Hes·so VALAIS WALLIS

Haute Ecole de Gestion
Hochschule für Wirtschaft

Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Configuration de la sécurité de base des comptes et des accès aux fichiers, répertoires

Introduction aux technologies de l'information & Infrastructures et réseaux

Élève : Zotrim Uka

Professeurs : Xavier Barmaz et David Russo

Déposé le : 05 janvier 2023

Site internet : https://www.hes-so.ch

Résumé exécutif

La sécurité informatique est très importante parce qu'elle protège contre les mauvaises choses qui peuvent arriver aux ordinateurs, comme les piratages et les virus. Pour s'assurer que le système est en sécurité, il faut bien gérer les comptes des utilisateurs et les groupes.

On peut créer, supprimer et changer ces éléments en utilisant différentes commandes. Par exemple, "useradd" permet de créer un nouveau compte, et "userdel" permet de supprimer un compte existant ainsi que « usermod » qui nous donne la possibilité de modifier les informations d'un compte.

En plus de gérer les comptes et les groupes, il faut aussi protéger les serveurs contre les connexions non autorisées. Nous examinons également fail2ban. Cet outil bloque temporairement les adresses IP des utilisateurs qui essaient de se connecter de manière non autorisée, ce qui rend le serveur plus sécurisé. En comprenant comment utiliser ces outils et en les mettant en pratique, on peut protéger le système contre les éléments néfastes et ainsi assurer une gestion plus sécurisée et le gérer de manière sécurisée.

Mots clés : accès aux fichiers et répertoires, comptes, sécurité de base, commandes

Remerciement

Je tiens à remercier chaleureusement mon cousin Leutrim Rogova pour son aide précieuse dans la correction des fautes d'orthographe et de syntaxe de mon travail. Sa précision et son attention aux détails ont été essentielles pour améliorer la qualité de mon travail et me permettre de remettre un document professionnel et bien écrit.

Sa contribution a été précieuse et m'a permis de me concentrer sur le contenu de mon travail, sachant que la forme était en de bonnes mains. Je suis reconnaissant envers Leutrim pour son soutien et sa collaboration, et je lui suis très reconnaissant pour son temps et son effort.

Je suis convaincu que cette expérience de travail en équipe sera bénéfique pour moi dans le futur et je suis heureux de pouvoir compter sur Leutrim pour son expertise et son soutien à l'avenir. Encore une fois, merci Leutrim pour ton aide précieuse et ta contribution précieuse à mon travail.

Table des matières

Table des illustrations

Index

Sudo	:	De l’anglais « substitute user do » C'est un logiciel qui permet à un utilisateur d'exécuter des commandes avec les privilèges de super utilisateur, également appelé "root".
UID	:	De l’anglais « User id » est un identifiant unique attribué à chaque utilisateur
GID	:	De l’anglais « Group id » est un identifiant unique attribué à chaque groupe.
su	:	De l’anglais « switch user »
chown	:	De l’anglais «change owner » une commande qui sert à changer le propriétaire d'un fichier ou d'un répertoire dans un système de fichiers
chmod	:	De l’anglais «change mode » une commande qui sert à changer les permissions d'un fichier ou d'un répertoire dans un système de fichiers
chgrp	:	De l’anglais « change group »
ip	:	De l’anglais « internet protocole »
useradd	:	Commande pour ajouter un utilisateur
userdel	:	Commande pour supprimer un utilisateur
cut	:	De l’anglais « couper » est une commande pour récupérer du contenu d’un fichier avec délimiteur et numéro de colonne
grpadd	:	Commande pour ajouter un groupe
grpdel	:	Commande pour supprimer un groupe

1. Introduction

Pour commencer, nous allons définir les termes clés qui seront utilisés tout au long de notre présentation sur la configuration de la sécurité de base des comptes et des accès aux fichiers et répertoires. Ces termes clés comprennent :

- Les comptes :

Les comptes sont des identifiants qui permettent à un utilisateur de se connecter à un système informatique ou à un réseau. Ils sont généralement associés à un nom d'utilisateur et à un mot de passe, et leur utilisation permet de limiter l'accès aux différentes parties du système ou du réseau.

- Accès aux fichiers et répertoires :

L'accès aux fichiers et répertoires désigne la capacité d'un utilisateur à lire, écrire ou exécuter des fichiers et répertoires stockés sur un système informatique ou un réseau.

- Sécurité de base :

Un ensemble de mesures destinées à protéger les systèmes informatiques et les réseaux contre les menaces potentielles, telles que les virus, les logiciels espions et les attaques de hackers. Elle comprend des mesures comme la création de mots de passe forts, la mise à jour régulière des logiciels de sécurité et la configuration adéquate des pares-feux et autres dispositifs de sécurité.

2. Développement

2.1 L'importance de la sécurité et les menaces potentielles

Pour protéger notre ordinateur, nous devons faire attention à la sécurité informatique. Nous pouvons le faire en gérant les permissions et les comptes d'utilisateurs correctement. Cela nous permet de contrôler qui peut accéder à quels fichiers et dossiers et de protéger nos données importantes.

Il y a beaucoup d'éléments qui peuvent causer des problèmes à notre ordinateur. Les virus, les logiciels espions, les rançongiciels et les attaques par force brute sont quelques exemples de menaces qui peuvent nous nuire.

Il est important de prendre des mesures de sécurité pour protéger notre ordinateur contre ces menaces, c'est pour cela qu'il est important de gérer correctement les comptes et les permissions. Ainsi, nos données et notre réseau sont protégés contre les potentiels attaques.

