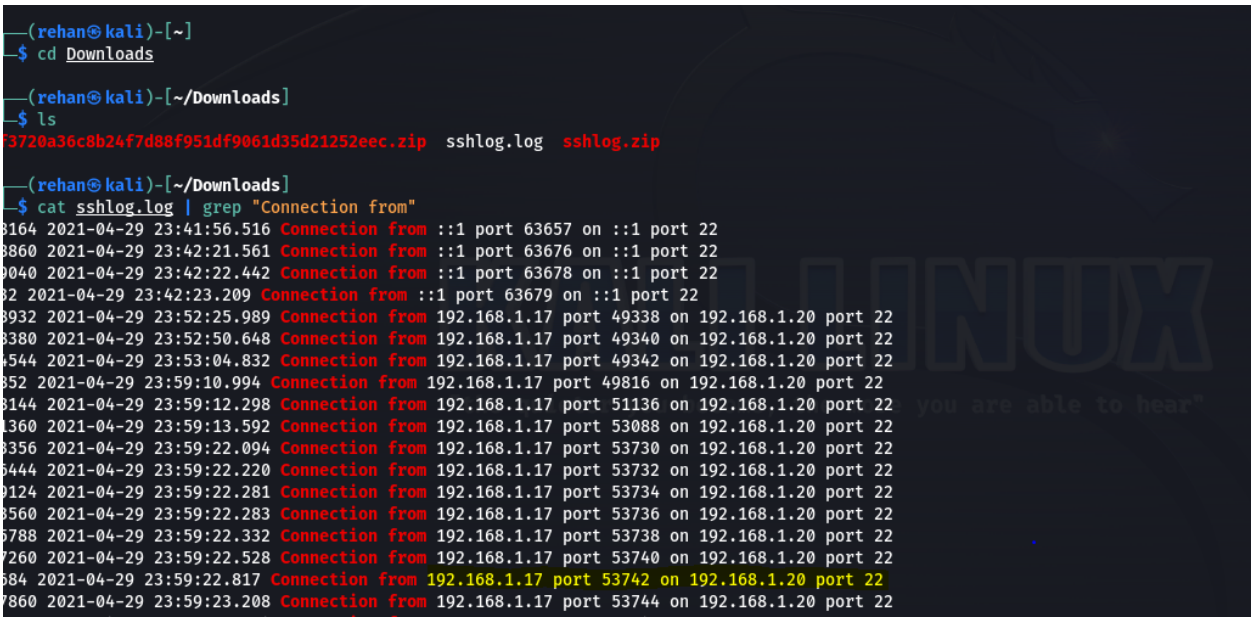
# BTLO –Secure Shell |Writeup

## Scenario:

Hey! We had a SSH service on a system and noticed unusual change in size of the log file. Don't panic, it was the new IT guys' daughter who said she was able to break into the system. I had given her permission to test some of these services. I am giving you the log file, can you solve the following queries?

