Linux – Brute Force Attack Detection

Problem: identify failed password login attempts.

Goal: find and extract failed login attempts from auth log file.

Process:

- Find columns with ‘failed password’ values in auth log
- Exclude ‘invalid’ user accounts
- Grab month, date, time, user, and source IP address fields
- Filtered Result:

```
steven@DESKTOP-6KVS52N:/mnt/c/Users/steven/Desktop/Brutus$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4,10,12
Mar  6 06:31:33 backup 65.2.161.68
Mar  6 06:31:33 backup 65.2.161.68
Mar  6 06:31:34 backup 65.2.161.68
Mar  6 06:31:34 backup 65.2.161.68
Mar  6 06:31:34 backup 65.2.161.68
Mar  6 06:31:34 backup 65.2.161.68
Mar  6 06:31:36 backup 65.2.161.68
Mar  6 06:31:39 root 65.2.161.68
Mar  6 06:31:39 root 65.2.161.68
Mar  6 06:31:39 root 65.2.161.68
Mar  6 06:31:41 root 65.2.161.68
Mar  6 06:31:41 root 65.2.161.68
Mar  6 06:31:41 root 65.2.161.68
Mar  6 06:31:42 backup 65.2.161.68
Mar  6 06:31:42 backup 65.2.161.68
```