2.2 Mesures de sécurité

Il y a plusieurs manières de protéger notre ordinateur. L'une d'elles est d'utiliser un pare-feu. Un pare-feu nous pouvons imager cela avec un mur qui bloque les connexions non autorisées à notre réseau, ce qui va donc nous aider à contrôler qui peut accéder à notre ordinateur et à protéger nos données importantes.

Un autre moyen de protection est l'utilisation d'un logiciel antivirus. Un antivirus détecte et bloque les virus et autres programmes malveillants avant qu'ils ne causent des problèmes à notre ordinateur.

Il est aussi important de mettre régulièrement à jour notre ordinateur et nos logiciels, ce qui va permettre d'apporter des correctifs de sécurité qui corrigent les failles de sécurité connues et renforcent la sécurité de notre ordinateur.

Nous pouvons aussi protéger notre ordinateur en utilisant la double authentification, il s'agit d'une méthode de sécurité qui nous demande de vérifier notre identité. La double authentification nécessite un appareil mobile, comme un téléphone, pour générer les codes temporaires.

Enfin, nous devons gérer correctement les comptes et les permissions pour protéger notre ordinateur. En contrôlant les accès à quels fichiers et dossiers, ainsi qu'en utilisant des mots de passe sécurisés, nous pouvons empêcher les personnes n'ayant pas les autorisations d'accéder à nos données importantes. Malgré toutes les précautions mises en place, il se peut qu'il subsiste tours des failles.

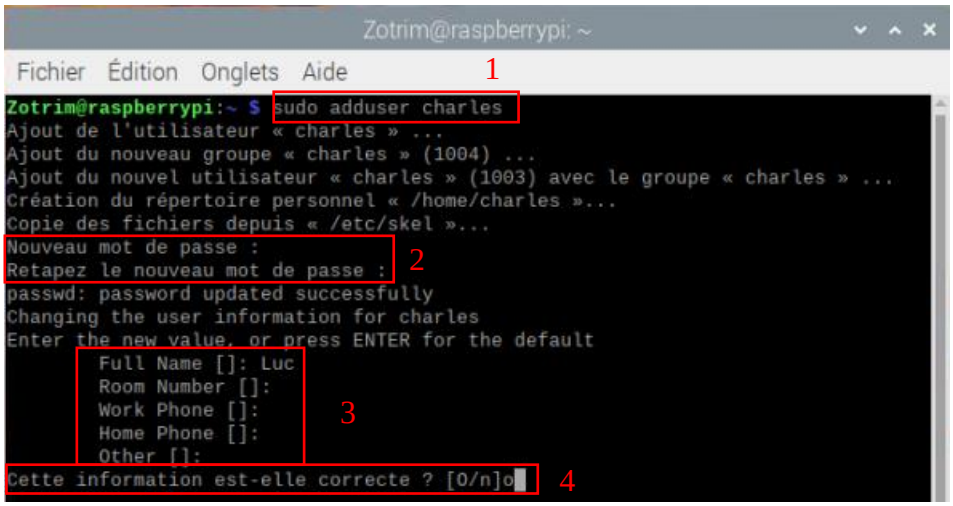
2.3 Comment créer et gérer les comptes utilisateurs

2.3.1 Créer un utilisateur

Pour créer un utilisateur, nous devons :

1. Utiliser la commande : sudo adduser nom_utilisateur.
2. Entrer un mot de passe et le retaper pour le confirmer.
3. Remplir les informations personnelles de l'utilisateur, mais nous pouvons aussi sauter cette étape en appuyant sur "Entrée".
4. Si les informations sont correctes, nous pouvons entrer la lettre "o" et appuyer sur "Entrée".

Figure 1: Créer un utilisateur



Source : Auteur

Pour commencer, nous devons utiliser sudo pour créer un utilisateur, car seuls les administrateurs peuvent créer, modifier et supprimer des utilisateurs.

Pour finir, un mot de passe idéal doit contenir au moins 16 caractères, avec des majuscules, des chiffres et des caractères spéciaux.

Nous pouvons vérifier si notre utilisateur a bien été créé en utilisant la commande « id nom_utilisateur ».

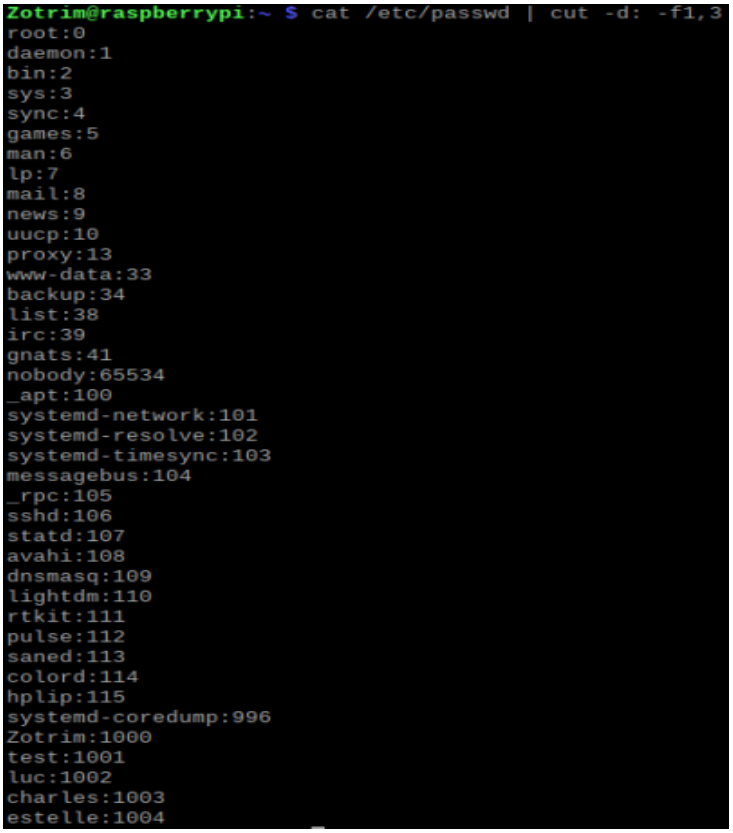
Figure 2 : commande id

Source : Auteur

Nous donnons un numéro unique à chaque utilisateur (UID). Si nous avons deux utilisateurs différents, le système va leur donner deux numéros différents. Il y a également un numéro unique qui est à chaque groupe (GID). Un utilisateur peut appartenir à plusieurs groupes différents, et chacun de ces groupes à son propre numéro unique.

