Reset mot de passe ou utilisateurs contrôleur de domaine





Windows 10



Yohan Fresneau

Sommaire

1.	Dans quel cas Réinitialisation le mot de passe	. 3
2.	Comment procéder	. 3
3.	Mise en place de la faille	. 4
4.	Exploitation de la faille	13
a	Compte utilisateur local	13
b	Contrôleur de domaine	15
5.	Comment remettre tout en ordre	16

1. Dans quel cas Réinitialisation le mot de passe

Il y a différentes situations qui nous force à réinitialiser notre mot de passe, comme par exemples ces situations :

- → Perte du mot de passe ou de l'identifiant administrateur
- ➔ Pirate du compte
- → Changement du mot de passe par accident
- → Pour une blague (qui ne ferra rire que vous)
- Possibilité de rentrer en administrateur sur une machine (illégale si elle ne vous appartient pas)
- → Toutes les situations possibles

Nous allons voir maintenant comment le faire

2. Comment procéder

Pour faire cette manipe, nous allons devoir prendre un CD ou une clé d'installation Windows serveur ou une installation de Windows 8, 10 ou serveur 2012, 2016.

Cette faille va exploiter les outils d'ergonomie, qui se trouve au moment de saisir le mot de passe de Windows.



Le but de cette manipe est de cliquer sur la loupe et avoir un invité de commande en administrateur et changer le mot de passe Windows.

3. Mise en place de la faille

Pour mettre en place ceci, nous allons avoir besoin de démarrer sur la clé USB d'installation.

i Installation de Windows	
. Windows	:
Langue à installer : <mark>Français (France)</mark> Eormat horaire et monétaire <mark>; Français (France)</mark>	<u> </u>
<u>C</u> lavier ou méthode d'entrée : <mark>Français</mark>	• sur Suinest nour zonlinuer
© 2016 Microsoft Corporation. Tous droits réservés.	ez sur survant pour continuer.

Cliquez sur "**suivant**" pour continuer

🔹 Installation de Windows		0 🛋	
	Windows		
	Installer maintenant		
Réparer l'ordinateur	, den de		
€ 2016 Microsoft Corporation. Tous drive	reserves.		

Choisir "Réparer l'ordinateur"

\rightarrow	Ontinuer Itter et passer à Windows 10		
	Épannage nitialiser le PC ou afficher les ions avancées		
ب ا	eindre votre PC		

Sélectionner l'option "Dépannage"

Réinitialiser ce PC Are cette epiton, vous pouver choisir de reinstaller Windows
Signal Spitions avancées Options avancées

Choisir l'option "Réinitialiser ce PC"

	Restauration du système Utiliser un point de restauration sur votre PC pour restaurer Windows	C:\	Invite de commandes Utilise l'invite de commandes pour un déparmage avancé
+	Récupération de l'image système Récupérer Windows à l'aide d'un fichier image système spécifique	₽	Rétrograder vers la version précédente
<¢>	Outil de redémarrage système Corriger les problèmes qui empêchent le chargement de Windows		

Cliquer l'option "Récupération du l'image système"

• Récupération de l'image système	
Chobir un système d'exploitation able. Windows 10	

Cliquer l'option "Windows 10"



Il ne trouve pas d'image, on va donc fait "annuler"

Sélectionner une sauvegarde d'image système. Cet ordnateur sera restauré à l'aide de l'mage système. Contraction de toroux sur cet d'antateur sera restauré à l'aide de l'mage système. Informations incluses dans l'image système. Informations de résolution des problèmes pour la récupération complète : http://go.microsoft.com/fwlink/p//Linktd=225039 Utiliser la dernière image système (recommandé)
Informations de résolution des problèmes pour la récupération complète : http://go.microsoft.com/fwlink/p//LinkId=225039 Utiliser la dernière image système (recommandé)
Utiliser la dernière image système (recommandé)
Emplacement :
Date et heure :
Sélectionner une image système
< Précédent: Suivant > Annule

On va donc spécifier "Sélectionner une image système", puis "suivant"

Réimager l'ordinateur		2
Sélectionnez l'emplace Si l'image système se t ordinateur, puis dique:	ment de la sauvegarde pour l'or rouve sur un périphérique externe, c z sur Actualiser.	rdinateur à restaurer
Cliquez sur Avancé pour périphérique de sauvega Fuseau horaire actuel : (ajouter un emplacement réseau ou in ride s'il ne figure pas dans la liste ci-d SMT+01:00	uvegarde de innage systeme. Istaller un pilote pour un essous.
Emplacement	Image système la plus récente	Ordinateur
Avancé		Actualiser
	< Précédent	Sulvant > Annuler

Cliquez sur "avancer", ce qui permet normalement de sélectionner notre image.

