Examen MEDI – partie SELinux

Université Paris 12 – Master SSI 2e année

26 février 2008

Exercice 1: [2pts] On veut lancer le programme `monprog.exe` dans le domaine `user_t`, et ce programme essaie de lire et d'écrire dans le fichier `monfich.txt` de caractéristiques suivantes :

```
-rw-r--r--   root root   system_u:object_r:object_t:s0:c1.c3    monfich.txt
```

Décrire la/les règle(s) AV nécessaires à `monprog.exe` pour qu'il s'exécute correctement.

Exercice 2: [3pts] Écrire l'ensemble minimal de règles AV permettant de lancer, à partir du domaine `user_t`, un programme dont le type est `game_exec_t`, de sorte que le processus lancé soit dans le domaine `game_t`.

Ne donner que les règles `allow` et `type_transition` minimales impliquées dans la transition de contexte (pas les macros m4).

Exercice 3: [3pts] Expliquer le message suivant :

```
avc : denied { getattr } for comm="a.out" dev=devpts egid=0 euid=0 exe="/root/selinux/a.out"
exit=0 fsgid=0 fsuid=0 gid=0 items=0 name="1" path="/dev/pts/1" pid=3616
scontext=system_u:system_r:myapp_t sgid=0 suid=0 tclass=chr_file tcontext=root:object_r:devpts_t
tty=pts1 uid=0
```

Donner aussi une règle AV supprimant ce message.

Exercice 4: [2pts] Écrire un fichier `documents.fc` permettant d'étiquetter les fichiers `.exe` du répertoire `/home/utilisateur/appli` en `appli_type_exec_t`, et les autres en `appli_file_t`.

Indication : Pour `grep`, le point doit être préfixé du backslash pour ne pas être interpreté.
