TP GS11

Ce TP est une application directe du cours GS11 sur la partie « Linux sécurisé ».
Vous serez guidé pas à pas au cours de plusieurs activités qui viseront à renforcer la sécurité d'une distribution Linux à base de Fedora.

La durée du TP sera de 3 heures.

Chaque thème abordé, précisera les objectifs de l'activité ainsi que les connaissances à mettre en œuvre pour y parvenir.

Consignes générales :
- Vous travaillerez sous le compte « root ».
- Vous utiliserez la commande « man » si nécessaire.

Connaissances requises :
- Bonne maîtrise de Linux et des bases de l'administration système (UV LO14/NF19).
- Cours GS11.

Moyens utilisés :
- Salle D202, PC sous linux Fedora Core 8 avec une image spécifiquement préparée.

Compétences acquises :
- Être capable de sécuriser un serveur linux
- Être capable de rédiger des éléments de la PSSI
- Sensibiliser les utilisateurs à la nécessité de respecter la PSSI

1. Suppression du mot de passe « root »

Objectif :
- Mettre en évidence la nécessité dans un PSSI de sécuriser les accès physiques à un serveur.

Connaissances nécessaires :
- Arborescence linux, comptes utilisateurs, fichier d'initialisation.
- Commandes & pistes : vi, cd, ls, reboot, passwd, shadow

Votre travail :

a) En démarrant votre machine linux en mode « Single », supprimez le mot de passe « root ».
b) Faites en sorte qu'un mot de passe soit demandé en démarrage en mode « Single ».
c) Redémarrer la machine.

2. Vérifier l'heure (ntp)

Objectif :
- Pour une analyse de logs efficace, s'assurer que le serveur est à la bonne heure.

Connaissances nécessaires :
- Arborescence linux, daemons, services, tâche répétitive.
- Commandes : ntpdate, date, chkconfig, nslookup, grep, vi, cat, cd, ls, crontab.

Votre travail :
a) **En utilisant la commande « date », vérifiez si votre machine est à l'heure.**
b) **En éditant le fichier /etc/services, notez les ports et protocoles utilisés par le service « ntp ».**
c) **Le service ntp est-il lancé au démarrage ?**
d) **En utilisant la commande « ntpdate » et le serveur uran01 de l'Utt, mettez la machine à l'heure.**
e) **Faites en sorte que cette commande soit exécutée tous les 1ers jours de chaque mois.**

3. Inhiber le ctrl-alt-del

Objectif :
- Renforcer la sécurité du serveur vis-à-vis des utilisateurs.

Connaissances nécessaires :
- Arborescence linux, comptes et gestion des utilisateurs.
- Commandes : useradd, passwd, vi, ls, cd

Votre travail :
a) **Créer un utilisateur « gs11 » avec la commande « useradd », lui affecter un mot de passe.**
b) **Passez en mode console (ctrl-alt-F1), et connectez-vous avec le compte « gs11 ».**
c) **Pressez les touches ctrl-alt-del. La machine devrait redémarrer.**
d) **Faites le nécessaire au niveau du fichier /etc/inittab pour empêcher ce type d'action.**

4. Déconnexion automatique

Objectif :
- Renforcer la sécurité du serveur vis-à-vis des utilisateurs.

Connaissances nécessaires :
- Arborescence linux, comptes des utilisateurs, administration système.
- Commandes : set, env, grep, vi, ls, cd, reboot

Votre travail :
a) **En tant que « root », affichez les variables d'environnement.**
b) **Y-trouvez-vous la variable TMOUT ?**
c) **Arrangez-vous pour que tous les utilisateurs sans activité depuis 30 minutes soient déconnectés.**
d) **Redémarrez. Vérifiez la valeur de cette variable en tant que « root » et en tant que « gs11 »**

5. Droits sur les fichiers

Objectif :

- Assurer la sécurité du serveur en renforçant les droits sur les fichiers.

Connaissances nécessaires :

- Arborescence linux, gestion des services et des fichiers.
- Commandes & pistes : find, chmod, ls, vi, cd

Votre travail :

a) **Les scripts des services sont stockés dans /etc/init.d. Arrangez-vous pour que seul, le « root » puisse y avoir accès, et le cas échéant, les exécuter.**
b) **Rechercher l'ensemble des fichiers sur le disque qui n'ont pas de propriétaire identifié.**
c) **Trouvez l'ensemble des binaires avec bit SUID. Précisez quelques programmes critiques qui présentent cette caractéristique, et surtout mettre en évidence un éventuel trou de sécurité en considérant le fichier /etc/shadow …**
d) **Vous allez devoir trouver un shell dérobé basé sur le même trou de sécurité qu'en c) et utiliser l'option –p afin de réaliser le danger que représente un accès non surveillé.**

6. Partitionnement « optimal »

Objectif :

- Assurer la sécurité du serveur en optimisant la gestion du système de fichiers.

