Notes

Basic function of vm:

- ordinateur virtuel disposant un cpu, ram, hard disk qui sont empruntés depuis la machine hôte

- le logiciel hyperviseur permet de créer et faire fonctionner la machine virtuelle

Pros:

- faire tourner un système d'exploitation (os) différent de celui de la machine hôte (mh)

- tester un programme instable qui peut avoir de virus ou tester un programme qui ne peut pas tourner dans la mh

- installer plusieurs vm au lieu de devoir multiplier plusieurs machines physiques, économisant la dépense, l'électricité

Cons:

- ram trop petite = lenteur et latence

- si la mh est cassée, on risque de ne plus pouvoir accéder à la vm

- plus vulnérable aux attaques s'il fait tourner plusieurs vm plutôt qu'un seul os

Why I chose Debian and the difference between Debian and Centos:

- Debian est plus facil à set up et à mettre à jour alors que Centos est difficile à set up et l'installation complète est recommandée pour une nouvelle version

- Debian est supporté par une communauté plutôt grande et active alors que Centos est organisé par une entreprise

- Debian propose une plus grande quantité de paquet par rapport à Centos

- différents gestionnaires de paquets: YUM/DNF vs dpkg/APT

What is a packet:

- dans les os comme Debian, l'installation des logiciels se fait à l'aide des paquets, qui contiennent les fichiers nécessaires à la mise en place des commandes ou des fonctionnalités

Difference between APT and Aptitude:

- Aptitude est un gestionnaire de paquets de plus haut niveau

- Aptitude propose une meilleure qualité de gestionnaire de paquet, ex: il peut supprimer automatiquement les paquets non utilisés, il dispose deux commandes 'why' et 'why not' qui explique pourquoi tel ou tel paquet est recommandé

- Aptitude offre de plus une interface graphique (ui) alors que apt est restraint au ligne de commande

What is AppArmor:

- logiciel de sécurité (proposant le MAC) permettant de restreindre l'accès d'un programme au os

- il donne à chaque programme des règles qui les autorise ou empêche d'accéder tel ou tel fichier

- c'est une alternative de SELinux mais moins sécurisée

Check os:

- **$ sudo uname -a** => afficher les informations du système d'exploitation

- **$ cat /etc/os-release** => vérifier les infos du système d'exploitation

Users and groups:

- **$ sudo useradd <new_user>** => créer un nouveau utilisateur

- **$ sudo userdel -r <user>** => supprimer un utilisateur

- **$ sudo usermod <user>** => modifier les paramètres de l'utilisateur

- **$ sudo usermod -aG <group> <user>** => ajouter un utilisateur à un groupe

- **$ users** => afficher la liste des utilisateurs connectés à l'instant

- **$ cat /etc/passwd | cut -d ":" -f1** ou **cat /etc/passwd | awk -F '{print $1}'** => afficher la liste des utilisateurs

- **$ id -u** => afficher le numéro d'identification de l'utilisateur

- **$ sudo groupadd <new_group>** => créer un nouveau groupe

- **$ sudo groupdel <group>** => supprimer un groupe

- **$ sudo gpasswd -a <user> <group>** => ajouter un utilisateur à un groupe

- **$ sudo gpasswd -d <user> <group>** => enlever un utilisateur d'un groupe

- **$ groups** => afficher les groupes contenant au moins un utilisateur

- **$ getent group** => afficher la liste des groupes et des utilisateurs appartenant à chaque groupe

- **$ id -g** => montrer le numéro d'identification du groupe principal d'un utilisateur

How did I set up the rules for password:

• Pour les trois premières règles

- changer les paramètres dans **$ sudo nano /etc/login.defs**

- comme ca arrive que les utilisateurs déjà créés ne soient pas affectés, on impose les règles en faisant **$ sudo chage -M/m/W 30/2/7**

• Pour le reste

- **$ sudo apt install libpam-pwquality** => pour installer la librairie de vérification de qualité des mots de passe

- changer les paramètres dans **$ sudo nano /etc/security/pwquality.conf**

- diftok = différence entre vieux et nouveau mdp

- minlen = la taille minimum du mdp

- dcredit = le minimum de chiffres si le credit est négatif, et le maximum de chiffres si le crédit est positif

- ucredit = le minimum de majuscules si le credit est négatif, et le maximum de majuscules si le crédit est positif

- maxrepeat = le nombre de même caractères consécutifs autorisés dans le nouveau mdp

- usercheck = vérifier si le mdp contient le nom de l'user

- retry = le nombre maximum qu'on peut retry le mdp

- enforce_for_root = permettre pwquality de vérifier le mdp de root

Pros of the password policy:

- difficile à cracker

- empêcher les utilisateurs à reprendre le meme mdp et ajouter plus de caractères

- empêcher la brute force

Cons of the password policy:

- risque d'oublier son mdp

- certains caractères sont beaucoup plus utilisés que d'autre par exemple le 'e'

Hostname and partitions:

- **$ sudo hostnamectl set-hostname <new_hostname>** ou **$ sudo nano /etc/hostname** => changer le hostname

- **$ sudo hostnamectl status** => status du hostname

Check partitions:

- **$ lsblk** => vérifier les partitions

What is LVM:

- système d'organisation de l'espace mémoire du hard disk qui est facile à manipuler

- les espaces peuvent facilement être déplacés, redimensionnés ou freeze sans avoir redémarrer la vm

What is sudo:

- programme qui permet aux autres utilisateurs d'exécuter des commandes en tant que root sans devoir connaître le mdp du root

- **$ sudo --version** => status sudo

What is UFW:

- un pare-feu, i.e. logiciel qui surveille et contrôle le trafic de données entre l'ordinateur et le réseau, il peut autoriser ou bloquer le trafic selon les règles imposées

- UFW nous permet la modification du pare-feu de manière simple sans risque de sécurité

- **$ sudo service ufw status**

- **$ sudo ufw status verbose** => afficher la liste des règles

- **$ sudo ufw allow/deny <port>** => autoriser/interdire tel ou tel port

- **$ sudo ufw delete allow/deny <port>** => supprimer la règle de tel ou tel port

What is SSH:

- protocole réseau qui permet à l'utilisateur modifier son serveur internet depuis un terminal ou de se connecter à distance depuis un autre terminal

- il permet au transfert des données entre deux ordinateurs d'être cryptés à l'aide du mdp d'utilisateur et la création de clefs publiques et privées

- **$ sudo service ssh status** => status de ssh

- **> ssh <user>@<ip> -p <port>** => log in avec ssh depuis un autre terminal

What is cron:

- programme permettant d'exécuter les scripts, les commandes ou les logiciels automatiquement, à une date et heure ou un intervalle spécifié

What is WordPress:

- système de gestion de contenu permettant l'entretien d'un site internet

- facile à utiliser et gratuit

What is PHP:

- langage de programmation pour créer des pages web, indispensable pour WordPress

What is lighttpd:

- logiciel de serveur web HTTP qui est optimisé pour la rapidité tout en restant sécurisé et flexible

- il a une plus petite empreinte mémoire que les autres serveurs web

What is FastCGI:

- protocole binaire permettant à un serveur HTTP d'interagir avec des applications externes (ce qui permet l'interaction entre lighttpd et PHP dans notre cas, pour accéder la page info.php)

What is MariaDB:

- gestionnaire de base de données libre et gratuit, fondé sur MySQL

- il inclus tous les principaux moteurs de stockage de données open source

What is Fail2ban:

- logiciel qui analyse les journaux d'un serveur pour identifier et interdire les adresses IP suspectes.

- il peut bloquer avec le pare-feu, toutes les tentatives de connexions échouées, soit temporairement soit définitivement

Commandes utiles:

• **$ cat /etc/os-release** => vérifier les infos du système d'exploitation

• **$ lsblk** => vérifier les partitions

• **$ apt --version** => vérifier que le gestionnaire de paquets est installé par défaut

• **$ date** => pour vérifier le fuseau horaire

• **$ exit ou logout** => terminer la session en cours et renvoyer à l'écran de connexion

• **$ su** => se connecter en tant que root

• **$ su <other_login>** => se connecter en tant qu'un autre utilisateur

• **$ systemctl reboot** => redémarrer le système

• **$ systemctl poweroff** => éteindre le système

• **$ sudo useradd <new_uer>** => créer un nouveau utilisateur

• **$ sudo userdel -r <user>** => supprimer un utilisateur

• **$ sudo usermod <user>** => modifier les paramètres de l'utilisateur

• **$ sudo usermod -aG <group> <user>** => ajouter un utilisateur à un groupe

• **$ users** => afficher la liste des utilisateurs connectés à l'instant

• **$ cat /etc/passwd | cut -d ":" -f 1** ou **cat /etc/passwd | awk -F '{print $1}'** => afficher la liste des utilisateurs

• **$ id -u** => afficher le numéro d'identification de l'utilisateur

• **$ sudo groupadd <new_group>** => créer un nouveau groupe

• **$ sudo groupdel <group>** => supprimer un groupe

• **$ sudo gpasswd -a <user> <group>** => ajouter un utilisateur à un groupe

• **$ sudo gpasswd -d <user> <group>** => enlever un utilisateur d'un groupe

• **$ groups** => afficher les groupes contenant au moins un utilisateur

• **$ getent group** => afficher la liste des groupes et des utilisateurs appartenant à chaque groupe

• **$ id -g** => montrer le numéro d’identification du groupe principal d’un utilisateur

• **$ wall <message>** => afficher un message avec bandeau

• **$ sudo wall -n <message>** => afficher un message sans bandeau

• **$ sudo service ufw status** => status du pare-feu

• **$ sudo ufw status verbose** => afficher la liste des règles

• **$ sudo ufw allow/deny <port>** => autoriser/interdire tel ou tel port

• **$ sudo ufw delete allow/deny <port>** => supprimer la règle de tel ou tel port

• **$ sudo service ssh status** => status de ssh

• **> ssh <user>@<ip> -p <port>** => log in depuis un autre terminal

• **$ sudo uname -a** => afficher les informations du système d’exploitation

• **$ sudo passwd <user>** => changer/donner un mot de passe d’un utilisateur

• **$ sudo nano /etc/login.defs** => accéder aux configurations de mot de passe

• **$ sudo hostnamectl set-hostname <new_hostname>** ou **$ sudo nano /etc/hostname** => changer le hostname

• **$ sudo hostnamectl status** => status du hostname

• **$ sudo --version** => status sudo

• *** * * * * bash /root/sleep.sh && bash /root/monitoring.sh**
*** * * * * sleep 30; bash /root/sleep.sh && bash /root/monitoring.sh**
=> exécuter les scripts sleep et monitoring tous les 30 secondes