Les utilisateurs
partie 2

Découverte et définitions

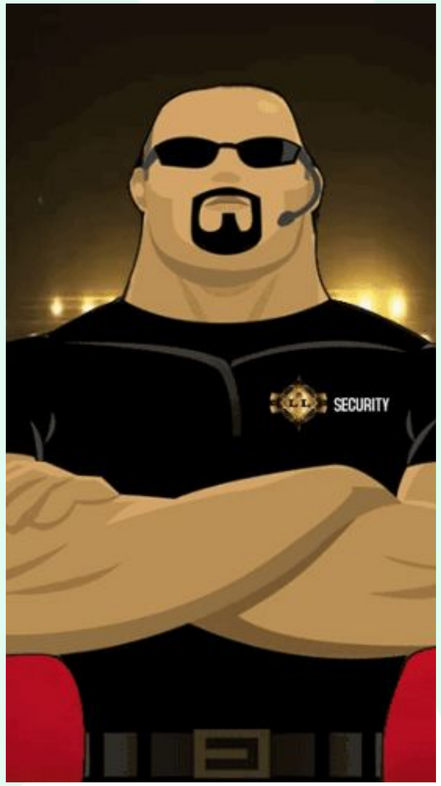
Que pouvez-vous dire sur la sécurité des utilisateurs sur les systèmes Windows ?

Et sur Linux ?

Sommaire

De quoi s'agit-il ?

La sécurité



Gestion des identités et des accès (IAM)

Comment faire ?

- Pratique qui consiste à s’assurer que les personnes et les entités ayant une identité numérique ont le bon niveau d’accès aux ressources de l’entreprise (réseaux et BDD).
- Les rôles d’utilisateur et les privilèges d’accès sont définis et gérés par un système IAM.

Identification

Qui suis-je ?

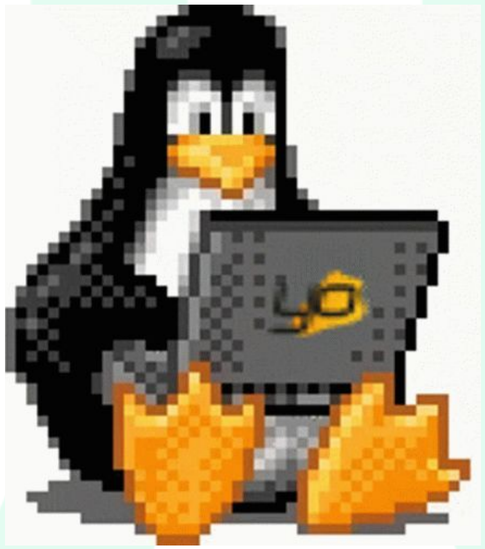
- Étape indispensable où l'on doit enregistrer **l'identité** de l'utilisateur. Avant de pouvoir se connecter à son compte, il doit entrer un **identifiant (login)**.
- Cette information est un renseignement attribué à titre **individuel** et est unique.

Authentification

Vous pouvez rentrer !

- Cumule l’identification et l’authentification afin d’accéder à un service.
- Consiste à vérifier qu’une tentative de connexion est légitime. L’autorisation est accordée après une authentification réussie.

Gestion des utilisateurs GNU/Linux



Liste des utilisateurs

La liste des utilisateurs locaux

Fichier texte **/etc/passwd**

- 1 ligne par utilisateur
- 7 colonnes séparées par **“:” avec les informations suivantes** :
  - nom de connexion
  - validation du mot de passe (x,*)
  - identifiant utilisateur (uid)
  - identifiant de groupe principal (gid)
  - champs Gecos ➜ commentaire, description, ...
  - répertoire personnel (home directory)
  - shell de lancement
- Convention : root uid=0

Exemple de fichier passwd

cat /etc/passwd

```
wilder@Ubuntu:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
wilder:x:1000:1000:Some Heroic Wilder,,,:/home/wilder:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:126:65534::/run/sshd:/usr/sbin/nologin
```

Administration des utilisateurs

Quelques commandes utiles

passwd : modifier un mot de passe

adduser : ajout d'utilisateurs

deluser : suppression d'utilisateurs

usermod : modifier un utilisateur

chfn : modifier la description d'un utilisateur

chsh : modifier le shell par défaut d'un utilisateur

chage : modifier durée de validité

newusers : création d'utilisateurs par lot

pwck : vérification du format des fichier passwd et shadow

Base des mots de passe

Les empreintes de mots de passe

Fichier texte **/etc/shadow**

- 1 ligne par utilisateur
- 9 colonnes séparées par **“:” avec les informations suivantes** :
  - nom de connection
  - mot de passe (+sel) ➜ (! ou * => connexion impossible)
  - date de dernière modification
  - nombre de jours minimum
  - nombre de jours maximum
  - nombre de jours d'avertissement
  - nombre de jours de tolérance de mot de passe expiré
  - fin de validité du compte
  - champ sans utilisation actuelle

