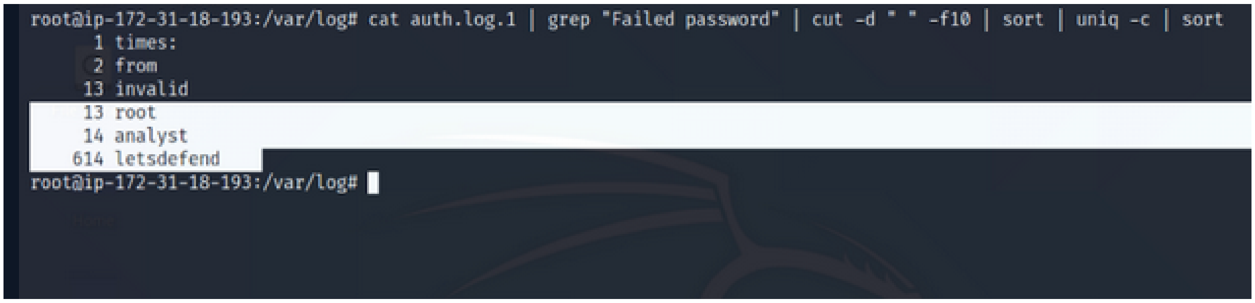
SSH Brute Force Attacks

By: Ryan Stewart

Attackers attempting SSH brute force attacks often target servers with **simple passwords.** Detecting such attacks involves analyzing server logs, such as the "auth.log.1" file on a Linux machine. The following commands demonstrate how to identify failed and successful login attempts:

1. **Identifying Failed Login Attempts:**

```
cat auth.log.1 | grep "Failed password" | cut -d " " -f10 | sort | uniq -c | sort
```



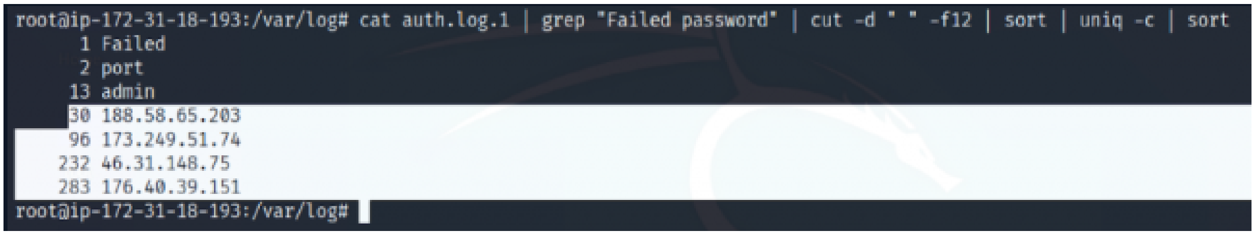
```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Failed password" | cut -d " " -f10 | sort | uniq -c | sort
      1 times:
      2 from
     13 invalid
     13 root
     14 analyst
    614 letsdefend
root@ip-172-31-18-193:/var/log#
```

This command extracts **failed login attempts** from the log, displaying the usernames along with the number of occurrences. It provides insights into which users are targeted.

2. **Locating IP Addresses of Failed Attempts:**

```
cat auth.log.1 | grep "Failed password" | cut -d " " -f12 | sort | uniq -c | sort

```

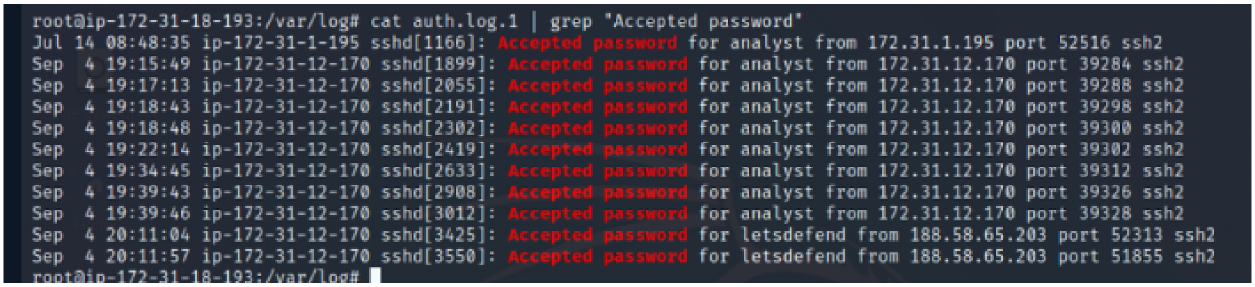


```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Failed password" | cut -d " " -f12 | sort | uniq -c | sort
      1 Failed
      2 port
     13 admin
     30 188.58.65.203
     96 173.249.51.74
    232 46.31.148.75
    283 176.40.39.151
root@ip-172-31-18-193:/var/log# 
```

This command focuses on identifying the IP addresses associated with the failed attempts, aiding in pinpointing the source of the attacks.

