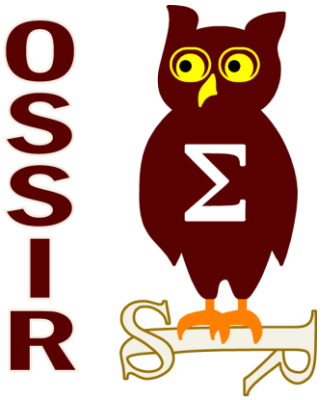

xmco®
we deliver security expertise


OSSIR

Faiblesses des méthodes d'administration en environnement Windows et État des lieux de l'outillage intrusif

Présentation

- **Marc LEBRUN**
  - Consultant Sécurité chez XMCO depuis 2012

- **XMCO**
  - Cabinet de conseil et d'audit en sécurité informatique
  - Créé en 2002, le cabinet est aujourd'hui constitué de 25 consultants

- **Activités**
  - Tests d'intrusion
  - Audits de sécurité
  - Certification PCI-DSS
  - CERT-XMCO : Réponse à incident, veille en vulnérabilité
  - Conseil et expertise sécurité

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

Trois objectifs

- Identifier quelles méthodes d'administration distantes laissent des traces d'authentification exploitables par un attaquant

- Quels outils utiliser pour récolter ces données efficacement et de manière fiable afin de poursuivre l'intrusion ?

- Quelles actions simples et rapides prendre pour se prémunir face à ce type d'attaque ?

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

Le SSO Microsoft

Pourquoi ? Comment ?

- Single Sign-On (SSO) de Microsoft : limiter au maximum les authentifications manuelles
  - Une meilleure « *User Experience* »
  - Mais il faut bien conserver en « cache » de quoi s'authentifier à la demande : les *hashes* des mots de passe (voire les mots de passe)

- *Local Security Authority Subsystem Service* (LSASS) s'en charge, via les *Authentication Packages :*
  - *MSV1_0*
  - *Wdigest*
  - *Kerberos*
  - *TsPkg*

Le SSO Microsoft

Pourquoi ? Comment ?

- *LSASS & Authentication Packages* implémentent le SSO et manipulent les données d'authentification

- Mais il n'y a pas que les *hashes* LM/NTLM et les mots de passe :
  - *Access Tokens* des Processus et des Threads
  - Tickets *Kerberos*
  - Tâches planifiées / *Credential manager*

Types de données recherchées

Les *hashes* LM/NTLM

- Condensat cryptographique du mot de passe, non salé
- Ces *hashes* sont présents sur le disque dans la ruche SAM (pour les postes de travail), et dans la base NTDS.DIT (pour les contrôleurs de domaine)

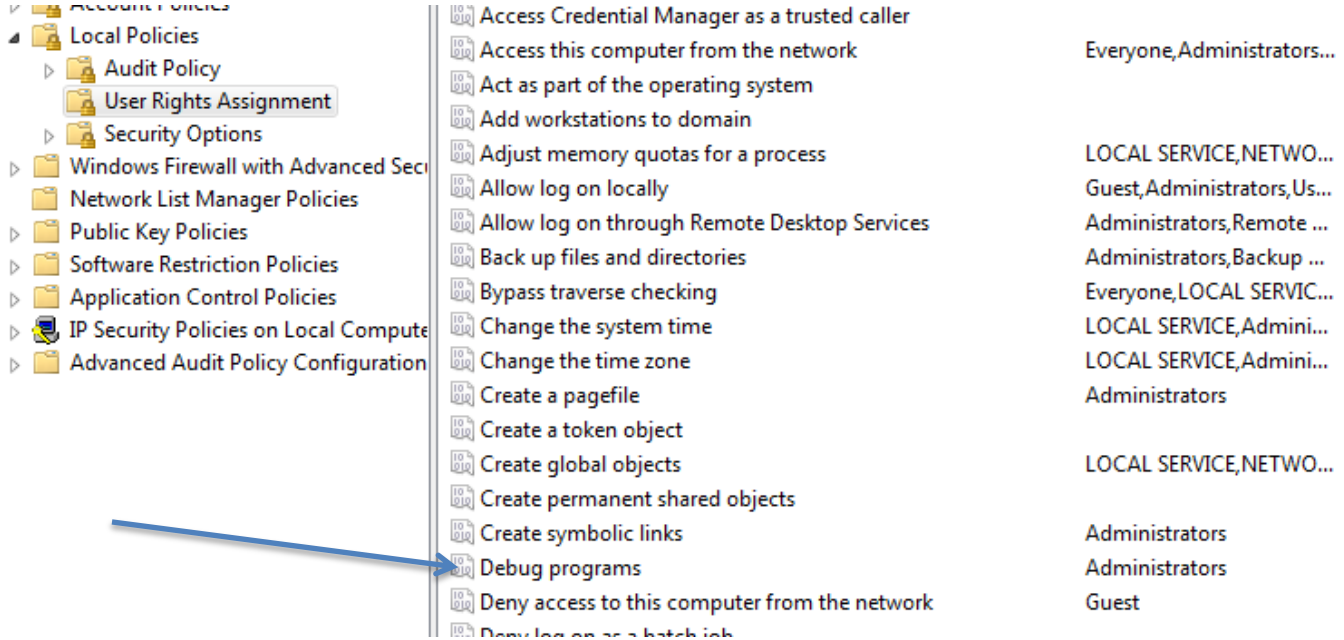
```
Who you gonna call ? > samdump
Dumping hashes from SAM hive :

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Marc:1000:AAD3B435B51404EEAAD3B435B51404EE:8846F7EAEE8FB117AD06BDD830B7586C
```

- … mais aussi en mémoire, manipulés par l'*Authentication Package msv1_0*

Types de données recherchées

Les *hashes* LM/NTLM

- Un compte Windows faisant partie du groupe d'administration local peut ajuster ses privilèges
- Ces privilèges correspondent à des droits utilisateurs :



