1) Sur le PC du correcteur : sur son intra, git clone le repo, faire un cat sur le fichier signature.txt
2) Sur mon PC : aller dans C:\Users\julie\VirtualBox VMs
3) Clic droit sur born2beroot
4) Afficher d'autres options
5) Open in Terminal
6) certUtil -hashfile born2beroot.vdi sha1
7) Comparer le fichier signature.txt avec le résultat de la commande
8) Ouvrir VirtualBox, sélectionner born2beroot, cliquer sur Cloner
9) Laisser cocher Clone Intégral
10) Sélectionner, dans MAC Address Policy, « Inclure toutes les adresses MAC de l'interface réseau »
11) Cocher préserver les noms de disque
12) Cocher Keep Hardware UUIDs
13) Cliquer sur Finish

Comment fonctionne une VM et quel est son but ?

Une machine virtuelle (VM) est un environnement simulé par un logiciel (comme VirtualBox) qui permet d'exécuter un système d'exploitation complet sur une machine hôte, sans interaction directe avec le matériel physique.

Chaque VM fonctionne de manière isolée, avec son propre système d'exploitation et ses ressources simulées (processeur, mémoire, disque).

Cela permet d'exécuter plusieurs VM sur une même machine physique.

Les VM sont souvent utilisées pour tester des applications, créer des environnements sécurisés, ou exécuter des systèmes incompatibles avec la machine hôte.

Quelles sont les différences entre Rocky et Debian ?

Debian est une distribution Linux polyvalente, maintenue par une communauté mondiale de bénévoles. Elle se distingue par sa flexibilité, sa stabilité, et sa grande bibliothèque de logiciels, adaptée aussi bien aux environnements de bureau qu'aux serveurs. Elle propose trois branches (stable, testing, unstable) pour répondre à différents besoins. Debian utilise APT comme gestionnaire de paquets et offre une large compatibilité avec divers matériels et architectures.

Rocky Linux, en revanche, est une distribution orientée entreprise, conçue comme une alternative à CentOS après son changement de modèle. Compatible avec Red Hat Enterprise Linux (RHEL), Rocky est stable et offre un support à long terme (10 ans). Cependant, il est davantage ciblé sur les serveurs en production, avec un écosystème moins flexible et une bibliothèque logicielle plus restreinte. Il utilise DNF comme gestionnaire de paquets.

En résumé, Debian est plus adapté aux utilisateurs cherchant polyvalence, personnalisation et support communautaire, tandis que Rocky Linux est optimisé pour les besoins professionnels des entreprises.

Pourquoi choisir Debian ?

Debian est un excellent choix pour ceux qui recherchent un système polyvalent, stable et sécurisé, que ce soit pour un usage personnel ou professionnel. Il bénéficie d'une vaste communauté, d'une bibliothèque de logiciels bien fournie, et d'un système de gestion de paquets (APT) efficace. Sa modularité et ses nombreuses options de personnalisation en font une solution adaptée aussi bien pour des postes de travail que pour des serveurs. De plus, son indépendance vis-à-vis des entreprises garantit une transparence totale et une véritable liberté logicielle.

Différence entre APT et Aptitude :

APT (Advanced Packaging Tool) est un gestionnaire de paquets bas niveau utilisé pour installer, mettre à jour ou supprimer des logiciels sous Linux, tout en gérant les dépendances nécessaires. Il agit comme un outil fondamental qui peut être utilisé par d'autres gestionnaires plus haut niveau, comme apt-get ou apt-cache, et fonctionne strictement en exécutant les commandes données.

Aptitude, en revanche, est un gestionnaire de paquets haut niveau basé sur APT, offrant une interface plus riche, avec des fonctionnalités supplémentaires. Il peut non seulement effectuer les tâches d'APT mais aussi gérer automatiquement les paquets inutilisés, proposer des solutions alternatives pour les dépendances, et faciliter la recherche ou la navigation dans les paquets installés. Aptitude est également disponible en mode texte interactif, ce qui le rend plus ergonomique pour certains utilisateurs.

Résumé : APT est simple et direct, idéal pour les scripts et les tâches spécifiques. Aptitude est plus flexible, convivial et puissant, conçu pour une gestion plus intelligente et interactive des paquets.

