

Rapport de Stage

Modifier un mot de passe d'une session utilisateur

12/02/2015

Romain Ledru stagiaire au CNAM de Nantes, du 05/01/2015 au 13/02/2015

Contenu

1. Sujet, Demande.....	2
2. Contexte.....	2
3. Recherches.....	3
3.1. Authentification	3
3.1.1. La biométrie	3
3.1.2. Le badge	3
3.1.3. Le téléphone portable.....	3
3.1.4. Interface interactive.....	3
3.1.5. Comparatif	4
Préconisation :	4
3.2. Active Directory.....	5
Résumé et informations complémentaires :	5
4. Technologies, langages utilisées.	6
4.1. Virtualisation.....	6
4.2. Langages.....	6
4.3. PowerShell	6
4.4. C#	8
4.4.1 C# mode console	9
4.4.1 C# Incident.	9
5. Réalisé : Maquette	10
6. Reste à faire	12
7. « Excuses »	12
8. Bilan.....	12

1. Sujet, Demande.

Le SI du CNAM Nantais a comme projet de concevoir une **application interne** permettant à un ses permanents de **réinitialiser** leur **mot de passe de session Windows**, le même que celui de la **messaging**.

Ma mission est **d'étudier** les différents **moyens techniques** pour arriver à ce résultat afin **d'établir** une première **maquette du projet**.

La première **problématique** est de pouvoir **authentifier** l'employé ayant perdu son mot de passe. Il ne **peut donc plus prouver son identité**.

La deuxième est de **pouvoir changer son mot de passe**. (Dans quelle **base** est-il stocké, et comment le **modifier via un script**)

La troisième est **d'étendre** cette **maquette** pour **d'autres applications** (logiciels internes).

2. Contexte

Sous la tutelle du ministère en charge de l'enseignement supérieur et de la recherche, le Cnam est un grand établissement public chargé de développer **trois missions** :

- **la formation** : agir pour l'emploi des actifs.
- **la diffusion du savoir** : favoriser la culture, la citoyenneté et le débat public.
- **la recherche appliquée** : innover et produire de nouveaux savoirs.



3. Recherches

3.1. Authentification

Le but des premières recherche était de lister et comparer différents moyens d'authentifier une personne physique.

3.1.1. La biométrie

L'identification en fonction de caractéristiques biologiques telles que les empreintes digitales, les traits du visage, etc.

3.1.2. Le badge

L'identification par une demande d'information supplémentaire : Un badge unique détenu par le permanent.

3.1.3. Le téléphone portable

L'identification par une demande d'information supplémentaire :

- Demande de réponse secrète par sms.
- Validation d'un code envoyé par sms.

3.1.4. Interface interactive

L'identification par une demande d'information supplémentaire depuis une interface interactive:

- Formulaire pour le changement de mot de passe s'appuyant sur une demande de réponse secrète.

3.1.5. Comparatif

Le tableau ci-contre regroupe et compare différents moyens d'authentications d'une personne physique afin de fournir au décideur une base de réflexion.

	SMS	Réponse secrète	Biométrie	Badge
Contraintes	- Les employés devront donner leur numéro au préalable.	- Les employés devront mémoriser leur réponse.	-Achat du matériel (couteux). - soumis à autorisation préalable de la CNIL. <i>Plus d'information sur la biométrie en entreprise :</i> http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/la-biometrie-sur-les-lieux-de-travail/	-Achat du matériel. -Perte, oubli du badge possible par l'employé.
Avantages	-Presque tout le monde a un téléphone portable. - Aucunes données (mot de passe ou réponse secrète) à mémoriser.	-Aucun identifiant matériel.	- Aucunes données (mot de passe ou réponse secrète) à mémoriser. - Aucun identifiant matériel.	- Aucunes données (mot de passe ou réponse secrète) à mémoriser.

Préconisation :

L'utilisation de badge ou de la biométrie sont à écarter, pour une raison de complexité et de coût.

L'authentification par téléphone (sms) ou via une interface utilisateur sont nettement plus envisageable, de par leurs faisabilités et leurs faibles coûts.