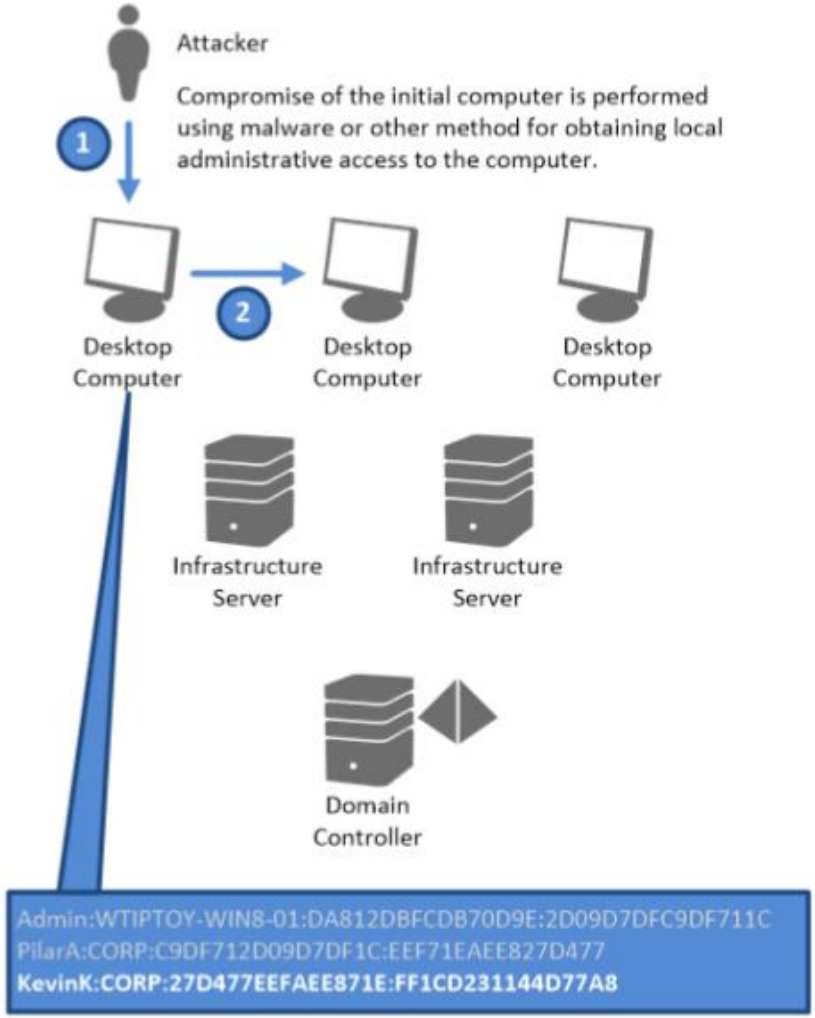
Types de données recherchées

Les *hashes* LM/NTLM

- Privilège SE_DEBUG_NAME
  - Accessible aux comptes administrateurs
  - Accès à la mémoire du processus LSASS
  - … et en extraire des données d'authentification

Types de données recherchées

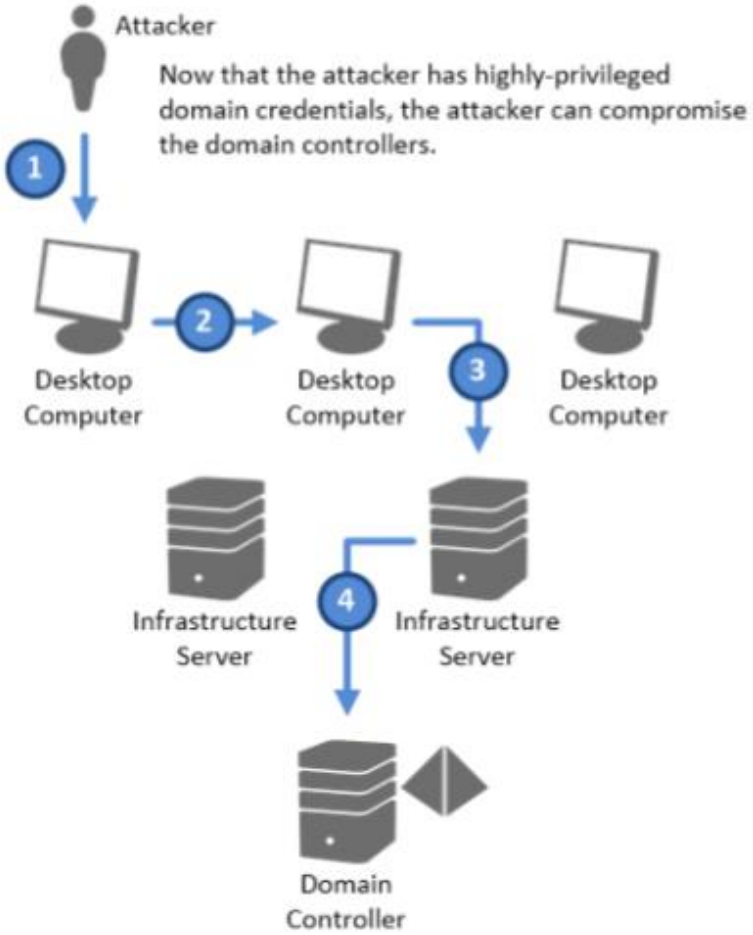
L'attaque « Pass-The-Hash »



Source : Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques (Microsoft)

Types de données recherchées

L'attaque « Pass-The-Hash »



Source : Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques (Microsoft)

Types de données recherchées

Les *hashes* MS-Cache / MS-Cache V2

- Condensat cryptographique du mot de passe, salé avec le nom d'utilisateur :
  - **MD4(MD4(Unicode(Mot de passe)) + Unicode(Lowercase(Utilisateur)))**

- Présents dans le registre Windows (ruches SYSTEM / SECURITY)

- « Cassable » par brute-force ou grâce à des *Rainbow Tables* spécifiques

Types de données recherchées

Les *Access Tokens*

- Objets générés et manipulés par Windows
- Décrivent le contexte de sécurité d'un Processus ou d'un Thread :
  - Identité de l'utilisateur (Secure Identifier, Session ID, …)
  - Privilèges activés et disponibles
  - Type de jeton
  - Etc.
- Il en existe 2 grands types :
  - *Primary* : généré lors de la création d'un processus, non exploitable
  - *Impersonation* : permet de réaliser des actions dans un contexte de sécurité différent du processus courant

