**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** ?

**s2 fait partie du groupe g1, le groupe g1 a les autorisations "r w x"**

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** ?

**s2 fait partie du groupe g1, le groupe g1 a les autorisations "r w x"**

**mais le dossier a l'autorisation "sticky".**

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: \_\_\_\_\_\_\_\_\_\_\_\_ **s4**
3. quel est le nom du groupe qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_ **s4**
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: \_\_\_\_\_\_\_\_\_\_\_\_ **s4**
3. quel est le nom du groupe qui a des autorisations sur le fichier: \_\_\_\_\_\_\_\_\_\_\_\_ **s3**
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**" ? \_\_\_\_\_\_\_\_\_\_\_\_ **oui**
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**" ? \_\_\_\_\_\_\_\_\_\_\_\_ **non**
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.