

Lab – Authentification et autorisation

Introduction

Dans le monde de l'informatique, la gestion des autorisations d'accès aux ressources est essentielle pour garantir la sécurité et la confidentialité des données.

Sur le système d'exploitation GNU/Linux, cette gestion est réalisée à travers la configuration des **utilisateurs**, des **groupes** et des permissions associées à chaque élément du système.

Utilisateur : Dans le contexte de GNU/Linux, un utilisateur représente une entité autorisée à se connecter et à interagir avec le système informatique. Chaque utilisateur possède ses propres fichiers, dossiers et paramètres personnalisés, déterminant ainsi son espace de travail individuel sur le système.

Root : L'administrateur système, souvent désigné sous le nom de "root", détient les privilèges les plus élevés sur le système. Comparable à un super-utilisateur, le compte root a un accès complet et illimité à toutes les fonctions et ressources du système, lui permettant d'effectuer des tâches d'administration critique telles que la configuration du système, l'installation de logiciels et la gestion des utilisateurs et des groupes.

Groupe : Les groupes sont des ensembles d'utilisateurs ou de processus partageant des autorisations similaires sur les fichiers et les répertoires. En associant des utilisateurs à des groupes, l'administrateur peut simplifier la gestion des autorisations en définissant des règles d'accès pour des ensembles d'utilisateurs ayant des besoins similaires.

Dans ce Lab, nous allons explorer comment créer, gérer et attribuer des droits d'accès aux utilisateurs et aux groupes sur un système GNU/Linux. Nous allons apprendre à manipuler les permissions pour restreindre ou permettre l'accès à des fichiers et des répertoires spécifiques, assurant ainsi la sécurité des données sur le système.

Objectifs

Partie 1 : Ajouter des groupes, des utilisateurs et des mots de passe sous un système Linux

Partie 2 : Vérifier les utilisateurs, les groupes et les mots de passe

Partie 3 : Utiliser les droits d'accès symboliques

Partie 4 : Autorisations absolues

Contexte/Scénario

Vous mettrez en œuvre la sécurité d'un hôte en ligne de commande tout en respectant les bonnes pratiques de sécurité :

- Ajouter des groupes, des utilisateurs et des mots de passe
- Vérifier des groupes, des utilisateurs et des mots de passe
- Configurer des droits d'accès symboliques

- Configurer des droits d'accès absolus

Ressources requises

PC équipé d'une VM Ubuntu.

Partie 1 : Ajouter des groupes, des utilisateurs et des mots de passe sous un système Linux.

Dans cette partie, vous ajouterez des utilisateurs, des groupes et des mots de passe sur la machine hôte locale.

Étape 1 : Ouvrez une fenêtre de terminal

Connectez-vous à votre VM Ubuntu à l'aide de vos informations d'identification : Utilisateur **et** Mot de passe

Étape 2 : Accordez les privilèges root en entrant la commande `sudo su`. Saisissez le mot de passe dès que vous y êtes invité :

```
cisco@ubuntu:~$ sudo su
```

```
cisco@ubuntu:~$ sudo su
[sudo] password for cisco:
root@ubuntu:/home/cisco#
```

Attention : pour des raisons de confidentialité le mot de passe ne s'affichera pas à l'écran, c'est normal !!).

Étape 3 : Ajoutez un groupe nommé HR en saisissant la commande `groupadd HR`.

```
root@ubuntu:/home/cisco# groupadd HR
```

```
root@ubuntu:/home/cisco# groupadd HR
root@ubuntu:/home/cisco#
```

Partie 2 : Vérifier les utilisateurs, les groupes et les mots de passe

Étape 1 : Vérifiez que le nouveau groupe a été ajouté à la liste du fichier de groupe en saisissant la commande `cat`.

```
root@ubuntu:/home/cisco# cat /etc/group
```

```
root@ubuntu:/home/cisco# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cisco
Bob:x:1002:
Eve:x:1003:
Eric:x:1004:
HR:x:1005:
root@ubuntu:/home/cisco#
```

Le nouveau groupe HR sera ajouté en bas du fichier /etc/group avec l'identifiant de groupe 1005.

