Fonctionnalité SELinux et principaux outils d'administration / KB – mai 2014

1 SELinux / Type Enforcement

1.1 Introduction SELinux

Brève historique de SELinux

Histoire du module LSM et Architecture Selinux (patch kernel -> module LSM)

Intégrité/confidentialité/règles définies

Zéro-day exploits / bac à sable des applications

Modèle classique vs figure domaines

1.2 Objectif de SELinux

SELinux ajoute des méthodes de contrôle d'accès

{Mandatory Access Control (Type enforcement) [MAC/TE]

Role Base Access Control [RBAC]

Mult-Category Security/Multi-Level Security (optionnel)} [MCS/MLS]

Certaines distributions **Linux** livrées avec plusieurs milliers de règles (démo summary APOL)

L'administrateur système peut customiser et ajouter des règles, des modules

Liste blanche

Fine granularité

1.3 Contexte/Label de sécurité (MAC/TE)

Composé de trois identificateurs obligatoires :

Utilisateur:Rôle:**Type**

Toutes les ressources du système (fichiers, sockets, processus…) ont **un** contexte de sécurité

Ex. afficher cons fichier / processus (démo)

Terminologie (label, contexte ou domaine de sécurité)

1.4 AUTORISATION

Classe d'objets

Permissions

Autoriser un sujet avec un cons source d'avoir permissions sur un objet avec un cons cible

Config les accès de chaque processus (sujet) pour les restreindre au strict minimum (objets)

ex. password shadow figure autorisation (démo figure 14 en partie)

1.5 CHANGEMENT DE TYPE/DOMAINE

Shell avec contexte A (ex.), comment arrive à contexte B (démo Figure 14-15)

Point d'entrée Transition Type destination

1.6 AVC LOG

Résoudre messages de refus avc (Prévenir de l'impact !!)

1.7 PROBLÈME LABELLING FICHIER

Copie dossier www

Archivage d'un dossier

Ré-étiquetage des fichiers et systèmes de fichiers

Montage d'un système de fichier

Backup et restore du système

1.8 PORT (EX. APACHE)

Ecoute port non par défaut

1.9 BOOLÉENS

Modification booléen (démo exécution interdites)

1.10 MODULES

Lister les modules / Ajout modules (à l'installation automatique par l'appli ou installation manuelle)

But et structure de la reference policy (Développeur et administrateur système)

Étude d'un module existant (apache, sVirt ?) (Développeur et administrateur système)

Création modules

1.11 RÔLES

1.12 MCS/MLS

1.13 LABO PRATIQUE

sestatus

ls -Z

id -Z

ps –Z

APOL

semanage

audit2why

fixfiles / restorecon / chcon

audit2allow

semodule

2 REFERENCE

SElinux by Example

Deployment_Guide__CentOS5 (sVirt)

Red_Hat_Enterprise_Linux-6-Security-Enhanced_Linux-en-US (MCS/MLS, backup system)

The_SELinux_Notebook_Volume_1_The_Foundations (macro refpolicy)

The_SELinux_Notebook_Volume_2_Sample_Policy_Source

gosselin_apache (étudier module apache)

imm4446 (RBAC)