🙀 Réimager l'ardinateur			23	9
Sélectionnez l'emplace	ement de la cauvenarde	e nour l'ordinateur à re	actauror A	
Reininger Lorainateur				
Rechercher et installer un ne se trouve pas dans la l	pilote pour un périphériq iste des images système o	que qui est connecté à l'a disponibles.	ordinateur, mais	
			Annuler	-
Avancé			Actualiser	_
	< Pr	récédent Suivant >	Annuler	

Sélectionner "Installer un pilote"

Reimoger l'ordinateur	
Si limage système et urove sur un pérchérique externe, convecter le à cet ordinateur, puis cliquez sur Actualiser. Si limage système est sur DVD, insérez le dernier DVD de la sauvegarde de limage système.	
Cliquez sur Avance pour ajouter un emplacement réseau ou installer un pilote pour un périphérique de <i>Ajouter des pilotes</i> Fuseau horaire Emplacement Insérez le suport d'installation du périphérique	
	0
Avancé Actualiser	
< Précédent Suivent > Annuler	

Cliquez sur "**OK**", pour ouvrir le gestionnaire de fichiers

Regarder dans : 📃 Bureau 🗸 🎯 🏂 💬 🛄 🗸	
Accès rapide 🔊 Système	
Bibliothèques Bi	
Corbeille Ce PC	
Non du febiar :	
Types de fichiers : Infomations d'installation v Annuler	

Nous avons donc le gestionnaire de fichiers qui s'ouvre, nous allons dans "**Ce PC**"

-				×
Regarder dans :	Ce PC	~ G (Ø 🖻 🛄	
Bibliothèques	Videos Périphériques et lecteurs (Réservé au systè 163 Mo libres sur Disque local (D:) 48,9 Go libres sur 0 octet(s) libres sur Boot (X:) 27,2 Mo libres sur	4) me (C.) 499 Mo 59.5 Go 59.5 Go 59.5 Go 14 Go r 29.6 Mo		~
	Nom du fichier :		✓ Ou	vrir 🛛 🔻
	Types de fichiers : Information	ns d'installation	~ Ar	nuler

Nous avons donc bien nos disques, dont le Disque "D:" qui en réalité est le disque "C:" système

Begarder dans	Disque local (D:)	a a 🕫 🖂 -	×
Accès rapide	Nom Logs PerfLogs Program Files (x86) Programmes Utilisateurs Windows Windows Windows Windows Windows Windows	Modifié le 27/04/2016 06:48 30/10/2015 08:24 30/10/2015 08:24 23/09/2017 17:32 23/09/2017 21:27 23/09/2017 21:27 23/09/2017 22:41	Type Dossier de Dossier de Dossier de Dossier de Dossier de Dossier de Dossier de
	Nom du fichier : Types de fichiers : Informations d'installation	× ×	> Ouvrir 😽 Annuler

Nous allons ensuite dans "Windows"

- Ouvin				×
Regarder dans	: Windows		G Ø 🕫 🗔 •	
-	Nom	^	Modifié le	Type ^
X	Speech		30/10/2015 08:24	Dossie
Accès rapide	Speech_One	Core	30/10/2015 08:24	Dossie.
-	System		30/10/2015 08:24	Dossie
111	System32		23/09/2017 21:18	Dossie
Bibliothèques	SystemApps	5°	27/04/2016 06:30	Dossie
	SystemReso	urces	30/10/2015 08:24	Dossie
	SysWOW64		27/04/2016 06:44	Dossie
Ce PC	TAPI		30/10/2015 08:24	Dossie
	- Tasks		27/04/2016 06:44	Dossie
	Temp		23/09/2017 21:38	Dossie.
	tracing		30/10/2015 08:24	Dossie
	twain_32		30/10/2015 08:24	Dossie
	UpdateAssis	stantV2	23/09/2017 21:12	Dossie.
	Vss Vss		30/10/2015 08:24	Dossie 🗸
	<			>
	Nom du fichier :		~	Ouvrir 🖛
	Types de fichiers	Informations of installation		Annular

Nous allons ensuite dans "System32"