3.2. Active Directory

Pour **modifier le mot de passe** d'une session Windows, il faut d'abord savoir **comment** et à **quel endroit** est stocker cette information.

La contrainte donnée est Active Directory (déjà mis en œuvre dans l'entreprise).

Active Directory est le nom du **service d'annuaire de Microsoft**. Le terme de service d'annuaire doit être entendu au sens large, c'est-à-dire qu'il s'agit d'un annuaire référençant :

- des personnes (nom, prénom, numéro de téléphone, etc.)
- des serveurs, des imprimantes, des applications, des bases de données, etc.

En permettant de recenser de nombreuses informations concernant le réseau, Active Directory constitue le moyen central de toute l'architecture réseau. Cela permet :

- à un utilisateur de retrouver et d'accéder à n'importe quelle ressource recensée.
- d'avoir une représentation globale de l'ensemble des ressources et des droits/accès associés et constitue de ce fait un outil d'administration et de gestion centralisé du réseau.

Résumé et informations complémentaires :

Dans un réseau structuré, les différents utilisateurs et leurs informations personnelles (login, nom, prénom, tel, mail, etc) sont enregistrés dans un annuaire.

L'annuaire est une « base de données » spécialisé dans la gestion d'utilisateur et d'administration de droits) :

Active Directory.

Les informations personnelles sont structurées, organisés et enregistré dans des attributs prévu par Active Directory.

Voir annexes : **1.1. Attributs de la classe utilisateurs** (page 2 et 3).

La **création** d'un **attribut** (pour stocké question/réponse secrète) a été envisagé, mais **non retenu** car c'est une solution **non parraine**.

En effet, un identifiant unique doit être donné à l'attribut crée, si Microsoft utilise l'id que l'on a choisie l'ors d'une prochaine mise à jours, cela entrainerai un conflit dans Active Directory).

Voir annexes : **1.2. Créer un attribut** (page 4 à 6)

4. Technologies, langages utilisées.

4.1. Virtualisation

Afin de tester différents langages, scripts pour modifier un mot de passe,

Deux machine virtuels (situés dans un réseau fermé) ont été mis à ma disposition :

- Une machine virtuelle client.
- Une machine virtuelle serveur, avec les services Active Directory et Serveur IIS.

L'Active Directory coté serveur a été configuré par le stagiaire en système et réseau, des utilisateurs et des règles d'administrations ont été créés.

4.2. Langages

Deux langages différents ont été imposés pour modifier le mot de passe de session utilisateur :

- PowerShell
- C# (Framework .net)

4.3. PowerShell

PowerShell est une interface en ligne de commande et un langage de script développé par Microsoft.