Nous pouvons également voir la liste de tous les utilisateurs. Pour cela nous devons utiliser la commande « cat /etc/passwd | cut -d : -f1,3 » qui permet d'afficher les colonnes 1 et 3 du fichier « /etc/passwd ».

Figure 3 : liste utilisateurs



Source : Auteur

Le fichier « /etc/passwd » est un fichier de données que nous utilisons pour stocker des informations sur les utilisateurs du système. Nous y mettons généralement le nom d'utilisateur et un numéro unique.

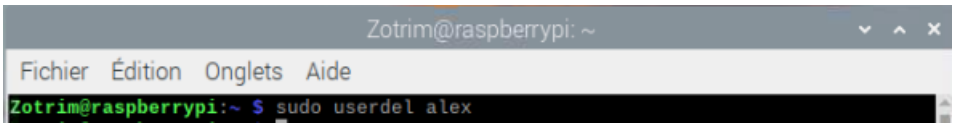
Nous utilisons la commande « cut » pour couper (extraire) des colonnes d'un fichier texte qui nous montre seulement certaines colonnes d'un fichier. Nous pouvons dire à cut quelles colonnes nous voulons voir en utilisant « -f numéro_colonne ». Nous pouvons donc demander plusieurs colonnes en les mettant dans une liste séparée par des virgules. Par exemple, « -f 1,3 » affichera les colonnes 1 et 3 comme sur l'image ci-dessus.

2.3.2 Supprimer un utilisateur

Nous avons la possibilité de supprimer des utilisateurs, pour cela nous utilisons la commande « sudo userdel nom_utilisateur », l'inconvénient de cette commande est qu'elle garde le répertoire.

Pour supprimer l'utilisateur ainsi que son répertoire, nous utilisons la commande suivante « sudo userdel -r nom_utilisateur ».

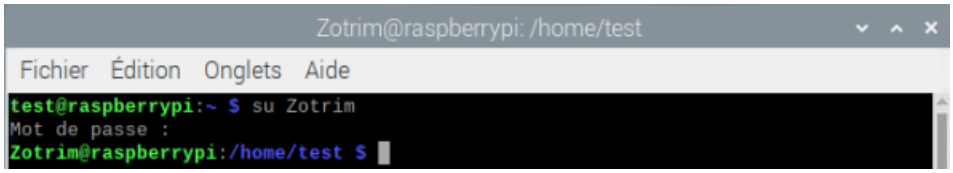
Figure 4 : supprimer un utilisateur



Source : Auteur

Nous avons la possibilité de changer d'utilisateur à l'aide de la commande « su nom_utilisateur » et nous devons entrer le mot de passe du compte. Dans l'exemple ci-dessous, le compte connecté est « test ». Ce compte n'a aucun droit, nous voulons nous connecter à un compte root pour pouvoir : ajouter, modifier et supprimer un utilisateur.

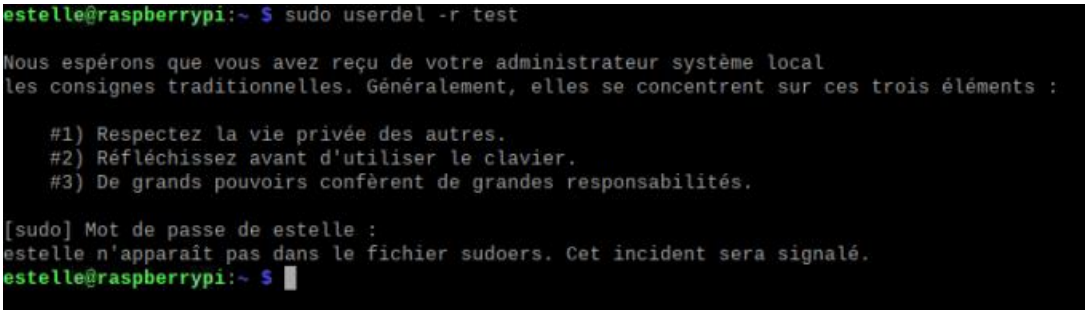
Figure 5 : changer d'utilisateur



Source : Auteur

Si nous voulons supprimer un compte alors que nous ne sommes pas administrateur, nous avons un message d'erreur comme sur l'image ci-dessous.

Figure 6 : supprimer un utilisateur et son répertoire



Source : Auteur

2.3.3 Modifier un utilisateur

Nous avons la possibilité de modifier un utilisateur. Notamment lorsqu'une personne change de nom de famille. Pour cela nous employons la commande : « sudo usermod nom_utilisateur ».

