Teste Préliminaire et consignes

. Cloner le dépôt Git sur la station
. Assurez-vous que le signature.txt est identique à celui du .vdi
. Par précaution, vous pouvez dupliquer la machine virtuelle initiale afin d'en conserver une copie.
. Démarrer la machine virtuelle

Faire le fichier texte signature.txt
shasum [nom-machine].vdi > signature.txt

ÉVALUATION PARTIE DEUX :

Expliquez le fonctionnement de base de la machine virtuelle.

Pourquoi ai-je choisi Debian plutôt que Rocky ?

- **Debian** est recommandé pour les débutants.
  - Il est plus facile à installer, configurer et à mettre à niveau
  - Il dispose d'une interface utilisateur graphique (GUI)

- **Rocky** est principalement recommandé pour les utilisateurs avancés.
  - Il est plus stable et a moins de mises à jour.
  - L'interface graphique existe, mais il est préférable d'utiliser des lignes de commande.
  - Il est recommandé aux utilisateurs ou aux petites entreprises qui souhaitent configurer un serveur pour le partage de fichiers, l'hébergement Web et d'autres tâches au niveau de l'entreprise.

Qu'est-ce qu'une machine virtuelle ?

- Une machine virtuelle (VM) est la **même chose qu'un autre ordinateur physique**
- Il dispose d'un processeur, d'une mémoire, de disques pour stocker vos fichiers et peut se connecter à Internet si nécessaire.
- Alors que les éléments qui composent votre ordinateur (appelés matériel) sont physiques et tangibles, les machines virtuelles sont souvent considérées comme **des ordinateurs virtuels**

Voici quelques façons dont les machines virtuelles sont utilisées/utilisé

- **Essayer un nouveau système d'exploitation** (OS), y compris les versions bêta.

- Créer un nouvel environnement pour permettre aux développeurs des test de développement.
- **Accéder à des données infectées par un virus** ou exécuter une ancienne application en installant un système d'exploitation plus ancien.
- **Exécuter des logiciels ou des applications sur des systèmes d'exploitation pour lesquels ils n'étaient pas initialement destinés** .
- **tester des applications dans un environnement sécurisé** . :)

Comment fonctionne une machine virtuelle ?

- **La virtualisation est le processus de création d'une version logicielle** , ou « virtuelle », d'un ordinateur, **avec des quantités dédiées de CPU, de mémoire et de stockage qui sont « empruntées » à un** ordinateur hôte physique (tel que votre ordinateur personnel)

  Une machine virtuelle est un **fichier informatique** (généralement appelé image) qui se comporte comme un ordinateur réel.

  Il **peut s'exécuter dans une fenêtre en tant qu'environnement informatique distinct** , souvent pour exécuter un système d'exploitation différent

  La machine virtuelle **est partitionnée du reste du système** , ce qui signifie que le logiciel à l'intérieur d'une VM **ne peut pas interférer avec le système d'exploitation principal de l'ordinateur hôte** .

Quelle est la différence entre Aptitude et APT ?

- Aptitude et apt sont deux des outils les plus populaires qui **gèrent la gestion des paquets** .
- **Aptitude** est un gestionnaire de paquets de haut niveau et fournit une interface de menu de terminal.
- **APT** est un gestionnaire de paquets de niveau inférieur

Qu'est-ce qu'AppArmor ?

- AppArmor (« Application Armor ») est un **module de sécurité du noyau Linux qui permet à l'administrateur système de restreindre les capacités des programmes avec des profils par programme** .

Qu'est-ce que SSH ?

- SSH ou Secure Shell est un protocole de communication réseau qui permet à deux ordinateurs de communiquer (cf http ou protocole de transfert hypertexte, qui est le protocole utilisé pour transférer des hypertextes tels que des pages Web) et de partager des données. Une caractéristique inhérente à ssh est que la communication entre les deux ordinateurs est cryptée, ce qui signifie qu'elle est adaptée à une utilisation sur des réseaux non sécurisés.
- SSH est souvent utilisé pour « se connecter » et effectuer des opérations sur des ordinateurs distants, mais il peut également être utilisé pour transférer des données.

CONFIGURATION SIMPLE

. Pas d'environnement graphique au lancement.

```
ls /usr/bin/*session
```

. Un mot de passe sera demandé avant de tenter de se connecter à cette machine.

. Connectez-vous avec un utilisateur (ne doit pas être root).