Exemple de fichier shadow

cat /etc/shadow

```
wilder@Ubuntu:~$ sudo cat /etc/shadow
root:!:19081:0:99999:7:::
daemon:*:18912:0:99999:7:::
bin:*:18912:0:99999:7:::
man:*:18912:0:99999:7:::
lp:*:18912:0:99999:7:::
nobody:*:18912:0:99999:7:::
systemd-timesync:*:18912:0:99999:7:::
messagebus:*:18912:0:99999:7:::
syslog:*:18912:0:99999:7:::
wilder:$6$Je34t19kkZ2ZGs9f$PleinDeCaracteresCryptiques:19081:0:99999:7:::
sshd:*:19090:0:99999:7:::
```

Base des groupes

La liste des groupes

Fichier texte **/etc/group**

- 1 ligne par groupe
- 4 colonnes séparées par **“:”** avec les informations suivantes :
  - nom de groupe
  - mot de passe (x,*)
  - gid
  - liste des membres du groupe

- Convention : root uid=0

Exemple de fichier group

cat /etc/group

```
wilder@Ubuntu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
tape:x:26:
sudo:x:27:wilder
users:x:100:
nogroup:x:65534:
crontab:x:105:
nopasswdlogin:x:124:
wilder:x:1000:
sambashare:x:135:wilder
```

Administration des groupes

D'autres
commandes utiles

newgrp : prendre un nouveau groupe

groupadd : ajout d'un groupe

groupdel : suppression d'un groupe

groupmod : modifier un groupe

grpck : vérification du format des fichier group et gshadow

Interagir avec les utilisateurs

Encore plus de commandes !!!

id : affiche ses uid/gid et groupes

whoami : alias de id -un

who : affiche les utilisateurs connectés

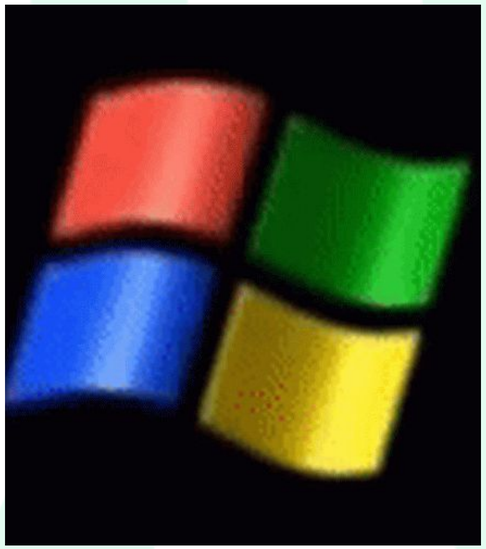
su : changer d'utilisateurs

sudo : lancer une commande avec un autre uid

exit : quitter une session

logout : quitter une session login

Gestion des utilisateurs Windows



Liste des utilisateurs

Comment les avoir ?

Les utilisateurs qui ont eu un compte activé au moins 1 fois ont leur dossier de profile dans **C:\Users**

Méthode basique: **Get-LocalUser**

- 1 ligne par utilisateur
- 3 colonnes :
  - Nom
  - Activation
  - Description

Exemple de liste utilisateurs

Liste simple

```
PS C:\> Get-LocalUser

Name                Enabled Description
----                ------- -----------
Administrateur      False   Compte d'utilisateur d'administration
wilder              True    Compte utilisateur de test
DefaultAccount      False   Compte utilisateur géré par le système.
Invité              False   Compte d'utilisateur invité
WDAGUtilityAccount  False   Compte d'utilisateur géré et utilisé par le …
```

Liste des utilisateurs

La méthode détaillée

Méthode Wmi: **Get-WmiObject**

Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'" | Format-Table -AutoSize

- 1 ligne par utilisateur
- 6 colonnes:
  - Type de compte
  - Légende (emplacement)
  - Domaine
  - SID
  - Nom complet
  - Nom

Exemple de liste utilisateurs

La liste détaillée

```
PS C:\> Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'" | Format-Table -AutoSize

AccountType  Caption                 Domain SID                                                 FullName      Name
-----------  -------                 ------ ---                                                 --------      ----
512          PCLab\Administrateur    PCLab  S-1-5-21-3909285403-2394092363-769350273-500                      Administrateur
512          PCLab\wilder            PCLab  S-1-5-21-3909285403-2394092363-769350273-1001 wilder wilder wilder
512          PCLab\DefaultAccount    PCLab  S-1-5-21-3909285403-2394092363-769350273-503                      DefaultAccount
512          PCLab\Invité            PCLab  S-1-5-21-3909285403-2394092363-769350273-501                      Invité
```

La base SAM

La méthode détaillée

Le Gestionnaire de comptes de sécurité (**SAM**) est une base de données qui est présente sur les ordinateurs exécutant un OS Windows.