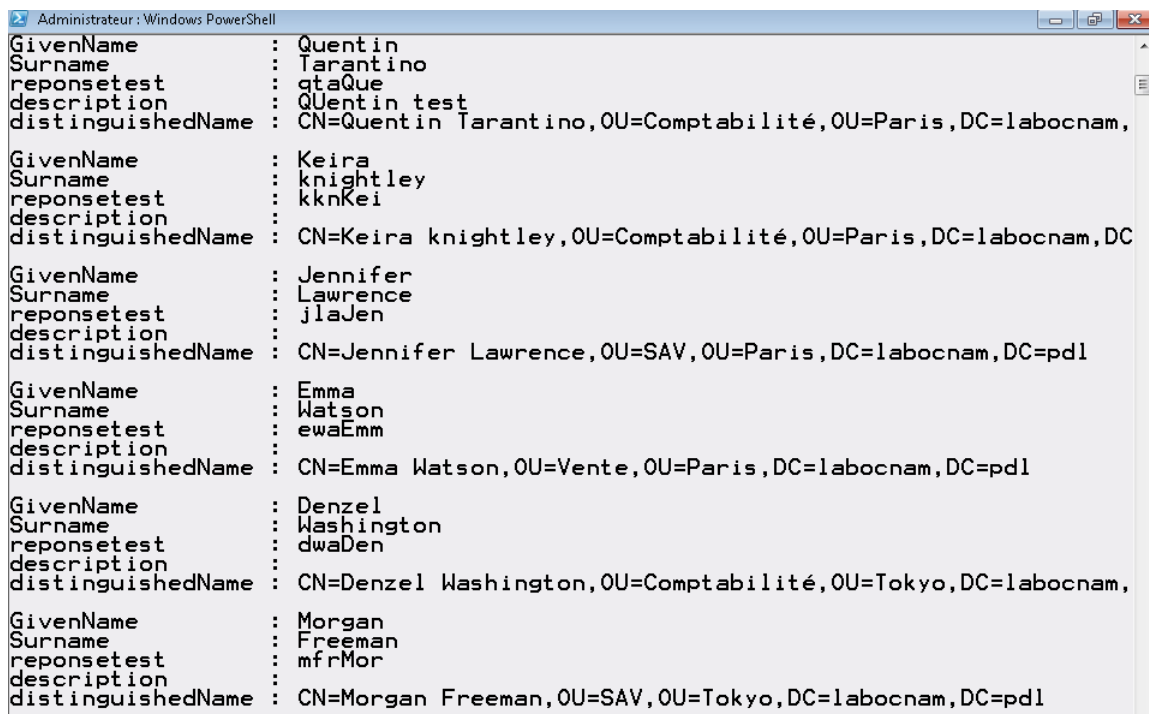
Requis et installation : voir annexe : **2.1 PowerShell : Ajout du module Active Directory** (page 7 et 8).

Les objectifs :

- Afficher les utilisateurs enregistrés dans Active Directory.
- Modifier le mot de passe d'un utilisateur.
- Gérer le cas particulier : deux utilisateurs ont le même nom.

Production :

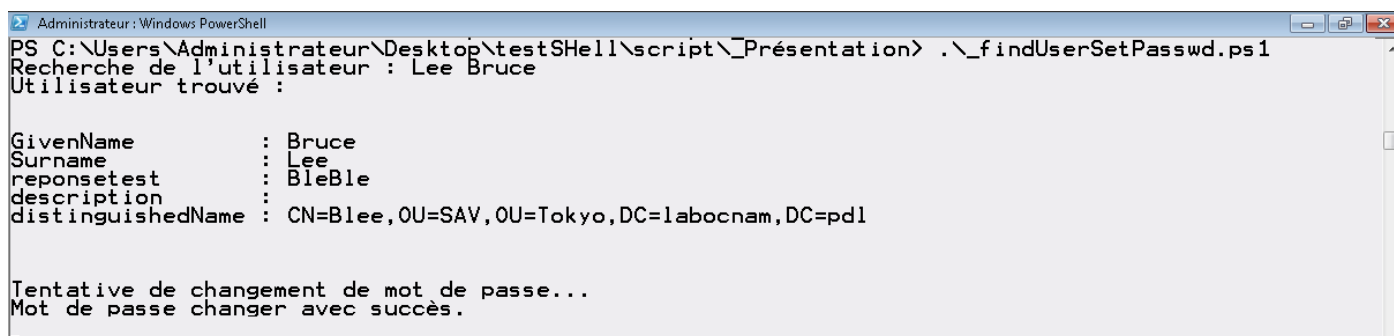
7 Modifier un mot de passe d'une session utilisateur.



```
Administrateur : Windows PowerShell
GivenName      : Quentin
Surname        : Tarantino
reponsetest    : qtaQue
description    : Quentin test
distinguishedName : CN=Quentin Tarantino,OU=Comptabilité,OU=Paris,DC=labocnam,
GivenName      : Keira
Surname        : knightley
reponsetest    : kknKei
description    :
distinguishedName : CN=Keira knightley,OU=Comptabilité,OU=Paris,DC=labocnam,DC
GivenName      : Jennifer
Surname        : Lawrence
reponsetest    : jlaJen
description    :
distinguishedName : CN=Jennifer Lawrence,OU=SAV,OU=Paris,DC=labocnam,DC=pd1
GivenName      : Emma
Surname        : Watson
reponsetest    : ewaEmm
description    :
distinguishedName : CN=Emma Watson,OU=Vente,OU=Paris,DC=labocnam,DC=pd1
GivenName      : Denzel
Surname        : Washington
reponsetest    : dwaDen
description    :
distinguishedName : CN=Denzel Washington,OU=Comptabilité,OU=Tokyo,DC=labocnam,
GivenName      : Morgan
Surname        : Freeman
reponsetest    : mfrMor
description    :
distinguishedName : CN=Morgan Freeman,OU=SAV,OU=Tokyo,DC=labocnam,DC=pd1
```