. Faites attention au mot de passe choisi, il doit suivre les règles imposées :

- Expiration : 30 days
- Minimum 2 days before be able to modify
- Expiration warning : 7 days
- Minimum 10 characters with a majuscule and a number. But not more than 3 consecutive identical characters.
- Username is forbidden
- At least 7 characters that aren't in the last password.
- Same thing for root password
- Don't forget to change existing passwords

. Vérifiez que le service UFW est démarré :

- sudo service ufw status

. Vérifiez que le service SSH est démarré :

- sudo service ssh status

. Vérifiez que le système d'exploitation choisi **est Debian** :

- $ uname -o
- uname -v
- uname --kernel-version

UTILISATEUR

. Nécessite un utilisateur avec le login de l'étudiant évalué qui appartient aux groupes « sudo » et « user42 ».

- $ groups USERNAME

  getent group sudo
  getent group user42

- Créez un nouvel utilisateur et attribuez-lui un mot de passe respectant les règles du sujet.

  - $ sudo adduser USERNAME

- Expliquez comment configurer les règles (il devrait y avoir un ou deux fichiers modifiés).
  - Politique de mot de passe

  - $ sudo chage -l USERNAM

—> Création du fichier sudo_config : /etc/sudoers.d/sudo_config
Defaults passwd_tries=3
Defaults badpass_message="Mensaje de error personalizado"
Defaults logfile="/var/log/sudo/sudo_config"
Defaults log_input, log_output
Defaults iolog_dir="/var/log/sudo"
Defaults requiretty
Defaults secure_path=« /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

—> Editer les règles a appliquer du sujet
—> Editer /etc/login.defs : changer parm
➤ PASS_MAX_DAYS 99999 -> PASS_MAX_DAYS 30
➤ PASS_MIN_DAYS 0 -> PASS_MIN_DAYS 2

—> nano /etc/pam.d/common-password

Editer common-passeword —->. rajouter après rétry 3 = :
minlen=10 ucredit=-1 dcredit=-1 lcredit=-1 maxrepeat=3 reject_username difok=7 enforce_for_root

Vérifier l'expiration du mot de passe.

Créez un groupe nommé « évaluation », attribuez-le à cet utilisateur et vérifiez que cet utilisateur appartient au groupe « évaluation ».

- $ sudo groupadd evaluating
- $ sudo adduser USERNAME evaluating ◦ $ groups USERNAME

. Expliquez les avantages de cette politique de mot de passe, ainsi que les avantages et les inconvénients de sa mise en œuvre.

- Avantages : Meilleure sécurité
- Inconvénients : Besoin de mémoriser un nouveau mot de passe chaque mois, besoin de changer de mot de passe après avoir modifié les restrictions.

sudo chage -l username

Changer mot de passe : passwd [user-name]

Changer mot de passe root : sudo passwd root

Relance pour mise a jour : sudo reboot

Hostname ET PARTITIONS

. Vérifiez que le nom d'hôte de la machine est correctement formaté comme suit : login42 (longin de l'étudiant évalué)

- $ hostname

. Modifiez ce nom d'hôte en remplaçant le login par le vôtre, puis redémarrez la machine. Si au redémarrage, le nom d'hôte n'a pas été mis à jour, l'évaluation s'arrête ici.

- remplaçons notre login par le nouveau. : $ sudo vim /etc/hostname
- et nous remplaçons notre login par le nouveau

: $ sudo vim /etc/hosts ◦ $ sudo reboot

. Restaurer la machine au nom d'hôte d'origine ◦

. Vérifiez les partitions et comparez-les à l'exemple bonus.

- $ lsblk

. Expliquez comment fonctionne LVM et de quoi il s'agit.

- framework de mappage de périphériques qui fournit Logical Volume Manager for the Linux kernel / gestionnaire de volumes logiques pour le noyau Linux.
- Les volumes logiques (LV) : ce sont des «partitions virtuelles» (logiques parce qu'elles sont produites par un logiciel sans nécessairement correspondre à une portion d'un disque matériel.

  Les volumes logiques sont constitués d'étendues de blocs physiques réunis en un seul espace de stockage, et rendus lisibles par le système.

  On peut les utiliser comme des partitions ordinaires.

SUDO

. Vérifiez que le programme « sudo » est correctement installé sur la VM.

$ dpkg -l | grep sudo. dpkg -s sudo◦

. Affecter un nouvel utilisateur au groupe « sudo ».

- $ sudo adduser USERNAME sudo

. Expliquez la valeur et le fonctionnement de sudo avec un exemple

- est un programme pour les systèmes d'exploitation informatiques qui permet aux utilisateurs d'exécuter des programmes avec les privilèges de sécurité d'un autre utilisateur, par défaut le superutilisateur.
- $ sudo COMMAND

Règles de mise en place de sécurité sudo

root@gemartin42:/var/10g/sudo# nano /etc/sudoers.d/sudo_config

.

Montrer la mise en œuvre des règles imposées par le sujet

- Vérifiez que le /var/log/sudo dossier existe et contient au moins un fichier.
- Vérifiez le contenu des fichiers dans ce dossier. Vous devriez voir un historique des commandes utilisées avec sudo.
- Essayez d'exécuter une commande via sudo. Vérifiez si les fichiers du /var/log/sudodossier ont été mis à jour.