Étape 2 : Ajoutez un utilisateur nommé jenny.

```
root@ubuntu:/home/cisco# adduser jenny ↵
```

- Lorsque vous y êtes invité, saisissez le mot de passe **lasocial**. Appuyez sur **Entrée**.
- Lorsque vous y êtes invité à nouveau, saisissez **lasocial**. Appuyez sur **Entrée**.
- Lorsque vous êtes invité à indiquer un nom complet, saisissez **Jenny**. Appuyez sur **Entrée**.
- Pour le reste de la configuration, appuyez sur **Entrée** jusqu'à ce que l'on vous demande si les informations sont correctes.
- Appuyez sur **Y** pour « Yes » (Oui), puis sur **Entrée**.

```
root@ubuntu:/home/cisco# adduser jenny
Adding user `jenny' ...
Adding new group `jenny' (1006) ...
Adding new user `jenny' (1005) with group `jenny' ...
Creating home directory `/home/jenny' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jenny
Enter the new value, or press ENTER for the default
    Full Name []: Jenny
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
```

Étape 3 : Intégrez l'utilisateur jenny dans le groupe HR.

```
root@ubuntu:/home/cisco# usermod -G HR jenny ↵
```

```
root@ubuntu:/home/cisco# usermod -G HR jenny
root@ubuntu:/home/cisco#
```

Étape 4 : Ajoutez un utilisateur nommé joe.

```
root@ubuntu:/home/cisco# adduser joe
```

```
root@ubuntu:/home/cisco# adduser joe
Adding user `joe' ...
Adding new group `joe' (1007) ...
Adding new user `joe' (1006) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
    Full Name []: Joe
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
```

- Lorsque vous y êtes invité, saisissez le nouveau mot de passe **tooth**. Appuyez sur **Entrée**.
- Lorsque vous y êtes à nouveau invité, saisissez **tooth**. Appuyez sur **Entrée**.
- Lorsque vous y êtes invité, saisissez le nom complet **Joe**. Appuyez sur **Entrée**.
- Pour le reste de la configuration, appuyez sur **Entrée** jusqu'à ce que l'on vous demande si les informations sont correctes.
- Appuyez sur **Y** pour « Yes » (Oui), puis sur **Entrée**
- Intégrez l'utilisateur joe dans le groupe HR.

```
root@ubuntu:/home/cisco# usermod -G HR joe
```

```
root@ubuntu:/home/cisco# usermod -G HR joe
root@ubuntu:/home/cisco#
```

Étape 5 : Vérifiez les nouveaux utilisateurs créés dans le fichier passwd.

```
root@ubuntu:/home/cisco# cat /etc/passwd
```

```
root@ubuntu:/home/cisco# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
eve:x:1003:1003::/home/eve:
eric:x:1004:1004::/home/eric:
jenny:x:1005:1006:Jenny,,,:/home/jenny:/bin/bash
joe:x:1006:1007:Joe,,,:/home/joe:/bin/bash
```

Étape 6 : Affichez les utilisateurs créés dans le fichier shadow.

```
root@ubuntu:/home/cisco# cat /etc/shadow
```

Partie 3 : Utiliser les droits d'accès symboliques

Étape 1 : Dans le système Ubuntu, appuyez de manière prolongée sur les touches CTRL+ALT+F1 jusqu'à ce que l'écran passe au terminal tty1.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login:
```

Travaux pratiques – Authentification, autorisation et journalisation

Remarque : si vous ne pouvez pas utiliser le terminal tty1, retournez sur l'interface utilisateur graphique (GUI) de l'hôte à l'aide de la commande **CTRL+ALT+F7**, puis ouvrez une fenêtre de terminal dans l'interface graphique d'Ubuntu. À l'invite, saisissez **su -l jenny** et le mot de passe **lasocial**.

```
cisco@ubuntu:~$ su -l jenny
```

```
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Remarque : si la commande CTRL+ALT+F7 ne fonctionne pas, essayez CTRL+ALT+F8.

Étape 2 : Une fois que l'écran de connexion au terminal s'affiche, saisissez jenny et appuyez sur Entrée.

Étape 3 : Lorsque vous y êtes invité, saisissez le mot de passe lasocial, puis appuyez sur Entrée.

Étape 4 : Une fois

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jenny@ubuntu:~$
```

Comme nous ne sommes pas connectés en tant que *root* (superuser), le signe dollar est présenté au lieu du # si nous étions connectés en tant qu'utilisateur root.

Étape 5 : Affichez le répertoire actuel.

```
jenny@ubuntu:~$ pwd ↵
```

```
jenny@ubuntu:~$ pwd
/home/jenny
```

Étape 6 : Retournez au niveau du répertoire /home.

```
jenny@ubuntu:~$ cd .. ↵
```

```
jenny@ubuntu:~$ cd ..
jenny@ubuntu:/home$
```

Travaux pratiques – Authentification, autorisation et journalisation

Étape 7 : Dressez la liste de tous les répertoires et de leurs droits d'accès.

```
jenny@ubuntu:/home$ ls -l ↵
```

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:28 jenny
drwxr-xr-x  2 joe   joe   4096 Jun 28 19:18 joe
jenny@ubuntu:/home$
```

Le système d'exploitation Linux a un total de dix lettres ou tirets dans le champ Droits d'accès :

- Le premier champ consiste en un tiret pour un fichier et une lettre « d » pour un répertoire
- Les champs 1 à 4 sont consacrés aux utilisateurs
- Les champs 5 à 7 sont consacrés aux groupes
- Les champs 8 à 10 sont consacrés aux autres (comptes autres que ceux du groupe)



Étape 8 : Entrez dans le dossier de Joe sous l'identité de Jenny en saisissant la commande `cd joe`.

```
jenny@ubuntu:/home$ cd joe ↵
```

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$
```

Notez que nous sommes capables d'entrer dans *le répertoire personnel de Joe*.