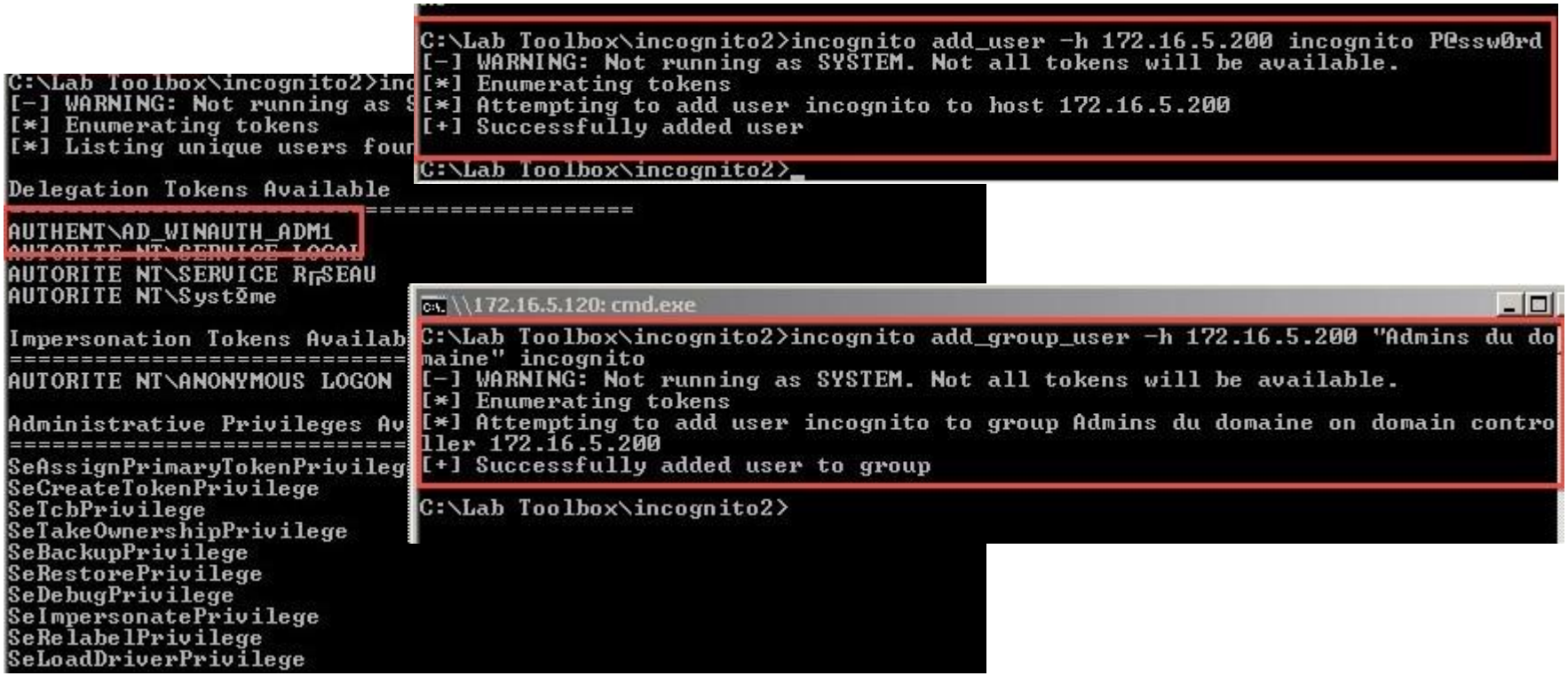
Types de données recherchées

Les *Access Tokens* : les *Impersonation Tokens*

- Il en existe 4 sous-types :
  - *Anonymous* : non utilisé
  - *Identify* : identification de l'utilisateur, ne permet pas d'effectuer des actions dans son contexte
  - *Impersonate* : permet d'effectuer des actions dans le contexte de l'utilisateur **sur le système local**
  - *Delegation* : permet d'effectuer des actions dans le contexte de l'utilisateur **sur le système local ou sur un système distant**

Types de données recherchées

Les *Access Tokens* : les *Delegation Tokens*



Types de données recherchées

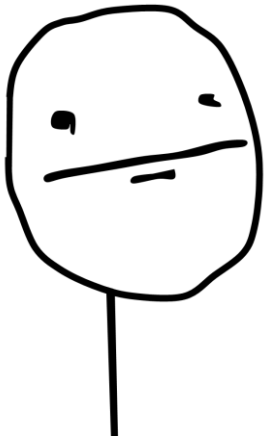
Les mots de passe en clair

- Présents en mémoire, manipulés par les *Authentication Packages* :
  - *Wdigest*
  - *Kerberos*
  - *TsPkg*
  - *Etc.*
- Un formidable raccourci pour les (tests d')intrusions
- Peut-être plus pour longtemps…

Mais des outils pas toujours fiables

Avec des problèmes de …

- Stabilité



- Compatibilité inter-systèmes (XP, 7, 2003, 2008, 2012, …)
- Compatibilité 64 bits

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

Inventaire des méthodes d'administration

en environnement Windows / Active Directory

- Authentification locale (*Local Logon*)
- Commande *RunAs*
- Bureau à distance (Terminal Services)
- Ligne de commande WMI (WMIC)
- Psexec de la suite *Sysinternals*
- *Telnet*
- Montage de partages réseau via *NET USE*
- *Microsoft Management Console* (MMC Snap-Ins)
- *Regedit* à distance
- Tâches planifiées
- Authentification AD sur Microsoft IIS

Inventaire des méthodes d'administration

en environnement Windows / Active Directory

- Short-list couvrant la plupart des méthodes d'administration fournies ou embarquées par le système de Microsoft
- Générant des évènements « Ouverture de session » de Type 2 (*Interactive*) ou 3 (*Network*)

Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

Source : Microsoft

Inventaire des méthodes d'administration

Les exclusions

- Ruches locales
  - SAM : pas de garantie de pouvoir réutiliser les identifiants
  - NTDS.DIT : post-exploitation
- Credential Manager
  - Stockage persistant non sécurisé
- Solutions tierces (VNC, LogMeIn, etc.)
  - Authentification via les mécanismes de Windows : redondants et superflus
  - Authentification via des mécanismes autres : hors-contexte

Inventaire des outils

Critères de sélection

- Programme public et gratuit
- Capable d'extraire au moins un type des données recherchées
- Stable / fiable
- Non obsolète
- Open-source est un plus

Inventaire des outils

Critères de sélection

virustotal

SHA256: f5ee689060cfc737702169983c857223ca558c64dd85e1be9c21b14e10a1cb53

File name: mimikatz.exe

Detection ratio: 11 / 52

Analysis date: 2014-05-07 09:39:26 UTC (2 hours, 40 minutes ago)

SHA256: c91eb1bb34ca94e1773864d281ba268369ab2ef8bbb98106939dead93938b243

File name: mimikatz.exe

Detection ratio: 1 / 51

Analysis date: 2014-05-07 12:10:19 UTC (0 minutes ago)

Analysis | File detail | Additional information | Comments | Votes

virustotal

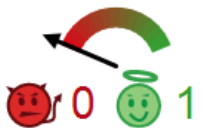
Update
20140507

SHA256: c6333c684762ed4b4129c7f9f49c88c33384b66dfb1f100e459ec6f18526dff7

File name: wce.exe

Detection ratio: 40 / 52

Analysis date: 2014-05-02 07:12:25 UTC (5 days, 5 hours ago)



Inventaire des outils

Short-list

- *Gsecdump* (*TrueSec*)
- *Pwdump7* (*Tarasco Security*)
- *Fgdump* (*fizzgig @ foofus.net*)
- *Mimikatz (Benjamin Delpy)*
- *Meterpreter hashdump / cachedump* (*Rapid7*)
- *PWDumpX* (*Reed Arvin*)
- *Windows Credentials Editor* (*Hernan Ochoa* / *Amplia Security*)
- *QuarksPwDump* (*QuarksLab*)
- *Cachedump* (*Arnaud Pilon*)
- *Incognito* (*MWR Labs*)

