115 Failed password for invalid user admin from 192.168.1.17 port 38048 ssh2
3952 2021-04-30 00:20:55.971 Failed password for invalid user webadmin from 192.168.1.17 port 38062 ssh2
8968 2021-04-30 00:20:56.301 Failed password for invalid user sysadmin from 192.168.1.17 port 38064 ssh2
8568 2021-04-30 00:20:56.428 Failed password for invalid user netadmin from 192.168.1.17 port 38074 ssh2
6764 2021-04-30 00:20:56.835 Failed password for invalid user user from 192.168.1.17 port 38066 ssh2
3420 2021-04-30 00:20:56.888 Failed password for invalid user web from 192.168.1.17 port 38092 ssh2
7444 2021-04-30 00:20:57.142 Failed password for invalid user test from 192.168.1.17 port 38080 ssh2
8016 2021-04-30 00:20:57.217 Failed password for invalid user admin from 192.168.1.17 port 38070 ssh2
3340 2021-04-30 00:20:57.217 Failed password for invalid user root from 192.168.1.17 port 38090 ssh2
6948 2021-04-30 00:20:57.390 Failed password for invalid user webadmin from 192.168.1.17 port 38088 ssh2
7432 2021-04-30 00:20:57.513 Failed password for invalid user netadmin from 192.168.1.17 port 38084 ssh2
1476 2021-04-30 00:20:57.514 Failed password for invalid user sysadmin from 192.168.1.17 port 38098 ssh2
8000 2021-04-30 00:20:57.642 Failed password for invalid user user from 192.168.1.17 port 38100 ssh2
84 2021-04-30 00:20:57.781 Failed password for invalid user web from 192.168.1.17 port 38104 ssh2
2616 2021-04-30 00:20:58.054 Failed password for invalid user test from 192.168.1.17 port 38108 ssh2
8548 2021-04-30 00:20:58.124 Failed password for invalid user root from 192.168.1.17 port 38112 ssh2
1480 2021-04-30 00:20:58.282 Failed password for invalid user admin from 192.168.1.17 port 38114 ssh2
7036 2021-04-30 00:20:58.580 Failed password for invalid user webadmin from 192.168.1.17 port 38116 ssh2
6628 2021-04-30 00:20:58.580 Failed password for invalid user sysadmin from 192.168.1.17 port 38122 ssh2
```

Look all those users, and they are not valid users cause it gives Failed password entry. Let's filter that out.

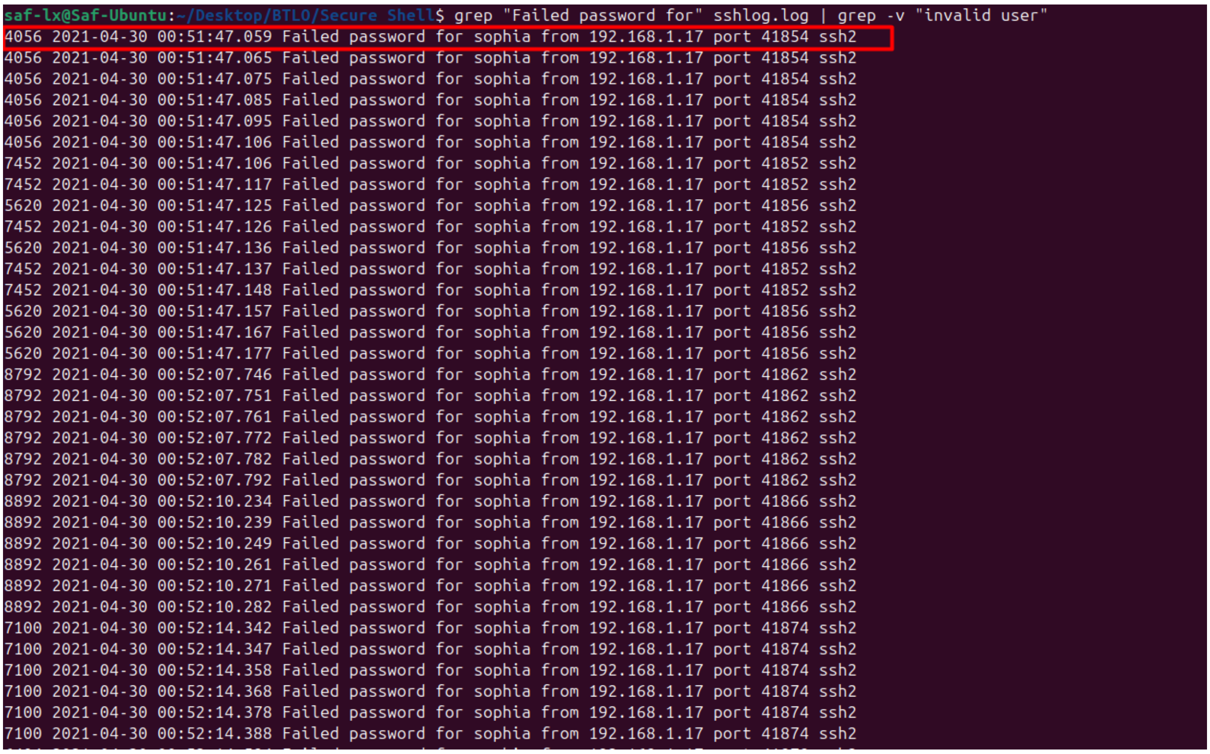
grep "Failed password for invalid user" sshlog.log | awk '{print $9}' | sort | uniq -c | sort -nr



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Failed password for invalid user" sshlog.log | awk '{print $9}' | sort | uniq -c | sort -nr
   2972 jake
    363 janet
    359 sammy
    357 meghan
    348 chris
     82 admin
     79 webadmin
     78 sysadmin
     78 netadmin
     77 user
     76 web
     76 root
     74 test
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ 
```

