

TP n°2

Droits d'accès

Pour cet exercice, vous créez un utilisateur banalisé

- Vous est-il possible de faire une copie du fichier `/etc/passwd` ? Vous est-il possible de supprimer ou de modifier le fichier `/etc/passwd` ?

Oui il est possible de faire la copie du fichier `/etc/passwd`

Il est impossible de supprimer ou de modifier le fichier `/etc/passwd`. Seul le propriétaire du fichier peut le supprimer (ROOT)

Répéter ces tentatives en tant qu'utilisateur root.

Expliquer la situation à l'aide de la commande `ls -l`.

```
(bamba@kali)-[~]  
$ ls -l /etc/passwd  
rw-r--r-- 1 root root 3289 17 févr. 21:30 /etc/passwd
```

- À l'aide de la commande `id`, vérifier votre identité et le(s) groupe(s) au(x)quel(s) vous appartenez.

```
(bamba@kali)-[~]  
$ id  
uid=1000(bamba) gid=1000(bamba) groupes=1000(bamba),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),122(bluetooth),128(lpadmin),135(scanner),145(kaboxer)
```

- Créer un petit fichier texte (de contenu quelconque), qui soit lisible par tout le monde, mais non modifiable (même pas par vous).

```
bamba@kali: ~  
  
(bamba@kali)-[~]  
$ cat > test  
un  
deux  
trois  
  
(bamba@kali)-[~]  
$ chmod +r test  
  
(bamba@kali)-[~]  
$ ls -l test  
-rw-r--r-- 1 bamba bamba 15  7 juin  00:38 test  
  
(bamba@kali)-[~]  
$ chmod -w test  
  
(bamba@kali)-[~]  
$ ls -l test  
-r--r--r-- 1 bamba bamba 15  7 juin  00:38 test
```

- Créer un répertoire nommé **"Secret"**, dont le contenu est visible uniquement par vous-même.

```
(bamba@kali)-[~]  
$ mkdir secret  
  
(bamba@kali)-[~]  
$ chmod 700 secret  
  
(bamba@kali)-[~]  
$ ls -l  
total 40  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Bureau  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Documents  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Images  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Modèles  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Musique  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Public  
drwx----- 2 bamba bamba 4096  7 juin  00:45 secret  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Téléchargements  
-r--r--r-- 1 bamba bamba  15  7 juin  00:38 test  
drwxr-xr-x 2 bamba bamba 4096 17 févr. 21:33 Vidéos
```

Les fichiers placés dans ce répertoire sont-ils lisibles par d'autres membres de votre groupe ?
Non ; car ils n'ont pas d'autorisation

- Créer un répertoire nommé **"Connaisseurs"** tel que les autres utilisateurs ne puissent pas

lister son contenu mais puissent lire les fichiers qui y sont placés.

On obtiendra:

Is Connaisseurs

Is : Connaisseurs: Permission denied

cat Connaisseurs/toto

<...le contenu du fichier toto (s'il existe)...>

```
(bamba@kali)-[~]
$ mkdir connaisseurs

(bamba@kali)-[~]
$ chmod 711 connaisseurs

(bamba@kali)-[~]
$ su test
Mot de passe :
$ ls
Bureau connaisseurs Documents Images Modèles Musique Public secret Téléchargements Vidéos
$ ls connaisseurs
ls: impossible d'ouvrir le répertoire 'connaisseurs': Permission non accordée
$
```

- Chercher dans le répertoire **/usr/bin** des exemples de commandes ayant la permission **SUID**.

De quelle genre de commande s'agit-il ?

/usr/bin/passwd

/usr/bin/gpasswd

/usr/bin/readcd

Les utilisateurs

- Votre compte d'utilisateur est-il défini dans le fichier **/etc/passwd** ? Pourquoi ? Il y a-t-il d'autres alternatives ?

- Quel est le répertoire de connexion de l'utilisateur root ?

Répertoire : /root

- Quel est le shell de l'utilisateur root ?

Le shell est /bin/bash

- Quelle est la particularité de l'utilisateur **nobody** ? Et de l'utilisateur **shutdown** ?

L'utilisateur Nobody n'a pas de home valide, son home devient /.

- Quels sont les utilisateurs définis dans **/etc/passwd** qui font partie du même groupe que l'administrateur ?

Sync, postfix, sshd, partimag et distccd

Redirections, méta-caractères

Le répertoire /usr/include contient les fichiers d'entête standards en langage C (stdlib.h, ...).

- Créer un répertoire nommé inc dans votre répertoire de connexion (HOME).

En utilisant une seule commande, y copier les fichiers du répertoire /usr/include dont le nom commence par std.

```

(bamba@kali)-[~]
$ mkdir inc

(bamba@kali)-[~]
$ cp /usr/include/std* /home/bamba/inc

(bamba@kali)-[~]
$ ls -l inc
total 88
-rw-r--r-- 1 bamba bamba 2290 7 juin 01:24 stdc-predef.h
-rw-r--r-- 1 bamba bamba 8474 7 juin 01:24 stdint.h
-rw-r--r-- 1 bamba bamba 2800 7 juin 01:24 stdio_ext.h
-rw-r--r-- 1 bamba bamba 30002 7 juin 01:24 stdio.h
-rw-r--r-- 1 bamba bamba 36061 7 juin 01:24 stdlib.h

```

- Afficher la liste des fichiers de /usr/include dont le nom commence par a, b ou c.

```

(bamba@kali)-[~]
$ find /usr/include/ \( -name 'a*' -o -name 'b*' -o -name 'c*' \)

```

- Modifier la commande de la question précédente pour qu'au lieu d'afficher le résultat, celui-ci soit placé dans un fichier nommé "Abc.list" de votre répertoire de connexion.

```

(bamba@kali)-[~]
$ find /usr/include/ \( -name 'a*' -o -name 'b*' -o -name 'c*' \) > /home/bamba/Abc.list

(bamba@kali)-[~]
$ cat Abc.list
/usr/include/capstone
/usr/include/capstone/arm.h
/usr/include/capstone/capstone.h
/usr/include/capstone/arm64.h
/usr/include/aliases.h
/usr/include/argz.h
/usr/include/cursesw.h
/usr/include/assert.h
/usr/include/byteswap.h
/usr/include/cursesm.h

```