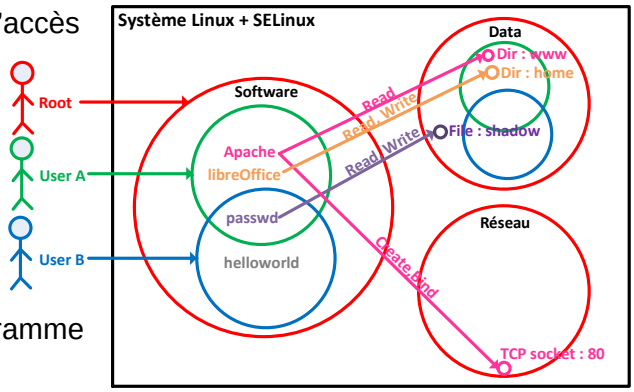
h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2012
Session de bachelor

Résumé: Security Enhanced for Linux (SELinux)

SELinux implémente plusieurs modèles de contrôle d'accès (MAC par TE, RBAC, MCS/MLS) qui améliorent grandement la sécurité des systèmes d'exploitation Linux. Le but de ce travail est, dans un premier temps, d'étudier d'un point de vue théorique le fondement des modèles présents dans SELinux. Puis, dans un second temps, d'analyser les règles fournies dans Fedora Core 16 (FC16) et de sélectionner les outils de gestion adéquats afin de faciliter l'administration du système. Ce travail sera poursuivi dans un programme exploratoire financé par la HES-SO.



L'étude s'est déroulée en huit semaines et a été réalisé en cinq étapes.

1. Lecture de l'excellent livre « SELinux by Example » qui traite de l'écriture de règles et qui décrit les différents mécanismes de contrôle.
2. Étude de nombreux documents et présentations trouvés sur le web.
3. Prise en main de Fedora 16, des outils d'analyse de règles et d'administration.
4. Définition de scénarios qui démontrent le fonctionnement du Type Enforcement (TE) et de Role Base Access Control (RBAC).
5. Réalisation d'un scénario où un système, sans et avec le renforcement SELinux, est attaqué en utilisant une porte dérobée.

J'ai choisi de commencer par étudier le modèle TE car c'est le modèle fondamental à la solution SELinux. Après avoir compris le concept de TE, je me suis attaqué à l'étude de la syntaxe et à la signification des règles TE. La compréhension des règles m'a été grandement bénéfique et m'a permis de simplifier mon travail lors de l'analyse des règles de FC16. L'avantage d'avoir commencé par TE est qu'il permet de comprendre aisément le modèle RBAC car il est implémenté avec un petit ajout à TE.

J'ai beaucoup utilisé l'excellent logiciel GUI d'analyse de règles APOL et ainsi que la commande indispensable d'administration semanage. Ces deux outils importants ont été utilisés pour :

- Démontrer TE, RBAC et MCS (Multi-Category Security).
- Expliquer la démarche que doit avoir un administrateur système lorsqu'il est confronté à une situation de blocage pour comprendre sa provenance et la résoudre.
- Restreindre les droits d'un utilisateur.

J'ai expliqué comment générer des règles à l'aide de l'outil polgengui pour sécuriser un logiciel auquel il n'existe pas de règles écrites dans la communauté, ainsi que la limitation de cette méthode.

Vers la fin du travail, j'ai récupéré les sources d'un serveur FTP vulnérable à un exploit Metasploit et décrit l'installation pour que les règles SELinux contenues dans F16 soient appliquées au serveur FTP. Au final j'ai récupéré un shell distant grâce à BackTrack 5 en exploitant cette faille et démontré l'intérêt de SELinux pour contrer cette attaque.

Diplômant :
M. BASBOUS KHALED
Classe : TE3
Filière d'études : Télécommunications
Ingénierie des Technologies de l'Information

Timbre de la direction