Ouvrir				— ×
Regarder dans :	System 32		O Ø Ø 😕 🔜	•
4	Nom	^	Modifié le	Type
X	Magnificati	ion.dll	30/10/2015 08:18	Extensi
Accès rapide	Magnify		30/10/2015 08:17	Applic
-	🗟 main.cpl		30/10/2015 08:18	Élémer
100	Maintenand	ceUI.dll	30/10/2015 08:17	Extensi
Bibliothèques	📧 makecab		30/10/2015 08:17	Applici
	🙀 manage-ba	le	30/10/2015 08:18	Applice
	🌋 manage-ba	le	30/10/2015 08:18	Windo
Ce PC	MapConfig	MapConfiguration.dll		Extensi
	MapControl	lCore.dll	27/04/2016 06:16	Extensi
	MapContro	lStringsRes.dll	27/04/2016 06:16	Extensi
	Mapi32.dll		30/10/2015 08:17	Extensi
	mapistub.d	u	30/10/2015 08:17	Extensi
	MapsBtSvc.	dll	27/04/2016 06:16	Extensi
	MapsBtSvc	Proxy.dll	27/04/2016 06:16	Extensi
	¢.	<u></u>		,
	Nom du fichier :	Magnify	~	Ouvrir
	Types de fichiers :	Informations d'installation	1 ×	Annuler

Localiser le fichier "Magnify" et le renommer en "Magnifyold"

🖣 Ouvrir				×
Regarder dans :	System 32		🖂 🧿 🎓 🛄 🕇	
-4	Nom	^	Modifié le	Type ^
X	clusapi.dll		30/10/2015 08:19	Extensi
Accès rapide	cmcfg32.dll		30/10/2015 08:17	Extensi
-	os. cmd		30/10/2015 08:17	Applic
100	Cmdext.dll		30/10/2015 08:17	Extensi
Bibliothèques	cmdial32.dl	1	30/10/2015 08:17	Extensi
	🔳 cmdkey		30/10/2015 08:17	Applic
	cmdl32		30/10/2015 08:17	Applic
Ce PC	Crogrespps.c	HU	30/10/2015 08:17	Extensi
	Crmifw.dll		30/10/2015 08:17	Extensi
	cmintegrate	or.dll	30/10/2015 08:18	Extensi
	Contraction of the second seco		30/10/2015 08:17	Extensi
	cmmon32		30/10/2015 08:17	Applice
	cmpbk32.dli	1	30/10/2015 08:17	Extensi
	a cmstp		30/10/2015 08:17	Applici 🗸
	<			>
	Nom du fichier :	cmd	~	Ouvrir 🗸
	Types de fichiers :	Informations d'installation	~	Annuler

Localiser le fichier "**cmd**", en faire une copie

Ouvrir				×
Regarder dans	: System 32		- 🕒 🗘 🔁 🗔	
4	Nom	^	Modifié le	Type ^
X	CloudNotifie	cations	30/10/2015 08:18	Applic
Accès rapide	Cloud Storag	eWizard	30/10/2015 08:18	Applico
-	clrhost.dll		30/10/2015 08:18	Extensi
	🗟 clusapi.dll		30/10/2015 08:19	Extensi
Bibliothèques	cmcfg32.dll		30/10/2015 08:17	Extensi
	on cmd - Copie		30/10/2015 08:17	Applic
	cmd		30/10/2015 08:17	Applic
Ce PC	cmdext.dll		30/10/2015 08:17	Extensi
	cmdial32.dll		30/10/2015 08:17	Extensi
	📧 cmdkey		30/10/2015 08:17	Applic
	Scmdl32		30/10/2015 08:17	Applic
	cmgrcspps.o	III.	30/10/2015 08:17	Extensi
	Crifw.dll		30/10/2015 08:17	Extensi
	cmintegrato	r.dll	30/10/2015 08:18	Extensi 🗸
	<			>
	Nom du fichier :	cmd - Copie	~	Ouvrir 🔻
		and the second second		1000 Contract (1000)

Renommer la copie du fichier "**cmd**", en "**Magnify**"

Ouvrir				×
Regarder dans :	System 32	~	G 👌 📂 🗔 •	
-	Nom	^	Modifié le	Type ^
X	Jz32.dll		30/10/2015 08:17	Extensi
Accès rapide	Magnificati	on.dll	30/10/2015 08:18	Extensi
-	Magnify		30/10/2015 08:17	Applic
-	Magnifyold		30/10/2015 08:17	Applic
Bibliothèques	main.cpl		30/10/2015 08:18	Élémer
	Maintenand	eUI.dll	30/10/2015 08:17	Extensi
	📧 makecab		30/10/2015 08:17	Applic
Ce PC	🙀 manage-ba	e	30/10/2015 08:18	Applic
	S manage-ba	le	30/10/2015 08:18	Windo
	MapConfigu	uration.dll	27/04/2016 06:16	Extensi
	MapControl	Core.dll	27/04/2016 06:16	Extensi
	MapControl	StringsRes.dll	27/04/2016 06:16	Extensi
	🔄 mapi32.dll		30/10/2015 08:17	Extensi
	🗟 mapistub.di	u –	30/10/2015 08:17	Extensi 🗸
	<			>
	Nom du fichier :	Magnify	~	Ouvrir 🖛
	Types de fichiers	Types de fichiers : Informations d'installation		Annular