They all are invalid user. Let’s find out the valid user.

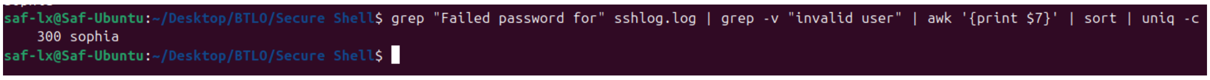
grep "Failed password for" sshlog.log | grep -v "invalid user"



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Failed password for" sshlog.log | grep -v "invalid user"
4056 2021-04-30 00:51:47.059 Failed password for sophia from 192.168.1.17 port 41854 ssh2
4056 2021-04-30 00:51:47.065 Failed password for sophia from 192.168.1.17 port 41854 ssh2
4056 2021-04-30 00:51:47.075 Failed password for sophia from 192.168.1.17 port 41854 ssh2
4056 2021-04-30 00:51:47.085 Failed password for sophia from 192.168.1.17 port 41854 ssh2
4056 2021-04-30 00:51:47.095 Failed password for sophia from 192.168.1.17 port 41854 ssh2
4056 2021-04-30 00:51:47.106 Failed password for sophia from 192.168.1.17 port 41854 ssh2
7452 2021-04-30 00:51:47.106 Failed password for sophia from 192.168.1.17 port 41852 ssh2
7452 2021-04-30 00:51:47.117 Failed password for sophia from 192.168.1.17 port 41852 ssh2
5620 2021-04-30 00:51:47.125 Failed password for sophia from 192.168.1.17 port 41856 ssh2
7452 2021-04-30 00:51:47.126 Failed password for sophia from 192.168.1.17 port 41852 ssh2
5620 2021-04-30 00:51:47.136 Failed password for sophia from 192.168.1.17 port 41856 ssh2
7452 2021-04-30 00:51:47.137 Failed password for sophia from 192.168.1.17 port 41852 ssh2
7452 2021-04-30 00:51:47.148 Failed password for sophia from 192.168.1.17 port 41852 ssh2
5620 2021-04-30 00:51:47.157 Failed password for sophia from 192.168.1.17 port 41856 ssh2
5620 2021-04-30 00:51:47.167 Failed password for sophia from 192.168.1.17 port 41856 ssh2
5620 2021-04-30 00:51:47.177 Failed password for sophia from 192.168.1.17 port 41856 ssh2
8792 2021-04-30 00:52:07.746 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8792 2021-04-30 00:52:07.751 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8792 2021-04-30 00:52:07.761 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8792 2021-04-30 00:52:07.772 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8792 2021-04-30 00:52:07.782 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8792 2021-04-30 00:52:07.792 Failed password for sophia from 192.168.1.17 port 41862 ssh2
8892 2021-04-30 00:52:10.234 Failed password for sophia from 192.168.1.17 port 41866 ssh2
8892 2021-04-30 00:52:10.239 Failed password for sophia from 192.168.1.17 port 41866 ssh2
8892 2021-04-30 00:52:10.249 Failed password for sophia from 192.168.1.17 port 41866 ssh2
8892 2021-04-30 00:52:10.261 Failed password for sophia from 192.168.1.17 port 41866 ssh2
8892 2021-04-30 00:52:10.271 Failed password for sophia from 192.168.1.17 port 41866 ssh2
8892 2021-04-30 00:52:10.282 Failed password for sophia from 192.168.1.17 port 41866 ssh2
7100 2021-04-30 00:52:14.342 Failed password for sophia from 192.168.1.17 port 41874 ssh2
7100 2021-04-30 00:52:14.347 Failed password for sophia from 192.168.1.17 port 41874 ssh2
7100 2021-04-30 00:52:14.358 Failed password for sophia from 192.168.1.17 port 41874 ssh2
7100 2021-04-30 00:52:14.368 Failed password for sophia from 192.168.1.17 port 41874 ssh2
7100 2021-04-30 00:52:14.378 Failed password for sophia from 192.168.1.17 port 41874 ssh2
7100 2021-04-30 00:52:14.388 Failed password for sophia from 192.168.1.17 port 41874 ssh2
```

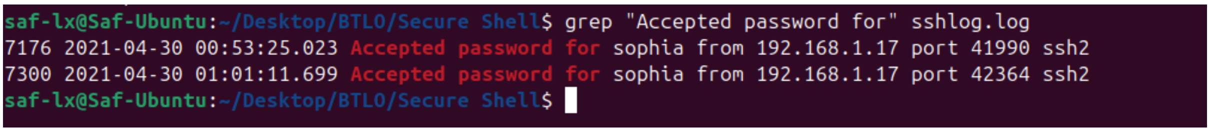
Instead of invalid user, it gives actual name of the user Sophia. So, Sophia is the only one valid user.

grep "Failed password for" sshlog.log | grep -v "invalid user" | awk '{print $7}' | sort | uniq -c



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Failed password for" sshlog.log | grep -v "invalid user" | awk '{print $7}' | sort | uniq -c
    300 sophia
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ 
```