Qu’est-ce que AppArmor ?

AppArmor est un système de sécurité de type MAC (Mandatory Access Control) qui limite les actions qu'un processus peut exécuter sur un système. Basé sur des profils attachés à des applications spécifiques, il utilise un contrôle basé sur les chemins de fichiers, rendant ses règles plus simples à écrire et à comprendre. AppArmor est inclus par défaut dans certaines distributions Linux comme Debian, et il est souvent considéré comme plus transparent et facile à utiliser. La commande /usr/sbin/aa-status permet de vérifier son état.

Qu’est-ce que SELinux ?

SELinux (Security-Enhanced Linux) est également un système de sécurité MAC, mais il est basé sur un modèle plus complexe et puissant. Les règles de SELinux définissent comment les applications, utilisateurs et fichiers peuvent interagir, en fournissant un contrôle précis grâce à des contextes de sécurité. Bien que SELinux offre une meilleure isolation et une granularité supérieure, il est réputé pour sa complexité et sa difficulté d’utilisation. La création et la gestion des règles nécessitent souvent plus d'expertise, bien que certains outils permettent de les générer automatiquement.

Différences principales

- **Facilité d’utilisation** : AppArmor est plus simple à configurer grâce à son contrôle basé sur les chemins, tandis que SELinux est plus complexe mais offre une sécurité plus fine.
- **Gestion des règles** : AppArmor utilise des règles lisibles et adaptées à l'humain, tandis que les règles de SELinux sont basées sur des contextes et sont plus détaillées.
- **Support natif** : AppArmor est souvent préinstallé sur des distributions comme Debian, tandis que SELinux est principalement associé à des distributions comme Red Hat et CentOS.

En résumé, AppArmor est idéal pour les systèmes nécessitant une sécurité rapide et simple, tandis que SELinux est préférable pour des environnements nécessitant un contrôle avancé et une isolation stricte.

14) Lancer le clone de la VM
15) Montrer que la machine n'a pas d'environnement graphique au démarrage
16) Entrer la passphrase de décryptage
17) Se connecter à la machine en tant que juduchar
18) Entrer le mot de passe de juduchar
19) sudo nano /etc/login.defs
    PASS_MAX_DAYS 30
    PASS_MIN_DAYS 2
    PASS_WARN_AGE 7

20) sudo chage -l juduchar
    Minimum number of days between password change : 2
    Maximum number of days between password change : 30
    Number of days before password expires : 7

Cette politique de mot de passe assure un équilibre entre sécurité et facilité de gestion des mots de passe pour les utilisateurs

Empêche les utilisateurs de changer rapidement plusieurs fois leur mot de passe pour revenir à un ancien mot de passe connu, tout en laissant une flexibilité suffisante

Oblige les utilisateurs à renouveler régulièrement leur mot de passe pour limiter l'exposition d'un mot de passe compromis

Prévient à l'avance qu'un changement de mot de passe sera bientôt obligatoire

21) sudo ufw status
    status : active

22) sudo systemctl status ssh
    status : active

23) lsb_release -a || cat /etc/os-release

    Debian

24) getent group sudo
    juduchar
25) getent group user42
    juduchar

26) sudo adduser new_username
27) Lui assigner un mot de passe de son choix, de 10 caractères minimums, dont une majuscule, une minuscule et un chiffre, pas plus de 3 caractères consécutifs à la suite, et ne contenant pas le nom de l'utilisateur
28) Le module pwquality permet de définir des règles de mot de passe
    Ces règles sont configurées avec cette commande :
    sudo nano /etc/security/pwquality.conf
29) sudo groupadd evaluating
30) sudo usermod -aG evaluating new_username
31) getent group evaluating