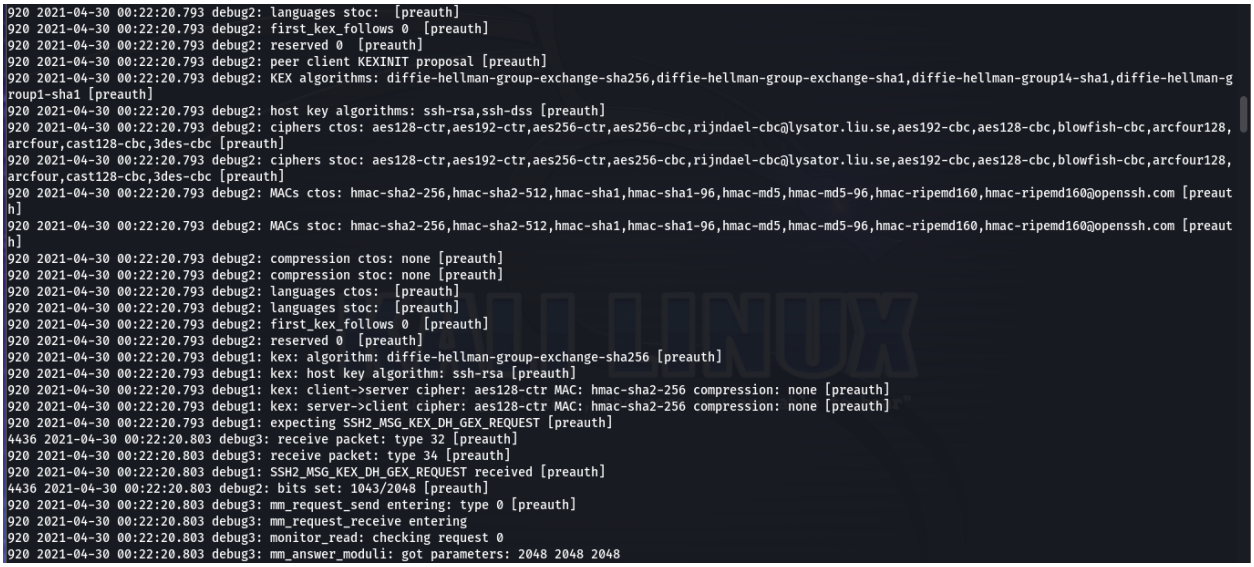
Is it an internal or external attack, what is the attacker IP?

Ans. . Internal:192.168.1.17



How many valid accounts did the attacker find, and what are the usernames?

Here's some of accounts attacker tried to logged in




Since lets grep the authenticated account attacker tries to use

The accounts deleted and didn’t exist anymore

```
┌──(rehan㉿kali)-[~/Downloads]
└─$ cat sshlog.log | grep "does not exist" | cut -d " " -f 13| sort -u

admin
chris
jake
janet
meghan
netadmin
not
root
sammy
sysadmin
test
user
<username>
web
webadmin
```

Ans. 1: Sophia

How many times did the attacker login to these accounts?

There’s  two successful attempts

```
┌──(rehan㉿kali)-[~/Downloads]
└─$ cat sshlog.log|grep "Accepted password"
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
```

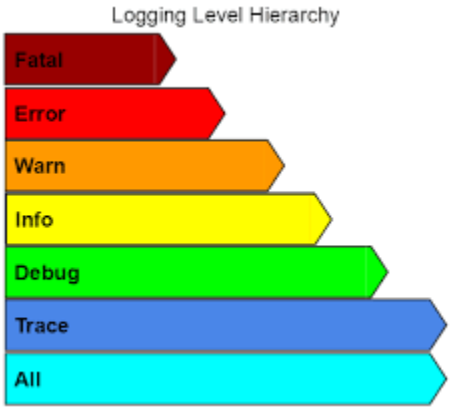
When was the first request from the attacker recorded?

The attacker first attempt  from internal ip  to talk with port 22

```
┌──(rehan㉿kali)-[~/Downloads]
└─$ cat sshlog.log|grep "Accepted password"
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

┌──(rehan㉿kali)-[~/Downloads]
└─$ cat sshlog.log|grep "Connection from"
8164 2021-04-29 23:41:56.516 Connection from ::1 port 63657 on ::1 port 22
8860 2021-04-29 23:42:21.561 Connection from ::1 port 63676 on ::1 port 22
9040 2021-04-29 23:42:22.442 Connection from ::1 port 63678 on ::1 port 22
32 2021-04-29 23:42:23.209 Connection from ::1 port 63679 on ::1 port 22
8932 2021-04-29 23:52:25.989 Connection from 192.168.1.17 port 49338 on 192.168.1.20 port 22
8380 2021-04-29 23:52:50.648 Connection from 192.168.1.17 port 49340 on 192.168.1.20 port 22
4544 2021-04-29 23:53:04.832 Connection from 192.168.1.17 port 49342 on 192.168.1.20 port 22
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
7260 2021-04-29 23:59:22.528 Connection from 192.168.1.17 port 53740 on 192.168.1.20 port 22
684 2021-04-29 23:59:22.817 Connection from 192.168.1.17 port 53742 on 192.168.1.20 port 22
```

What is the log level for the log file?




