1. **Change your user to another (for example from regular user to root) and input a wrong password. How and from what log file in /var/log path you can retrieve the information from this failed login attempt?**

```
user@AC4892-Ubuntu:~$ su
Password:
3su: Authentication failure
```

```
user@AC4892-Ubuntu:~$ cat /var/log/auth.log
```

```
Nov 23 20:05:13 AC4892-Ubuntu su: pam_unix(su:auth): authentication failure; logname=user uid=1000 euid=0 tty=pts/0 ruse
r=user rhost=  user=root
Nov 23 20:05:15 AC4892-Ubuntu su: FAILED SU (to root) user on pts/0
```

2. **How do you retrieve the logged information from journald from last 24 hours so that newest entries are displayed first (at the top)?**

```
user@AC4892-Ubuntu:~$ journalctl --since="24 hours ago" -r
```

```
-- Logs begin at Wed 2022-10-19 01:46:19 EEST, end at Wed 2022-11-23 21:09:38 EET. --
Nov 23 21:09:38 AC4892-Ubuntu multipathd[36461]: sda: failed to get sgio uid: No such file or directory
Nov 23 21:09:38 AC4892-Ubuntu multipathd[36461]: sda: failed to get sysfs uid: Invalid argument
Nov 23 21:09:38 AC4892-Ubuntu multipathd[36461]: sda: failed to get udev uid: Invalid argument
Nov 23 21:09:38 AC4892-Ubuntu multipathd[36461]: sda: add missing path
Nov 23 21:09:33 AC4892-Ubuntu multipathd[36461]: sda: failed to get sgio uid: No such file or directory
Nov 23 21:09:33 AC4892-Ubuntu multipathd[36461]: sda: failed to get sysfs uid: Invalid argument
Nov 23 21:09:33 AC4892-Ubuntu multipathd[36461]: sda: failed to get udev uid: Invalid argument
Nov 23 21:09:33 AC4892-Ubuntu multipathd[36461]: sda: add missing path
Nov 23 21:09:28 AC4892-Ubuntu multipathd[36461]: sda: failed to get sgio uid: No such file or directory
Nov 23 21:09:28 AC4892-Ubuntu multipathd[36461]: sda: failed to get sysfs uid: Invalid argument
```

3. **How much do stored journal files take up disk space?**

```
user@AC4892-Ubuntu:~$ journalctl --disk-usage
Archived and active journals take up 1.5G in the file system.
user@AC4892-Ubuntu:~$
```

4. **Open journald for real-time logging. Now open SSH connection to your Ubuntu (refer to Putty guide in here). Try to login by typing first the invalid and then the correct password. How are these entries logged?**

When inserting wrong password

```
user@AC4892-Ubuntu:~$ journalctl -f
```

```
login as: user
user@172.21.6.28's password:
Access denied
user@172.21.6.28's password:
```

```
Nov 23 21:42:54 AC4892-Ubuntu multipathd[36461]: sda: add missing path
Nov 23 21:42:54 AC4892-Ubuntu multipathd[36461]: sda: failed to get udev uid: Invalid argument
Nov 23 21:42:54 AC4892-Ubuntu multipathd[36461]: sda: failed to get sysfs uid: Invalid argument
Nov 23 21:42:54 AC4892-Ubuntu multipathd[36461]: sda: failed to get sgio uid: No such file or directory
Nov 23 21:42:59 AC4892-Ubuntu multipathd[36461]: sda: add missing path
Nov 23 21:42:59 AC4892-Ubuntu multipathd[36461]: sda: failed to get udev uid: Invalid argument
Nov 23 21:42:59 AC4892-Ubuntu multipathd[36461]: sda: failed to get sysfs uid: Invalid argument
Nov 23 21:42:59 AC4892-Ubuntu multipathd[36461]: sda: failed to get sgio uid: No such file or directory
Nov 23 21:43:04 AC4892-Ubuntu multipathd[36461]: sda: add missing path
```

When giving the correct password

```
Nov 23 21:46:00 AC4892-Ubuntu sshd[240025]: Accepted password for user from 192.168.53.44 port 52004 ssh2
Nov 23 21:46:00 AC4892-Ubuntu sshd[240025]: pam_unix(sshd:session): session opened for user user by (uid=0)
Nov 23 21:46:00 AC4892-Ubuntu systemd[1]: Started Session 185 of user user.
Nov 23 21:46:00 AC4892-Ubuntu systemd-logind[825]: New session 185 of user user.
```

5. **Open authentication log file (auth.log) and check the content. How can you print only lines from this log file to the CLI containing new sessions from your user (tip: use grep)?**

```
user@AC4892-Ubuntu:~$ cat /var/log/auth.log | grep uid=0
```

6. **In previous exercise (EX-11) you installed Apache2 web server (if you haven't, install it with sudo apt install apache2). What log files does this service have (see /var/log directory)?**