Also grep Accepted Password for.

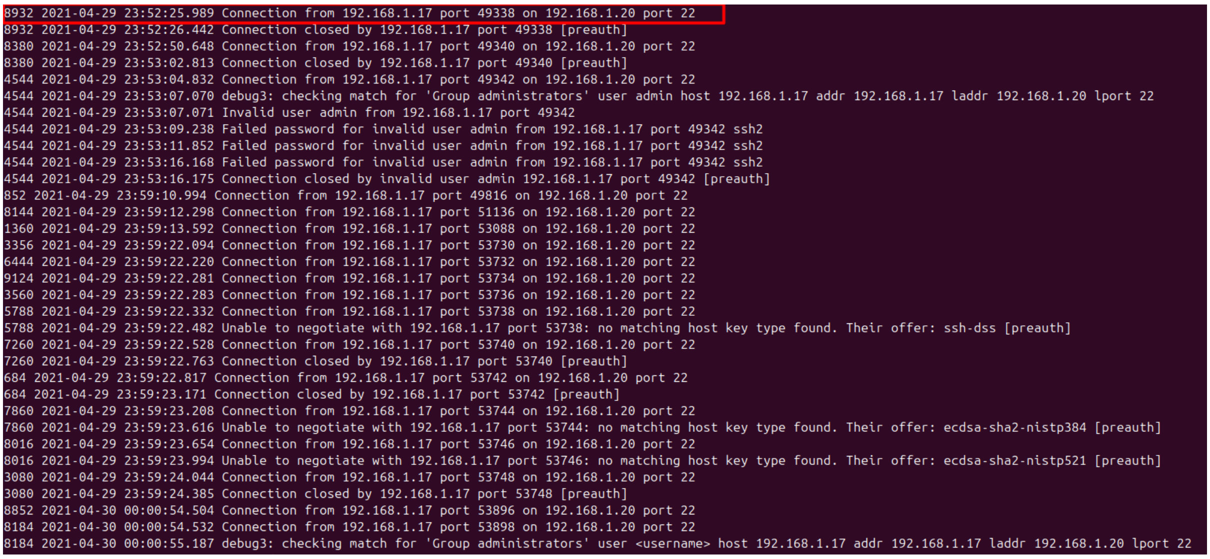


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ grep "Accepted password for" sshlog.log
7176 2021-04-30 00:53:25.023 Accepted password for sophia from 192.168.1.17 port 41990 ssh2
7300 2021-04-30 01:01:11.699 Accepted password for sophia from 192.168.1.17 port 42364 ssh2
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Secure Shell$ 
```

From this, we can conclude that Sophia is the valid user and the attacker succeed to login via her password.

Let’s find out at what time and date of request by an attacker. We can find by grep with ip address of an attacker as.

grep "192.168.1.17" sshlog.log | less



