IUT Charlemagne
Département Informatique

LP ASRALL
21 janvier 2015

Sécurité et système Linux

Ce premier TD a pour but de vous familiariser avec l'environnement UNIX/Linux et de manipuler les quelques commandes de bases qui vous permettent de faire rapidement un premier bilan de sécurité sur une machine.

Le but n'est pas d'apprendre ces commandes par cœur mais de savoir quel type d'information on cherche lorsque l'on cherche à sécuriser une machine (et la liste n'est pas exhaustive).

1. Le système de fichier

Les droits des fichiers sont le cœur de la sécurité d'un système unix.

1.1. Chercher les fichiers en écriture pour tous (dans votre home puis sur tout le système).

1.2. Chercher les fichiers en écriture pour le groupe (dans votre home puis sur tout le système).

1.3. Chercher les répertoires en écriture pour tous (dans votre home puis sur tout le système).

1.4. Chercher les répertoires en écriture pour le groupe (dans votre home puis sur tout le système).

1.5. Quels sont les droits attachés au répertoire /tmp ? Pourquoi ?

1.6. Cherchez les fichier possédant des droits suid et sgid dans le dans votre répertoire home et dans le répertoire /bin ?

1.7. Quel est l'intérêt de ces droits ? Quelle est l'alternative ?

1.8. Quels sont les fichiers modifiés ces 60 dernières minutes ?

1.9. Quelles sont les partitions montées en ce moment sur votre machine ? Quels sont les droits déclarés sur ces partitions ?

2. Augmentation de privilège par les fichiers suid

En préparations, effectuez les commandes suivantes.

sudo mkdir /var/meslogs

sudo touch /var/meslogs/log

sudo apt-get install perl-suid # Pour l'installation de perl suid.

et créez EN ROOT le fichier ~/suitest avec les données suivantes :

```
#!/usr/bin/perl -wTU
system("whoami");
```

sudo chmod 4755 ~/suitest

2.1. Lancez le. Que constatez vous ?

2.2. Détournez ce script.

La commande whoami est dans le PATH, dans /usr/bin. En modifiant son PATH et en créant un fichier exécutable, essayer de faire exécuter à ce script en root autre chose que cette commande.

3. Les comptes

Sur les systèmes informatiques modernes, il existe des comptes privilégiés permettant d'administrer la machine et d'exécuter différentes tâches. Ces comptes sont de fait des cibles privilégiés des pirates informatiques puisqu'ils permettent de contrôler complètement une machine avec la possibilité d'effacer toutes traces d'intrusions.

Sur le architectures de type linux/unix, le compte root est le compte administrateur par défaut et doit donc faire l'objet de la plus grande attention.

3.1. Vérifiez les droits de votre home directory. Comment faire que tout nouveau fichier créé ait des droits spécifiques (lecture owner uniquement par exemple) ?

3.2. Vérifier les comptes existants dans le fichier /etc/passwd

3.3. Création d'utilisateurs et de groupes.

Vous allez créer un nouveau groupe unix, et deux utilisateurs (avec une home mais pas de password ni de shell) dont ce groupe sera leur groupe principal. Ainsi ces deux utilisateurs pourront partager des données uniquement entre eux en mettant les fichiers concernés dans ce groupe avec les droits ad-hoc.

3.4. A quoi peuvent servir des comptes utilisateurs sans possibilité de s'y connecter ?

3.5. Créez un fichier et un répertoire lisible uniquement par ce groupe et vérifiez que vous n'y accédez pas.

3.6. Rajoutez vous dans le groupe que vous avez créé. Vérifiez que vous accédez désormais aux fichiers et répertoires précédents.

3.7. Si vous créez un fichier, sera-t-il dans ce groupe ? Comment faire pour que ce soit le cas ?

3.8. Comment partager un répertoire en rwx pour deux utilisateurs et eux seuls, sans leur dédier un group ?

4. Le système de log (/var/log)

Pour trouver les commandes : apropos log.

4.1. Qui est loggé en ce moment sur votre machine ?

4.2. Qui s'est loggé sur les 10 derniers jours sur votre machine ?

4.3. Quelles sont les 3 dernières tentative de login qui ont échoué ?

4.4. Que fait la commande dmesg

4.5. Quel est le processus qui occupe le plus de mémoire ?

4.6. Effacer ses traces

Dans cette partie vous allez prendre la place du pirate et essayer d'effacer toute trace de votre passage, afin d'en mesurer la difficulté.

Pour cela, connectez vous en ssh localhost en temps qu'utilisateur, puis passez root. Effectuez une commande quelconque comme envoyer un mail ou changer la configuration d'un service.

Lorsque cela est fait, essayez d'effacer toutes trace de cette connexion, du passage root et de l'action faite.

Quelles actions faites vous ?

Comment se prémunir « simplement » contre cela ?

5. Les services et les ports réseaux

5.1. Listez les ports tcp/udp utilisés en ce moment sur votre machine (commande netstat).

5.2. Identifiez la configuration des services sur votre machine : lesquels doivent être démarrés ?

6. Bibliographie

man chmod find ls grep last netstat who ...