**Effet de l'autorisation "sticky" sur un répertoire**

**En tant qu'usager tech**

* Vous devez créer le groupe g1

**sudo groupadd g1**

* Vous devez créer les deux utilisateurs s1 et s2

**pour chaque utilisateur, vous devez créer le dossier personnel, configurer l'interpréteur de commandes à /bin/bash et le groupe principal sera le groupe g1**

**sudo useradd -m -s /bin/bash -g g1 s1**

**sudo useradd -m -s /bin/bash -g g1 s2**

* Vous devez attribuer un mot de passe aux utilisateurs s1 et s2

**sudo passwd s1**

**sudo passwd s2**

**En tant qu'usager s1**

**note: la commande "su - s1" permet d'emprunter l'identité de l'utilisateur "s1"**

1. créer le répertoire **/tmp/test\_sticky/**
2. vous devez créer les fichiers **s1\_f1.txt** et **s1\_f2.txt** dans le répertoire **/tmp/test\_sticky/**
3. donner les droits 775 sur le répertoire **/tmp/test\_sticky/**
4. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s2**

**note: la commande "su - s2" permet d'emprunter l'identité de l'utilisateur "s2"**

1. Vous devez créer le fichier **s2\_f1.txt** dans le répertoire **/tmp/test\_sticky/**
2. Pourquoi l'utilisateur **s2** peut supprimer le fichier **/tmp/test\_sticky/s1\_f1.txt** ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s1**

**note: la commande "su - s1" permet d'emprunter l'identité de l'utilisateur "s1"**

1. Vous devez ajouter le droit "**sticky**" sur le répertoire **/tmp/test\_sticky/**

**chmod o+t /tmp/test\_sticky/**

1. vérifier les autorisations sur le répertoire **/tmp/test\_sticky/** avec la commande

**ls -l /tmp**

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s2**

**note: la commande "su - s2" permet d'emprunter l'identité de l'utilisateur "s2"**

1. Pourquoi l'utilisateur **s2** ne peut pas supprimer le fichier **/tmp/test\_sticky/s1\_f2.txt** ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**Effet de l'autorisation SGID sur un répertoire**

**En tant qu'usager tech**

* Vous devez créer les deux utilisateurs s3 et s4

**pour chaque utilisateur, vous devez créer le dossier personnel et configurer l'interpréteur de commandes à /bin/bash**

**sudo useradd -m -s /bin/bash s3**

**sudo useradd -m -s /bin/bash s4**

* Vous devez attribuer un mot de passe aux utilisateurs s3 et s4

**sudo passwd s3**

**sudo passwd s4**

**En tant qu'usager s3**

**note: la commande "su - s3" permet d'emprunter l'identité de l'utilisateur "s3"**

1. créer le répertoire **/tmp/test\_SGID/**
2. donner les droits 757 sur le répertoire **/tmp/test\_SGID/**
3. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s4**

**note: la commande "su - s4" permet d'emprunter l'identité de l'utilisateur "s4"**

1. créer un fichier dans le répertoire **/tmp/test\_SGID/**
2. quel est le nom de l'utilisateur qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_
3. quel est le nom du groupe qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_
4. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s3**

**note: la commande "su - s3" permet d'emprunter l'identité de l'utilisateur "s3"**

1. Vous devez ajouter le droit **SGID** sur le répertoire **/tmp/test\_SGID/**

**chmod g+s /tmp/test\_SGID/**

1. vérifier les autorisations sur le répertoire **/tmp/test\_SGID/** avec la commande

**ls -l /tmp**

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager s4**

**note: la commande "su - s4" permet d'emprunter l'identité de l'utilisateur "s4"**

1. créer un autre fichier dans le répertoire **/tmp/test\_SGID/**
2. quel est le nom de l'utilisateur qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_
3. quel est le nom du groupe qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_
4. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**Effet de l'autorisaion SUID sur un fichier**

**En tant qu'usager s3**

**note: la commande "su - s3" permet d'emprunter l'identité de l'utilisateur "s3"**

1. Vérifier les autorisations sur le fichier **/bin/passwd** avec la commande

**ls -l /bin/passwd**

1. Est-ce que s3 peut changer son mot de passe avec la commande "**passwd**" ? \_\_\_\_\_\_\_\_\_\_\_\_
2. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager tech**

1. Vous devez enlever le droit **SUID** sur le fichier **/bin/passwd**

**chmod u-s /bin/passwd**

1. Vérifier les autorisations sur le fichier **/bin/passwd** avec la commande

**ls –l /bin/passwd**

**En tant qu'usager s3**

**note: la commande "su - s3" permet d'emprunter l'identité de l'utilisateur "s3"**

1. Est-ce que s3 peut changer son mot de passe avec la commande "**passwd**" ? \_\_\_\_\_\_\_\_\_\_\_\_
2. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

