Assignment 01

1. What is the command to determine the kernel version of your OS? Please write the command and its output.

```
ubuntu@primary:~$ uname -v
#63-Ubuntu SMP Thu Nov 24 13:48:31 UTC 2022
```

2. What is the command to determine the current user logged in? Please write the command and its output.

```
ubuntu@primary:~$ whoami
ubuntu
```

3. What is the Linux command or commands to list all user accounts on a Linux system? ONLY user account names should be shown!

```
ubuntu@primary:~$ awk -F: '{print $1}' /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-network
systemd-resolve
messagebus
systemd-timesync
syslog
_apt
tss
```

```
uuidd
tcpdump
sshd
pollinate
landscape
fwupd-refresh
ubuntu
lxd
```

4. Using your answer from the previous question, what would be the command or commands to show the the list of users as a comma separated list.

i. You may need to use the | (pipe command) to link two commands together.

```
ubuntu@primary:~$ awk -v ORS=',' -F: '{print $1}' /etc/passwd
root,daemon,bin,sys,sync,games,man,lp,mail,news,uucp,proxy,www-
data,backup,list,irc,gnats,nobody,systemd-network,systemd-
resolve,messagebus,systemd-
timesync,syslog,_apt,tss,uuidd,tcpdump,sshd,pollinate,landscape,fwupd-
refresh,ubuntu,lxd,
```

5. What is the command or commands that will show you the last 15 lines of the /var/log/kern.log file? Please write the commands and copy the output.

a. If your system does not have a kern.log, simply print which ever file in your system stores system logs.
b. Note, WSL2 may not have a kern.log file at all.

```
ubuntu@primary:~$ tail -15 /var/log/kern.log
Feb 11 23:56:12 primary kernel: [    5.146678] audit: type=1400
audit(1676188568.472:15): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="/snap/snapd/17885/usr/lib/snapd/snap-confine" pid=542
comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.146681] audit: type=1400
audit(1676188568.472:16): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="/snap/snapd/17885/usr/lib/snapd/snap-confine//mount-
namespace-capture-helper" pid=542 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.155333] audit: type=1400
audit(1676188568.484:17): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="/snap/snapd/17954/usr/lib/snapd/snap-confine" pid=543
comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.155338] audit: type=1400
audit(1676188568.484:18): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="/snap/snapd/17954/usr/lib/snapd/snap-confine//mount-
namespace-capture-helper" pid=543 comm="apparmor_parser"
```

```
Feb 11 23:56:12 primary kernel: [    5.158835] audit: type=1400
audit(1676188568.484:19): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap-update-ns.lxd" pid=544 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.162826] audit: type=1400
audit(1676188568.488:20): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap-update-ns.multipass-sshfs" pid=545
comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.173914] audit: type=1400
audit(1676188568.500:21): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap.lxd.activate" pid=546 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.183175] audit: type=1400
audit(1676188568.512:22): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap.lxd.benchmark" pid=547 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.191085] audit: type=1400
audit(1676188568.520:23): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap.lxd.buginfo" pid=548 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    5.217079] audit: type=1400
audit(1676188568.544:24): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="snap.lxd.check-kernel" pid=549 comm="apparmor_parser"
Feb 11 23:56:12 primary kernel: [    7.323093] random: crng init done
Feb 11 23:56:12 primary kernel: [    7.323107] random: 241 urandom warning(s)
missed due to ratelimiting
Feb 11 23:56:12 primary kernel: [    7.417164] ISO 9660 Extensions: Microsoft
Joliet Level 3
Feb 11 23:56:12 primary kernel: [    7.417279] ISOFS: changing to secondary root
Feb 11 23:56:15 primary kernel: [   11.773401] loop8: detected capacity change from
0 to 8
```

6. What is the command or commands that will show you all the login attempts for your username? Please write the commands and copy the output.

The `-u` argument specifies the user. This user's name is `ubuntu`.

```
ubuntu@primary:~$ lastlog -u ubuntu
Username         Port     From             Latest
ubuntu           pts/0    192.168.64.1     Sat Feb 11 15:12:07 -0800 2023
```

7. Using the dmesg command, show only the messages relating to warnings and errors. Also ensure the output is using a human readable time format. To verify that only error and warning messages are being show what option of dmesg would you use? Show both commands that were used.

