Linux Questions Solution

Helpful tools/commands:

tldr -> brief explanation and examples (not installed by default)
man -> detailed information about a command (built-in manual)

1.) How can you list all users in Linux?

cat /etc/passwd

-> Example:
root:x:0:0:root:/root:/bin/bash

-> Explanation:
username: root
password: "x" found in a different encrypted file "/etc/shadow"
user id (UID): 0
group id (GID): 0
user id comment/info: root
home directory of user: /root
default shell for this user: /bin/bash

-> Format
username:password:UID:GID:comment:home:shell

[Q]-> How can we get only a specific field, like username?
cut -f 1 -d ":" /etc/passwd

The cut command can segment text, here we take the first field (-f) using the delimiter (-d) : from the file /etc/passwd.

2.) How can you list all active connections?

netstat -tupn

-> Explanation
Netstat displays network-related information such as open connections, open socket ports, etc.
(-t): TCP Connections
(-u): UDP Connections

(-p): Shows program names
(-n): Shows numeric IP addresses instead of symbolic names

[Q]-> How can we continuously list active connections to monitor for new ones?
netstat -tupn --continuous /or/ watch lsof -i

[Q]-> What's the difference between a process and a connection?
A process is a running file/program on your machine, while a connection is a communication between devices on a network or over the internet.

[Q]-> How can we show all running processes?
ps aux

[Q]-> How can you continuously monitor all processes?
top (for more specific examples run and look at 'tldr top')

https://www.booleanworld.com/guide-linux-top-command/

[Q]-> How can we look at root processes?
ps -U root -u root u

3.) Where can you change sudo permissions?

/etc/sudoers (file)
/etc/sudoers.d (directory)

-> Examples

> User privilege specification (root gets ALL privileges)
> root ALL=(ALL:ALL) ALL

> Members of the admin group may gain root privileges
> %admin ALL=(ALL) ALL

> Allow members of group sudo to execute any command
> %sudo ALL=(ALL:ALL) ALL

> Reads files in the given directory)
> @includedir /etc/sudoers.d

[Q]-> How can we modify the sudoers file?
sudo visudo

[Q]-> How can we modify a file in the /etc/sudoers.d directory?
sudo visudo -f /etc/sudoers.d/somefilename

4.) How can you add and remove users?

sudo useradd -m newuser
sudo userdel -r newuser

-> Resource
https://www.booleanworld.com/how-to-add-remove-and-modify-users-in-linux/

-> Explanation
sudo: You need root privilege to add/delete users
useradd -m newuser: Makes a home directory for newuser and creates the newuser account

sudo: Same thing, we need root privilege to delete newuser
userdel -r newuser: Remove all files in newuser's home directory and remove their account

[Q]-> How can we view a user's GroupID (GID) and User ID (UID)?
id newuser

[Q]-> How can we add a user to a Group?
sudo usermod -a -G newgroup newuser

[Q]-> How can we remove a user from a Group?
sudo usermod -G newgroup newuser

[Q]-> How can we change the password of a user?
sudo passwd newuser

[Q]-> How can we "lock out" a user? By preventing them from logging in?
sudo passwd -l newuser

[Q]-> How can we "unlock" a user?
sudo passwd -u newuser

[Q]-> How can we grant sudo permissions to a user?
sudo usermod -a -G sudo newuser (By adding them to sudo group)

Note: For CentOS/RHEL (other Linux distros besides Ubuntu) you replace sudo with wheel
sudo usermod -a -G wheel newuser

[Q]-> How can we remove sudo permissions from a user?
sudo usermod -G sudo newuser

```
! Also make sure to check the /etc/sudoers file mentioned above in 3.)
```

5.) How can you audit CronJobs? (add, delete, modify)

> List cron jobs for current user
> crontab -l

> Edit crontab file to add, delete, or edit cron jobs
> crontab -e

> List other cron job files
> ls /etc/cron.d

[Q]-> How can you list another user's crontab
crontab -u username -l

-> Format of a cron job

```
*   *   *   *   *  sh /path/to/script/script.sh
|   |   |   |   |              |
|   |   |   |   |      Command or Script to Execute
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   | Day of the Week(0-6)
|   |   |   |
|   |   | Month of the Year(1-12)
|   |   |
|   | Day of the Month(1-31)
|   |
| Hour(0-23)
|
Min(0-59)

Note: * represents any value
```

