Sécurité - TP
Contrôle d'accès

Virginie Van den Schrieck

22 septembre 2015

L'objectif de ce TP est de permettre aux étudiants de mettre en pratique les concepts liés au contrôle d'accès, dans le cadre de Linux.

Le temps prévu de ce TP est d'environ trois heures, séance comprise, en binôme.

Ce TP est inspiré des TPs et tutoriels disponibles sur le web aux adresses suivantes :

- http ://ddata.over-blog.com/xxxyyy/0/03/40/10/Cours/TPs-Unix-User-Polycope.pdf
- http ://www.tecmint.com/how-to-monitor-user-activity-with-psacct-or-acct-tools/

1 Préambule

Ce TP suit le schéma AAA : Authentication, Authorization and Accountability. Nous avons déjà abordé la partie Authentication lors des deux TPs précédents (mots de passe et certificats), et nous allons donc examiner les deux autres. La seconde partie, Authorization, constituera le coeur de ce TP, avec l'exploration du contrôle d'accès Linux. Pour la troisième partie, Accountability, nous verrons comment activer un système de monitoring de l'activité des utilisateurs, toujours sous Linux.

Au niveau technique, le TP se base toujours sur des machines virtuelles Linux. Vous pouvez vous baser sur la machine CentOS-Netkit, disponible sur les machines du labo.

2 Contrôle d'accès aux fichiers Unix

Le contrôle d'accès Unix sera abordé dans le cours théorique de la semaine prochaine. Pour vous plonger dans la matière, vous pouvez partir des liens indiqués sur la page du Campus Virtuel consacrée au cours. Soyez sûrs de bien comprendre :

- Les notions d'utilisateur, de groupe, de User ID et de Group ID.

– Le principe des bits d'accès : rwx, pour chacune des trois catégories owner, group et other.
– Les bits d'accès particuliers : Le sticky bit, le bit SetUID et le bit SetGID, dans le cadre d'un fichier et d'un groupe

Nous allons directement mettre en pratique ces notions dans les exercices ci-dessous, puis nous verrons qu'il est possible d'aller au-delà de ce modèle traditionnel avec des Access List (ACLs). Nous aborderons ensuite quelques risques liés au système de contrôle d'accès UNIX.

2.1 Utilisation du contrôle d'accès

Pour les exercices suivants, vous allez devoir trouver les commandes permettant d'effectuer les actions demandées. Notez-bien ces commandes dans un fichier afin de pouvoir réutiliser ces infos plus tard.

1. Commencez par créer trois utilisateurs : userX, userY, userZ.
2. Créez deux groupes : gr1 et gr2. Attribuez userX et userY au gr1, et userY et user Z au gr2.
3. Ouvrez le fichier /etc/group/. Qu'affiche-t'il ? Quelles informations s'y trouvent ?
4. Comparez les contenus des fichiers /etc/group, /etc/passwod, /etc/shadow. Quelles informations s'y retrouvent ? Quels sont les liens entre ces fichiers ?
5. Loggez-vous en tant que userX, et créez un répertoire rep1. Quels sont les droits d'accès à ce répertoire ? Partagez-le avec le groupe gr1. Vérifiez que seuls les personnes autorisées y ont bien accès.
6. Créez un fichier test dans ce répertoire. Quels sont les droits d'accès qui lui sont donnés ? Comment faire pour que le prochain fichier créé soit accessible à tous les membres du groupe ?
7. Comment faire pour que, dans le répertoire partagé rep1, chaque utilisateur ne puisse supprimer que les fichiers qu'il a lui-même créés ?
8. Quels sont les droits d'accès minimaux pour :
   – Créer un fichier
   – Copier un fichier
   – Renommer un fichier
   – Exécuter un fichier
   – Lister le contenu d'un répertoire
   – Créer un répertoire, avec les droits `rw- rw- --`, puis `rwx rwx r-x`. Quels seront, dans chaque cas, les doits d'accès d'un nouveau fichier dans ce répertoire, et d'un sous-répertoire de ce répertoire ?
9. Quels sont les droits d'accès aux fichiers spéciaux suivants (et que sont ces fichiers spéciaux ?) :
   – /dev/sda*