Inventaire des outils

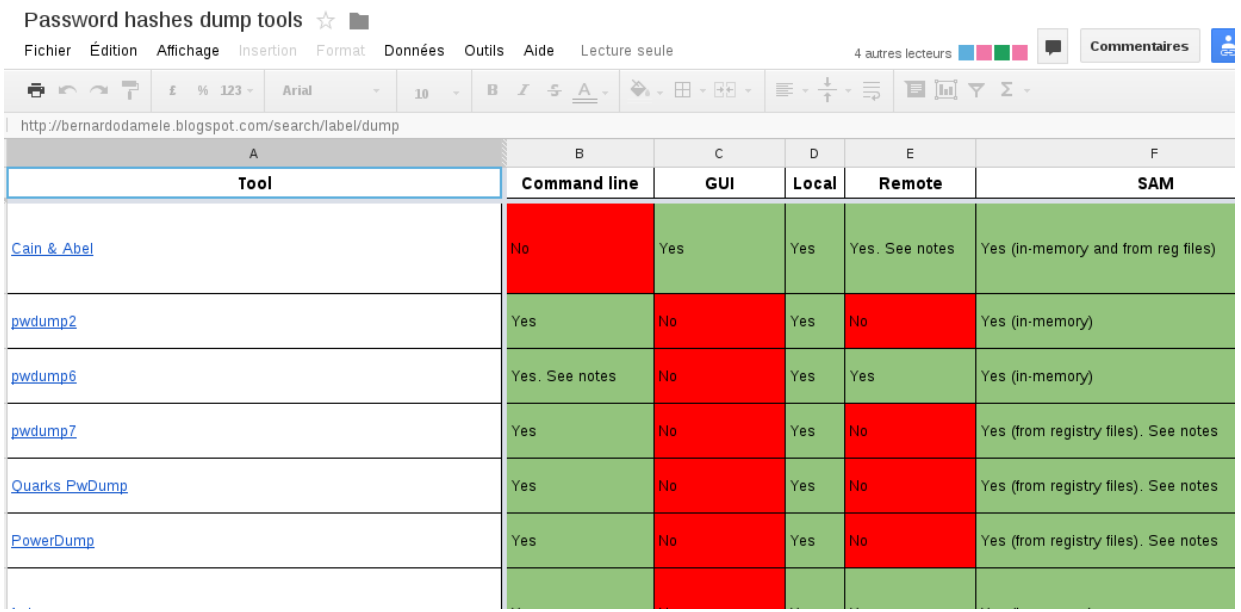
Fonctionnalités et procédure

Programme	Procédure mise en œuvre lors des tests	Données récupérables
gsecdump	gsecdump.exe -a	*Hashes* LM/NTLM de comptes locaux *Hashes* LM/NTLM en mémoire
pwdump7	pwdump7.exe	*Hashes* LM/NTLM de comptes locaux
fgdump	fgdump.exe -s -r -v -v -k -T 3 -O [32|64]	*Hashes* LM/NTLM de comptes locaux *Hashes* MS-CACHE
Mimikatz	privilege::debug sekurlsa::logonPasswords Full divers::secrets Full	*Hashes* LM/NTLM de comptes locaux *Hashes* LM/NTLM en mémoire Mots de passes en mémoire
Meterpreter	hashdump cachedump	*Hashes* LM/NTLM de comptes locaux *Hashes* MS-CACHE
PWDumpX	pwdumpx.exe -clph 127.0.0.1 + +	*Hashes* LM/NTLM de comptes locaux *Hashes* MS-CACHE
WCE	wce.exe -w wce.exe -l -v	*Hashes* LM/NTLM en mémoire Mots de passe en mémoire
QuarksPwDump	quarkspwdump.exe –dhl quarkspwdump.exe –dhdc	*Hashes* LM/NTLM de comptes locaux *Hashes* MS-CACHE
cachedump	cachedump.exe -v	*Hashes* MS-CACHE
Incognito	incognito.exe -h 127.0.0.1 list_tokens -u	Access Tokens

Inventaire des outils

Sources

- Inventaire très complet de l'outillage existant par Bernardo Damele Assumpcao Guimaraes :



Password hashes dump tools

Fichier Édition Affichage Insertion Format Données Outils Aide Lecture seule

4 autres lecteurs Commentaires

http://bernardodamele.blogspot.com/search/label/dump

Tool	Command line	GUI	Local	Remote	SAM
Cain & Abel	No	Yes	Yes	Yes. See notes	Yes (in-memory and from reg files)
pwdump2	Yes	No	Yes	No	Yes (in-memory)
pwdump6	Yes. See notes	No	Yes	Yes	Yes (in-memory)
pwdump7	Yes	No	Yes	No	Yes (from registry files). See notes
Quarks PwDump	Yes	No	Yes	No	Yes (from registry files). See notes
PowerDump	Yes	No	Yes	No	Yes (from registry files). See notes

- Ainsi qu'une série de blogposts sur le sujet : « Dumping Windows password hashes efficiently »

Environnement de test

Prérequis et méthodologie

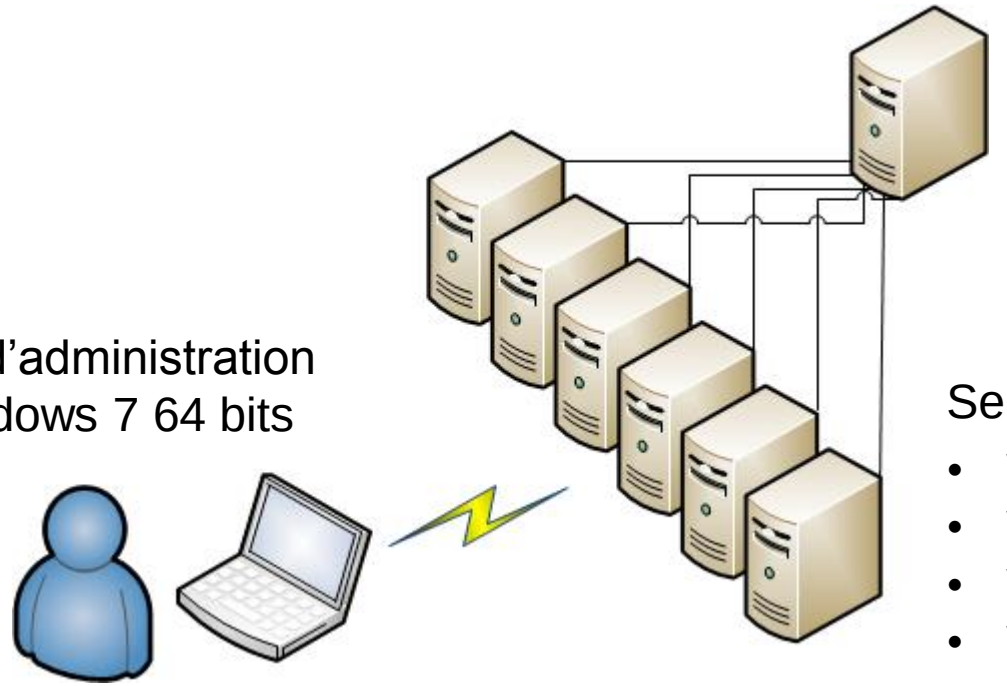
- Sur chaque machine virtuelle, on réalise un snapshot :
  - Services installés et lancés (*Telnet*, RDP, etc…)
  - Pas d'antivirus
  - Firewall désactivé
  - « Boîte à outils » déposée sur la machine
- Méthodologie *in a nutshell* :

```
:begin
Restauration du snapshot
Authentification (via la méthode testée)
Utilisation de l'outil
Récupération des résultats
Outil++
goto :begin
```