Un premier script permettant d'afficher dans une console les utilisateurs enregistrés d'Active Directory.

Voir annexe : **2.2.1. Afficher les utilisateurs** (page 9)



```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur\Desktop\testShell\script\_Présentation> .\_findUserSetPasswd.ps 1
Recherche de l'utilisateur : Lee Bruce
Utilisateur trouvé :

GivenName      : Bruce
Surname        : Lee
reponsetest    : BleBle
description    :
distinguishedName : CN=Blee,OU=SAV,OU=Tokyo,DC=labocnam,DC=pd1

Tentative de changement de mot de passe...
Mot de passe changer avec succès.
```

Deuxième script permettant d'afficher dans une console l'utilisateur choisie(en dure) ainsi que de modifier son mot de passe.

Voir annexe : **2.2.2. Modifier le mot de passe d'un utilisateur** (page 9,10)

8 Modifier un mot de passe d'une session utilisateur.

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur\Desktop\testShell\script\_Présentation> .\_2UsersSameAttribut.ps1
recherche de l'utilisateur : Test Romain
Attention : 3 utilisateurs ont été trouvés pour nom : Test et prénom : Romain
-----
utilisateur n° 0

GivenName      : Romain
Surname        : Test
sAMAccountName : rtest

-----
utilisateur n° 1

GivenName      : Romain
Surname        : Test
sAMAccountName : rtest2

-----
utilisateur n° 2

GivenName      : Romain
Surname        : Test
sAMAccountName : rtest3

-----
quel utilisateur êtes-vous?
entrer votre numéro: 2

-----
Vous avez choisi l'utilisateur répertorié: CN=rtest3,OU=SAV,OU=New York,DC=labocnam,DC=pd1
-----

Tentative de changement de mot de passe...

-----
Mot de passe changé avec succès.
-----
```

Script permettant de gérer la multiplicité d'un nom d'utilisateur.

Voir annexe : **2.2.2. Cas particulier** (page 11, 12,13).

4.4. C#

Le C# (prononcé si-charpe), est un langage objet récemment développé par Microsoft pour sa plate-forme .NET. Sa syntaxe ressemble beaucoup au langage Java de Sun Microsystems et au C++. C# est supposé être le langage le plus adapté pour le développement .NET .

Requis et installation : Visual Studio (community).

4.4.1 C# mode console

Les objectifs :

- Afficher les utilisateurs enregistrés dans Active Directory.
- Modifier le mot de passe d'un utilisateur.
- Gérer le cas particulier : deux utilisateurs ont le même nom.

Le code C# que j'ai développé est sous forme d'un menu regroupant toutes les fonctions manipulant les utilisateurs AD que j'ai pu écrire.

C'est pourquoi il n'est pas pertinent de présenter une impression écran du résultat du code.

Le code C# produit est disponible annexe : **3.1. Script C# mode console** (page 13 à 25).

On remarquera que les scripts PowerShell ou C# nous permettent tous les deux de modifier les attributs d'un utilisateur.

Néanmoins, Le PowerShell étant un langage de Scripting, il n'est pas évident de l'interfacé avec une IHM,

En revanche, le C# avec le Framework asp.net nous permet aisément ce genre de choses.

4.4.1 C# Incident.

Afin d'optimiser mes phases de test, j'ai développé des scripts permettant de réinitialiser à une valeur choisie, leurs attributs de mot de passe et de réponse secrète.

Le script C# permettant de réinitialiser le mot de passe s'exécute sans rapport d'erreur de la part de l'IDE, les utilisateurs sont toujours manipulables avec des scripts C#.

Mais il devient alors impossible de connecter un utilisateur sur sa session, et les scripts PowerShell ne fonctionnent plus correctement.

Le problème ne venait pas d'un changement trop rapide des mots de passe utilisateurs successifs, car même en ajoutant une pause entre chaque changement dans la boucle prévue à cet effet, le problème persiste.

J'ai donc restauré un snapshot de l'AD afin de régler ce problème.

La modification successive des utilisateurs de la manière suivante est à ne surtout pas mettre en production

Boucle pour tous les utilisateurs {

