ICS 344

TERM 242

TEAM PROJECT

GROUP 7

Mohammed Al Lail => ID/202152850

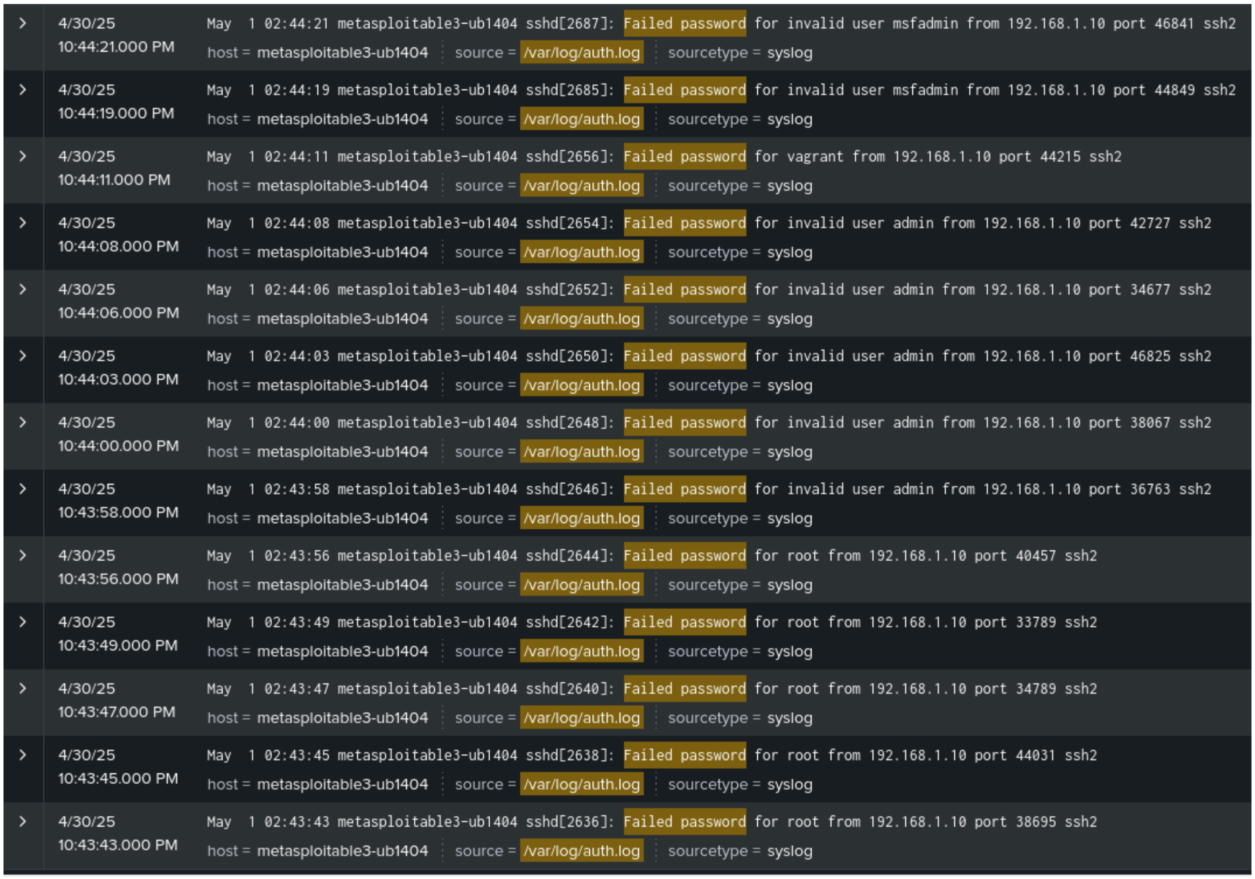
Ali Almatar => ID/202158190

Hassan Al Nasser => ID/202163950

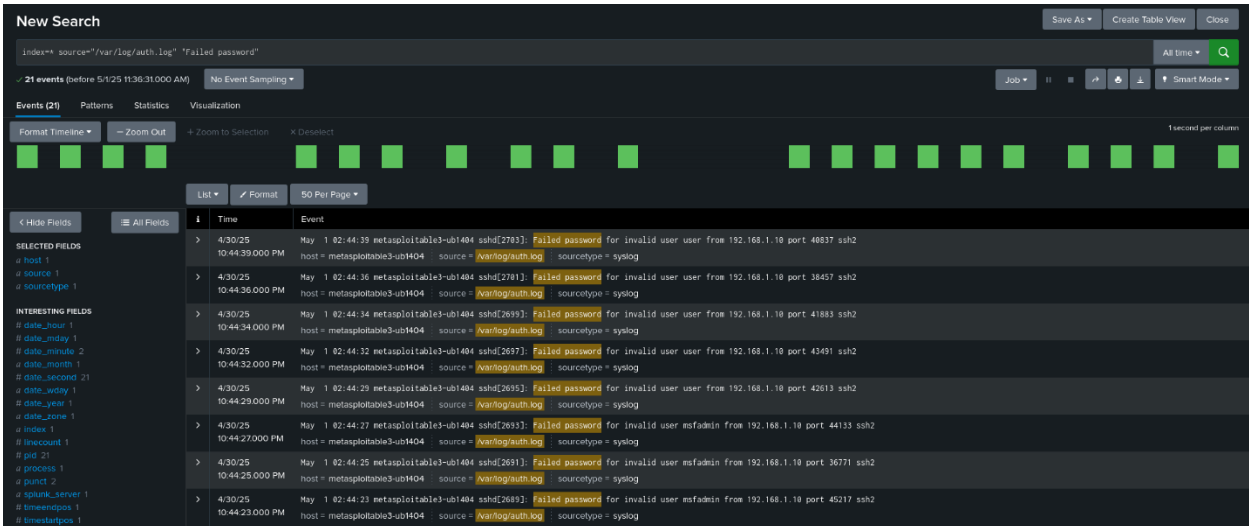
Phase 2

Logs

- Attacker
  - Failed passwords



```
> 4/30/25      May  1 02:44:21 metasploitable3-ub1404 sshd[2687]: Failed password for invalid user msfadmin from 192.168.1.10 port 46841 ssh2
  10:44:21.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:19 metasploitable3-ub1404 sshd[2685]: Failed password for invalid user msfadmin from 192.168.1.10 port 44849 ssh2
  10:44:19.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:11 metasploitable3-ub1404 sshd[2656]: Failed password for vagrant from 192.168.1.10 port 44215 ssh2
  10:44:11.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:08 metasploitable3-ub1404 sshd[2654]: Failed password for invalid user admin from 192.168.1.10 port 42727 ssh2
  10:44:08.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:06 metasploitable3-ub1404 sshd[2652]: Failed password for invalid user admin from 192.168.1.10 port 34677 ssh2
  10:44:06.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:03 metasploitable3-ub1404 sshd[2650]: Failed password for invalid user admin from 192.168.1.10 port 46825 ssh2
  10:44:03.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:44:00 metasploitable3-ub1404 sshd[2648]: Failed password for invalid user admin from 192.168.1.10 port 38067 ssh2
  10:44:00.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:58 metasploitable3-ub1404 sshd[2646]: Failed password for invalid user admin from 192.168.1.10 port 36763 ssh2
  10:43:58.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:56 metasploitable3-ub1404 sshd[2644]: Failed password for root from 192.168.1.10 port 40457 ssh2
  10:43:56.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:49 metasploitable3-ub1404 sshd[2642]: Failed password for root from 192.168.1.10 port 33789 ssh2
  10:43:49.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:47 metasploitable3-ub1404 sshd[2640]: Failed password for root from 192.168.1.10 port 34789 ssh2
  10:43:47.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:45 metasploitable3-ub1404 sshd[2638]: Failed password for root from 192.168.1.10 port 44031 ssh2
  10:43:45.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25      May  1 02:43:43 metasploitable3-ub1404 sshd[2636]: Failed password for root from 192.168.1.10 port 38695 ssh2
  10:43:43.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
```

