born2beroot

correction :

1 - the main different between Debian and Rocky :

Debian :

- is more easy to use .
- it has a big community so that mean more source of information .
- it’s more stable and more reliable.
- it’s use the Debian package management system (dpkg), and the Advanced package tool (apt).

Rocky :

- it’s almost used in companies because it’s more secure.
- Rocky Linux is a relatively new project.
- it’s use YellowDog Updater, modified (YUM), and the Red Hat package management (RPM) .

---

2 - The different between APT and APTITUDE, and what is AppArmor :

APT and Aptitude both are package management tools, they used install, update, and remove a software packages from the system.

- `apt` command is designed to be simple and easy to use, and it is well-suited for performing basic package management tasks .
- `aptitude` has a terminal-based user interface, it can be used to search for packages, show package information, and handle package dependencies in a more advanced way than `apt`

AppArmor is widely used in Linux distributions and is integrated into many popular server and desktop environments. It provides a simple and effective way to improve the security of a system, especially for those who run services that are exposed to the public Internet.

---

3 - simple check-in on the server :

- check the UFW ⇒ systemctl status ufw.
- check SSH ⇒ systemctl status ssh.
- check the OS used ⇒ uname -a.

---

4 - user management :

- check if the user is append to a group ⇒ getent group (sudo/user42).
- create a user ⇒ sudo adduser (user_name).
- how i set my password policy :

  - I change in this 2 files “/etc/login.defs” and “/etc/pam.d/common-password”.
- create a group ⇒ sudo groupadd (group_name).
- append a user to a group ⇒ sudo usermod -aG (group_name) (user_name).

the advantage of the password policy is actually a security reason because it’s force you to

change your psswd every month and keep it Hard.

---

5 - hostname and partitions :

- to show the patitions ⇒ lsblk.
- to show the hostname ⇒ (hostname), or you can go to this file “/etc/hostname”.
- to modify the hostname, you need to change in this directory ⇒ “/etc/hosts”,

  and run this command ⇒ sudo hostnamectl set-hostname (new_host_name).

---

6 - SUDO :

- check if sudo is exist ⇒ sudo —version.
- asign a user to sudo ⇒ sudo adduser (user_name) sudo.
- check the logfile ⇒ go to “/var/log/sudo/sudo.log”.

---

7 - UFW :

- check if ufw is exist ⇒ sudo ufw —version.

- check if it’s working ⇒ systemcl status ufw.
- show the ufw rules ⇒ sudo ufw status
- to add a rule the let the a port lisening ⇒ sudo ufw allow 8080 (port_num).
- to delete a rule ⇒ sudo ufw delete (rule_name >>in this case “allow 8080”).

---

7 - SSH :

- check if the ssh is existing and working properly ⇒ sudo service ssh status.
- ssh (or secure shell) it is a protocol for securely connecting and communicating with remote

  systems. it’s widely used to access servers, applications, and other networked systems.
- **The value :**

  when you used ssh to connect with a system, the coonection is encrypted and protected from attackers, This makes it ideal for sending sensitive information.

  there is 3 types of the encryption that the SSH using :

  -symmetric encryption ⇒ it use same secret key for both encyption and decryption.

  -asymmetric encryption ⇒ it use 2 secret keys one for encryption and other for decryption.

  -hashing = an other form of cryptographic ssh, Hash functions are made in a way that they don't need to be decrypted, if a client has the correct input, they can create a cryptographic hash and SSH will check if both hashes are the same.
- if wan’t to check if th ssh can use the root or not ⇒ go to “/etc/ssh/sshd_config/” and search

  “PermitRootLoging”, it should be (No).

---

8 - cron and wall :

- cron = Linux task manager that allows us to execute commands at a certain time. We can automate some tasks just by telling cron what command we want to run at a specific time. For example, if we want to restart our server every day at 4:00 am, instead of having to wake up at that time, cron will do it for us.

- wall = command used by the root user to send a message to all users currently connected to the server. If the system administrator wants to alert about a major server change that could cause users to log out, the root user could alert them with wall.