Mais nous avons plusieurs types de modification grâce aux options. Pour les utiliser nous devons formuler de cette manière la commande : « sudo usermod -*lettre* nom_utilisateur » Nous voyons différentes options disponibles :

- -c : modifie le champ "commentaire" de l'utilisateur. Cette option permet de mettre à jour les informations de contact de l'utilisateur, comme son nom complet, son adresse de bureau, son numéro de téléphone, etc.
- -d : modifie le répertoire personnel de l'utilisateur. Cette option permet de changer l'emplacement du répertoire personnel de l'utilisateur (par exemple, /home/utilisateur).
- -e : modifie la date d'expiration de l'utilisateur. Cette option permet de définir une date à laquelle l'utilisateur ne pourra plus se connecter au système.
- -l : changer le nom d'utilisateur. Cette option permet de changer le nom d'utilisateur de l'utilisateur (par exemple, de utilisateur1 à utilisateur2).

Pour voir toutes les options, nous saisissons la commande « man usermod » dans un terminal.

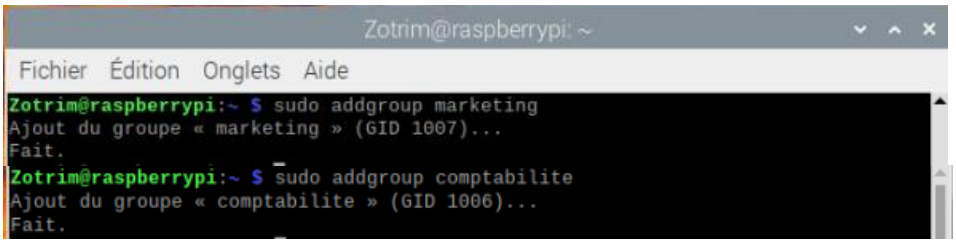
2.3.4 Créer un groupe

Maintenant, nous allons voir comment les groupes fonctionnent. Pour commencer, les groupes sont utilisés pour regrouper des utilisateurs, ce qui peut être utile pour la gestion des autorisations d'accès à des fichiers et des répertoires. Par exemple, nous avons la possibilité de donner rapidement les accès à plusieurs utilisateurs à un certain répertoire, en créant à un groupe. Ainsi, il suffit de donner les autorisations d'accès directement à cegroupe, pour que l'ensemble des membres puissent en bénéficier, plutôt que de les octroyer individuellement. Ainsi, vous pouvez facilement gérer les accès des utilisateurs à des ressources partagées sur le système en utilisant les groupes.

Lors de la création d'un un utilisateur, nous créons également un groupe du même nom avec son numéro. Par exemple, si nous créons maintenant le compte d'utilisateur Charles, nous créons également un groupe Charles.

Pour créer un groupe nous saisissons la commande « sudo addgroup nom_groupe ». Lorsque nous entrons cette commande, nous obtenons un GID qui apparaît.

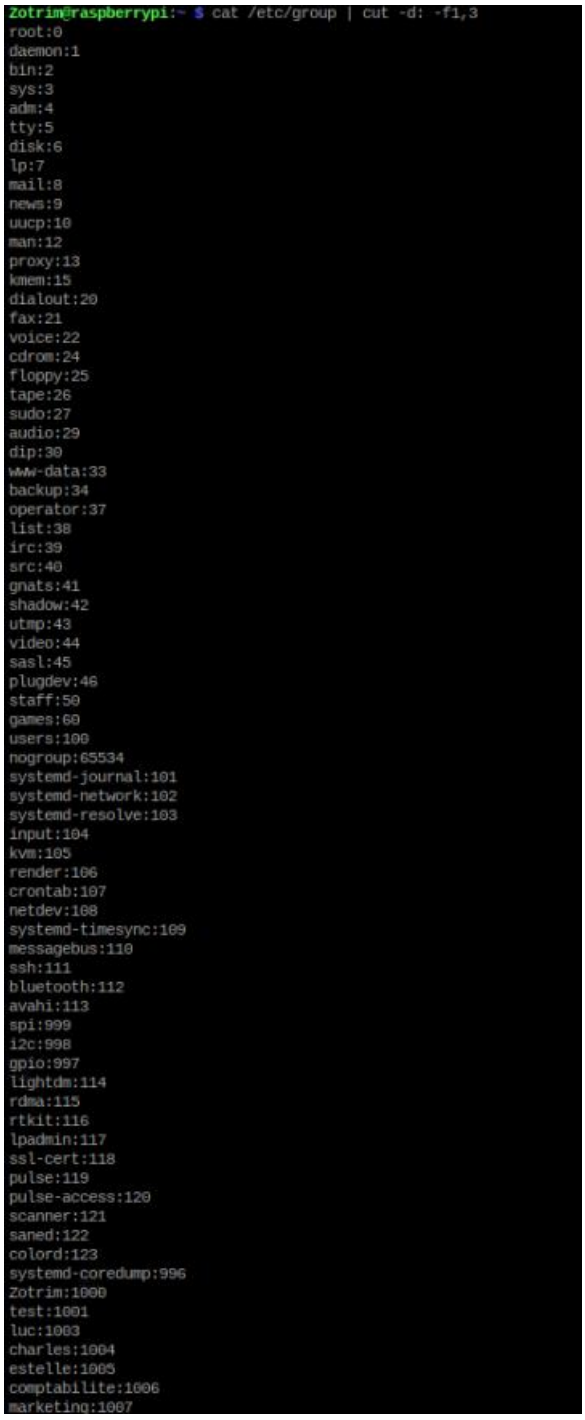
Figure 7 : Créer groupes



Source : Auteur

Comme pour la liste des utilisateurs, nous pouvons également voir la liste des groupes. Nous utilisons la même commande mais nous remplaçons « passwd » par « group ». Nous avons vu précédemment ce que fait la commande cut (page 5).

