Born2BeRoot

Feuille de correction

Comment fonctionne une machine virtuelle ?

La machine physique crée un système informatique virtuel grâce a l'hyperviseur, un logiciel qui permet de séparer les ressources pour en allouer une partie a la VM et qu'elle puisse fonctionner individuellement.

Pourquoi Debian ?

L'utilisation de Debian est fortement conseillée pour quelqu'un débutant dans ce domaine.
Une des distribution les plus anciennes donc très stable
Logiciel 100% libre, gratuite, livre avec de nombreux packages ce qui permet un déploiement rapide.

CentOS vs Debian

CentOS utilise yum comme gestionnaire de packages, qui est plus lent que apt sur Debian.
CentOS légèrement plus stable.
Debian est plus accessible car plus simple.
CentOS plutôt réservé a une communauté plus qualifiée.

Objectif des machines virtuelles

Une machine virtuelle permet de un autre système d'exploitation. Exécuter des applications conçues pour Windows sous macOS ou exécuter d'autres applications Linux sur un système Windows.
Réduction des couts matériels.

apt vs aptitude

aptitude gère mieux les dépendances que apt.
Par exemple, aptitude supprimera les paquets inutiles lors de la désinstallation d'un paquet.

AppArmor

AppArmor permet de gérer les ressources allouées à un programme dans le but de mieux sécuriser le système.

1. **Pare feu UFW**

is ufw started : `sudo ufw status`
is ssh started : `ps aux | grep ssh`
chosen OS : `uname -a`

2. **User**

check groups for user : `groups <user>`
check password policy : `chage -l <user>`
create a new user : sudo `adduser <user>`
create a new group : `sudo groupadd <group>`
add user to group : sudo `usermod -aG <group> <user>`

files modified to change password policy : `/etc/security/pwquality.conf`
`/etc/pam.d/common-password`

3. **Hostname & partitions**

change hostname : `sudo vim /etc/hostname`
to view partitions : `lsblk`
LVM :

Permet la création et la gestion de volumes logiques sous Linux. Partitionne un disque physique en disques logiques, que l'utilisateur pourra organiser selon ses besoins.

4. **Sudo**

is sudo install : `sudo <cmd>`
add user to sudo group : `sudo usermod -aG sudo <user>`

Sudo permet à un utilisateur d'exécuter des commandes root selon des restrictions définies. Sa configuration s'effectue à l'aide de la commande sudo visudo. Le journal des actions sudo se trouve dans /var/log/sudo/sudo.log

5. **UFW**

UFW est un pare-feu simple et rapide à configurer. Le pare-feu est chargé d'analyser et de filtrer les échanges entre l'internet public et le réseau privé. Les ports permettent de gérer l'accès de programmes extérieurs à l'ordinateur (exemple SSH).

list active rules : `sudo ufw status`
add a new rule : `sudo ufw allow 8080`
remove the rule : `sudo ufw status numbered puis sudo ufw delete <number>`

6. SSH

ssh service is running : `ps aux | grep sshd`
ssh is working : `ssh -p 4242 login@127.0.0.1`
ssh only uses port 4242 : `grep -i port /etc/ssh/sshd_config`

Protocole qui facilite les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur et permet aux utilisateurs de se connecter à distance à des systèmes hôte de serveurs.

7. Script monitoring

cron est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance, ou selon un cycle défini à l'avance.

Modifier heure et fichier a exécuter : `en su, crontab -e`