```
userEntry.Invoke("SetPassword", new object[] { leNouveauMotDePasse });
```

```
System.Threading.Thread.Sleep(1000);
```

```
userEntry.CommitChanges();
```

```
System.Threading.Thread.Sleep(1000);
```

```
}
```

5. Réalisé : Maquette

Mon travail était d'utiliser mes scripts antérieurs afin que les interactions avec l'utilisateur se fasse depuis un navigateur et non une console.

Vérifier que le Framework asp.net fonctionne correctement avec la Library AD.

Le moyen d'authentification retenu pour cette maquette est la réponse à une question secrète.

La question secrète n'est pas encore déterminée.

Code C# voir annexe : **3.1.2 Script C# IHM, asp.net** (page 26 à 52).

Liste des contrôleurs pour le domaine trouvé:
srv-romain.cnam.local

Serveur AD atteint: LDAP://CNAM.local

Cherche un utilisateur (* : champs obligatoires):

Nom :

Utilisateur: " Lee " obtient: 1 Résultat(s).

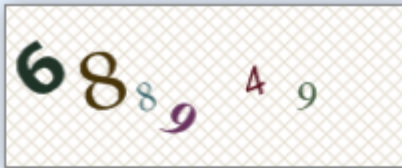
	Login	Nom	Prénom
<input type="button" value="Selectionner"/>	blee	Lee	Bruce

Vous avez sélectionné l'utilisateur dont le login est : blee

Quelle est votre réponse secrète?

Votre réponse est correcte.

Protection
anti-bot



Recopiez
la suite
de
nombres:

Captcha bon.

Votre nouveau mot de
passe:

Confirmation du mot de
passe :

Mot de passe
changé avec
succès de
l'utilisateur (login)
: blee.

6. Reste à faire

Le choix du moyen d'authentification n'est pas encore décidé :

-Pour l'utilisation du téléphone portable, un sondage interne pourra être effectué afin de savoir combien de permanents seraient prêt à fournir leur numéro personnel.

-Pour l'utilisation de réponse à une question secrète, il faudra déterminer une ou plusieurs questions pouvant s'appliqué à tous mais dont la réponse est personnel et inconnu par les autres permanents.

L'IHM proposé a été développé sans charte graphique, il faut en définir une respectant les normes de l'entreprise.

La sécurité lié à l'écriture du code est à revoir : les identifiants administrateurs sont écrits en dure, non chiffré dans le code.

La sécurité concernant la navigation sur les pages web n'est pas suffisante :

Possibilité de faire des retours arrière pendant les différentes phases de saisies et de vérifications.

7. « Excuses »

La maquette déployée ne fonctionnait pas correctement :

La VM virtualisant le serveur n'était plus à jours car le mois d'essais de la licence était écouler et le temps manquait pour résoudre ce problème.

8. Bilan

C'est dans un cadre agréable et dynamique que j'ai pu mener à bien mon projet.

J'ai aussi pu découvrir une facette de la vie en entreprise que je ne connaissais pas.

Ce stage m'as permis d'apprécier ma progression en développement, mais aussi de découvrir l'intérêt et les enjeux de la création d'une maquette et des recherches nécessaires à celle-ci.

Pour un élève en option développement, j'ai également pus être confronté aux problèmes de sécurité et de l'administration du système réseau (problème pour joindre le domaine « bac à sable » depuis le domaine sur lequel ce trouvais mon poste et les droit que me donnait ma session stagiaire.

L'équipe était contente de mon travail et considère ma mission comme réussite.