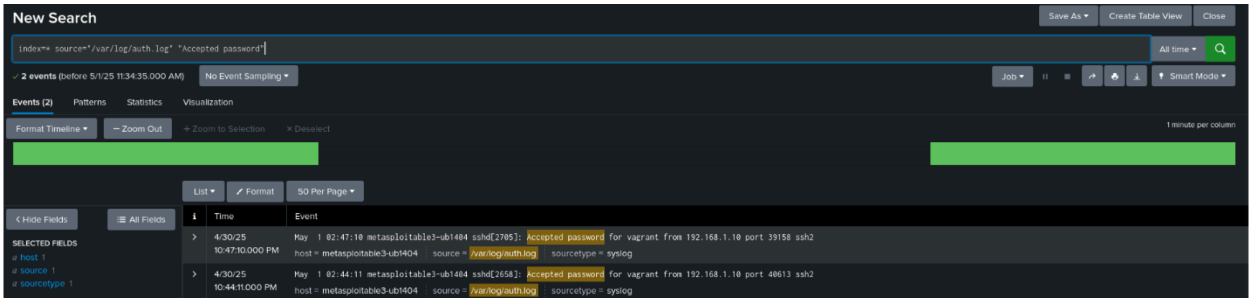


```
index=* source="/var/log/auth.log" "Failed password"
```

✓ 21 events (before 5/1/25 11:36:31.000 AM)

```
i  Time            Event
> 4/30/25          May  1 02:44:39 metasploitable3-ub1404 sshd[2703]: Failed password for invalid user user from 192.168.1.10 port 40837 ssh2
  10:44:39.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:36 metasploitable3-ub1404 sshd[2701]: Failed password for invalid user user from 192.168.1.10 port 38457 ssh2
  10:44:36.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:34 metasploitable3-ub1404 sshd[2699]: Failed password for invalid user user from 192.168.1.10 port 41883 ssh2
  10:44:34.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:32 metasploitable3-ub1404 sshd[2697]: Failed password for invalid user user from 192.168.1.10 port 43491 ssh2
  10:44:32.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:29 metasploitable3-ub1404 sshd[2695]: Failed password for invalid user user from 192.168.1.10 port 42613 ssh2
  10:44:29.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:27 metasploitable3-ub1404 sshd[2693]: Failed password for invalid user msfadmin from 192.168.1.10 port 44133 ssh2
  10:44:27.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:25 metasploitable3-ub1404 sshd[2691]: Failed password for invalid user msfadmin from 192.168.1.10 port 36771 ssh2
  10:44:25.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
> 4/30/25          May  1 02:44:23 metasploitable3-ub1404 sshd[2689]: Failed password for invalid user msfadmin from 192.168.1.10 port 45217 ssh2
  10:44:23.000 PM  host = metasploitable3-ub1404 | source = /var/log/auth.log | sourcetype = syslog
```

- Accepted passwords



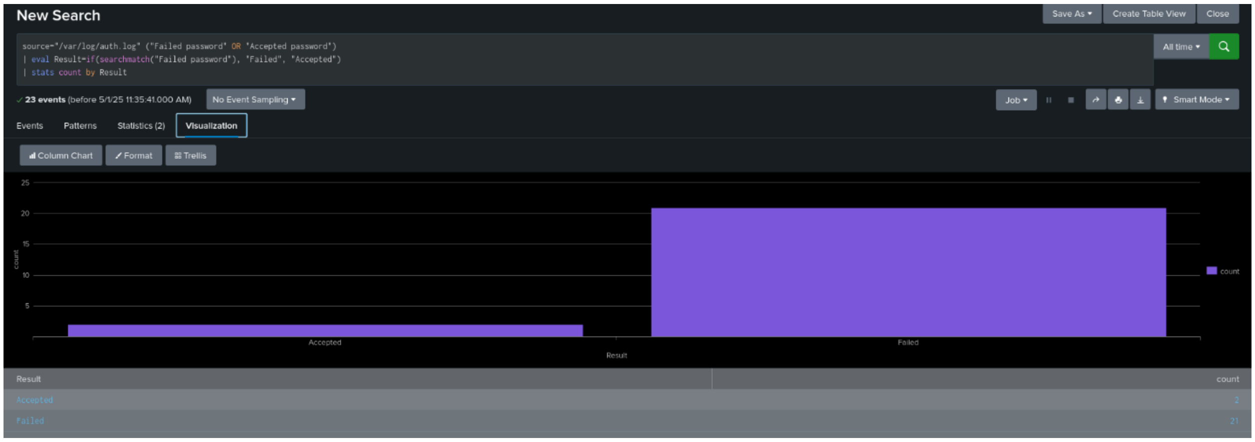
```
index=* source="/var/log/auth.log" "Accepted password"
```