- `-H` to enable human-readable output.
- `-x` to "verify that only error and warning messages are being [shown]."

- `-l` with argument `warn,err` to “show only the messages relating to warnings and errors.”

```
ubuntu@primary:~$ sudo dmesg -Hx -l warn,err
kern  :warn  : [Feb 9 18:45] ACPI: SRAT not present
kern  :warn  : [  +0.000000] KASLR disabled due to lack of seed
kern  :warn  : [  +0.123766] SPI driver altr_a10sr has no spi_device_id for
altr,a10sr
kern  :warn  : [  +0.002636] device-mapper: core: CONFIG_IMA_DISABLE_HTABLE is
disabled. Duplicate IMA measurements will not be recorded in the IMA lo>
kern  :warn  : [  +0.455917] sd 0:0:0:0: Power-on or device reset occurred
kern  :warn  : [  +0.010839] GPT:Primary header thinks Alt. header is not at the
end of the disk.
kern  :warn  : [  +0.000202] GPT:4612095 != 10485759
kern  :warn  : [  +0.000093] GPT:Alternate GPT header not at the end of the disk.
kern  :warn  : [  +0.000160] GPT:4612095 != 10485759
kern  :warn  : [  +0.000093] GPT: Use GNU Parted to correct GPT errors.
kern  :warn  : [ +25.082931] kauditd_printk_skb: 19 callbacks suppressed
kern  :warn  : [Feb10 01:31] kauditd_printk_skb: 24 callbacks suppressed
kern  :warn  : [Feb10 08:48] hrtimer: interrupt took 40848802 ns
```

Example without the `-l` argument to specify level. First few lines shows that the logs are of `info` and `notice` levels. Output truncated for brevity.

```
ubuntu@primary:~$ sudo dmesg -Hx
kern  :info  : [Feb 9 18:45] Booting Linux on physical CPU 0x0000000000
[0x410fd083]
kern  :notice: [  +0.000000] Linux version 5.15.0-57-generic (buildd@bos02-arm64-
057) (gcc (Ubuntu 11.3.0-1ubuntu1~22.04) 11.3.0, GNU ld (GNU Binutils>
kern  :info  : [  +0.000000] efi: EFI v2.70 by EDK II
kern  :info  : [  +0.000000] efi: SMBIOS 3.0=0x7f700000 MEMATTR=0x7cf05698 ACPI
2.0=0x7bf70018 MOKvar=0x7ceef000 MEMRESERVE=0x7c371118
kern  :info  : [  +0.000000] secureboot: Secure boot disabled
kern  :info  : [  +0.000000] ACPI: Early table checksum verification disabled
```

8. What command would you use to display free disk space? List the command and its output.

```
ubuntu@primary:~$ df -h
Filesystem        Size  Used Avail Use% Mounted on
tmpfs              97M  1.2M   96M   2% /run
/dev/sda1         4.7G  2.1G  2.6G  45% /
tmpfs             482M     0  482M   0% /dev/shm
tmpfs             5.0M     0  5.0M   0% /run/lock
/dev/sda15         98M  5.1M   93M   6% /boot/efi
tmpfs              97M  4.0K   97M   1% /run/user/1000
:/Users/mosguinz 1000G     0 1000G   0% /home/ubuntu/Home
```

9. What is the command or commands that would list the contents of the /var/log directory in alphanumeric order? List the command and its output.

Files are listed in alphanumeric order by default.

```
ubuntu@primary:~$ ls /var/log
alternatives.log  auth.log  cloud-init-output.log  dist-upgrade  dpkg.log  kern.log
lastlog  syslog                      unattended-upgrades
apt               btmp      cloud-init.log         dmesg         journal
landscape  private  ubuntu-advantage-timer.log  wtmp
```

`-l` option can be used for a more detailed, list format. `head -5` is used here for brevity.

```
ubuntu@primary:~$ ls -l /var/log | head -5
total 440
-rw-r--r--  1 root      root             6862 Feb 10 06:50 alternatives.log
drwxr-xr-x  2 root      root             4096 Feb 10 06:51 apt
-rw-r-----  1 syslog    adm             26695 Feb 11 15:59 auth.log
-rw-rw----  1 root      utmp                0 Jan  6 18:15 btmp
```