Figure 8 : liste des groupes



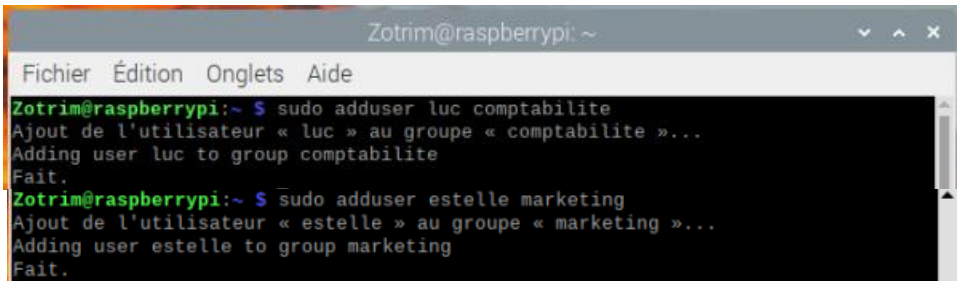
Source : Auteur

2.3.5 Ajouter un utilisateur dans un groupe

Pour ajouter des utilisateurs à différents groupes, il nous suffit de saisir la commande suivante : sudo adduser nom_utilisateur nom_groupe.

Dans l'exemple ci-dessous, nous ajoutons « estelle » dans le groupe marketing. Nous faisons de même pour « luc », mais nous l'ajoutons dans le groupe comptabilité.

Figure 9 : ajouter un utilisateur dans un groupe

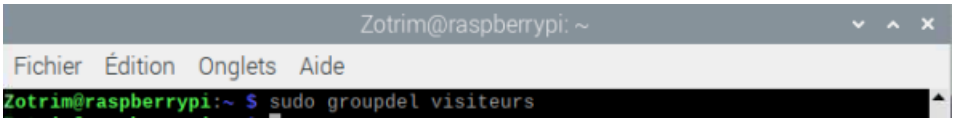


Source : Auteur

2.3.6 Supprimer un groupe

Pour supprimer un groupe nous utilisons la commande : « sudo groupdel nom_groupe ».

Figure 10 : supprimer un groupe



Source : Auteur

La suppression d'un groupe est impossibl tant qu'il contient des utilisateurs. Nous devons d'abord retirer ces utilisateurs du groupe avant de pouvoir le supprimer, pour cela, nous pouvons utiliser la commande gpasswd pour retirer des utilisateurs d'un groupe « sudo gpasswd -d nom_utilisateur nom_groupe ».

2.3.7 Modifier un groupe

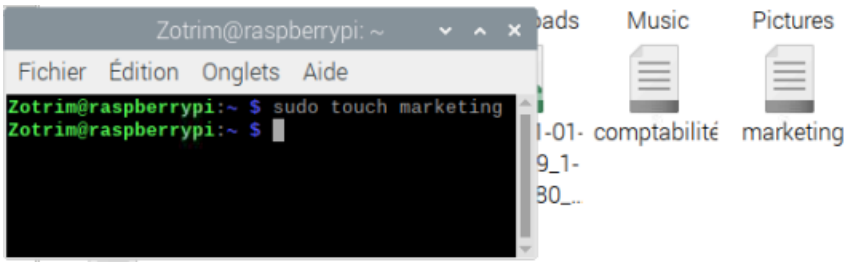
La commande chgrp (abréviation de "change group") nous permet de changer le groupe d'un fichier ou d'un répertoire sur un système Linux.

Pour utiliser la commande chgrp, nous spécifions le nom du groupe auquel nous souhaitons que le fichier ou le répertoire appartienne, ainsi que le nom du fichier ou du répertoire en question « sudo chgrp nom_groupe nom_fichier »

2.3.8 Les permissions d'un fichier

Nous allons créer deux fichiers pour le département de la comptabilité et celui du marketing. Pour cela nous utilisons la commande « sudo touch marketing » pour créer le fichier « marketing », idem pour créer le fichier de « comptabilité » mais dans la commande nous remplaçons « marketing » par « comptabilité », c'est-à-dire « sudo touch comptabilité » comme sur l'image ci-dessous.

Figure 11 : Créer des fichiers



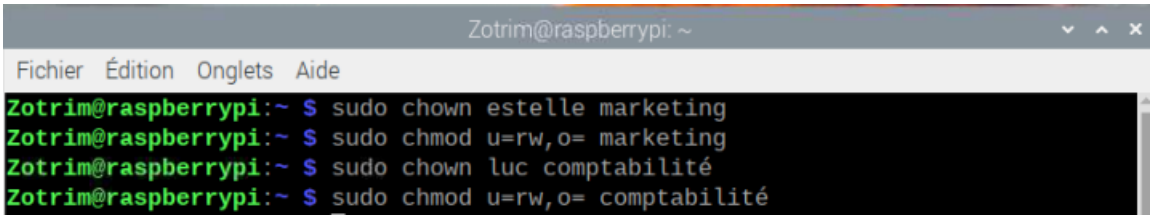
Source : Auteur

Maintenant nous allons limiter les accès aux groupes.

Pour commencer nous utilisons la commande « sudo chown estelle marketing » qui va nous permettre de changer le propriétaire d'un fichier ou d'un répertoire.

Pour finir, nous entrons la commande « sudo chmod u=rw, o = marketing ». Elle permet de changer les permissions d'un fichier ou d'un répertoire nommé "marketing".

Figure 12 : limiter les accès



Source : Auteur

u=rw signifie que le propriétaire du fichier ou du répertoire a le droit de lire et d'écrire dans ce fichier ou ce répertoire.