```
8932 2021-04-29 23:52:25.989 Connection from 192.168.1.17 port 49338 on 192.168.1.20 port 22
8932 2021-04-29 23:52:26.442 Connection closed by 192.168.1.17 port 49338 [preauth]
8380 2021-04-29 23:52:50.648 Connection from 192.168.1.17 port 49340 on 192.168.1.20 port 22
8380 2021-04-29 23:53:02.813 Connection closed by 192.168.1.17 port 49340 [preauth]
4544 2021-04-29 23:53:04.832 Connection from 192.168.1.17 port 49342 on 192.168.1.20 port 22
4544 2021-04-29 23:53:07.070 debug3: checking match for 'Group administrators' user admin host 192.168.1.17 addr 192.168.1.17 laddr 192.168.1.20 lport 22
4544 2021-04-29 23:53:07.071 Invalid user admin from 192.168.1.17 port 49342
4544 2021-04-29 23:53:09.238 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:11.852 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:16.168 Failed password for invalid user admin from 192.168.1.17 port 49342 ssh2
4544 2021-04-29 23:53:16.175 Connection closed by invalid user admin 192.168.1.17 port 49342 [preauth]
852 2021-04-29 23:59:10.994 Connection from 192.168.1.17 port 49816 on 192.168.1.20 port 22
8144 2021-04-29 23:59:12.298 Connection from 192.168.1.17 port 51136 on 192.168.1.20 port 22
1360 2021-04-29 23:59:13.592 Connection from 192.168.1.17 port 53088 on 192.168.1.20 port 22
3356 2021-04-29 23:59:22.094 Connection from 192.168.1.17 port 53730 on 192.168.1.20 port 22
6444 2021-04-29 23:59:22.220 Connection from 192.168.1.17 port 53732 on 192.168.1.20 port 22
9124 2021-04-29 23:59:22.281 Connection from 192.168.1.17 port 53734 on 192.168.1.20 port 22
3560 2021-04-29 23:59:22.283 Connection from 192.168.1.17 port 53736 on 192.168.1.20 port 22
5788 2021-04-29 23:59:22.332 Connection from 192.168.1.17 port 53738 on 192.168.1.20 port 22
5788 2021-04-29 23:59:22.482 Unable to negotiate with 192.168.1.17 port 53738: no matching host key type found. Their offer: ssh-dss [preauth]
7260 2021-04-29 23:59:22.528 Connection from 192.168.1.17 port 53740 on 192.168.1.20 port 22
7260 2021-04-29 23:59:22.763 Connection closed by 192.168.1.17 port 53740 [preauth]
684 2021-04-29 23:59:22.817 Connection from 192.168.1.17 port 53742 on 192.168.1.20 port 22
684 2021-04-29 23:59:23.171 Connection closed by 192.168.1.17 port 53742 [preauth]
7860 2021-04-29 23:59:23.208 Connection from 192.168.1.17 port 53744 on 192.168.1.20 port 22
7860 2021-04-29 23:59:23.616 Unable to negotiate with 192.168.1.17 port 53744: no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
8016 2021-04-29 23:59:23.654 Connection from 192.168.1.17 port 53746 on 192.168.1.20 port 22
8016 2021-04-29 23:59:23.994 Unable to negotiate with 192.168.1.17 port 53746: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth]
3080 2021-04-29 23:59:24.044 Connection from 192.168.1.17 port 53748 on 192.168.1.20 port 22
3080 2021-04-29 23:59:24.385 Connection closed by 192.168.1.17 port 53748 [preauth]
8852 2021-04-30 00:00:54.504 Connection from 192.168.1.17 port 53896 on 192.168.1.20 port 22
8184 2021-04-30 00:00:54.532 Connection from 192.168.1.17 port 53898 on 192.168.1.20 port 22
8184 2021-04-30 00:00:55.187 debug3: checking match for 'Group administrators' user <username> host 192.168.1.17 addr 192.168.1.17 laddr 192.168.1.20 lport 22
```

The first request came at 2021-04-29 23:52:25.989 from attacker where he requests ssh from port 49338 with IP **192.168.1.17** to IP **192.168.1.20** on port 22. Looks like the **attack is internal** by looking the structure of IP address of the victim and attacker.

Takeaway:

1. Analysis of ssh log file.
2. Distinguish the level of log file.
3. How to separate valid and invalid users.