Formation « Comprendre SELinux et savoir modifier la politique de sécurité »

Réf : SELinux

SELinux vise à renforcer la sécurité d'un système Linux en mettant en œuvre une politique de contrôle d'accès obligatoire. SELinux est intégré en standard au noyau Linux depuis 2003 et certaines distributions (Fedora depuis 2004, Red Hat Enterprise Linux et CentOS depuis 2005) l'activent par défaut.

On constate en pratique que beaucoup d'administrateurs de systèmes Linux sur lesquels SELinux est activé par défaut le désactivent parce qu'ils ne comprennent pas son fonctionnement et que SELinux les empêche de travailler. S'il est gênant pour les administrateurs, il est également gênant pour les intrus et c'est son intérêt.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Comprendre les mécanismes du fonctionnement de SELinux
- Analyser les problèmes pratiques liés à SELinux
- Savoir adapter les contextes de sécurité des fichiers et les booléens
- Savoir personnaliser la politique de sécurité

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Professionnels de la sécurité
- Administrateurs systèmes expérimentés
- Auditeurs et gestionnaires d'incidents
- Analystes en sécurité, auditeurs et membres de CSIRT (CERT)

Pré-requis

- Avoir les bases en administration de systèmes Unix, idéalement 3 à 5 ans d'expérience

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Introduction

- Contexte de sécurité
- L'option `-Z` (ou `--context`)
- Mise en évidence des problèmes pratiques posés par SELinux
- États de fonctionnement
- La commande `sestatus`
- Les commandes `getenforce` et `setenforce`
- La commande `selinuxenabled`

Les booléens SELinux

- La commande `getsebool`
- La commande `setsebool`

Gestion de la politique de sécurité

- La commande `setfiles`
- La commande `restorecon`
- La commande `fixfiles`
- La commande `chcon`
- La commande `newrole`
- La commande `runcon`
- La commande `seinfo`
- La commande `semanage`
- La commande `apol`
- Les commandes `audit2why` et `audit2allow`

Modification de la politique de sécurité

- Types de fichiers permettant d'étendre la politique de sécurité
- Procédure d'extension de la politique de sécurité
- Exemple de module simple
- Exemple de module de politique
- Cas pratiques