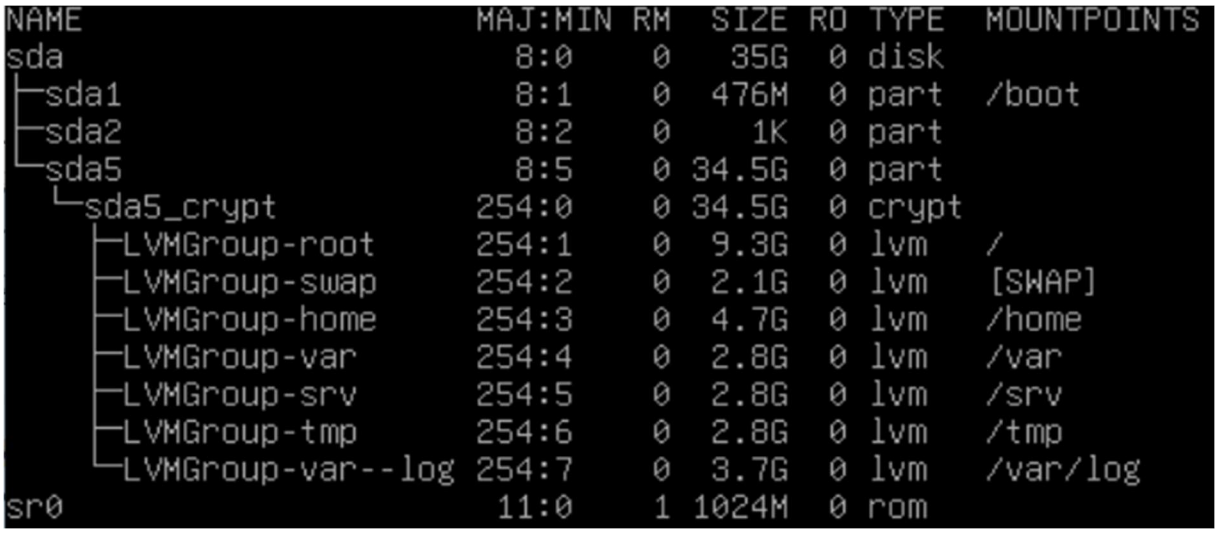
Cette politique de mot de passe permet une résistance accrue aux attaques par force brute, par dictionnaire et ciblées, tout en restant raisonnable à suivre pour les utilisateurs

Inconvénients : difficile et complexe à mettre en place pour les utilisateurs, pas facile à retenir donc peut être écrits sur des supports non sécurisés (post-it, carnet), risque d'oubli, fausse impression de sécurité, impact sur l'expérience utilisateur

32) hostnamectl
    juduchar42

33) Modifier le hostname et redémarrer la VM
    sudo hostnamecrl set-hostname new_hostname
    sudo reboot

34) lsblk



Qu’est-ce que LVM ?

LVM (Logical Volume Manager) est un outil de gestion des volumes logiques sous Linux. Contrairement à la gestion classique des partitions, LVM permet une gestion flexible et dynamique de l’espace disque. Cela inclut la création, la redimension des partitions (volumes), et l’allocation de l’espace disque sans devoir redémarrer ou perturber le système.

Comment fonctionne LVM ?

LVM repose sur une abstraction qui découpe et regroupe le stockage physique en plusieurs niveaux :

1. Physical Volumes (PV) :
    - Ce sont les disques ou partitions physiques (ex. : /dev/sda1) qui constituent la base de LVM.
    - Les PV sont ajoutés à un groupe pour être utilisés dynamiquement.
2. Volume Groups (VG) :
    - Les Physical Volumes sont regroupés dans un Volume Group, qui agit comme une "réserve" globale d’espace disque.
    - Exemple : Si vous ajoutez deux disques de 1 To chacun à un VG, ce groupe disposera de 2 To d’espace disponible.
3. Logical Volumes (LV) :
    - À partir du Volume Group, vous pouvez créer des Logical Volumes, qui fonctionnent comme des partitions classiques (par exemple, pour monter un système de fichiers ou swap).
    - Les LV peuvent être redimensionnés dynamiquement ou déplacés sans affecter les données.

35) dpkg -l | grep sudo
36) sudo usermod -aG sudo new_username
37) sudo visudo ls
38) cd /var/log/sudo
39) tail /var/log/sudo/sudo.log
40) sudo whoami
41) tail /var/log/sudo/sudo.log

42) sudo ufw status numbered

UFW (Uncomplicated Firewall) est une interface simplifiée pour gérer le pare-feu Netfilter intégré au noyau Linux. Il offre une méthode simple et intuitive pour configurer des règles de pare-feu, même pour les utilisateurs avec peu d'expérience en administration système.