Environnement de test

Parc Active Directory virtualisé

Contrôleur de domaine
- Windows Server 2008 R2



Poste d'administration
- Windows 7 64 bits

Serveurs et Stations de travail
- Windows 2008 R2 64 bits
- Windows 2003 32 bits
- Windows XP 32 bits / 64 bits
- Windows 7 32 bits / 64 bits

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

Résultats

Les méthodes d'administration

Méthode / service	Hashes en mémoire	Access Token	Hashes MS-CACHE	Mot de passe en mémoire
Local Logon	Oui	Delegation	Oui	Oui
RunAs	Oui	Delegation	Oui	Oui
Terminal Services	Oui	Delegation	Oui	Oui
Psexec	Non / Oui	Delegation	Non	Non
Telnet	Non	Delegation	Non	Non
WMIC	Non	Impersonation	Non	Non
NET USE	Non	Impersonation	Non	Non
MMC Snap-in	Non	Impersonation	Non	Non
Remote Regedit	Non	Impersonation	Non	Non
IIS	Non	Impersonation	Non	Non
Tâches planifiées *	Oui	Delegation	Non	Oui

* La tâche a été lancée au moins une fois

Conclusions

Les méthodes d'administration

- Toutes les formes de sessions interactives laissent des traces exploitables
- Préférer *RunAs* + *Psexec* plutôt que *Psexec -u*
- Back to scripting ?

- Pas forcément !
  - Fermer ces sessions interactives correctement (*Log Off*) et les *hashes* et mots de passe disparaissent de la mémoire de LSASS
  - De nombreuses tâches d'administration peuvent être réalisées à distance via la *Microsoft Management Console*

Conclusions

Les outils

- Mimikatz :
  - Mots de passe et *hashes* NT/NTLM en mémoire
  - Pas (plus) d'injection dans LSASS
  - Compatible avec toutes les versions Windows supportées par Microsoft (32 / 64 bits)
  - Mention spéciale pour toute les fonctionnalités supplémentaires (récupération de clefs privées, du contenu du *Credential Manager,* Kerberos etc.) ☺
  - Open-source

```
C:\>mimikatz
mimikatz 1.0 x64 (RC)   /* Traitement du Kiwi (Jul  4 2013 01:26:01) */
// http://blog.gentilkiwi.com/mimikatz

mimikatz # sekurlsa::help
Module : 'sekurlsa' identifié, mais commande 'help' introuvable

Description du module : Dump des sessions courantes par providers LSASS
         msv     - énumère les sessions courantes du provider MSV1_0
     wdigest     - énumère les sessions courantes du provider WDigest
    kerberos     - énumère les sessions courantes du provider Kerberos
       tspkg     - énumère les sessions courantes du provider TsPkg
     livessp     - énumère les sessions courantes du provider LiveSSP
         ssp     - énumère les sessions courantes du provider SSP (msv1_0)
logonPasswords   - énumère les sessions courantes des providers disponibles
searchPasswords - rechere directement dans les segments mémoire de LSASS des mots de passes
```

Conclusions

Les outils

- Windows Credentials Editor :
  - Mots de passe en mémoire (*Wdigest* seulement)
  - Réalise l'attaque Pass-The-Hash, Pass-The-Ticket
  - Compatible 64 bits

```
C:\>wce -h
WCE v1.41beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.
Options:
        -l              List logon sessions and NTLM credentials (default).
        -s              Changes NTLM credentials of current logon session.
                        Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
        -r              Lists logon sessions and NTLM credentials indefinitely.
                        Refreshes every 5 seconds if new sessions are found.
                        Optional: -r<refresh interval>.
        -c              Run <cmd> in a new session with the specified NTLM credentials.
                        Parameters: <cmd>.
        -e              Lists logon sessions NTLM credentials indefinitely.
                        Refreshes every time a logon event occurs.
        -o              saves all output to a file.
                        Parameters: <filename>.
        -i              Specify LUID instead of use current logon session.
                        Parameters: <luid>.
        -d              Delete NTLM credentials from logon session.
                        Parameters: <luid>.
        -a              Use Addresses.
                        Parameters: <addresses>
        -f              Force 'safe mode'.
        -g              Generate LM & NT Hash.
                        Parameters: <password>.
        -K              Dump Kerberos tickets to file (unix & 'windows wce' format)
        -k              Read Kerberos tickets from file and insert into Windows cache
        -w              Dump cleartext passwords stored by the digest authentication package
        -v              verbose output.
```

Conclusions

Les outils

- QuarksPwDump :
  - *Hashes* LM/NTLM et MS-Cache locaux (SAM et NTDS.DIT)
  - Stable et compatible 64 bits
  - Pas d'injection dans LSASS
  - Open-source

Conclusions

Les outils

- L'outil que vous avez développez vous-même :
  - Inconnu des antivirus
  - Vous savez ce qui se passe sous le capot
  - Vous pouvez corriger les bugs vous-même (ex: support tardif des mots de passe accentués dans WCE)
  - Vous pouvez implémenter plusieurs méthodes d'exploitation à utiliser en fonction du contexte et des privilèges disponibles

```
C:\test>ProtonPack_amd64.exe -h
Usage : ProtonPack.exe
        [ -h | --help ] :       print this message
        [ -b | --blind ] :      blind mode
        [ -o | --outfile ] :    specify output file
        [ -v | --verbose ] :    set verbosity level (0, 1, 2)
        [ -a | --adrien ] :     fully automated mode :-)
        [ -s | --samdump ] :    dump local passwords from SAM
        [ -sp | --samparse ] :  offline samdump from SAM and SYSTEM hives
        [ -p | --ppth ] :       pass pass the hash
        [ -m | --memdump ] :    dump hashes from LSASS memory
        [ -u | --vnc ] :        dump VNC passwords
        [ -n | --ntdsdump ] :   dump domain hashes from NTDS.DIT
        [ -w | --shadow ] :     establish a shadow copy of a drive and retreive a file from it
        [ -np | --ntdsparse ] :         offline ntds dump from NTDS.DIT file and SYSTEM hive or raw SYSKEY
        [ -y | --system ] :     open an elevated shell (i.e. as NT AUTHORITY\SYSTEM)
        [ -g | --test ] :       I dare you to run it :)
        [ -k | --syskey ] :     dump system key (SYSKEY)
        [ -c | --creddump ] :   dump secrets from the Credential Manager
        [ -i | --iedump ] :     dump passwords stored by Internet Explorer
        [ -f | --ftpdump ] :    dump passwords from common FTP clients
```

