Born2beRoot

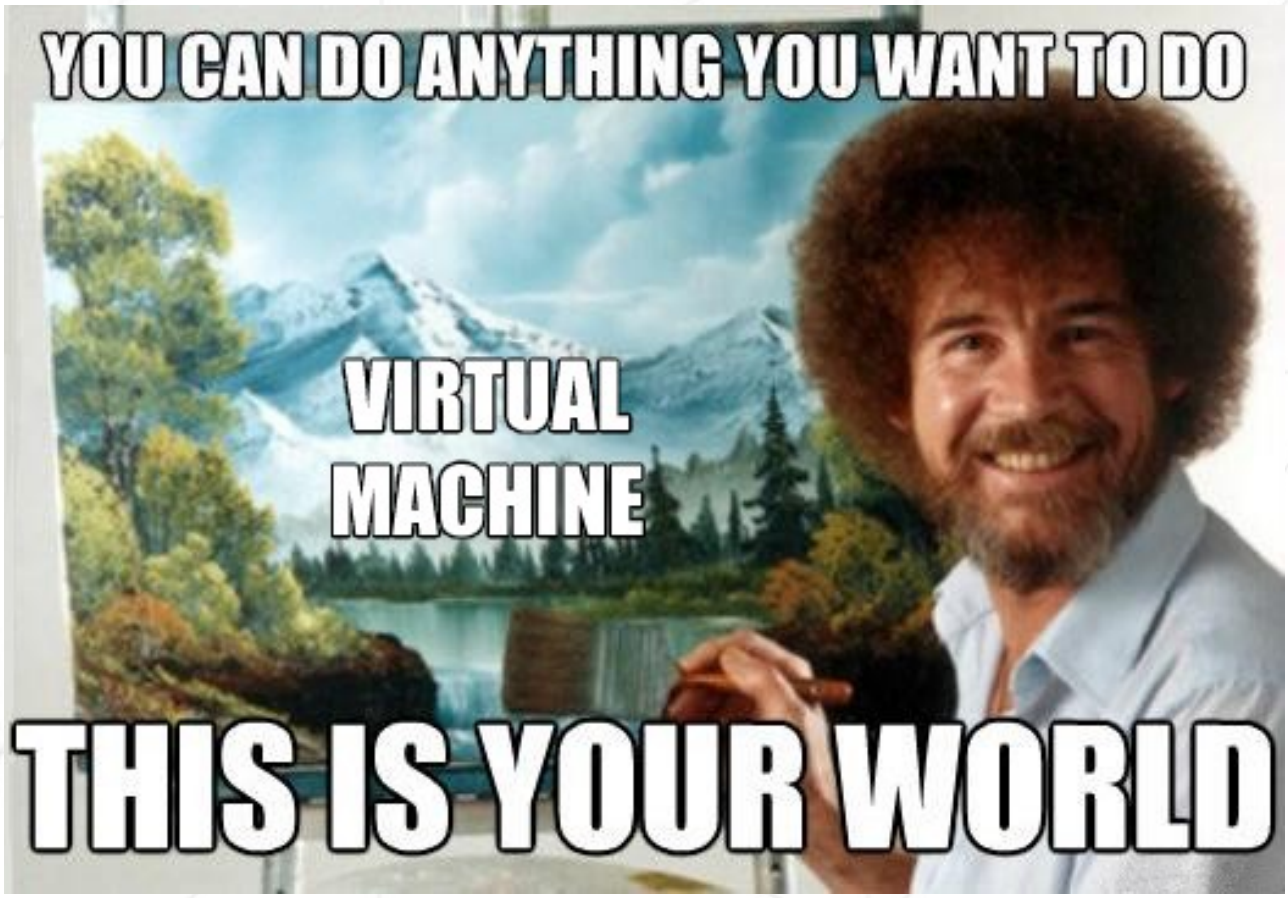
Résumé : *Ce document est un exercice lié à l'administration système.*

Version : 4

Contenu

Chapitre I

Préambule



Chapitre II

Introduction

Ce projet a pour objectif de vous faire découvrir le monde merveilleux de la virtualisation.

Vous allez créer votre première machine dans VirtualBox (ou UTM si vous ne pouvez pas utiliser VirtualBox) en suivant des instructions spécifiques. À la fin de ce projet, vous serez en mesure de configurer votre propre système d'exploitation tout en appliquant des règles strictes.