```
jenny@ubuntu:/home/joe$ cd .. ↵
```

```
jenny@ubuntu:/home/joe$ cd ..
jenny@ubuntu:/home$
```

Étape 9 : Appuyez de manière prolongée sur `CTRL+ALT+F2` pour passer à une autre session du terminal (`tty2`).

```
Ubuntu 16.04 LTS ubuntu tty2
ubuntu login: _
```

Étape 10 : Connectez-vous en tant qu'utilisateur `root` avec le mot de passe `root`.

```
Ubuntu 16.04 LTS ubuntu tty2
ubuntu login: root
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.
```


Remarque : si vous ne pouvez pas utiliser le terminal tty2, retournez sur l'interface utilisateur graphique (GUI) de l'hôte à l'aide de la commande **CTRL+ALT+F7**, puis ouvrez une fenêtre de terminal dans l'interface graphique de l'OS Ubuntu. À l'invite, saisissez **sudo -i** et le mot de passe **password**.

```
cisco@ubuntu:~$ sudo -i
[sudo] password for cisco:
root@ubuntu:~#
```

Étape 11 : Passez au répertoire /home.

```
root@ubuntu:~# cd /home ↵
```

```
root@ubuntu:~# cd /home
root@ubuntu:/home#
```

Étape 12 : Modifiez le droit d'accès « autre » sur le répertoire de Joe en le rendant non exécutable.

```
root@ubuntu:/home# chmod o-x joe ↵
```

```
root@ubuntu:/home# chmod o-x joe
root@ubuntu:/home#
```

Étape 13 : Répertoirez à nouveau les répertoires et leurs droits d'accès respectifs.

```
root@ubuntu:/home# ls -l ↵
```

```
root@ubuntu:/home# ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr--  2 joe   joe   4096 Jun 28 19:18 joe
root@ubuntu:/home#
```

Notez que le champ « autres » du répertoire de Joe possède désormais deux tirets.

Étape 14 : Appuyez de manière prolongée sur CTRL+ALT+F1 pour basculer sur l'autre session du terminal (tty1). Assurez-vous que l'invite de commande suivante s'affiche :
jenny@ubuntu:/home\$

Étape 15 : Essayez d'accéder à nouveau au répertoire de Joe.

```
jenny@ubuntu:/home$ cd joe ↵
```

```
jenny@ubuntu:/home$ cd joe
-bash: cd: joe: Permission denied
jenny@ubuntu:/home$
```

Notez que vous n'êtes plus autorisé.

GNU/Linux

Le graphique ci-dessous montre des exemples d'autres manières dont la commande **chmod** peut être utilisée :

Commande chmod	Résultats
chmod u+rwx	Accorde à l'utilisateur des autorisations de lecture, d'écriture et d'exécution.
chmod u+rw	Accorde à l'utilisateur des autorisations de lecture et d'écriture.
chmod o+r	Accorde aux autres des autorisations de lecture.
chmod g-rwx	Supprime des autorisations de lecture, d'écriture et d'exécution pour le groupe.

Étape 16 : Saisissez **exit**, puis appuyez sur **Entrée** pour vous déconnecter de la session du terminal.

Partie 4 : Autorisations absolues

Étape 1 : Connectez-vous en tant qu'utilisateur **joe** avec le mot de passe **tooth** sur **tty1**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: joe
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/
```

Remarque : si vous ne pouvez pas utiliser le terminal **tty1**, retournez à l'interface utilisateur graphique (GUI) de l'hôte en appuyant sur **CTRL+ALT+F7**, puis ouvrez une fenêtre de terminal dans l'interface graphique de l'OS Ubuntu. Lorsque vous y êtes invité, saisissez **sudo -l joe** et le mot de passe **tooth**.

```
jenny@ubuntu:/home$ exit
logout
cisco@ubuntu:~$ su -l joe
Password:
joe@ubuntu:~$
```

Étape 2 : Affichez votre répertoire de travail actuel.

```
joe@ubuntu:~$ pwd
```

```
joe@ubuntu:~$ pwd
/home/joe
joe@ubuntu:~$
```

Étape 3 : Retournez au niveau du répertoire **/home**.

```
joe@ubuntu:~$ cd ..
```

```
joe@ubuntu:~$ cd ..
joe@ubuntu:/home$
```