Agenda

- Objectifs
- Contexte de l'étude
  - Le SSO Microsoft
  - Types de données recherchées
- Réalisation
  - Inventaire des méthodes d'administration et des outils d'intrusion
  - Environnement de test
- Résultats & Conclusions
  - Sur les méthodes d'administration
  - Sur les outils
- « Quick Wins »

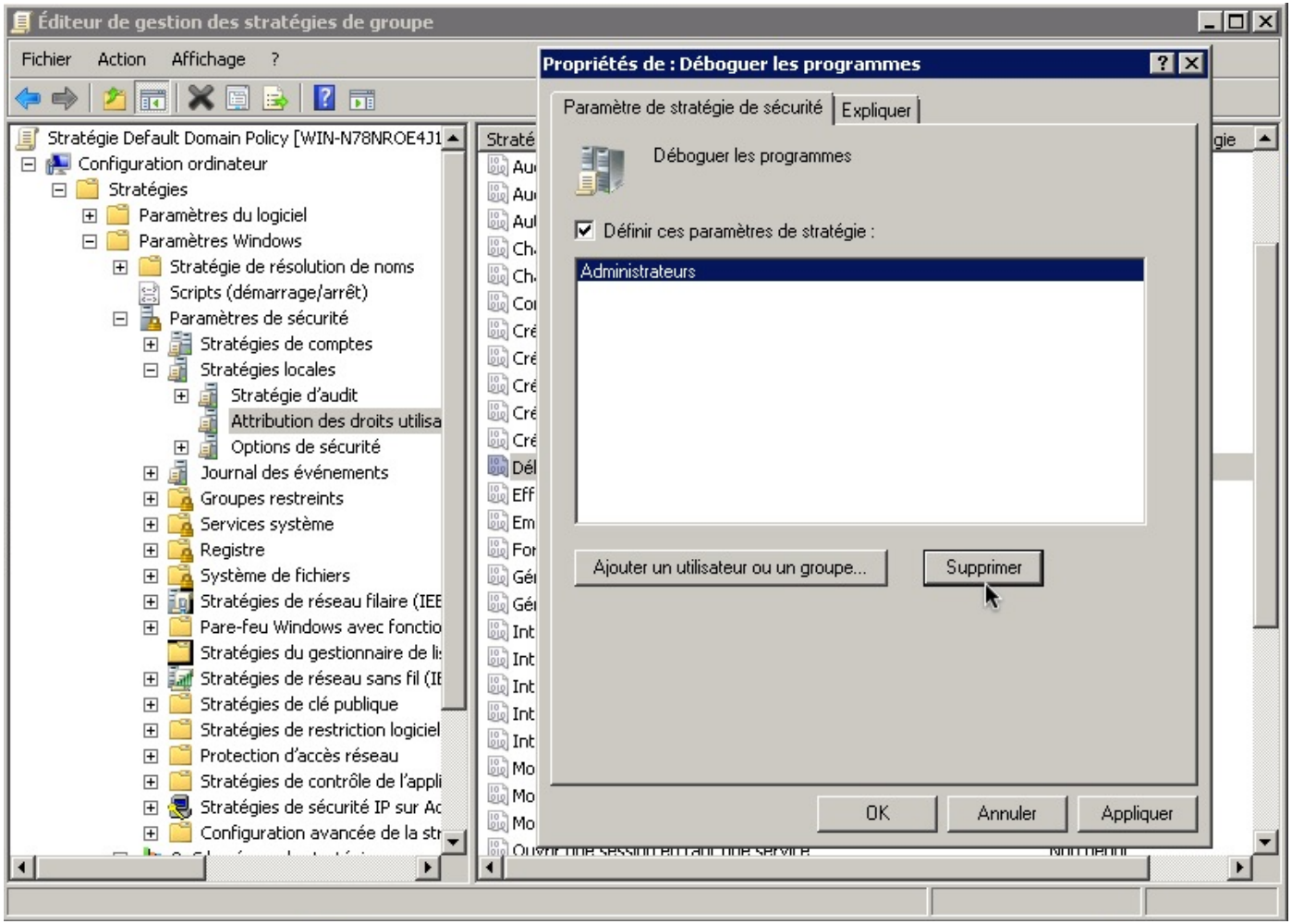
QuickWin #1

Désactiver le privilège SE_DEBUG_NAME

- La présence de fonctionnalités de débuggage n'a pas de sens sur des serveur en production, ni sur des postes de travail non dédiés au développement
- Sans ce privilège, les outils ne peuvent pas accéder à la mémoire du processus LSASS
- Les groupes pouvant activer ce privilèges peuvent être définis via une Stratégie de Groupe