Chapitre III

Directives générales

- L'utilisation de VirtualBox (ou UTM si vous ne pouvez pas utiliser VirtualBox) est obligatoire.
- Vous devez uniquement soumettre un fichier signature.txt à la racine de votre dépôt. Vous devez y coller la signature du disque virtuel de votre machine. Rendez-vous sur la page Soumission et évaluation par les pairs pour plus d'informations.
- L'utilisation de snapshots est interdite.

Chapitre IV

Instructions relatives à l'IA

Contexte

Ce projet est conçu pour vous aider à découvrir les éléments fondamentaux de votre formation en TIC.

Pour bien ancrer les connaissances et les compétences clés, il est essentiel d'adopter une approche réfléchie dans l'utilisation des outils et du soutien de l'IA.

Un véritable apprentissage fondamental nécessite un réel effort intellectuel, à travers des défis, des répétitions et des échanges entre pairs.

Pour un aperçu plus complet de notre position sur l'IA, en tant qu'outil d'apprentissage, dans le cadre du programme d'études en TIC et en tant qu'attente du marché du travail, veuillez vous reporter à la FAQ dédiée sur l'intranet.

Message principal

- ☛ Construisez des bases solides sans prendre de raccourcis.
- ☛ Développez réellement vos compétences techniques et vos capacités.
- ☛ Faites l'expérience d'un véritable apprentissage entre pairs, commencez à apprendre comment apprendre et résoudre de nouveaux problèmes.
- ☛ Le parcours d'apprentissage est plus important que le résultat.
- ☛ Découvrez les risques associés à l'IA et développez des pratiques de contrôle et des contre-mesures efficaces pour éviter les pièges courants.

Règles pour les apprenants :

- Vous devez faire preuve de raisonnement dans les tâches qui vous sont assignées, en particulier avant de vous tourner vers l'IA.

- Vous ne devez pas demander de réponses directes à l'IA.
- Vous devez vous informer sur l'approche globale 42 en matière d'IA.

Résultats de la phase :

Au cours de cette phase fondamentale, vous obtiendrez les résultats suivants :

- Acquérir les bases techniques et de codage appropriées.
- Comprendre pourquoi et comment l'IA peut être dangereuse au cours de cette phase.

Commentaires et exemples :

- Oui, nous savons que l'IA existe, et oui, elle peut résoudre vos projets. Mais vous êtes ici pour apprendre, pas pour prouver que l'IA a appris. Ne perdez pas votre temps (ni le nôtre) à démontrer que l'IA peut résoudre le problème donné.
- Apprendre à 42, ce n'est pas connaître la réponse, c'est développer la capacité à la trouver. L'IA vous donne directement la réponse, mais cela vous empêche de construire votre propre raisonnement. Or, le raisonnement demande du temps, des efforts et implique des échecs. Le chemin vers le succès n'est pas censé être facile.
- Gardez à l'esprit que pendant les examens, l'IA n'est pas disponible : pas d'Internet, pas de smartphones, etc. Vous vous rendrez vite compte si vous avez trop compté sur l'IA dans votre processus d'apprentissage.
- L'apprentissage entre pairs vous expose à différentes idées et approches, améliorant ainsi vos compétences interpersonnelles et votre capacité à penser de manière divergente. C'est bien plus précieux que de simplement discuter avec un bot. Alors ne soyez pas timide : discutez, posez des questions et apprenez ensemble !
- Oui, l'IA fera partie du programme d'études, à la fois comme outil d'apprentissage et comme sujet à part entière. Vous aurez même la possibilité de créer votre propre logiciel d'IA. Pour en savoir plus sur notre approche crescendo, consultez la documentation disponible sur l'intranet.

✓ Bonne pratique :

> Je suis bloqué sur un nouveau concept. Je demande à quelqu'un à proximité comment il l'a abordé. Nous discutons pendant 10 minutes, et soudain, ça fait tilt. Je comprends.

✗ Mauvaise pratique :

> J'utilise secrètement l'IA, je copie du code qui semble correct. Lors de l'évaluation par les pairs, je ne peux rien expliquer. J'échoue. Pendant l'examen, sans IA, je suis à nouveau bloqué. J'échoue.

Chapitre V Partie obligatoire

Ce projet consiste à configurer votre premier serveur en suivant des règles spécifiques.

Comme il s'agit de configurer un serveur, vous installerez le minimum de services. Pour cette raison, une interface graphique est inutile ici. Il est donc interdit d'installer X.org ou tout autre serveur graphique équivalent. Sinon, votre note sera de 0.

Vous devez choisir comme système d'exploitation soit la dernière version stable de Debian (pas la version testing/unstable), soit la dernière version stable de Rocky. Debian est fortement recommandé si vous êtes novice en administration système.