Elle stocke les comptes d'utilisateur et les descripteurs de sécurité pour les utilisateurs sur l'ordinateur local.

La base SAM est située dans **%SystemRoot%\system32\Config\SAM**

Les mots de passe en GUI

La méthode détaillée

Méthode 1 :

Dans le menu Windows, aller sur le **Gestionnaire d’identification**.

Méthode 2 :

Dans une invite de commande, taper la ligne de commande :

rundll32.exe keymgr.dll,KRShowKeyMgr

Liste des groupes

La liste des groupes

Méthode basique: **Get-LocalGroup**

- 1 ligne par groupe
- 2 colonnes :
  - Nom
  - Description

Exemple de listing de groupes

La manière rapide

```
PS C:\> Get-LocalGroup

Name                  Description
----                  -----------
Administrateurs       Les membres du groupe Administrateurs dispo…
Administrateurs Hyper-V  Les membres de ce groupe disposent d'un acc…
Duplicateurs          Prend en charge la réplication des fichiers dans…
IIS_IUSRS             Groupe intégré utilisé par les services Internet (IIS).
Invités               Les membres du groupe Invités disposent par déf…
```

Liste des groupes

La manière détaillée

Méthode WMI: **Get-WmiObject Win32_group**

- 1 ligne par groupe
- 4 colonnes :
  - Légende (emplacement)
  - Domaine
  - Nom
  - Description

Exemple de listing de groupes

La liste détaillées

```
PS C:\> Get-WmiObject win32_group

Caption                                  Domain  Name                                 SID
-------                                  ------  ----                                 ---
PCLab\Administrateurs                    PCLab   Administrateurs                      S-1-5-32-544
PCLab\Administrateurs Hyper-V            PCLab   Administrateurs Hyper-V              S-1-5-32-578
PCLab\Duplicateurs                       PCLab   Duplicateurs                         S-1-5-32-552
PCLab\IIS_IUSRS                          PCLab   IIS_IUSRS                            S-1-5-32-568
PCLab\Invités                            PCLab   Invités                              S-1-5-32-546
PCLab\Opérateurs de chiffrement          PCLab   Opérateurs de chiffrement            S-1-5-32-569
PCLab\Opérateurs de configuration réseau PCLab   Opérateurs de configuration réseau   S-1-5-32-556
PCLab\Opérateurs de sauvegarde           PCLab   Opérateurs de sauvegarde             S-1-5-32-551
PCLab\Propriétaires d'appareils          PCLab   Propriétaires d'appareils            S-1-5-32-583
PCLab\System Managed Accounts Group      PCLab   System Managed Accounts Group        S-1-5-32-581
PCLab\Utilisateurs                       PCLab   Utilisateurs                         S-1-5-32-545
PCLab\Utilisateurs avec pouvoir          PCLab   Utilisateurs avec pouvoir            S-1-5-32-547
PCLab\Utilisateurs de gestion à distance PCLab   Utilisateurs de gestion à distance   S-1-5-32-580
PCLab\Utilisateurs du Bureau à distance  PCLab   Utilisateurs du Bureau à distance    S-1-5-32-555
```

Administration des utilisateurs

Quelques
commandes utiles

Disable-LocalUser : permet de désactiver un compte utilisateur.

Enable-LocalUser : permet d'activer un compte utilisateur.

Get-LocalUser : liste l'ensemble des comptes utilisateur locaux présents sur le poste de travail.

New-LocalUser : crée un nouveau compte utilisateur local.

Administration des utilisateurs

D'autres commandes utiles

Get-LocalGroup : liste l’ensemble des groupes de sécurité locaux présents sur le poste de travail.

New-LocalGroup : crée un nouveau groupe de sécurité local.

Remove-LocalGroup : supprime un groupe de sécurité.

Add-LocalGroupMember : ajoute un membre dans un groupe local.

Get-LocalGroupMember : récupère les membres présents dans un groupe local.

En résumé

A retenir

- La gestion des identités
- La gestion des utilisateurs

MERCI

pour votre participation.

C’est à vous maintenant.
Des questions ?
Des remarques ?