Étape 4 : Dressez la liste de tous les répertoires et de leurs autorisations dans le répertoire de travail actuel.

```
joe@ubuntu:/home~$ ls -l
```

```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr--  3 joe  joe  4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Notez que le dossier de Joe est défini de sorte que les « autres » ne puissent pas y accéder.

En dehors des autorisations symboliques, l'autre manière d'attribuer des autorisations est d'utiliser des autorisations absolues. Les autorisations absolues s'appuient sur un numéro octal à trois chiffres pour représenter les autorisations du propriétaire, du groupe et des autres.

Le tableau ci-dessous présente chaque valeur absolue et ses autorisations correspondantes :

Numéro	Autorisations
7	Lecture, écriture et exécution
6	Lecture et écriture
5	Lecture et exécution
4	Lecture
3	Écriture et exécution
2	Écriture
1	Exécuter
0	Aucune

Si vous saisissez la commande **chmod 764 examplefile**, examplefile disposera des autorisations suivantes :

- o L'utilisateur disposera d'autorisations de lecture, d'écriture et d'exécution
- o Le groupe disposera des autorisations de lecture et d'écriture
- o Les autres auront un accès de lecture

Répartition de la manière dont 764 représente ces autorisations :

Chiffre	Équivalent binaire	Autorisation
7(utilisateur)	111	1-Lecture 1-Écriture 1-Exécution
6(groupe)	110	1-Lecture 1-Écriture

		0-Aucune exécution
4 (autres)	100	1-Lecture 0-Aucune écriture 0-Aucune exécution

Étape 5 : Modifiez le champ « autres » dans le dossier de Joe pour que les autres utilisateurs puissent lire et exécuter, mais pas écrire, tout conservant la lecture, l'écriture et l'exécution pour le champ « utilisateur ».

```
joe@ubuntu:/home$ chmod 705 joe ↵
```

```
joe@ubuntu:/home$ chmod 705 joe
joe@ubuntu:/home$
```

Étape 6 : Répertoriez les autorisations de fichier du répertoire actuel pour vérifier que des modifications absolues ont été effectuées.

```
joe@ubuntu:/home$ ls -l ↵
```

```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwx--r-x  3 joe  joe  4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Étape 7 : Passez au répertoire `/home/joe`.

```
joe@ubuntu:/home$ cd joe ↵
```

```
joe@ubuntu:/home$ cd joe
joe@ubuntu:~$
```

Étape 8 : Créez un fichier texte simple nommé `test.txt` à l'aide de la commande `touch`.

```
joe@ubuntu:~$ touch test.txt ↵
```

```
joe@ubuntu:~$ touch test.txt
joe@ubuntu:~$
```

- Saisissez **exit**, puis appuyez sur **Entrée** pour vous déconnecter de la session de Joe.
- Sur le Terminal `tty1`, reconnectez-vous en tant que **jenny** et saisissez le mot de passe **lasocial**. Appuyez sur **Entrée**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
```

Remarque : si vous ne pouvez pas utiliser le terminal tty1, retournez sur l'interface utilisateur graphique (GUI) de l'hôte à l'aide de la commande **CTRL+ALT+F7** , puis ouvrez une fenêtre de terminal dans l'interface graphique de l'OS Ubuntu. À l'invite, saisissez **su -l jenny** et le mot de passe **lasocial**.

```
cisco@ubuntu:~$ su -l jenny
```

```
joe@ubuntu:~$ exit
logout
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```



Étape 9 : Passez au répertoire /home.

```
jenny@ubuntu:~$ cd /home
```

```
jenny@ubuntu:~$ cd /home
jenny@ubuntu:/home$
```

Étape 10 : Répertoriez tous les répertoires et leurs autorisations respectives.

```
jenny@ubuntu:/home$ ls -l
```

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwx--r-x  3 joe  joe  4096 Jun 29 00:32 joe
jenny@ubuntu:/home$
```

Étape 11 : Passez au répertoire /home/joe et répertoriez son contenu.

```
jenny@ubuntu:/home$ cd joe
```

```
jenny@ubuntu:/home/joe$ ls -l
```

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
total 12
-rw-r--r-- 1 joe joe 8980 Jun 28 19:18 examples.desktop
-rw-rw-r-- 1 joe joe    0 Jun 29 00:22 test.txt
jenny@ubuntu:/home/joe$
```

Notez que nous pouvons entrer dans le dossier de Joe et lire les fichiers du répertoire. Nous avons pu voir le fichier *test.txt*.

Étape 12 : Essayez de créer un fichier.

```
jenny@ubuntu:/home/joe$ touch jenny.txt
```

```
jenny@ubuntu:/home/joe$ touch jenny.txt
touch: cannot touch 'jenny.txt': Permission denied
jenny@ubuntu:/home/joe$
```

Notez que nous n'avons pas l'autorisation de créer un fichier.