Introduction à GNU/Linux

Sécurisation

Pascal Bessonneau

Starinux

11/2017

Compte ROOT

Être *root* permet de tout faire sur un poste *GNU/Linux*. C'est le super utilisateur qui permet notamment d'éditer les fichiers systèmes, arrêter/démarrer des services, ...
Mais il ne faut pas utiliser le compte *root*. En effet on peux supprimer, altérer des fichiers systèmes ou d'autres utilisateurs.
Et si vous le pouvez, surfer sur le web ou lancer des programmes vous expose considérablement car un malware peux de profondes modifications sur votre ordinateur.

Compte ROOT

C'est pour cette raison que le compte root doit absolument être désactivé sur un poste convenablement sécurisé. C'est le cas par défaut sur les distributions modernes.
Cette désactivation est visible dans le fichier */etc/passwd* car comme interpréteur de fichier il doit y avoir */bin/false*.
false est un programme qui échoue lorsqu'on le lance.

sudo

Comme il n'y a pas de compte *root* et qu'il faut quand même pouvoir modifier des fichiers systèmes, lancer/démarrer des services, ... il existe la possibilité d'utiliser l'utilitaire *sudo*.
Les administrateurs (et non le commun des mortels) doit avoir un accès à *sudo*. Cela est possible car les administrateurs appartiennent au groupe *sudo* (ou *wheel*).
Lorsque vous tapez une commande précédée par *sudo* alors cette commande est exécutée en tant que *root* après vous être authentifié avec votre mot de passe. Le mot de passe n'est pas redemandé pendant quelques minutes après une première utilisation de sudo.
Attention, vous pouvez tout casser avec une commande sudo comme si vous êtiez *root*.

sudo

La différence avec un compte *root* est que le fait d'être *root* est transitoire. Ce qui permet de se protéger de beaucoup de malwares. Le nombre de personnes pouvant être *sudoers* doit être limité au maximum. D'autant plus que la mise à jour des paquets non critiques est possible sur les dernières distributions par des administrateurs et non par le super utilisateur.

sudo

Enfin il est possible de limiter les commandes que peuvent lancer les *sudoers*. Ceci est possible en éditant le fichier de configuration de *sudo* avec la commande *visudo*.
Par exemple on peut ajouter paul qui a besoin de lancer/relancer apache car il est webmaster. Il suffit alors de rajouter :

```
paul ALL = /usr/bin/apachectl
```

Et il ne faut pas l'ajouter aux utilisateurs sudo.
Plus d'information sur ces modifications sont disponibles là.

Protocoles réseaux

On s'intéressera principalement à trois protocoles : TCP, UDP et ICMP.
Le protocole TCP est le plus utilisé. Il est utilisé quand une connexion stable et qui nécessite l'envoi et la réception de paquets dans un ordre défini.
Le protcole UDP est moins utilisé. Il sert souvent à envoyer des messages où l'aspect transactionnelle est moins importante comme la vidéo sur le LAN. Il ne garantit ni que les données arrivent dans l'autre ni que les deux ordinateurs ont établi une connexion.
Le protocole ICMP est un protocole dont on peux se passer mais qui permet d'envoyer des messages sur le réseau : saturation du réseau, écho, ... Il n'est pas associé à un port particulier contrairement à TCP et UDP.

Protocoles réseaux

Quand vous voulez ouvrir un port pour SSH, votre site web ou une autre application il s'agit souvent de TCP. Quelques applications comme la communication sur internet (genre Skype) peuvent demander d'ouvrir un port UDP.
Le protocole ICMP doit être accessible par exemple sur des opérateurs de serveurs tels qu'OVH qui utilisent ce protocole pour vérifier que la machine est bien « Up and running ».

Protocoles réseaux

Par défaut quand une application n'écoute pas sur le port, le port est fermé. Si une application l'utilise et peut établir une connexion dans le sens internet vers votre ordinateur, le port est ouvert. Si c'est dans l'autre sens le port est fermé : c'est votre ordinateur qui initiera la connexion dans le sens votre ordinateur vers internet.
Un pare-feu permet de protéger votre ordinateur en masquant des ports ouverts qui ne devraient pas être visibles depuis l'extérieur (imprimante 631, ssh 22, ...). Les ports sont alors masqués : votre ordinateur ne renvoie pas un message port fermé ce qui ne trahi pas sa présence et empêche la connexion depuis l'extérieur.

arno-iptables-firewall

C'est un petit pare-feu disponible sous Debian/Ubuntu.
A partir de quelques questions, il met en place un pare-feu tout à fait performant et sécuritaire.
Après installation, les réglages supplémentaires sont situés dans le fichier */etc/default/arno-iptables-firewall* et */etc/arno-iptables-firewall/firewall.conf*.
Vous trouverez un tutoriel là.

FirewallID

là là là là