- /dev/tty*
- /dev/lp*

10. quels sont les droits par défaut des répertoires des utilisateurs (dans /home) ?
11. Comment userX pourrait-il donner l'accès à son répertoire personnel à userY ?
12. Comparez les permissions de /etc/passwd et de /etc/shadow. Expliquez les différences.
13. En tant que root, copiez le fichier /etc/shadow dans /home/userX, et donnez la propriété de ce fichier à userX. En tant que userX, essayez ensuite de modifier cette copie. Que se passe-t-il ? Pourquoi ?
14. En tant que userX, créez un fichier texte quelconque, qui soit lisible par tout le monde, mais modifiable par personne (pas même vous).
15. Cherchez dans le répertoire /user/bin les commandes ayant la permission setUID (utilisez par exemple la commande find). Expliquez pourquoi elles ont cette configuration particulière.

2.2 Questions d'approfondissement

1. Le modèle traditionnel de contrôle d'accès Unix est un peu limitatif. Imaginons par exemple que nous souhaitions partager un répertoire entre des utilisateurs appartenant à deux groupes différents. Comment pourrait-on faire ? Est-ce une solution pratique ? Il existe une solution alternative, les ACLs. Expliquez-les en quelques mots, et expliquez comment mettre en place le partage décrit avec cette technique.
2. Donnez quelques éléments de comparaison entre le contrôle d'accès Unix et le contrôle d'accès Windows.

2.3 Vulnérabilités liées au contrôle d'accès Unix

1. Expliquez les risques liés à un mauvais ajustement des droits d'accès aux fichiers /etc/passwd et /etc/shadow.
2. Expliquez les risques liés à une mauvaise utilisation du setUID.
3. Vous trouverez dans cours_prof une machine virtuelle appelée Nebula. Il s'agit d'une machine virtuelle permettant de s'entraîner à l'exploitation de vulnérabilités systèmes. Vous trouverez plus d'informations à ce sujet sur `http://exploit-exercises.com`. Le but du jeu du premier exercice est d'usurper l'identité de l'utilisateur `flag00`.
   (a) Récupérez cette machine virtuelle, et démarrez-là avec VMWare. Loggez-vous avec le login et le mot de passe `level00`. Essayez l'exécutable `getflag` : Son rôle est de vérifier si vous avez réussi à pirater le compte-cible. Essayez également la commande `id` : Que vous apporte-t-elle comme information ?

(b) Essayez à présent de trouver un fichier exécutable permettant l'exécution en tant qu'utilisateur flag00. Une fois trouvé, exécutez-le. Puis, ré-essayez d'exécuter `id` et `getflag`. Que s'est-il passé ? Expliquez.

(c) Si vous le souhaitez, vous pouvez continuer les exercices proposés sur `exploit-exercice.com`, et approfondir le sujet des vulnérabilités système.

3 Tracabilité/Accountability

Dans le contrôle d'accès, il est important de garder la trace des opérations qui ont été effectuées (login, modifications aux fichiers, etc.). Sous Centos (et autres distributions), il existe un système de monitoring des utilisateurs appelé `psacct`. Vous trouverez les informations d'installation à l'URL suivante : http ://www.tecmint.com/how-to-monitor-user-activity-with-psacct-or-acct-tools

Testez cet utilitaire, et observez les informations que vous pouvez obtenir. En quoi cet outil peut-il vous être utile dans le cadre d'un audit de sécurité ?

En plus de cet utilitaire, vous pouvez plus simplement utiliser la commande `last`. Que fait-elle ? Comment fonctionne-t-elle ?

4 Déliverables

Avant le début du prochain cours, vous posterez sur le Campus Virtuel un document PDF d'une page ou deux documentant le travail effectué et répondant aux questions posées.