✓ 2 events (before 5/1/25 11:34:35.000 AM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

i	Time	Event
>	4/30/25 10:47:10.000 PM	May 1 02:47:10 metasploitable3-ub1404 sshd[2705]: Accepted password for vagrant from 192.168.1.10 port 39158 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:11.000 PM	May 1 02:44:11 metasploitable3-ub1404 sshd[2658]: Accepted password for vagrant from 192.168.1.10 port 40613 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

- Visualization

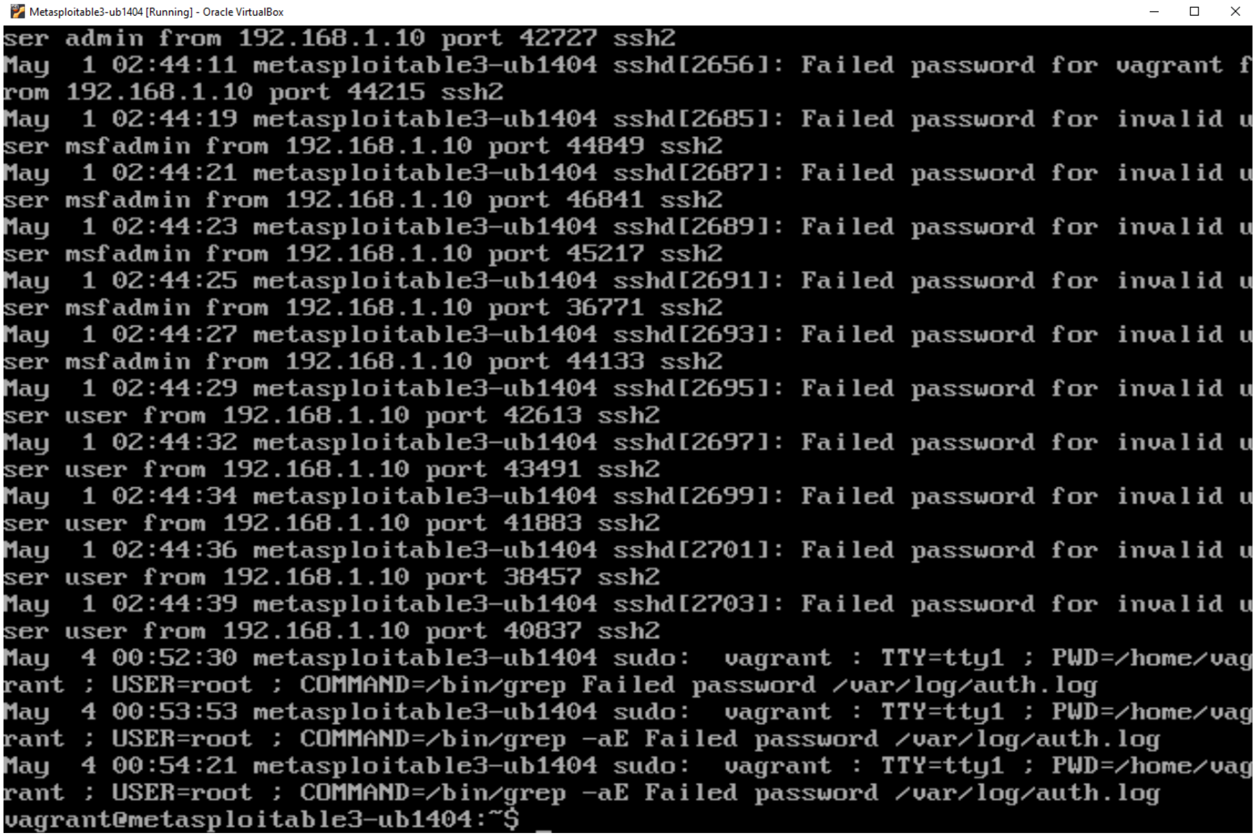


```
source="/var/log/auth.log" ("Failed password" OR "Accepted password")
| eval Result=if(searchmatch("Failed password"), "Failed", "Accepted")
| stats count by Result
```

