

Objectif spécifique :

- L'élève doit connaître le système des protections Linux en vue d'une utilisation multi-utilisateurs.

Equipements requis :

- 1 PC élève avec système d'exploitation Linux : Debian GNU/Linux Sarge Stable 3.1.

1 PHASE 1 – LISTER LES PROTECTIONS :

Objectif opérationnel :

Lister les protections de fichiers ou répertoires.

P1.1 - Lister les protections d'un fichier et d'un répertoire

Pour afficher les protections d'un fichier ou d'un répertoire on utilisera les commandes :

ls -l liste dans le répertoire ou racine en cours les répertoires et fichiers ainsi que leurs protections

ls -ld liste les protections du répertoire ou de la racine en cours

exemple pour le fichier /etc/passwd

Type fichier et permissions	Nb liens	Utilisateur	Groupe	Taille (Octets)	Date heure dernière modification	Nom
-rwxrwxrwx	1	root	root	935	2005-06-14 13 :33	/etc/passwd

Donner les protections du répertoire /home

Type fichier et permissions	Nb liens	Utilisateur	Groupe	Taille (Octets)	Date heure dernière modification	Nom

Donner la protection des répertoires utilisateurs contenus dans /home

Type fichier et permissions	Nb liens	Utilisateur	Groupe	Taille (Octets)	Date heure dernière modification	Nom

Donner la protection du fichier smb.conf, ce fichier se trouve dans /etc/samba

Type fichier et permissions	Nb liens	Utilisateur	Groupe	Taille (Octets)	Date heure dernière modification	Nom

2 PHASE 2 – SIGNIFICATIONS :

Type fichier et permissions	Nb liens	Utilisateur UID	Groupe GUID	Taille (Octets)	Date heure dernière modification	Nom fichier ou répertoire
-rwxrwxrwx	1	root	root	935	2005-06-14 13 :33	/etc/passwd

Type fichier	Permissions								
	Propriétaire			Groupe			Autres		
	lecture	écriture	exécution	lecture	écriture	exécution	lecture	écriture	exécution
– : ordinaire d : répertoire c : caractère b : bloc p : tube nommé l : lien symbol. S : socket	r	w	x ou (S [*])	r	w	x ou (S ^{**})	r	w	x
	1	1	1	1	1	1	1	1	1
	7			7			7		
	r	w	x	r	w	-	r	-	x
	1	1	1	1	1	0	1	0	1
	7			6			5		

* : SUID : (Set User ID) *indicateur positionné par l'utilisateur* : cette permission est positionnée par l'utilisateur et permet d'obtenir des permissions d'exécution sur des fichiers sensibles.

Exemple: le fichier /usr/bin/passwd possède les permissions:

```
-rwsr-xr-x 1 root root 26616 2004-11-06 13:42 /usr/bin/passwd
```

On comprend facilement que ce fichier qui contient tous les mots de passe (codés) des utilisateurs, ne peut être manipulé par n'importe qui.

Le root en a effectivement les droits, mais il est nécessaire que chaque utilisateur puisse modifier ce fichier lorsqu'il effectue un changement de son mot de passe.

L'utilisateur (loggé sous son user) peut donc modifier ce fichier lorsqu'il exécute la commande passwd, car cette permission est positionnée à s.

** : SGID : (Set Group ID) *indicateur positionné par le groupe* : idem que SUID mais la permission est accordée non pas selon l'utilisateur mais selon son groupe.

3 PHASE 3 – MODIFICATION DES PERMISSIONS :

Objectif opérationnel :

Modifier les protections de fichiers ou répertoires.

P3.1 - Modifier les protections d'un fichier et d'un répertoire

chmod : permet de modifier les permissions d'un fichier ou d'un répertoire.

P3.2 - Donner la commande permettant de donner, pour un fichier ou un répertoire quelconque, toutes permissions à tout profil d'utilisateur.

4 PHASE 4 – MODIFICATION DU PROPRIETAIRE ET DU GROUPE :

chown : permet de modifier le propriétaire et/ou le groupe.

chgrp : permet de modifier le groupe.

groupadd : permet d'ajouter un groupe

addgroup : script permettant d'ajouter un groupe (plus complet que groupadd, voir man **addgroup**)

P4.1 - En mode root, créer un fichier truc1 (vide ou avec du texte quelconque) et modifier son propriétaire par user1 et son groupe par staff. Donner le détail des commandes.