10. What is the command or commands that would list all the empty files or folders in your user's home directory?

```
ubuntu@primary:~$ find ~ -empty
/home/ubuntu/.config/procps
/home/ubuntu/snap/multipass-sshfs/147
/home/ubuntu/snap/multipass-sshfs/common
/home/ubuntu/Home/.android/avd
/home/ubuntu/Home/.config/joplin-desktop/cache
```

`-maxdepth` may be used to limit search to the home folder only.

```
ubuntu@primary:~$ find ~ -maxdepth 1 -empty
/home/ubuntu/.sudo_as_admin_successful
```

11. What is the command or commands used to list the files in /var/log in order of their size? List the command and its output.

Using `ls`:

- `-p` appends `/` to directories (to filter them out using `grep`).

- `-l` to display log listing format (to see size).
- `-S` to list the files by size.
- `-h` to display size in human-readable format (optional).

Piped to `grep` with `-v` to select lines that do not contain `/` to print files only.

```
ubuntu@primary:~$ ls -plSh /var/log | grep -v /
total 440K
-rw-rw-r--  1 root      utmp            290K Feb 11 15:12 lastlog
-rw-r-----  1 syslog    adm             120K Feb 11 22:47 syslog
-rw-r--r--  1 syslog    adm             108K Feb  8 20:43 cloud-init.log
-rw-r-----  1 syslog    adm              45K Feb  9 12:00 kern.log
-rw-r--r--  1 root      root             36K Feb 10 06:51 dpkg.log
-rw-r-----  1 root      adm              33K Feb  8 20:43 dmesg
-rw-r-----  1 syslog    adm              27K Feb 11 22:47 auth.log
-rw-rw-r--  1 root      utmp            7.5K Feb 11 15:12 wtmp
-rw-r--r--  1 root      root            6.8K Feb 10 06:50 alternatives.log
-rw-r-----  1 root      adm             4.7K Feb  8 20:43 cloud-init-output.log
-rw-r--r--  1 root      root            2.6K Feb 11 22:44 ubuntu-advantage-
timer.log
-rw-rw----  1 root      utmp               0 Jan  6 18:15 btmp
```

12. What is the command or commands used to list the top 10 file who use the most disk space? What is this command(s) and show its output?

1. Using `find ~`, searches all directories recursively from the home folder:
    - `-type -f` filters for regular files only.
    - `-print0` prints the actual filename to be passed on to `du`.
2. Using `du` to anaylze disk usage:
    - `-a` to include all files.
    - `-h` to display size in human-readable format (optional).
    - `--files0-from=-` to take filenames from the `find` result.
3. `sort` with options:
    - `-h` to sort the (human-readable) file sizes.
    - `-r` to sort in descending order.
4. Finally, `head -10` to print the first ten items.

> **Note**
> Virtual disk was dismounted prior to running this command. Searching every single file was taking forever. `head -10` is redundant here because it only returned eight lines.

```
ubuntu@primary:~$ find ~ -type f -print0 | du -ah --files0-from=- | sort -hr | head
-10
4.0K    /home/ubuntu/.ssh/authorized_keys
4.0K    /home/ubuntu/.profile
4.0K    /home/ubuntu/.lesshst
4.0K    /home/ubuntu/.bashrc
4.0K    /home/ubuntu/.bash_logout
4.0K    /home/ubuntu/.bash_history
0       /home/ubuntu/.sudo_as_admin_successful
0       /home/ubuntu/.cache/motd.legal-displayed
```

13. What is the command that will show you the last 15 commands you have typed? List the command and its output.

```
ubuntu@primary:~$ history 15
  100  man grep
  101  man du
  102  du -a
  103  man sort
  104  du -a | sort -h | head -10
  105  du -a | sort -hr | head -10
  106  du -a | sort -hr
  107  sudo du -a | sort -hr | head -10
  108  du -a
  109  du -a | head -10
  110  du -a | sort -hr | grep -v / | head -10
  111  last
  112  man last
  113  history
  114  history 15
```

14. What is the difference between the commands less and more?

~~From `less` manpage: `less` - opposite of `more`.~~

`more` allows scrolling downwards, while `less` has better scrolling support in both directions. `less` is a newer, more feature rich version of `more` including features such as searching and jumping between lines.