Projet 1 :

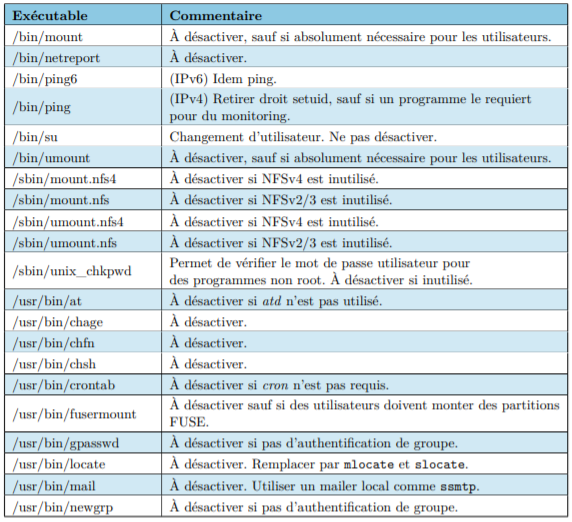
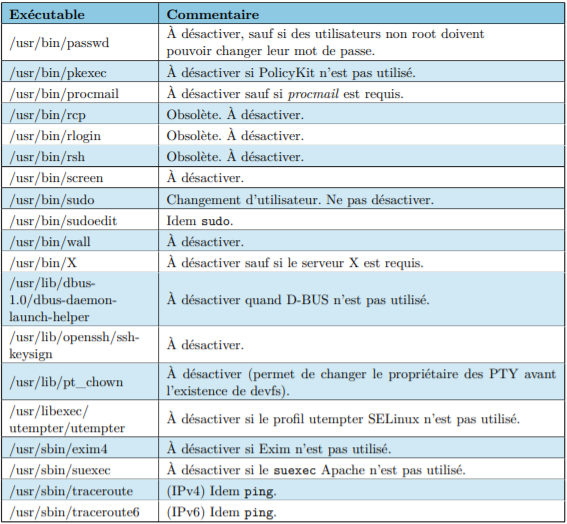
# Préparation des machines virtuelle

1. **Mot de passe**

* Trouver mot de passe : attaque au dictionnaire
* sudo unshadow /etc/passwd /etc/shadow > mypasswd
* john myfichier -users :nomuser
* john –show : voir les résultats
* Méthode pour bon mot de passe :
* phrase doit contenir au moins :
* Un nombre
* Une majuscule
* Un signe de ponctuation ou un caractère spécial (dollar, dièse, ...)
* Une douzaine de mots
* Puis prendre les premières lettres de chaque mot, garder les nombres et la ponctuation.
* /etc/shadow : pas en lecture pour tous car contient chaine codée : attaque par dictionnaire

1. **Setuid (-s)**

* Exécuter un programme avec les droits de l’utilisateur/du groupe
* **find / -type f \( -perm -u+s -o -perm -g+s \) -exec \ls -l {} \; 2> /dev/null** : trouver tous les fichiers/executables qui ont le setuid ensuite garder que ceux nécessaire
* A enlever : **sudo chmod u-s fichier | sudo chmod g-s fichier**
* **chage** *(permet de gérer aisément les contraintes liées à la validé des comptes et des mots de passe)*
* **chsch***(changer le shell par défaut)*
* **wall***(envoyer un message à tous les utilisateurs)*
* **chfn**(modifer les informations personnelles d’un utilisateur)
* **ssh-keysign***(used by ssh)*
* fusermount ? D’autres ?
* **Recommendations ANSSI :**



1. **Umask par défaut restrectif**

* Quand vous créez un fichier ou répertoire, les autorisations par défaut affectées au fichier ou répertoire sont contrôlées par le masque utilisateur.
* Dans le cas d'un fichier exécutable, les droits seront fixés comme **777-umask**
* Dans le cas d'un fichier non-exécutable (texte, image, etc.), les droits seront **666-umask**
* **umask** est un outil de gestion des droits sur la création des fichiers et des répertoires qui permet de gérer une certaines sécurité et une restriction des droits par défaut.
* **Umask utilisateur :** 077 tout fichier créer par un utilisateur n’est lisible et modifiable que par lui
* grep -u umask /etc/\* 2> /dev/null
* **/etc/login.def**
* **USERGROUPS\_ENABS : yes** alors 077 -> 007 par défaut groupe contient que l’user
* **Umask système :** 0027 par défaut tout fichier n’est lisible que par son propriétaire et son groupe et modifiable uniquement par son propriétaire

*(rajouter ligne dans /root/.bashrc : unmask 0027) : ici inutile car pareil umask utilisateur*

1. **Sticky bit (-t)**

* Postionné sur un dossier, le STICKY BIT permet d’interdire la suppression du répertoire et/ou de son contenu par quiconque n’en est pas propriétaire.
* *Ex : /tmp. N’importe quel utilisateur du système peut créer ou supprimer des fichiers ou des dossiers dans /tmp, mais il le pourra pas supprimer ceux créés par quelqu’un d’autre.*
* **find / -type d \ ( -perm /o+w -a \! -perm /+t \ ) -print 2> /dev/null** : trouver tous les fichiers que les autres utilisateurs peuvent modifier et pas sticky bit : on peut donc supprimer un fichier de quelqu’un autre
* *Le seul qu’on trouve /home/etu/bin* : rajouter sticky bit ?

1. **Anomalies**

* **find / -type d -perm /o+w -a \! -uid 0 -print 2> /dev/null :** *recherche des répertoire accessibles en écriture pour tous et dont root n’est pas le propriétaire*
* /home/etu/bin
* Qd on supprime un utilisateur penser à supprimer aussi son groupe et tous les fichiers qui se retrouvent sans propriété ni groupe
* **find / -type f \ ( -nouser -o -nogroup \ ) -print 2> /dev/null** : recherche tous les fichiers qui non ni propriétaire ni groupe
* **find / -type f -perm /u+x -perm /o+w -print 2> /dev/null** : fichiers dont user peut l’exécuter et les autres le modifier => pb modifier fichier à exécuter
* ls

1. **Suppression des services non sécurisés**

* **telnet :** comme ssh mais connexion son chiffré (on voit en clair le mot de passe)
* grep -u telnet /etc/\* 2> /dev/null
* /etc/inetd.conf
* /etc/group
* /etc/passwd

1. **Correction des anomalies dans /etc/passwd**

* **grep -v home /etc/passwd | grep bash :** affiche tous ceux qui n’on pas de home dans bash
* **grep -v nologin /etc/passwd | grep -v false** : affiche tous ceux qui n’ont pas nologin et false
* Lorsque / sbin / nologin est défini comme shell, si un utilisateur avec ce shell se connecte, il recevra un message poli disant "Ce compte n'est actuellement pas disponible."
* / bin / false est juste un binaire qui sort immédiatement, retournant false, quand il est appelé, donc quand quelqu'un qui a false comme shell se connecte, il est immédiatement déconnecté lorsque false sort.
* **anomalie www-data** : remplace usr/bin/bash par sbin/nologin car pas de home

1. **Rendre uniques machines après clonage**

* **Nom configuré**
* **hostname :** nom machine
* **sudo hostnamectl set-hostname nvNom :** changer de nom machine dans OS
* **modifier /etc/hosts** pour reflète se changement de nom
* **Machine id réinitialisée**
* Sudo rm /etc/machine-id
* Sudo systemd-machine-id-setup
* Redémarrer la machine
* **Clé ssh recrées**
* Sudo rm /etc/ssh/ssh\_host\_\*
* Générer nouvelles clés : sudo dpkg-reconfigure openssh-server

1. **Carte réseau**