UFW permet de restreindre les connexions réseau, en spécifiant quelles adresses, ports, ou services sont autorisés ou bloqués.

43) sudo ufw allow 8080
44) sudo ufw status numbered
45) sudo ufw delete 4
46) sudo ufw delete 2

47) sudo service ssh status
    ssh active port 4242

SSH (Secure Shell) est un protocole réseau qui permet d'établir une connexion sécurisée entre deux machines. Il est principalement utilisé pour accéder à distance à un serveur ou un autre ordinateur, tout en garantissant la confidentialité et l'intégrité des données échangées. SSH utilise un chiffrement fort pour protéger les communications, ce qui en fait un outil clé pour les administrateurs système et les développeurs.

Avantages de l'utilisation de SSH :

1. **Connexion sécurisée :**
    - Les données transmises sont chiffrées, empêchant les interceptions et les attaques de type "man-in-the-middle". Cela garantit la confidentialité des mots de passe, commandes, et données échangées.
2. **Authentification robuste :**
    - SSH prend en charge plusieurs méthodes d'authentification, notamment par mot de passe ou par clé publique/privée, cette dernière étant plus sûre et largement utilisée.

3. **Accès distant :**
    - Permet d'administrer des serveurs et systèmes à distance de manière sécurisée. Les utilisateurs peuvent exécuter des commandes, transférer des fichiers, ou gérer des processus comme s'ils étaient physiquement devant la machine.
4. **Transfert de fichiers sécurisé :**
    - Grâce à des outils comme **SCP** (Secure Copy Protocol) et **SFTP** (SSH File Transfer Protocol), SSH facilite le transfert de fichiers en toute sécurité.
5. **Port forwarding (tunnels sécurisés) :**
    - SSH permet de rediriger des ports de manière sécurisée, par exemple pour accéder à des services locaux d'un serveur distant ou pour contourner des restrictions réseau.
6. **Simplicité et disponibilité :**
    - SSH est facile à utiliser et est installé par défaut sur de nombreuses distributions Linux et Unix. Des clients SSH sont également disponibles pour Windows (ex. : PuTTY) et macOS.
7. **Compatibilité multi-plateforme :**
    - SSH fonctionne sur presque tous les systèmes d'exploitation, ce qui en fait un outil universel pour l'administration distante.
8. **Extensibilité et automatisation :**
    - Avec des clés SSH, il est possible d'automatiser des connexions ou des tâches entre machines sans avoir à entrer de mot de passe, ce qui est idéal pour les scripts ou les outils de déploiement.

48) Ouvrir un terminal
49) ssh new_user@127.0.0.1 -p 4242
50) ssh root@127.0.0.1 -p 4242
    permission denied

51) cd /root
52) nano monitoring.sh

Cron est un outil système sous Linux/Unix qui permet d'automatiser l'exécution de tâches répétitives à des moments précis ou selon une fréquence définie. Ces tâches, appelées **cron jobs**, sont spécifiées dans un fichier appelé **crontab**

53) sudo crontab -e
54) sudo crontab -r
55) sudo reboot
56) sudo crontab -e

Gitea est une application web open-source légère pour héberger des dépôts Git, alternative à GitHub, facile à installer et performante grâce à son développement en Go. Elle permet de créer, gérer et versionner des projets avec Git, tout en offrant une interface simple pour collaborer, suivre les tâches (issues), gérer les utilisateurs, et configurer des permissions.

Gitea est idéal pour un hébergement sur un serveur personnel ou privé, offrant un contrôle total des données, sans dépendance à un service tiers, et sans frais, même pour des fonctionnalités avancées comme l'intégration CI/CD. Elle est hautement personnalisable et adaptée aux projets nécessitant confidentialité ou fonctionnement hors ligne, comme dans des réseaux privés ou déconnectés.

GitHub, en revanche, est plus adapté aux projets open source publics nécessitant une collaboration mondiale ou des outils intégrés clé en main (GitHub Actions, Codespaces). Le choix entre les deux dépend des besoins en confidentialité, contrôle, coûts et accessibilité mondiale.