Sudo ► sudoers

I► Dans ce cours, nous allons voir comment intégrer un utilisateur (simple) dans les sudoers afin qu'il puisse accéder à des commandes de root sans avoir à connaître le mot de passe de root !

Une alternative à SUDO : **su root -c "mkdir /backup/"**
Exécute la commande en tant que root et restitue immédiatement le prompt à l'utilisateur …

Le fichier de configuration des sudoers est **/etc/sudoers**
Pour l'éditer il faut être root, mais cela ne suffit pas ?
On va préférer **visudo** qui ouvrira le fichier en édition :
C'est comme vi mais visudo corrigera ou alertera des éventuelles faute de syntaxe … Cool !

► **visudo -c -f /etc/sudoers** vérifie les erreurs de syntaxe du fichier

1er cas : on veut rendre accessible toutes les commandes root à un utilisateur :

On dé-commente les lignes contenant le groupe **wheel** …
Et on ajoute le(s) utilisateur(s) au groupe wheel pour qu'ils puissent bénéficier des droits sudo :
gpasswd -a michel wheel

Lorsqu'on voudra passer une commande root, il suffira de saisir **sudo fdisk /dev/sdb** par exemple …

2nd cas : on veut rendre accessible certaines commandes root à un utilisateur :

On édite à nouveau le fichier /etc/sudoers :

► **User_Alias STAFF = michel,tux,cyndi,linuz**
le groupe est STAFF et on y place 1 ou plusieurs users (le greoupe n'a pas besoin d'éxister)

► **Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, sbin/systemctl**

► ***Cmnd_Alias NET=/bin/ping,/usr/bin/traceroute,/usr/bin/ftp,/usr/bin/nmap***

Création d'un Alias de commandes

Les privilèges de Root :**root ALL=(ALL) ALL**
1er ALL : indique tous les hosts sur laquelle la cmd peut être éxécutée
2nd ALL : indique les droits du user que l'on prend
3ème ALL : indique les commandes du user que l'on peut utilise

Les privilèges des autres users :
► **tux ALL=(bruce) ALL** :
tux sur tous les hosts, prend les droits de bruce pour toutes ses commandes
► **tux 192.168.10.5,192.168.10.0/24=(ALL) /sbin/halt,sbin,reboot**
tux sur les hosts cités, peut éteindre et redémarrer les machines
► **Cedric ALL=(ALL) NOPASSWD:ALL**
(on ne demande pas le mot de passe de Cedric)
► **STAFF ALL=(ALL) SERVICES**

Michel BOCCIOLESI