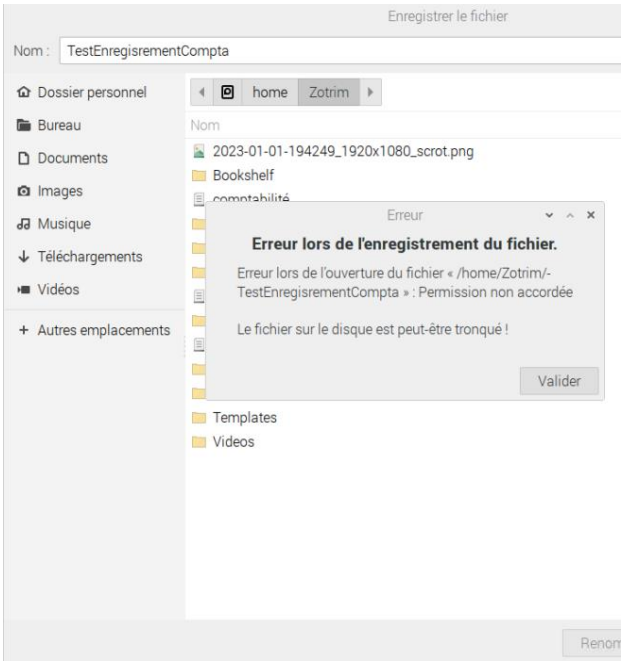
o=r signifique que les autres utilisateurs et groupes n'ont pas permissions ni d'écriture, ni de lecture et ni d'exécution.

Nous avons trois types de droits :

- r : droit de lecture (READ)
- w : droit d'écriture (WRITE)
- x : droit d'exécution (EXECUTE)

Nous avons précédemment créé un fichier « comptabilité » (c.f p.12). Sur ce fichier, seul « Luc » et le groupe peuvent y accéder. Nous essayons d'ouvrir ce fichier en utilisant un autre compte utilisateur et qui ne fait pas parti du groupe « comptabilité ». Nous apercevons sur l'image ci-dessous, que nous n'avons pas le droit modifier ou d'enregistrer le fichier même si nous changeons le nom.

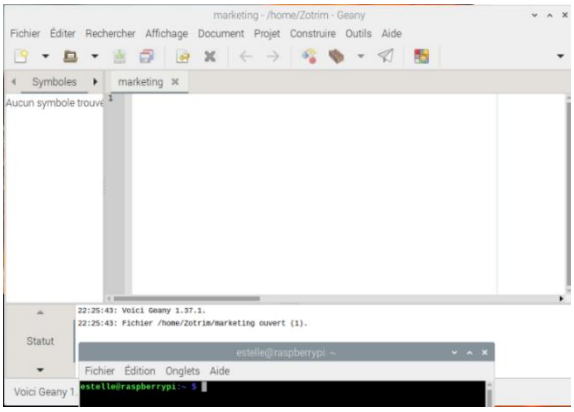
Figure 13 : Message d'erreur



Source : Auteur

Puis, nous nous connectons avec le compte « estelle » et nous essayons d'ouvrir le fichier « marketing ». Cette fois, il n'y pas de message d'erreur à l'ouverture du fichier, car, estelle et les membres du groupes, possède les accès adéquats.

Figure 14 : Ouvrir un fichier avec accès limité



Source : Auteur

2.3.9 Différences entre un groupe primaire et secondaire

Les groupes primaires et secondaires gèrent les accès et les permissions d'un utilisateur sur un système informatique.

Un groupe primaire d'un utilisateur détermine les permissions et les droits qui lui sont accordés sur le système. Un utilisateur ne peut avoir qu'un seul groupe primaire, et il hérite de toutes les permissions et droits associés à ce groupe.

Un groupe secondaire, quant à lui, est un groupe supplémentaire auquel un utilisateur peut appartenir. Un utilisateur peut appartenir à plusieurs groupes secondaires, ce qui lui permet de bénéficier de permissions et de droits supplémentaires sur le système. Cependant, les groupes secondaires ne sont pas prioritaires et n’exercent pas la même influence que le groupe primaire sur les permissions et les droits de l'utilisateur.

Lorsqu'un utilisateur crée une ressource, comme un fichier ou un dossier, cette ressource est automatiquement associée à l'utilisateur qui l'a créée et à son groupe primaire. Cependant, aucun groupe secondaire n'est associé à cette ressource. Si l'utilisateur souhaite partager la ressource avec d'autres utilisateurs appartenant à ses groupes secondaires, il devra le faire manuellement en modifiant les permissions de la ressource.