3. **Detecting Successful Logins:**

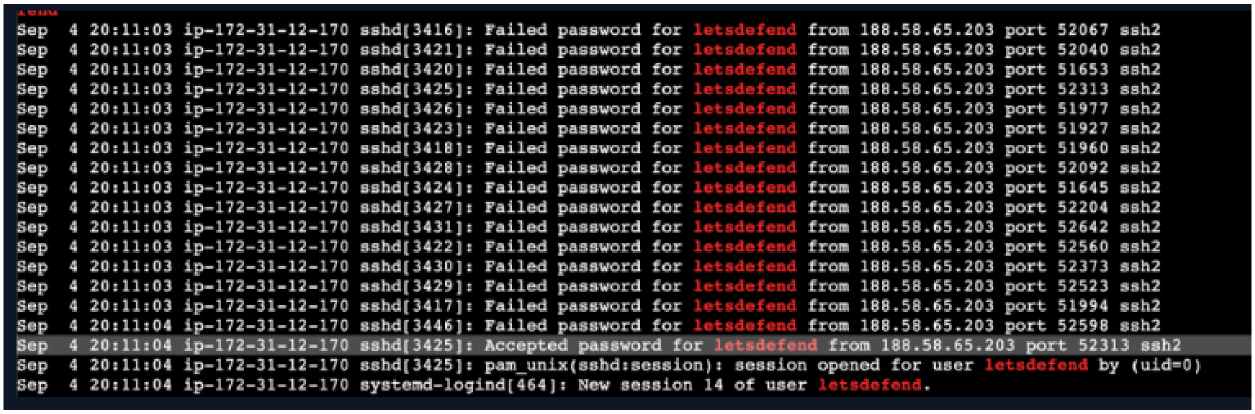
```
cat auth.log.1 | grep "Accepted password" ```



```
root@ip-172-31-18-193:/var/log# cat auth.log.1 | grep "Accepted password"
Jul 14 08:48:35 ip-172-31-1-195 sshd[1166]: Accepted password for analyst from 172.31.1.195 port 52516 ssh2
Sep  4 19:15:49 ip-172-31-12-170 sshd[1899]: Accepted password for analyst from 172.31.12.170 port 39284 ssh2
Sep  4 19:17:13 ip-172-31-12-170 sshd[2055]: Accepted password for analyst from 172.31.12.170 port 39288 ssh2
Sep  4 19:18:43 ip-172-31-12-170 sshd[2191]: Accepted password for analyst from 172.31.12.170 port 39298 ssh2
Sep  4 19:18:48 ip-172-31-12-170 sshd[2302]: Accepted password for analyst from 172.31.12.170 port 39300 ssh2
Sep  4 19:22:14 ip-172-31-12-170 sshd[2419]: Accepted password for analyst from 172.31.12.170 port 39302 ssh2
Sep  4 19:34:45 ip-172-31-12-170 sshd[2633]: Accepted password for analyst from 172.31.12.170 port 39312 ssh2
Sep  4 19:39:43 ip-172-31-12-170 sshd[2908]: Accepted password for analyst from 172.31.12.170 port 39326 ssh2
Sep  4 19:39:46 ip-172-31-12-170 sshd[3012]: Accepted password for analyst from 172.31.12.170 port 39328 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: Accepted password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:57 ip-172-31-12-170 sshd[3550]: Accepted password for letsdefend from 188.58.65.203 port 51855 ssh2
root@ip-172-31-18-193:/var/log# 
```

This command identifies users who successfully logged in, allowing a comprehensive view of both successful and unsuccessful attempts.

In a practical scenario, comparing the results reveals crucial information. For instance, a user like "analyst" may not have experienced unsuccessful login attempts before successfully logging in. On the other hand, the "letsdefend" user, associated with the IP address 188.58.65.203, had numerous unsuccessful attempts before a successful login. This suggests a successful brute force attack on the "letsdefend" user.
```



```
Sep  4 20:11:03 ip-172-31-12-170 sshd[3416]: Failed password for letsdefend from 188.58.65.203 port 52067 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3421]: Failed password for letsdefend from 188.58.65.203 port 52040 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3420]: Failed password for letsdefend from 188.58.65.203 port 51653 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3425]: Failed password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3426]: Failed password for letsdefend from 188.58.65.203 port 51977 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3423]: Failed password for letsdefend from 188.58.65.203 port 51927 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3418]: Failed password for letsdefend from 188.58.65.203 port 51960 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3428]: Failed password for letsdefend from 188.58.65.203 port 52092 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3424]: Failed password for letsdefend from 188.58.65.203 port 51645 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3427]: Failed password for letsdefend from 188.58.65.203 port 52204 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3431]: Failed password for letsdefend from 188.58.65.203 port 52642 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3422]: Failed password for letsdefend from 188.58.65.203 port 52560 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3430]: Failed password for letsdefend from 188.58.65.203 port 52373 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3429]: Failed password for letsdefend from 188.58.65.203 port 52523 ssh2
Sep  4 20:11:03 ip-172-31-12-170 sshd[3417]: Failed password for letsdefend from 188.58.65.203 port 51994 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3446]: Failed password for letsdefend from 188.58.65.203 port 52598 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: Accepted password for letsdefend from 188.58.65.203 port 52313 ssh2
Sep  4 20:11:04 ip-172-31-12-170 sshd[3425]: pam_unix(sshd:session): session opened for user letsdefend by (uid=0)
Sep  4 20:11:04 ip-172-31-12-170 systemd-logind[464]: New session 14 of user letsdefend.
```

In summary, using basic Linux commands to analyze logs can swiftly unveil patterns of failed and successful login attempts, aiding in the early detection of SSH brute force attacks and identification of compromised accounts.