La configuration de Rocky est assez complexe. Vous n'avez donc pas besoin de configurer KDump. Cependant, SELinux doit être exécuté au démarrage et sa configuration doit être adaptée aux besoins du projet. AppArmor pour Debian doit également être exécuté au démarrage.

Vous devez créer au moins deux partitions cryptées à l'aide de LVM. Voici un exemple de partitionnement possible :

```
wil@wil:~$ lsblk
NAME                  MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                     8:0    0    8G  0 disk
├─sda1                  8:1    0  487M  0 part  /boot
├─sda2                  8:2    0    1K  0 part
└─sda5                  8:5    0  7.5G  0 part
  └─sda5_crypt        254:0    0  7.5G  0 crypt
    ├─wil--vg-root    254:1    0  2.8G  0 lvm   /
    ├─wil--vg-swap_1  254:2    0  976M  0 lvm   [SWAP]
    └─wil--vg-home    254:3    0  3.8G  0 lvm   /home
sr0                    11:0    1 1024M  0 rom
wil@wil:~$ _
```

Au cours de la défense, on vous posera quelques questions sur le système d'exploitation que vous avez choisi. Par exemple, vous devrez connaître les différences entre aptitude et apt, ou savoir ce que sont SELinux ou AppArmor. En bref, vous devez comprendre ce que vous utilisez !

Un service SSH sera exécuté sur le port obligatoire 4242 de votre machine virtuelle.
Pour des raisons de sécurité, il ne doit pas être possible de se connecter via SSH en tant que root.

L'utilisation de SSH sera testée lors de la soutenance en créant un nouveau compte. Vous devez donc comprendre son fonctionnement.

Vous devez configurer votre système d'exploitation avec le pare-feu UFW (ou firewalld pour Rocky) et ainsi ne laisser ouvert que le port 4242 dans votre machine virtuelle.

L'exemple montre des tailles de disque arbitraires. Vous devez déterminer la taille appropriée pour chaque partition afin d'assurer un fonctionnement correct tout en évitant une utilisation inutile du disque.

Votre pare-feu doit être actif lorsque vous lancez votre machine virtuelle. Pour Rocky, vous devez utiliser firewalld à la place de UFW.

- Le nom d'hôte de votre machine virtuelle doit être votre identifiant de connexion suivi de 42 (par exemple, wil42). Vous devrez modifier ce nom d'hôte pendant votre évaluation.
- Vous devez mettre en place une politique de mots de passe forts.
- Vous devez installer et configurer sudo en suivant des règles strictes.
- En plus de l'utilisateur root, un utilisateur avec votre identifiant comme nom d'utilisateur doit être présent.
- Cet utilisateur doit appartenir aux groupes user42 et sudo.

Au cours de la défense, vous devrez créer un nouvel utilisateur et l'affecter à un groupe.

Pour mettre en place une politique de mot de passe forte, vous devez respecter les exigences suivantes :

- Votre mot de passe doit expirer tous les 30 jours.
- Le nombre minimum de jours autorisés avant la modification d'un mot de passe sera fixé à 2.

- L'utilisateur doit recevoir un message d'avertissement 7 jours avant l'expiration de son mot de passe.
- Votre mot de passe doit comporter au moins 10 caractères. Il doit contenir une lettre majuscule, une lettre minuscule et un chiffre. De plus, il ne doit pas contenir plus de 3 caractères identiques consécutifs.
- Le mot de passe ne doit pas inclure le nom de l'utilisateur.
- La règle suivante ne s'applique pas au mot de passe root : le mot de passe doit comporter au moins 7 caractères qui ne font pas partie de l'ancien mot de passe.
- Bien entendu, votre mot de passe root doit respecter cette politique.

Après avoir configuré vos fichiers de configuration, vous devrez modifier tous les mots de passe des comptes présents sur la machine virtuelle, y compris le compte root.

Pour mettre en place une configuration sécurisée pour votre groupe sudo, vous devez respecter les exigences suivantes :

- L'authentification à l'aide de sudo doit être limitée à 3 tentatives en cas de mot de passe incorrect.
- Un message personnalisé de votre choix doit s'afficher si une erreur due à un mot de passe incorrect se produit lors de l'utilisation de sudo.
- Chaque action utilisant sudo doit être archivée, tant les entrées que les sorties. Le fichier journal doit être enregistré dans le dossier /var/log/sudo/.
- Le mode TTY doit être activé pour des raisons de sécurité.
- Pour des raisons de sécurité également, les chemins d'accès pouvant être utilisés par sudo doivent être restreints. Exemple : /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

Enfin, vous devez créer un script simple appelé monitoring.sh. Il doit être développé en bash.