✓ 23 events (before 5/1/25 11:35:41.000 AM)

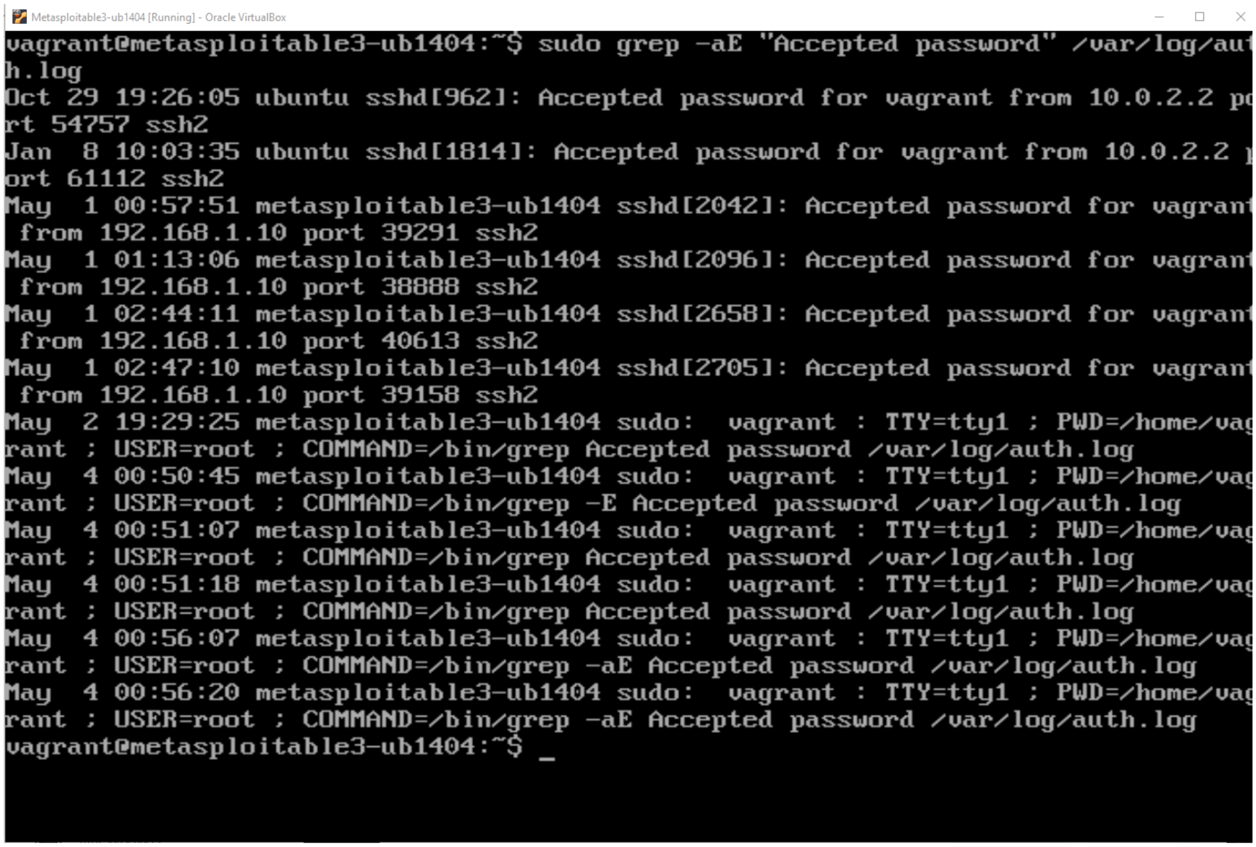
Result	count
Accepted	2
Failed	21

- **Victim**
  - Failed passwords



```
ser admin from 192.168.1.10 port 42727 ssh2
May  1 02:44:11 metasploitable3-ub1404 sshd[2656]: Failed password for vagrant f
rom 192.168.1.10 port 44215 ssh2
May  1 02:44:19 metasploitable3-ub1404 sshd[2685]: Failed password for invalid u
ser msfadmin from 192.168.1.10 port 44849 ssh2
May  1 02:44:21 metasploitable3-ub1404 sshd[2687]: Failed password for invalid u
ser msfadmin from 192.168.1.10 port 46841 ssh2
May  1 02:44:23 metasploitable3-ub1404 sshd[2689]: Failed password for invalid u
ser msfadmin from 192.168.1.10 port 45217 ssh2
May  1 02:44:25 metasploitable3-ub1404 sshd[2691]: Failed password for invalid u
ser msfadmin from 192.168.1.10 port 36771 ssh2
May  1 02:44:27 metasploitable3-ub1404 sshd[2693]: Failed password for invalid u
ser msfadmin from 192.168.1.10 port 44133 ssh2
May  1 02:44:29 metasploitable3-ub1404 sshd[2695]: Failed password for invalid u
ser user from 192.168.1.10 port 42613 ssh2
May  1 02:44:32 metasploitable3-ub1404 sshd[2697]: Failed password for invalid u
ser user from 192.168.1.10 port 43491 ssh2
May  1 02:44:34 metasploitable3-ub1404 sshd[2699]: Failed password for invalid u
ser user from 192.168.1.10 port 41883 ssh2
May  1 02:44:36 metasploitable3-ub1404 sshd[2701]: Failed password for invalid u
ser user from 192.168.1.10 port 38457 ssh2
May  1 02:44:39 metasploitable3-ub1404 sshd[2703]: Failed password for invalid u
ser user from 192.168.1.10 port 40837 ssh2
May  4 00:52:30 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep Failed password /var/log/auth.log