UFW

. Vérifiez que le programme « UFW » est correctement installé

- $ dpkg -l | grep UFW. dpkg -s ufw

. Vérifiez que cela fonctionne correctement

- $ sudo ufw status sudo service ufw status

. Expliquez fondamentalement ce qu'est l'UFW et l'intérêt de son utilisation.

- Pare-feu très simple et efficace
- Un pare-feu est un ensemble de filtres logiciels qui contrôlent (autorisent ou non l'ouverture des ports) le trafic entrant et sortant de votre ordinateur. En termes simples, il s'agit d'une sorte de mur entre votre ordinateur et le monde extérieur.

. Répertoriez les règles actives dans UFW.

sudo ufw status numbered

Une règle doit exister pour le port 4242.

Plus 80 si il y a le bonus

. Affectez une nouvelle règle pour ouvrir le port 8080. Vérifiez que celle-ci a été ajoutée en listant les règles actives.

- $ sudo ufw allow 8080

Pour afficher :

sudo ufw status numbered

. Supprimer cette nouvelle règle

- $ sudo ufw delete 3 (numero de la règle)

sudo ufw delete num_rule

SSH

. Vérifiez que le service SSH est correctement installé.

- $dpkg -l | grep ssh sudo service ssh status

. Vérifiez que cela fonctionne correctement.

- $ sudo systemctl status sshd

. Expliquez fondamentalement ce qu'est SSH et l'intérêt de son utilisation.

. Vérifiez que le service SSH utilise uniquement le port 4242.

sudo service ssh status

. Assurez-vous que vous ne pouvez pas utiliser SSH pour vous connecter avec root

- Utiliser un autre terminal
- $ ssh root@localhost -p 4242

Cela ne doit pas fonctionner

. Utilisez SSH pour vous connecter avec le nouvel utilisateur.

- $ ssh NEWUSER@localhost -p 4242

Surveillance des scripts

Ouvrire le scribe :

cd /usr/local/bin/

sudo nano monitoring.sh

Expliquez le fonctionnement du script en affichant le code

- $ sudo crontab -u root -e

crontab -l

Pour executer le monitoring , pour contrôle:

bash monitoring.sh

. Qu'est-ce que cron ?

- 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 spécifiées à l'avance, ou selon un cycle défini à l'avance.

. Comment configurer le script pour qu'il s'exécute toutes les 10 minutes au démarrage du serveur.

- */10 * * * * /root/monitoring.sh

. Comment arrêter le script sans modifier le script, redémarrer la VM et vérifier le script.

Pour stopper cron une fois

sudo systemctl stop cron

sudo /etc/init.d/cron stop

Pour arrêter cron durablement :

sudo systemctl disable cron

```bash
#!/bin/bash

# Affiche l'architecture du système et la version du noyau
wall $'#Architecture: ' `uname -a` \

# Compte le nombre de processeurs physiques
$'\n#CPU physical: ' `cat /proc/cpuinfo | grep processor | wc -l` \

# Compte le nombre de processeurs virtuels (vCPU)
$'\n#vCPU: ' `cat /proc/cpuinfo | grep processor | wc -l` \

# Affiche l'utilisation de la mémoire en MB et en pourcentage
$'\n'`free -m | awk 'NR==2{printf "#Memory Usage: %s/%sMB (%.2f%%)", $3,$2,$3*100/$2 }'` \

# Affiche l'utilisation du disque en GB et en pourcentage
$'\n'`df -h | awk '$NF=="/"{printf "#Disk Usage: %d/%dGB (%s)", $3,$2,$5}'` \

# Affiche la charge CPU
$'\n'`top -bn1 | grep load | awk '{printf "#CPU Load: %.2f\n", $(NF-2)}'` \

# Affiche la date et l'heure du dernier redémarrage
$'\n#Last boot: ' `who -b | awk '{print $3" "$4" "$5}'` \

# Vérifie si LVM est utilisé
$'\n#LVM use: ' `lsblk |grep lvm | awk '{if ($1) {print "yes";exit;} else {print "no"} }'` \

# Compte le nombre de connexions TCP établies
$'\n#Connection TCP:' `netstat -an | grep ESTABLISHED | wc -l` \

# Compte le nombre d'utilisateurs connectés
$'\n#User log: ' `who | cut -d " " -f 1 | sort -u | wc -l` \

# Affiche l'adresse IP et l'adresse MAC
$'\nNetwork: IP ' `hostname -I`"("`ip a | grep link/ether | awk '{print $2}'`")" \

# Compte le nombre de commandes sudo exécutées
$'\n#Sudo: ' `grep -a sudo /var/log/auth.log | wc -l`
```

-
-