Une fois rafraichi le dossier, on peut voir que notre fichier "cmd" est devenue "Magnify" et que nous avons l'original en "Magnifyold"

Nous pouvons redémarrer l'ordinateur directement et enlever le CD ou la clé Bootable

4. Exploitation de la faille

a. Compte utilisateur local

Démarrage de "L'invite de commande" grâce à la loupe



Le mot de passe à réinitialiser est celui du compte administrateur, pour cela aller sur "les options d'ergonomie" et plus cliquer sur "loupe"



Nous avons donc l'invité de commande qui est exécuté, on peut faire un "net users", pour voir les utilisateurs de la machine

Le texte du message assi	nyære ncié au numéro Øx2350 est introuv	able dans le fichier de	
messages pour Applicatio	on.		
(c) 2015 Microsoft Corp Espace insuffisant pour	pration. Tous droits réservés. traiter cette commande.		
C:\Windows\system32>net	users		
comptes d'utilisateurs (de //		
admin defaultuserØ Des erreurs ont affecté	Administrateur Defaul Invité l'exécution de la commande.	tAccount	
C:\Windows\system32>net	user admin Toor012		
La commande s'est termi	nee correctement.		
C:\Windows\system32>		155	
	Mot de passe		

Pour modifier le mot de passe, nous devons faire la commande "net user <utilisateur> <nouveau mot de passe>"



Voilà, le mot de passe a été réinitialisé

b. Contrôleur de domaine

Démarrage de "L'invite de commande" grâce à la loupe



Pour lancer le contrôleur de domaine, aller sur "les options d'ergonomie" et plus cliquer sur "loupe"



Nous avons donc l'invité de commande qui est exécuté, on peut faire un "dsa.msc" afin d'ouvrir le contrôleur de domaine

Eichier Action Affichage 2	ounsateur	secondinatedi	o Active Directory	
] @ 🔒 🛛 🗊	1 🙎 📚 🖆 🦷	1 🧕 🕱	
Utilisateurs et ordinateurs Active	Nom	Туре	Description	
Requêtes enregistrées	Administrat	Utilisateur	Compte d'utilisateur d'a	
⊿ 🚔 freshome.lan	😹 Administrat	Groupe de séc	Administrateurs désigné	
Builtin	🍇 Administrat	Groupe de séc	Administrateurs désigné	
Comptabilité	🍇 Admins du	Groupe de séc	Administrateurs désigné	
Computers Computers	🎎 Contrôleurs	Groupe de séc	Tous les contrôleurs de	
	Scontrôleurs	Groupe de séc	Les membres de ce grou	
	& Contrôleurs	Groupe de séc	Les membres de ce grou	
	🤽 Contrôleurs	Groupe de séc	Les membres de ce grou	
	A DnsAdmins	Groupe de séc	Groupe des administrate	
	😹 DnsUpdateP	Groupe de séc	Les clients DNS qui sont	
	& Éditeurs de c	Groupe de séc	Les membres de ce grou	
	Sroupe de r	Groupe de séc	Les mots de passe des	
	Sroupe de r	Groupe de séc	Les mots de passe des	
	🛃 Invité	Utilisateur	Compte d'utilisateur inv	
	Ma Invités du d	Groupe de séc	Tous les invités du dom	
	Crdinateurs	Groupe de séc	Toutes les stations de tr	
	Propriétaires	Groupe de séc	Les membres de ce grou	
	Protected Us	Groupe de séc	Les membres de ce grou	
82	Serveurs RA	Groupe de séc	Les serveurs de ce group	
	Utilisateurs	Groupe de séc	Tous les utilisateurs du	
	A REAL PROPERTY AND A REAL	Groupe de réc	Members of this group	
<	& WinRMRem	oroupe de sec	Weinbers of this group	
	KinRMRem	oroupe de sec	Members of this group	
ш >	KinRMRem	oroupe de sec	Members of ans group	

Nous avons accès au contrôleur de domaine, avec des droits administrateurs

5. Comment remettre tout en ordre

Pour remettre comme avant, il suffise de booter sur le CD ou la clé USB bootable et de supprimer le fichier "**Magnify**" créer précédemment et renommer le fichier "**Magnifyold**" en "**Magnify**".