QuickWin #1

Désactiver le privilège SE_DEBUG_NAME



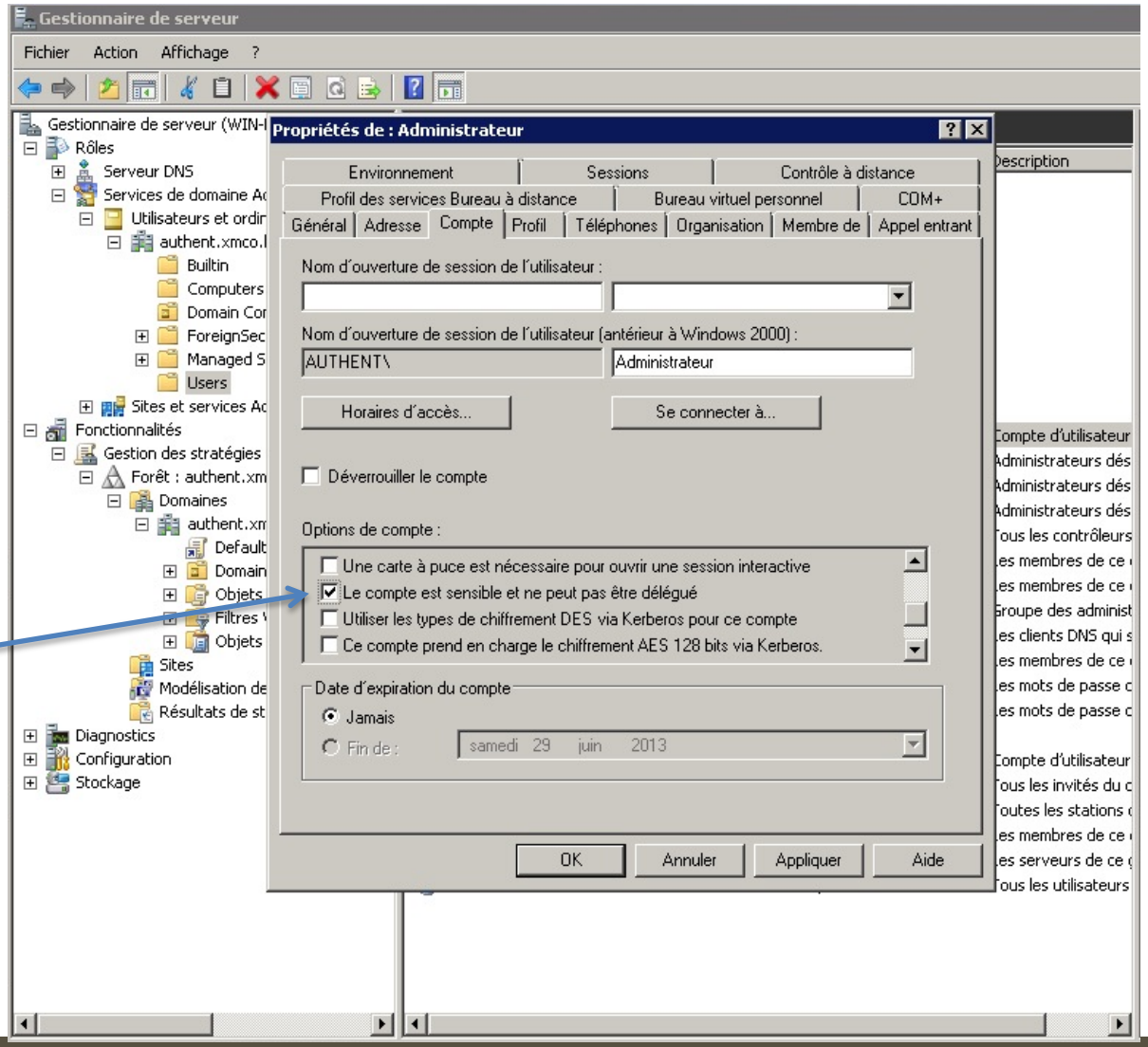
QuickWin #2

Désactiver la délégation pour les comptes sensibles

- Recommandé par Microsoft et par le *SANS Institute*
- Risque d'effet de bord avec certaines applications tierces si ce réglage est positionné sur tous les comptes du domaine
- Mais comme les comptes membres du groupe « Admins du domaine » ne sont utilisés que pour réaliser des tâches d'administration, aucun problème ☺
- Également applicable via des Stratégies de Groupe

QuickWin #2

Désactiver la délégation pour les comptes sensibles



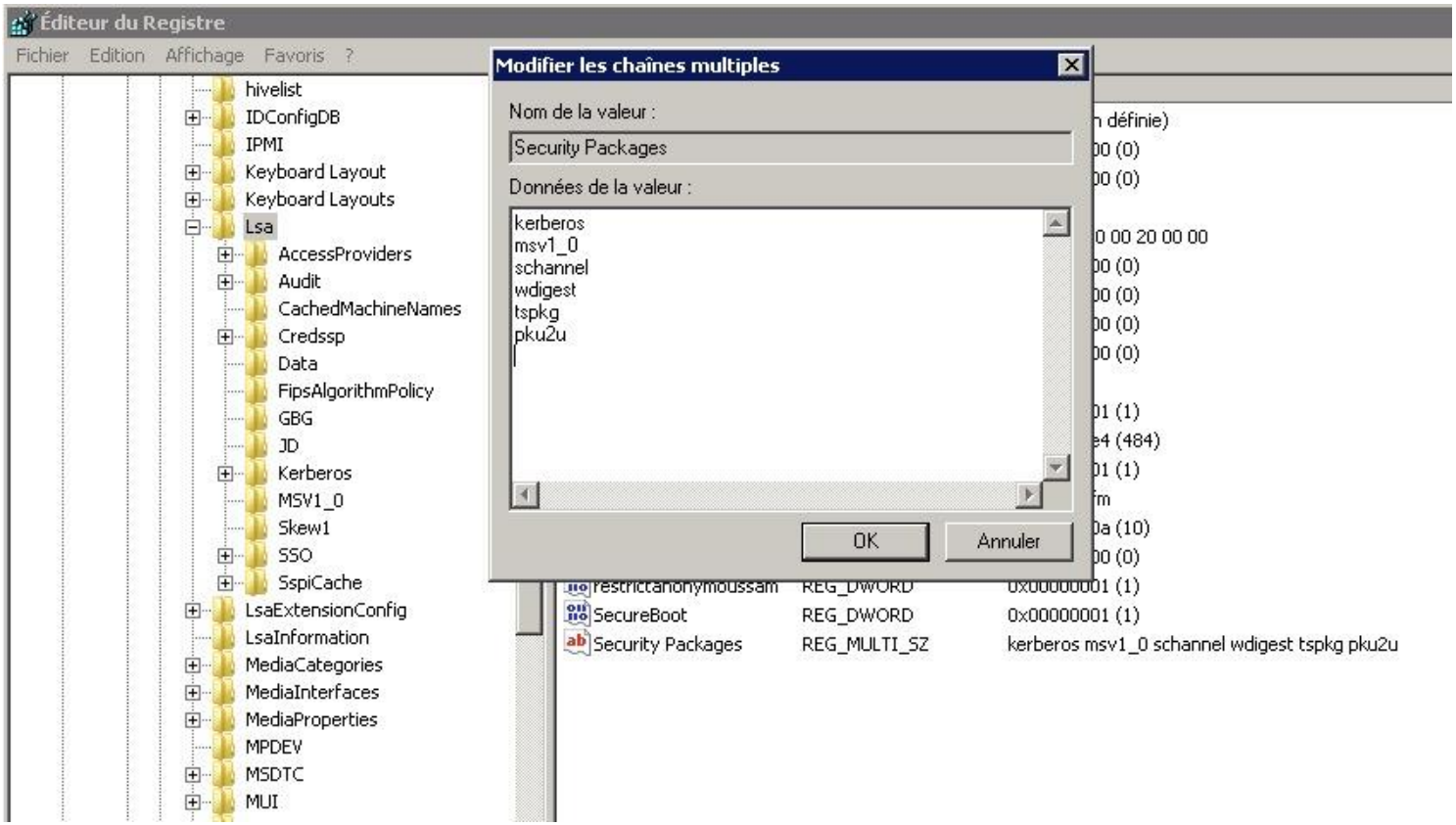
QuickWin #3

Désactiver les *Authentication Packages* non utilisés

- Désactiver *Wdigest* peut ne pas poser de problème
- Mais difficile de désactiver *Kerberos* ou *TsPkg…*
- Clef registre, donc applicable par Stratégie de Groupe