May  4 00:53:53 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep -aE Failed password /var/log/auth.log
May  4 00:54:21 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep -aE Failed password /var/log/auth.log
vagrant@metasploitable3-ub1404:~$ _
```

- Accepted passwords



```
vagrant@metasploitable3-ub1404:~$ sudo grep -aE "Accepted password" /var/log/aut
h.log
Oct 29 19:26:05 ubuntu sshd[962]: Accepted password for vagrant from 10.0.2.2 po
rt 54757 ssh2
Jan  8 10:03:35 ubuntu sshd[1814]: Accepted password for vagrant from 10.0.2.2 p
ort 61112 ssh2
May  1 00:57:51 metasploitable3-ub1404 sshd[2042]: Accepted password for vagrant
 from 192.168.1.10 port 39291 ssh2
May  1 01:13:06 metasploitable3-ub1404 sshd[2096]: Accepted password for vagrant
 from 192.168.1.10 port 38888 ssh2
May  1 02:44:11 metasploitable3-ub1404 sshd[2658]: Accepted password for vagrant
 from 192.168.1.10 port 40613 ssh2
May  1 02:47:10 metasploitable3-ub1404 sshd[2705]: Accepted password for vagrant
 from 192.168.1.10 port 39158 ssh2
May  2 19:29:25 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep Accepted password /var/log/auth.log
May  4 00:50:45 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep -E Accepted password /var/log/auth.log
May  4 00:51:07 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep Accepted password /var/log/auth.log
May  4 00:51:18 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep Accepted password /var/log/auth.log
May  4 00:56:07 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep -aE Accepted password /var/log/auth.log
May  4 00:56:20 metasploitable3-ub1404 sudo:  vagrant : TTY=tty1 ; PWD=/home/vag
rant ; USER=root ; COMMAND=/bin/grep -aE Accepted password /var/log/auth.log
vagrant@metasploitable3-ub1404:~$ _
```