# BASH Lab 6 Practical Uses

You manage your Ubuntu server remotely using SSH. As a result, it receives constant brute force password guessing attacks from the Internet. We will use simple BASH scripts to analyze the log file from the server. Moodle should have a file, auth.log, which is an actual log from a honeypot provided by Johannes Ulrich from the SANS Internet Storm Center.

WARNING: Bad guys are constantly scanning the Internet for open SSH ports that have poor passwords. If you put your home computer on SSH with poor passwords it will probably be compromised. The best solution is to configure your home SSH to only accept login by digital certificates (in /etc/ssh/sshd\_config, set PasswordAuthentication no<https://www.linux.org/threads/how-to-force-ssh-login-via-public-key-authentication.8726/>

## Hand in

Answer the questions in blue.

## Failed SSH Login

You can either use the technique from BASH module 5, Practical Uses, slides 4 and 5, or just use cut, sort, uniq -c and sort -nr in this lab. I think they used a for loop in the slides just to give you practice. Your job is to determine how many login attempts were made against valid users. Note: Since our log is from Ubuntu instead of CentOS, the format is different from the slides.

Helpful information:

1. All SSH log entries contain sshd
2. When someone has tried times against a valid user, the log message looks like this:  
    “Disconnecting: Too many authentication failures for root”  
   where root was the user under attack.

How many attempts were made against valid users? Note that there are other users besides root, so don’t include root in your search.

How many valid users were attacked?

## Failed SSH Login invalid users

When there is an attempt against a user that does not exist on the server, there are two log messages. One looks like this:   
“input\_userauth\_request: invalid user pi”.  
The other looks like this:  
“Invalid user pi from 52.26.219.151”.  
You can use either line in your search. List the user names the attacker is attempting to use.

What user names did the attacker try?

## Where are the attacks coming from?

For this one, you have to use “Invalid user pi from 52.26.219.151”.

What are the IP addresses that are attacking the server?