The log levels in the screen  like debug1, debug2, debug 3

```
8552 2021-04-30 00:52:15.196 debug3: mm_request_send entering: type 6 [preauth]
8552 2021-04-30 00:52:15.196 debug3: mm_sshkey_sign: waiting for MONITOR_ANS_SIGN [preauth]
8552 2021-04-30 00:52:15.196 debug3: mm_request_receive_expect entering: type 7 [preauth]
8552 2021-04-30 00:52:15.196 debug3: mm_request_receive entering [preauth]
8552 2021-04-30 00:52:15.196 debug3: mm_request_receive entering
8552 2021-04-30 00:52:15.197 debug3: monitor_read: checking request 6
8552 2021-04-30 00:52:15.197 debug3: mm_answer_sign
8552 2021-04-30 00:52:15.200 debug3: mm_answer_sign: KEX signature 000002083F3647C0(100)
8552 2021-04-30 00:52:15.200 debug3: mm_request_send entering: type 7
8552 2021-04-30 00:52:15.200 debug2: monitor_read: 6 used once, disabling now
8552 2021-04-30 00:52:15.200 debug3: send packet: type 31 [preauth]
8552 2021-04-30 00:52:15.200 debug3: send packet: type 21 [preauth]
8552 2021-04-30 00:52:15.200 debug2: set_newkeys: mode 1 [preauth]
8552 2021-04-30 00:52:15.200 debug1: rekey out after 4294967296 blocks [preauth]
8552 2021-04-30 00:52:15.200 debug1: SSH2_MSG_NEWKEYS sent [preauth]
8552 2021-04-30 00:52:15.200 debug1: Sending SSH2_MSG_EXT_INFO [preauth]
8552 2021-04-30 00:52:15.200 debug3: send packet: type 7 [preauth]
8552 2021-04-30 00:52:15.200 debug1: expecting SSH2_MSG_NEWKEYS [preauth]
8552 2021-04-30 00:52:15.201 debug3: receive packet: type 21 [preauth]
8552 2021-04-30 00:52:15.201 debug1: SSH2_MSG_NEWKEYS received [preauth]
8552 2021-04-30 00:52:15.201 debug2: set_newkeys: mode 0 [preauth]
8552 2021-04-30 00:52:15.201 debug1: rekey in after 4294967296 blocks [preauth]
8552 2021-04-30 00:52:15.201 debug1: KEX done [preauth]
8552 2021-04-30 00:52:15.252 debug3: receive packet: type 5 [preauth]
8552 2021-04-30 00:52:15.252 debug3: send packet: type 6 [preauth]
8552 2021-04-30 00:52:15.252 debug3: receive packet: type 50 [preauth]
8552 2021-04-30 00:52:15.252 debug1: userauth-request for user sophia service ssh-connection method none [preauth]
8552 2021-04-30 00:52:15.252 debug1: attempt 0 failures 0 [preauth]
8552 2021-04-30 00:52:15.252 debug3: mm_getpwnamallow entering [preauth]
8552 2021-04-30 00:52:15.252 debug3: mm_request_send entering: type 8 [preauth]
8552 2021-04-30 00:52:15.252 debug3: mm_getpwnamallow: waiting for MONITOR_ANS_PWNAM [preauth]
8552 2021-04-30 00:52:15.252 debug3: mm_request_receive_expect entering: type 9 [preauth]
8552 2021-04-30 00:52:15.252 debug3: mm_request_receive entering [preauth]
```

Since  Debug

Where is the log file located in Windows?

Lets search deeply with Microsoft documentation

## SyslogFacility

If you need file based logging, use LOCAL0. Logs are generated under *%programdata%\ssh\logs*. For any other value, including the default value, AUTH directs logging to ETW. For more info, see Logging Facilities in Windows.