Au démarrage du serveur, le script affichera certaines informations (énumérées ci-dessous) sur tous les terminaux et toutes les 10 minutes (jetez un œil à wall). La bannière est facultative. Aucune erreur ne doit être visible.

Votre script doit toujours être capable d'afficher les informations suivantes :

- L'architecture de votre système d'exploitation et la version de son noyau.
- Le nombre de processeurs physiques.
- Le nombre de processeurs virtuels.
- La mémoire RAM actuellement disponible sur votre serveur et son taux d'utilisation en pourcentage.
- L'espace de stockage actuellement disponible sur votre serveur et son taux d'utilisation en pourcentage.
- Le taux d'utilisation actuel de vos processeurs en pourcentage.
- La date et l'heure du dernier redémarrage.
- Si LVM est actif ou non.
- Le nombre de connexions actives.
- Le nombre d'utilisateurs utilisant le serveur.
- L'adresse IPv4 de votre serveur et son adresse MAC (Media Access Control).
- Le nombre de commandes exécutées avec le programme sudo.

Lors de la soutenance, vous devrez expliquer le fonctionnement de ce script. Vous devrez également l'interrompre sans le modifier. Jetez un œil à cron.

Voici un exemple du fonctionnement prévu du script :

```
Message diffusé depuis root@wil (tty1) (dimanche 25 avril 15:45:00 2021) :

    #Architecture : Linux wil 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux #CPU
    physique : 1
    #vCPU : 1
    #Utilisation de la mémoire :
    74/987 Mo (7,50 %) #Utilisation
    du disque : 1009/2 Go (49 %)
    #Charge CPU : 6,7 %
    #Dernier démarrage : 25/04/2021 14:45
    #Utilisation LVM : oui
    #Connexions TCP : 1 ÉTABLIES #Journal
    utilisateur : 1
    #Réseau : IP 10.0.2.15 (08:00:27:51:9b:a5)
    #Sudo : 42 cmd
```

Vous trouverez ci-dessous deux commandes que vous pouvez utiliser pour vérifier certaines des exigences du sujet : Pour Rocky :

```
[root@wil wil]# head -n 2 /etc/os-release
NAME="Rocky Linux"
VERSION="8.7 (Green Obsidian)"
[root@wil wil]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@wil wil]# ss -tunlp
Netid State  Recv-Q Send-Q  Local Address:Port   Peer Address:Port Process
tcp   LISTEN 0      128           0.0.0.0:4242        0.0.0.0:*     users:(("sshd",pid=28429,fd=6))
tcp   LISTEN 0      128              [::]:4242           [::]:*     users:(("sshd",pid=28429,fd=4))
[root@wil wil]# firewall-cmd --list-service
ssh
[root@wil wil]# firewall-cmd --list-port
4242/tcp
[root@wil wil]# firewall-cmd --state
running
[root@wil wil]# _
```

Pour Debian :

```
root@wil:~# head -n 2 /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
root@wil:/home/wil# /usr/sbin/aa-status
apparmor module is loaded.
root@wil:/home/wil# ss -tunlp
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:Port

tcp   LISTEN 0      128          0.0.0.0:4242       0.0.0.0:*     users:(("sshd",pid=523,fd=3))
tcp   LISTEN 0      128             [::]:4242          [::]:*     users:(("sshd",pid=523,fd=4))
root@wil:/home/wil# /usr/sbin/ufw status
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)
```

Chapitre VI

Partie bonus

Liste bonus :

- Configurez correctement les partitions afin d'obtenir une structure similaire à celle ci-dessous :

```
# lsblk
NAME                    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                       8:0    0  30.8G  0 disk
├─sda1                    8:1    0   500M  0 part  /boot
├─sda2                    8:2    0     1K  0 part
└─sda5                    8:5    0  30.3G  0 part
  └─sda5_crypt          254:0    0  30.3G  0 crypt
    ├─LVMGroup-root     254:1    0    10G  0 lvm   /
    ├─LVMGroup-swap     254:2    0   2.3G  0 lvm   [SWAP]
    ├─LVMGroup-home     254:3    0     5G  0 lvm   /home
    ├─LVMGroup-var      254:4    0     3G  0 lvm   /var
    ├─LVMGroup-srv      254:5    0     3G  0 lvm   /srv
    ├─LVMGroup-tmp      254:6    0     3G  0 lvm   /tmp
    └─LVMGroup-var--log 254:7    0     4G  0 lvm   /var/log
sr0                      11:0    1  1024M  0 rom
```

- Configurez un site Web WordPress fonctionnel avec les services suivants : lighttpd, MariaDB et PHP.
- Configurez un service de votre choix que vous jugez utile (NGINX / Apache2 exclus !). Lors de la soutenance, vous devrez justifier votre choix.