Connaissances nécessaires :

- Arborescence linux, gestion de système de fichiers, montages, disques et partitions.
- Commandes & pistes: fdisk, mount, df, cat, vi, cd, ls, reboot, fstab

Votre travail :

a) **Vérifiez les montages et partitionnement des disques grâce à la commande « fdisk ».**
b) **Notez la taille du disque dur.**
c) **Utilisez la commande « df » et noté l'espace libre/occupé par les partitions principales.**
d) **Arrangez-vous pour que /var et /home soient sur une partition (libre) séparée.**
e) **Assurez-vous des montages effectués au démarrage dans /etc/fstab.**
f) **Redémarrez. Assurez-vous de l'espace disponible sur les partitions grâce à la commande « df ».**

7. Authentification via ldap

Objectif :

- Assurer la PSSI, en authentifiant les utilisateurs à partir d'un référentiel « sûr ».

Connaissances nécessaires :

- Base de ldap, arborescence linux, manipulation de fichiers.
- Commandes : cp, ls, cd, id, finger, vi, grep

Votre travail :

a) **Copiez les fichiers /etc/ldap.conf (*fichier qui spécifie les modalités de communication avec le serveur ldap*) et /etc/nsswitch.conf (*fichier qui indique dans quels annuaires locaux ou réseau, rechercher les comptes) afin d'en créer une sauvegarde*).**

b) **Tapez la commande « finger votre_login_Utt ». Vous devriez avoir une erreur …**

c) **Dans le fichier /etc/ldap.conf, modifiez son contenu pour avoir au final les lignes ci-dessous :**

```
host uran01.utt.fr
base dc=utt,dc=fr
uri ldap://uran01.utt.fr
pam_password crypt
ssl no
tls_cacertfile /etc/ssl/ca.cert
```

d) **Dans le fichier /etc/nsswitch.conf, modifiez 3 lignes afin d'obtenir :**

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

e) **Tapez la commande « finger votre_login_Utt » : il devrait vous renvoyer des infos …**

8. Première approche de la PAM

Objectif :

- Contrôler la façon dont les utilisateurs se connectent au serveur.

Connaissances nécessaires :

- Base de ldap, arborescence linux, gestion des utilisateurs, gestion de fichiers, pam.
- Commandes : su, ln, ls, cd, pwd, touch, vi

Votre travail :

a) **Essayez à partir d'une console « root » de taper la commande « su – votre_login_Utt »**

b) **Vous devriez avoir 2 erreurs. Expliquez ce résultat et que faire pour que cela fonctionne (au moins au niveau du shell) ?**

c) **Grâce à la commande « touch », créez un fichier « test.txt ». Expliquez le résultat.**

d) **Editez le fichier /etc/pam.d/system_auth et rajoutez une ligne dans la section « session » :**

```
session     optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

e) **Essayez à partir d'une console « root » de taper la commande « su – votre_login_Utt »**

f) **Grâce à la commande « touch », créez un fichier « test.txt ».**

g) **Essayez de vous connecter en mode graphique à présent en utilisant votre login Utt. Expliquez les raisons de l'échec de connexion (*indice : allez voir les derniers fichiers de logs et pensez à LDAP …)***

9. Connexion via la pam ldap

Objectif :

- Assurer la PSSI, en contrôlant l'authentification avec la pam_ldap.

Connaissances nécessaires :

- Base de ldap, arborescence linux, gestion des utilisateurs, gestion de fichiers, pam, logs.
- Commandes : su, ln, ls, cd, pwd, touch, vi

Votre travail :

a) **Toujours dans le fichier /etc/pam.d/system-auth, rajoutez à l'avant dernière ligne de chaque section (auth, account, password, session) la ligne suivante : <section> sufficient pam_ldap.so**
b) **Tentez à présent de vous connecter en mode graphique et en mode console, avec votre identifiant et mot de passe Utt.**
c) **Vérifiez les traces laissées dans le fichier /var/log/secure par vos tentatives de connexion.**

10. Sécurité et mot de passe avec PAM

Objectif :

- Renforcer la PSSI en sécurisant le choix de mot de passe.

Connaissances nécessaires :

- Arborescence linux, gestion des utilisateurs, gestion de fichiers, pam.
- Commandes : su, ln, ls, cd, pwd, touch, vi

Votre travail :

a) **En utilisant le compte utilisateur « gs11 » précédemment créé, connectez-vous en mode console en tapant son login et mot de passe.**
b) **Changez son mot de passe en « azer2014»**
c) **Délogguez-vous et reconnectez-vous avec le compte « gs11 » et mot de passe « azer2014 »**
d) **Créez une règle dans la PAM qui oblige (required) un utilisateur à choisir un mot de passe d'au minimum 9 caractères, en y incluant obligatoirement : une minuscule, deux majuscules, 2 chiffres et 1 caractère spécial.**
e) **Testez plusieurs mots de passe que vous choisirez en fonction du critère précédent. Au final, vous pourrez affecter le mot de passe « GS2014er* »**