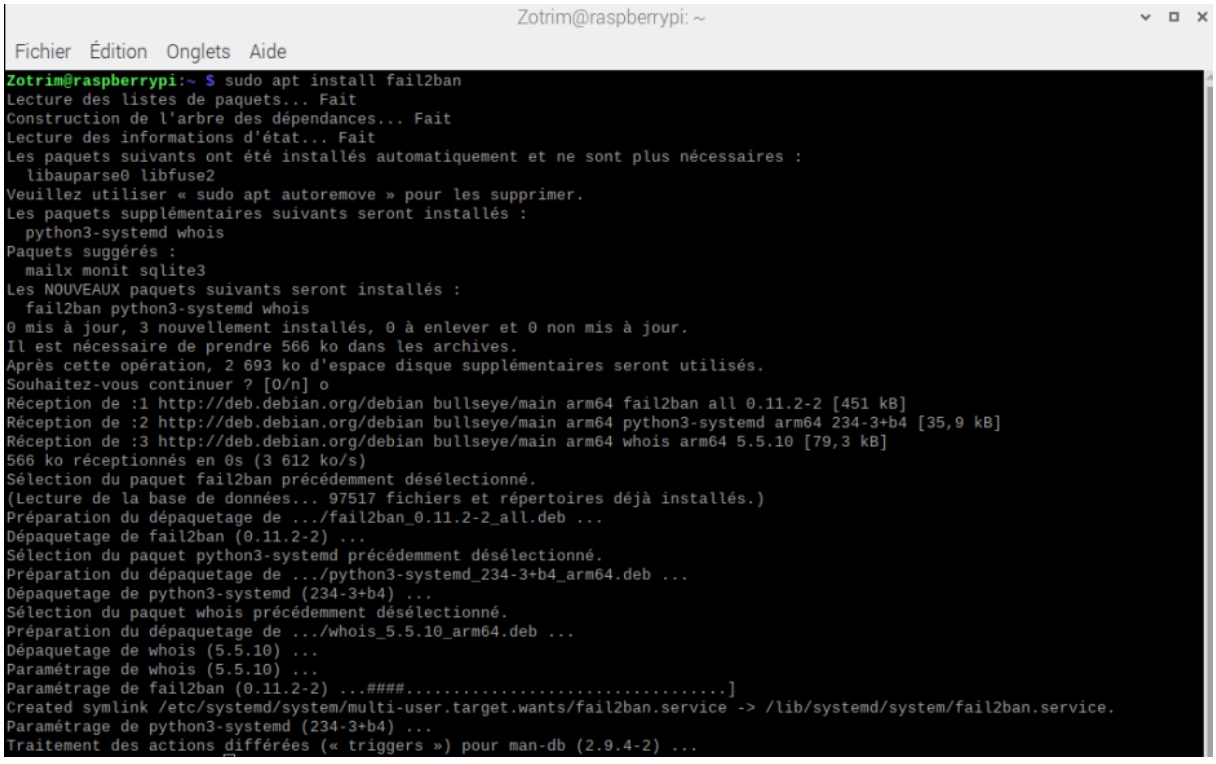
2.4 Fail2ban

Fail2ban : C'est un outil de sécurité qui nous aide à protéger notre ordinateur contre les tentatives de connexion répétées et non autorisées. Il fonctionne en regardant les logs du système pour trouver les tentatives de connexion suspectes et en bloquant l'adresse IP de la personne qui essaie de se connecter avec le pare-feu du système. Cela empêche les attaquants de continuer à essayer de se connecter et de causer des problèmes sur notre ordinateur.

Les logs sont très utiles pour les administrateurs de système et les développeurs, car ils nous permettent de comprendre ce qui se passe sur le système et de résoudre les problèmes qui peuvent survenir. Par exemple, si un service ne fonctionne pas correctement, les logs peuvent aider à identifier la cause de ce problème et à trouver une solution.

Pour installer fail2ban, nous entrons la commande « sudo apt install fail2ban ».

Figure 15 : installer fail2ban

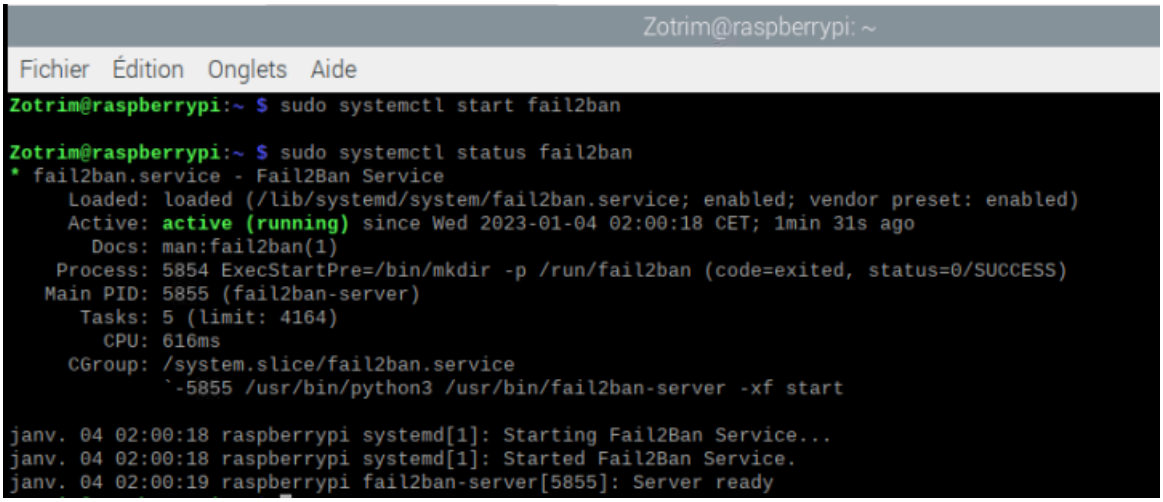


Source : Auteur

Pour démarrer le service, nous utilisons la commande « sudo systemctl start fail2ban ».

Nous pouvons également entrer la commande « sudo systemctl status fail2ban » qui nous sert à vérifier si le programme fonctionne.

Figure 16 : Démarrer fail2ban



Source : Auteur

Pour que le service se lance au démarrage, nous utilisons la commande « sudo systemctl enable fail2ban ».

Figure 17 : Activer fail2ban au démarrage du système

Source : Auteur

2.5 Les audits

Les audits sur Linux sont des outils très utiles pour surveiller et suivre les activités et les événements qui se déroulent sur un système Linux. Ils permettent de collecter et de stocker des informations sur les actions effectuées par les utilisateurs, les programmes et les services, ainsi que sur les modifications apportées aux fichiers et aux répertoires du système.