-> Examples
5 4 * * * echo "Hello world"
Prints "Hello World" at 04:05am every day

0 22 * * 1-5 echo "Hi"
Prints "Hi" at 22:00 (10:00pm) on Monday through Friday (1-5)

[Q] -> Where are system logs for cron jobs stored?
/var/log/cron

and on some distros
/var/log/syslog

6.) Explain read, write, execute permissions in Linux

-> Format of permission listing
Directory?-Owner-Group-Others
r (read): 4
w (write): 2
x (execute): 1

[Q]-> What does this mean for a file: -rwxrw-r--
Not a directory, owner can read write and execute, group can read and write, and others can read.

[Q]-> What does this mean for a file: drwxr-xr-x
It is a directory, owner has full permissions, group and others can only read and execute

[Q]-> Are directories file in Linux?
Yes

[Q]-> What do rwx permissions mean for a directory in linux?
Read: allows users to view the contents of the directory
Write: allows users to add, remove, or rename files within a directory
Execute: allows users to enter a directory

[Q]-> How can you check the permissions of a file?
ls -l (shows the files in the current directory

[Q]-> How can you change the permissions of a file?
chmod
chmod +x (allows everyone to execute the file)
chmod -x (removes permission from everyone to execute the file)

chmod 754 (sum of values for r/w/x for Owner-Group-Others)
Note: this means owner has rwx while group has rx and others have r only.

7.) How can you set up UFW? (Enable, disable, implement rules, remove rules)

https://help.ubuntu.com/community/UFW
https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu

> Enable
> sudo ufw enable

> Status
> sudo ufw status verbose

> Disable
> sudo ufw disable

> Implement Rules
> sudo ufw allow <port>/<optional: protocol>
> sudo ufw deny <port>/<optional: protocol>

-> Example
sudo ufw allow 53 (allow incoming UDP and TCP traffic on port 53)
sudo ufw allow 53/tcp (only allow incoming TCP traffic on port 53)

sudo ufw deny 53 (don't allow any incoming UDP or TCP traffic on port 53)

> Remove Rules
> prefix the rule with delete

-> Example
sudo ufw delete deny 80/tcp (removes the rule denying TCP traffic on port 80)

[Q]-> Can you use service names instead of ports with UFW?
Yes

sudo ufw allow <service name>
sudo ufw deny <service name>

sudo ufw allow ssh
sudo ufw deny ssh

[Q]-> What file does UFW use to resolve service names?
/etc/services

8.) How can you audit groups, list, add, modify?

> List groups
> groups

> List group of user
> id user1

> Add (create new) group
> sudo groupadd newgroup

> Delete group
> sudo groupdel newgroup

> Modify
> sudo groupmod --new-name {{new_group}} {{group_name}}
> sudo groupmod --gid {{new_id}} {{group_name}}

> Add users to group
> sudo usermod -aG newgroup user1

> Remove user from group
> sudo usermod -G newgroup user1

> View group data
> /etc/group

9.) How can you list all running background scripts?

---

ps

> Simple output
> ps -e

> More details
> ps -aux

10.) How can you create scripts, and how do you run them?

> How to create, use a text editor (nano, notepad, vim, etc...)
> ->Bash/shell scripting:

```
#!/bin/bash

previous_output=""

while true; do
    current_output=$(netstat -tupn)
    #check if netstat is successful
    if [ $? -ne 0 ]; then
        printf "\nERROR running netstat command"
```

```
    fi

    if [ "$current_output" != "$previous_output" ]; then
        printf "\n[!] Change in connections detected: $(date)"
        printf "\n$current_output\n"
        previous_output="$current_output"
    fi
    # Sleep for a short time before next check
    sleep 5
done
```

->Python:

```
#! /bin/python3

print("hello world")
```

> How to run them:
> chmod +x ./my_script
> ./my_script