Cours Gnu/Linux

su / sudo

alan.simon@free.fr

Présentation

su : switch-user

sudo : switch-user do

Commandes :

- su
- sudo
- visudo

Fichier /etc/sudoers /etc/sudoers.d/*

Utilisation de la commande su 1/2

Usage :

“su toto -c id”

Après passage du mots de passe du compte toto on execute la commande id avec son identité

“su toto”

Après passage du mots de passe de toto lance un shell sous son identité

si le compte est homis la valeur par défaut est le compte root

Testez ! :

su toto -c id

su toto

ps -f | grep (votre pts/X)

Utilisation de la commande su 2/2

Gestion de l'environnement

“**su - toto**” : On simule un login

Attention :

- Vous lancez le shell par défaut du compte cible
- Le compte doit être autorisé au login

“**su -m $user**” ou “**su -p $user**” : On conserve l'environnement d'orrigine

Validation

Comment valider la gestion de l'environnement avec la commande su?

- Créez un compte
- Editez son profile et ajoutez :
  - echo '.profile sourced'
- Testez le su et le su - sur ce compte.

Comment valider le comportement du su -m ?

Principes de sécurité en production

Environnement applicatif = Un compte

- Owner de ses fichiers et de ses processus
- Il est le gestionaire des droits d'accès à ses fichiers

Production :

- Un intervenant = Un compte : cela permet la tracibilité des actions.
- Les comptes non associés à une personne ne doivent pas se connecter
- problème du secret partagé : **Si le mot de passe est connu de tous alors il n'est plus secret.**

Il faut cependant permettre la gestion des applicatifs aux intervenants

- Exploitants
- Admins

La solution sudo 1/2

Usage simple :

“sudo -l” : liste authorisations sudo

“sudo -u $user $cmd” : lance la commande $cmd en tant que $user en demandant **le mot de passe du compte source**

Tests : sous root

apt-get install sudo

sudo -l

sudo -u toto id

La solution sudo 2/2

Gestion de l'environnement

- “sudo -iu $user $cmd” : simule une connexion (utilise donc l'environement de l'utilisateur)

- “sudo -Eu $user $cmd” : préserve l'environnement de l'utilisateur d'origine

- “sudo -u $user $cmd” : suit la configuration sudo pour la gestion de l'environnement

TD : mise en évidence : comment tester et voir l'effet des option -i et -E ?

Administration Sudo

“man sudo”

L'ensemble de la configuration est traitée dans le fichier /etc/sudoers

Defaults : permet de définir les options par défaut de l'outil sudo

Alias : Permet de definir des classes de

Host_Alias : Des Host
User_Alias : Utilisateur (intervenant)
Runas_Alias : Runas_user (applicatif)
Cmnd_Alias : Commandes (classe de commandes)

Definition des droits : **Who where = (as_whom) what**

U_alias H_alias=(R-as-user_alias) C_alias

Les alias 1/2

Host_Alias $name = item, item, item

- hostname
- Ip , network/netmask
- +netgroup
- Host_Alias
- ALL

Cmnd_Alias $name = item, item

- /chemin/commande
- /path/
- /chemin/commande arguments
- ALL

Exemple :

- Cmnd_Alias exploit = /opt/exploit/bin/

Les alias 2/2

User_Alias $name = item, item

Runas_Alias $name = item, item

avec pour item :

- user
- #uid
- %group
- +netgroup
- User_Alias / Runas_Alias

Exemple :

User_Alias admins = %admin, ! %app

User_Alias exp = admins, %expoit, ! %app

Runas_Alias app = %app, apache

Les droits

Droits :

Users host=(Runas_user) Item, item

Item : spec: cmds

- Specs :
  - PASSWD
  - NOPASSWD
  - NOEXEC : bloque les échapements

Exemple :

```
User_Alias U_OK = toto
Runas_Alias RA_TST = appli
Cmnd_Alias C_TST = /usr/bin/id, /home/test/bin/
Cmnd_Alias C_EDIT = /usr/bin/vi
U_OK    ALL=(RA_TST) PASSWD:C_TST, NOEXEC:C_EDIT
```

TD de cours

Tester la configuration présenté :

User_Alias U_OK = toto

Runas_Alias RA_TST = appli

Cmnd_Alias C_TST = /usr/bin/id, /home/test/bin/

Cmnd_Alias C_EDIT = /usr/bin/vi

U_OK ALL=(RA_TST) PASSWD:C_TST, NOEXEC:C_EDIT

Réflexion : Organisation de l'admin

Comment organiser une exploitation sécurisé des applications sur la production

- Les opérateur doivent pouvoir :
  - Passer les commandes de démarrage et d'arret des application (en tant que le compte applicatif)
  - Killer (-15) un processus applicatif
  - Lancer les batchs applicatif
- Les admin : prendre n'importe quel identité applicatif mais aucune opérateur

Vous devez spécifier les caractéristiques:

- Des comptes applicatifs
- Des comptes operateurs
- Des comptes admins
- Le fichiers sudoers