L'exemple montre des tailles de disque arbitraires. Vous devez déterminer la taille appropriée pour chaque partition afin d'assurer un fonctionnement correct tout en évitant une utilisation inutile du disque.

Pour compléter la partie bonus, vous avez la possibilité de configurer des services supplémentaires. Dans ce cas, vous pouvez ouvrir davantage de ports en fonction de vos besoins. Bien entendu, les règles UFW/Firewalld doivent être adaptées en conséquence.

La partie bonus ne sera évaluée que si la partie obligatoire est PARFAITE. Parfaite signifie que la partie obligatoire a été intégralement réalisée et fonctionne sans dysfonctionnement. Si vous n'avez pas satisfait à TOUTES les exigences obligatoires, votre partie bonus ne sera pas évaluée du tout.

Chapitre VII

Soumission et évaluation par les pairs

Vous devez uniquement remettre un fichier signature.txt à la racine de votre dépôt Git. Vous devez y coller la signature du disque virtuel de votre machine. Pour obtenir cette signature, vous devez d'abord ouvrir le dossier d'installation par défaut (il s'agit du dossier dans lequel vos machines virtuelles sont enregistrées) :

- Windows : %HOMEDRIVE%%HOMEPATH%\VirtualBox VMs\
- Linux : ~/VirtualBox VMs/
- MacM1 : ~/Bibliothèque/Conteneurs/com.utmapp.UTM/Données/Documents/
- MacOS : ~/VirtualBox VMs/

Ensuite, récupérez la signature du fichier « .vdi » (ou « .qcow2 » pour les utilisateurs UTM) de votre machine virtuelle au format sha1. Vous trouverez ci-dessous 4 exemples de commandes pour un fichier rocky_serv.vdi :

- Windows : certUtil -hashfile rocky_serv.vdi sha1
- Linux : sha1sum rocky_serv.vdi
- Pour Mac M1 : shasum rocky.utm/Images/disk-0.qcow2
- MacOS : shasum rocky_serv.vdi

Voici un exemple du type de résultat que vous obtiendrez :

- 6e657c4619944be17df3c31faa030c25e43e40af

Veuillez noter que la signature de votre machine virtuelle peut être modifiée après votre première évaluation. Pour résoudre ce problème, vous pouvez dupliquer votre machine virtuelle ou utiliser la fonction « Enregistrer l'état ».

Il est bien sûr INTERDIT de remettre votre machine virtuelle dans votre dépôt Git. Lors de la soutenance, la signature du fichier signature.txt sera comparée à celle de votre machine virtuelle. Si les deux ne sont pas identiques, votre note sera de 0.

L'utilisation de snapshots est INTERDITE. Lors de la défense, si un snapshot est détecté, votre note sera de 0.

Au cours de l'évaluation, une brève **modification du projet** peut parfois être demandée. Il peut s'agir d'un changement mineur de comportement, de quelques lignes de code à écrire ou à réécrire, ou d'une fonctionnalité facile à ajouter.

Bien que cette étape **ne s'applique pas à tous les projets**, vous devez vous y préparer si elle est mentionnée dans les directives d'évaluation.

Cette étape vise à vérifier votre compréhension réelle d'une partie spécifique du projet. La modification peut être effectuée dans n'importe quel environnement de développement de votre choix (par exemple, votre configuration habituelle) et devrait être réalisable en quelques minutes, sauf si un délai spécifique est défini dans le cadre de l'évaluation.
On peut par exemple vous demander d'apporter une petite mise à jour à une fonction ou à un script, de modifier un affichage ou d'ajuster une structure de données pour stocker de nouvelles informations, etc.

Les détails (portée, objectif, etc.) seront précisés dans les **directives d'évaluation** et peuvent varier d'une évaluation à l'autre pour un même projet.

0010 01 11 111 001 000 11 01 10 1 0000 01 1 1010 111 11 0 000
011 00 1 0000 1 0000 0 01 0100 1 0 010 10 01 1 0 0001 0 010 000
00 111 10 111 0010 001100 001100 001100