**En tant qu'usager tech**

1. Vous devez ajouter le droit **SUID** sur le fichier **/bin/passwd** pour revenir à la configuration de base

**chmod u+s /bin/passwd**

1. Vérifier les autorisations sur le fichier **/bin/passwd** avec la commande

**ls –l /bin/passwd**

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.
2. Pour créer le groupe g1, vous utilisez la commande suivante en tant qu'utilisateur tech :

bashCopy code

sudo groupadd g1

1. Pour créer les utilisateurs s1 et s2 avec les paramètres spécifiés, vous utilisez les commandes suivantes en tant qu'utilisateur tech :

bashCopy code

sudo useradd -m -s /bin/bash -g g1 s1 sudo useradd -m -s /bin/bash -g g1 s2

1. Pour attribuer un mot de passe à chaque utilisateur, vous utilisez les commandes suivantes en tant qu'utilisateur tech :

bashCopy code

sudo passwd s1 sudo passwd s2

En tant qu'utilisateur s1 :

1. Pour créer le répertoire **/tmp/test\_sticky/**, utilisez la commande suivante :

bashCopy code

mkdir /tmp/test\_sticky/

1. Pour créer les fichiers s1\_f1.txt et s1\_f2.txt dans le répertoire **/tmp/test\_sticky/**, utilisez les commandes suivantes :

bashCopy code

touch /tmp/test\_sticky/s1\_f1.txt touch /tmp/test\_sticky/s1\_f2.txt

1. Pour donner les droits 775 sur le répertoire **/tmp/test\_sticky/**, utilisez la commande suivante en tant qu'utilisateur tech :

bashCopy code

chmod 775 /tmp/test\_sticky/

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

En tant qu'utilisateur s2 :

1. L'utilisateur s2 peut supprimer le fichier **/tmp/test\_sticky/s1\_f1.txt** car il a des droits de lecture et d'écriture dans le répertoire **/tmp/test\_sticky/**.
2. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

En tant qu'utilisateur s1 :

1. Pour ajouter le droit "sticky" sur le répertoire **/tmp/test\_sticky/**, utilisez la commande suivante en tant qu'utilisateur tech :

bashCopy code

chmod +t /tmp/test\_sticky/

1. En tant qu'utilisateur s2, l'utilisateur s2 ne peut pas supprimer le fichier **/tmp/test\_sticky/s1\_f2.txt** car le répertoire est maintenant configuré avec l'autorisation "sticky". Cela signifie que seuls les propriétaires des fichiers peuvent les supprimer, même si d'autres utilisateurs ont des droits d'écriture dans le répertoire.
2. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

Effet de l'autorisation SGID sur un répertoire :

En tant qu'utilisateur tech :

1. Vous devez créer les utilisateurs s3 et s4 comme spécifié.
2. Pour donner les droits 757 sur le répertoire **/tmp/test\_SGID/**, utilisez la commande suivante en tant qu'utilisateur tech :

bashCopy code

chmod 757 /tmp/test\_SGID/

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

En tant qu'utilisateur s4 :

1. Créez un fichier dans le répertoire **/tmp/test\_SGID/**.
2. L'utilisateur qui a des autorisations sur le fichier est l'utilisateur s3.
3. Le groupe qui a des autorisations sur le fichier est le groupe principal de s3.
4. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

En tant qu'utilisateur s3 :

1. Pour ajouter le droit SGID sur le répertoire **/tmp/test\_SGID/**, utilisez la commande suivante en tant qu'utilisateur tech :

bashCopy code

chmod g+s /tmp/test\_SGID/

1. Vérifiez les autorisations sur le répertoire **/tmp/test\_SGID/** avec la commande :

bashCopy code

ls -l /tmp

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

En tant qu'utilisateur s4 :

1. Créez un autre fichier dans le répertoire **/tmp/test\_SGID/**.
2. L'utilisateur qui a des autorisations sur le fichier est l'utilisateur s3.
3. Le groupe qui a des autorisations sur le fichier est le groupe principal de s3.
4. La commande **exit** permet de revenir au prompt de l'utilisateur tech.

Effet de l'autorisation SUID sur un fichier :

En tant qu'utilisateur s3 :

1. Vérifiez les autorisations sur le fichier **/bin/passwd** avec la commande :

bashCopy code

ls -l /bin/passwd

1. En tant qu'utilisateur s3, vous pouvez changer votre propre mot de passe avec la commande "passwd".
2. La réponse est "Oui".
3. En tant qu'utilisateur tech, pour enlever le droit SUID sur le fichier **/bin/passwd**, utilisez la commande suivante :

bashCopy code

chmod u-s /bin/passwd

1. Vérifiez les autorisations sur le fichier **/bin/passwd** avec la commande :

bashCopy code

ls -l /bin/passwd

En tant qu'utilisateur s3 :

1. En tant qu'utilisateur s3, vous ne pouvez plus changer votre propre mot de passe avec la commande "passwd".
2. La réponse est "Non".

En tant qu'utilisateur tech :

1. Pour ajouter le droit SUID sur le fichier **/bin/passwd** pour revenir à la configuration de base, utilisez la commande suivante :

bashCopy code

chmod u+s /bin/passwd

1. Vérifiez les autorisations sur le fichier **/bin/passwd** avec la commande :

bashCopy code

ls -l /bin/passwd

1. La commande **exit** permet de revenir au prompt de l'utilisateur tech.