==========

Livrable: Présentation sur SELinux

==========

École Normale Supérieure Meknès
Département Informatique
Supervision: Dr. Mehdi Moukhafi
Auteur: Soussan Jawad
Date de présentation: 14 décembre 2023

==========

Sécurité avec SELinux : Guide Récapitulatif

1. Introduction

La sécurité dans les systèmes Linux est cruciale, et SELinux (Security-Enhanced Linux) joue un rôle clé dans le renforcement de cette sécurité. Cette section rappelle l'importance de SELinux pour assurer un contrôle d'accès obligatoire (MAC) efficace.

2. DAC vs MAC

Exploration des différences entre le contrôle d'accès discrétionnaire (DAC) et le contrôle d'accès obligatoire (MAC). Met en évidence les vulnérabilités potentielles dans le modèle DAC.

3. Histoire et Introduction à SELinux

Un aperçu du lancement de SELinux par la NSA et Red Hat dans les années 1990, son intégration dans le noyau Linux en 2003, et son adoption par des distributions majeures.

4. Fonctionnement de SELinux

Explication de la manière dont SELinux applique des contrôles d'accès obligatoires (MAC) et de l'importance des étiquettes (labels) et de l'application de types.

5. Gestion des Étiquettes

Démonstration de la manière dont SELinux attribue des contextes aux fichiers, processus, ports, etc. Utilisation des commandes telles que ls -Z, id -Z, et ps -Z.

6. Transition de Fichier

Exploration de l'exception à la gestion des étiquettes avec la transition de fichier. Exemple de transition de fichier avec le processus dhclient.

7. Booleans

Explication des booléens comme des paramètres on/off pour SELinux. Exemple d'utilisation de booléens pour contrôler l'accès FTP à certains répertoires.

8. Conclusion

En conclusion, Security-Enhanced Linux (SELinux) émerge comme une solution essentielle pour renforcer la sécurité des systèmes Linux. Face aux vulnérabilités potentielles du modèle de contrôle d'accès discrétionnaire (DAC), SELinux introduit le contrôle d'accès obligatoire (MAC) en imposant des politiques centralisées strictes.

9. Ressources Supplémentaires

Liens vers des documents officiels SELinux et références pour approfondir la compréhension de l'utilisation avancée de SELinux.

https://danwalsh.livejournal.com/56760.html
https://slideplayer.com/slide/5824372/
https://milestone-of-se.nesuke.com/en/sv-advanced/selinux/selinux-summary/
https://retro64xyz.gitlab.io/presentations/2018/10/16/firejail-and-apparmor/
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index
https://fr.wikipedia.org/wiki/SELinux

contact information :
jawadsoussan2001@gmail.com