Il existe de nombreux outils d'audit disponibles pour Linux, chacun ayant ses propres fonctionnalités et avantages. Parmi les plus populaires, on retrouve Auditd, Syslog et Logwatch.

Auditd est un outil intégré à la plupart des distributions Linux qui permet de surveiller en temps réel les activités du système et de stocker les informations dans un journal d'audit. Il offre de nombreuses options de configuration pour personnaliser les types d'événements qui sont enregistrés et la façon dont ils sont stockés.

Syslog est un autre outil d'audit couramment utilisé sur Linux. Il permet de collecter les messages générés par les programmes et les services du système et de les stocker dans des fichiers de log. Syslog est particulièrement utile pour suivre les erreurs et les problèmes rencontrés par les programmes et les services.

Enfin, Logwatch est un outil d'audit qui analyse les journaux du système et envoie des rapports résumant les activités et les événements importants par courriel ou par SMS. Il permet de surveiller de manière proactive les activités du système et de détecter rapidement les problèmes ou les anomalies.

En utilisant l'un de ces outils d'audit, les administrateurs peuvent suivre de près les activités du système et assurer la sécurité et la stabilité du système Linux.

3. Conclusion générale

Dans ce rapport, nous avons examiné l'importance de la sécurité informatique et les menaces potentielles qui peuvent affecter un système.

Nous avons également abordé différentes mesures de sécurité, telles que la gestion des comptes utilisateurs et des groupes. Nous avons expliqué comment créer, supprimer et modifier ces éléments à l'aide de différentes commandes, et comment utiliser fail2ban pour protéger les serveurs contre les tentatives de connexion non autorisées.

En conclusion, la sécurité informatique est cruciale pour protéger les systèmes contre les menaces potentielles. En comprenant comment mettre en place et gérer efficacement les mesures de sécurité, nous pouvons assurer une bonne couverture de nos systèmes informatiques et garantir une bonne protection de nos données sensibles.

4. Conclusion personnelle

Je trouve qu'il est très important d'avoir une bonne gestion des comptes utilisateurs et des groupes, car cela permet d'avoir des accès limités.

Par exemple, lors du lancement de mon entreprise, j'aurai besoin d'un système de gestion des utilisateurs et des groupes en règle, afin d'éviter que mon comptable ne puisse interférer à des contenus destinés au développeur.

De plus, si j'ai des apprentis ou des stagiaires, je dois limiter leur accès pour qu'ils ne poussent pas du code erroné sur une application ou qu'ils ne mettent pas en danger des fichiers confidentiels en cas de piratage.

En gérant correctement les comptes utilisateurs et les groupes, je peux protéger mon entreprise et ses données sensibles.

5. Références

1. Oracle (s.d.). Consulté le 3 janvier 2023, à l'adresse https://docs.oracle.com/cd/E19620-01/805-1608/6j1io9lh0/index.html
2. L, B. (21 octobre 2021). Pourquoi sécuriser et contrôler les accès administrateurs/ à privilèges élevés ? - LeBigData.fr. Consulté le 3 janvier 2023, à l'adresse https://www.lebigdata.fr/securiser-controler-acces-administrateurs
3. User identifier — Wikipédia. (s.d.). Consulté le 3 janvier 2023, à l'adresse https://fr.wikipedia.org/wiki/User_identifier
4. cut / Wiki / Debian-facile. (s.d.). Consulté le 3 janvier 2023 à l'adresse https://debian-facile.org/doc:systeme:cut
5. man usermod : usermod - Modifier un compte utilisateur. (s.d.). Consulté le 4 janvier 2023 à l'adresse http://www.man-linux-magique.net/man8/usermod.html#:~:text=Les%20options%20disponibles%20pour%20la,mots%20de%20passe%20pour%20lutilisateur.
6. Supprimer des groupes Linux. (s.d.). Consulté le 4 janvier 2023 à l'adresse https://www.ibm.com/docs/fr/psfa/7.1.0?topic=groups-delete-linux
7. Pouzadoux, O. (s.d.). Chmod et Chown, les droits sous GNU/Linux - Les Hirondelles du Net. Consulté le 4 janvier 2023, à l'adresse https://www.leshirondellesdunet.com/chmod-et-chown
8. N. (3 octobre 2022). La gestion des accès : un indispensable de la sécurité informatique - NowTeam, Spécialiste de l'infogérance et maintenance informatique. Consulté le 4 janvier 2023, à l'adresse https://www.nowteam.net/gestion-acces-indispensable-securite-informatique/
9. Sécuriser vos fichiers : Protégez vos données avec des astuces très simples ! (2019, mai, 9). Consulté le 4 janvier 2023, à l'adresse https://www.varonis.com/fr/blog/securiser-vos-fichiers-protegez-vos-donnees-avec-des-astuces-tres-simples
10. Hoarau, O. (s.d.). Sécuriser son poste linux. Consulté le 4 janvier 2023, à l'adresse https://www.funix.org/fr/linux/intrusions.htm

11. Fail2ban. (s.d.). Consutlé le 5 janvier 2023, à l'adresse https://www.fail2ban.org/wiki/index.php/Main_Page
12. On fait des groupes ? - Linux Attitude. (s.d.). Consulté le 5 janvier à l'adresse https://linux-attitude.fr/post/on-fait-des-groupes#:~:text=Un%20utilisateur%20est%20n%C3%A9cessairement%20dans,sur%20ces%20fichiers%20et%20r%C3%A9pertoires.
13. T. (s.d.). What You Need to Know About Linux Audit Framework. Consulté le 5 janvier 2023, à l'adresse https://goteleport.com/blog/linux-audit/

6. Références des illustrations