QuickWin #3

Désactiver les *Authentication Packages* non utilisés



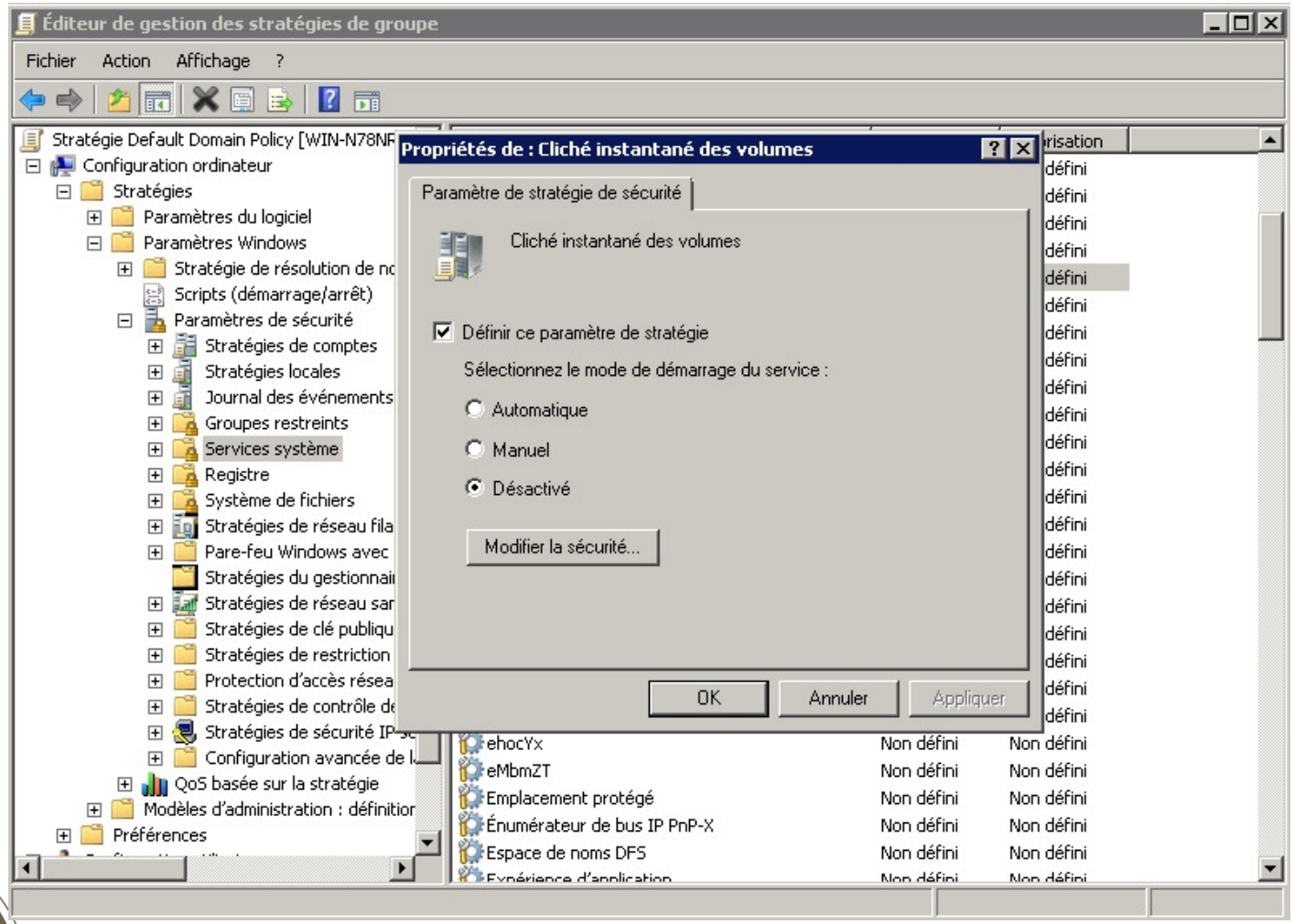
QuickWin #bonus

Désactiver la fonctionnalité *Volume Shadow Copy*

- Un service permettant d'effectuer des sauvegarde à chaud
  - Ouvre un accès « Shadow » sur un disque
  - …et permet la copie de fichiers verrouillés par le système
- Joker de l'attaquant / auditeur
  - Récupération des fichiers SAM, SYSTEM, NTDS.DIT, etc.
  - Sans actions « agressives » réalisées sur la machine
  - Sans risque de détection par les Antivirus
- Egalement applicable via une Stratégie de Groupe

QuickWin #bonus

Désactiver la fonctionnalité *Volume Shadow Copy*



Quoi de neuf ?

En 2014

- Ces résultats datent de presque 1 an, mais peu de changements constatés :
  - Mimikatz v2
  - Des améliorations sur Windows 8.1 / Server 2012 R2

	'Hash'		tspkg		wdigest	kerberos	livessp	ssp
	LM	*NTLM*	*off*	*on*				
	Windows 8.0							
Microsoft Account								
Local Account								
Domain Account								
	Windows 8.1 preview							
Microsoft Account				1			2	
Local Account				1				
Domain Account				1				

Password data in memory
No password data in memory

1. tspkg is off by default (but needed for remoteapps/ts)
2. little bug, not encrypted in memory : **real** cleartext

Source : Benjamin Delpy @gentilkiwi

Fin de la présentation

Questions ?

marc.lebrun@xmco.fr

www.xmco.fr

Twitter : @CERT-XMCO

Références

- http://digital-forensics.sans.org/blog/2012/03/21/protecting-privileged-domain-accounts-access-tokens
- https://files.sans.org/summit/forensics11/PDFs/Protecting%20Privileged%20Domain%20Accounts%20during%20Live%20Response.pdf
- http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf
- http://www.ampliasecurity.com/research/wcefaq.html#preventcleartextpwddump
- http://blog.gentilkiwi.com
- http://technet.microsoft.com/en-us/library/cc787567%28v=ws.10%29.aspx
- http://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf
- http://bernardodamele.blogspot.fr/
- https://docs.google.com/spreadsheet/ccc?key=0Ak-eXPencMnydGhwR1VvamhlNEljVHlJdVkxZ2RIaWc