JSSI 2014

Est-il possible de sécuriser un domaine Windows ?

Analyse et retours sur expérience

Florent DAQUET
Ary KOKOS
Arnaud SOULLIE

solucom
management & IT consulting

Agenda

1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
3. La réalité du terrain : état des lieux et perspectives

Du besoin de sécuriser les domaines Windows

La sécurité du domaine Windows est primordiale

En cas de compromission, ce ne sont pas seulement les postes de travail et les serveurs Windows qui sont impactés

⇩

Par rebond sur les postes des administrateurs *(dans 90% des cas sous Windows)* d'autres équipements sont concernés

- Les systèmes Un*x
- Les équipements réseau
- Les systèmes crypto (ex. PKI)
- Le MDM et donc la flotte mobile
- Le système de téléphonie
- Voir des systèmes SCADA

… en particulier lorsque l'on constate que le taux de réussite d'un pentest interne est proche des 90% en une semaine

Cible de la présentation

Présenter certaines techniques de sécurisation de domaine Windows

Sous l'angle de vue de pentesters

Évaluer l'intérêt de certaines solutions souvent présentées comme pouvant résoudre le problème

En particulier l'usage de cartes à puce et de trusts inter-domaines

REX #Fail

Avec REX terrain :)

REX #Fails

REX #Fail n°1

Domaine intégralement reconstruit suite à une attaque ciblée, avec forêt dédiée pour l'administration (trust unidirectionnel), tous les postes d'administrateurs sont changés

Seulement l'équipe forensics utilise un compte administrateur du domaine pour se connecter sur les systèmes suspectés d'être compromis…

REX #Fail n°2

Au moment de la reconstruction d'un domaine, l'équipe sécurité cherche à réduire la liste des près de 400 comptes administrateurs de domaine

Après avoir réduit d'une centaine à une quinzaine les administrateurs, elle se rend compte que 300 comptes sont utilisés par des applications métier critiques

Pour certaines applications, il sera nécessaire d'identifier tous les scripts et partie du code source ou le mot de passe a été codé en dur, et pour d'autres l'éditeur a déposé le bilan et ces application ne sont plus modifiables

REX #Fail n°3

Mot de passe administrateur du domaine hardcodé dans le script de masterisation de poste (disponible via PXEBoot)

Rappels sur quelques techniques d'attaque de domaines

Lucky auditor

- **Tâche planifiées / scripts / script du système de masterisation par PXE**
- **Compte administrateur local identique à celui de domaine**
- **Group Policy Preference**

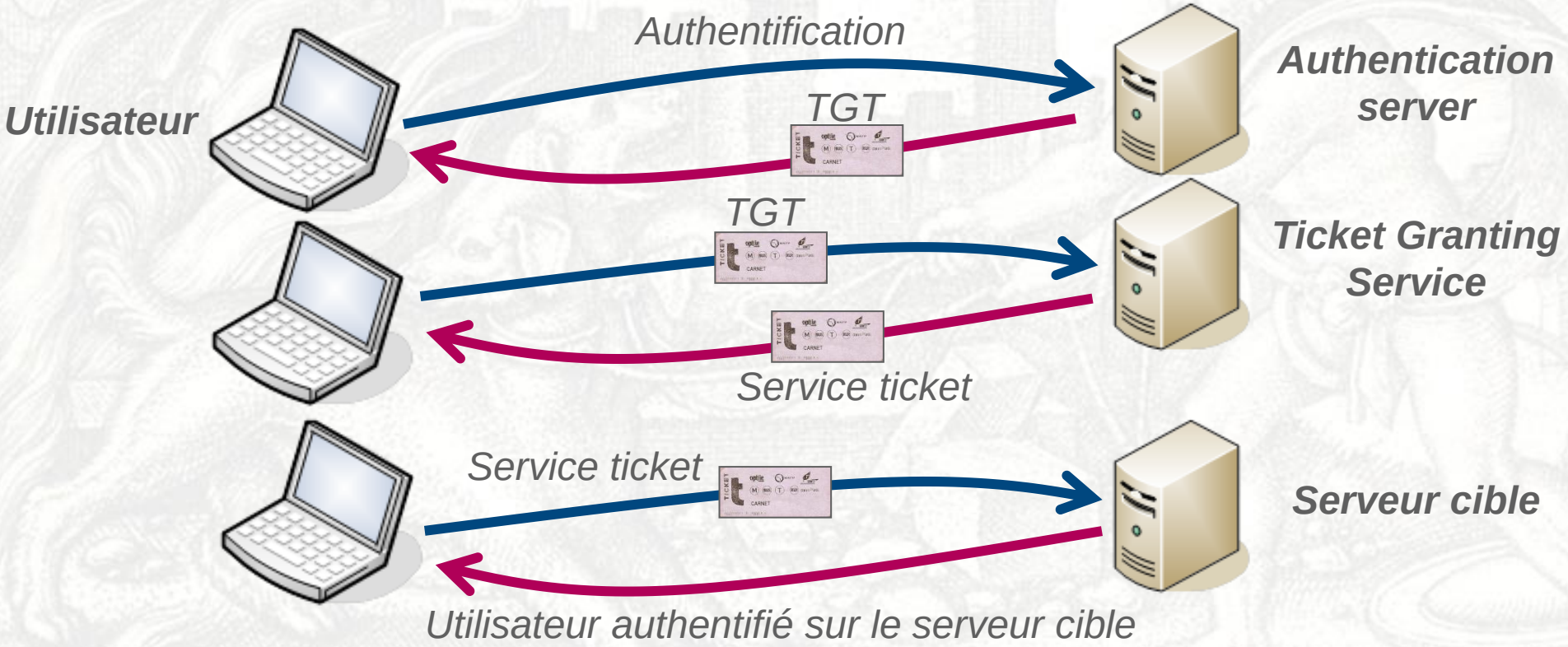
Balayage de systèmes

- **Compromission d'un système** *(local, JBoss, Tomcat, MS08-67, MS06-40, application web, interception réseau, etc.)* **et récupération des comptes présents en mémoire et en local** *(base SAM, navigateur, etc.)*
- **Utilisation de ces comptes pour rebondir sur s'autres systèmes (PTH, etc.) et récupérer d'autres mots de passe** *(le compte administrateur local est souvent le même sur l'ensemble des systèmes)*
- **Itération jusqu'à récupération d'un compte administrateur de domaine**

Une présentation détaillée des méthodes d'attaque a été présentée à la JSSI 2013 (slides sur http://www.ossir.org/jssi/jssi2013/1B.pdf)

Rappel : Kerberos

- Protocole d'authentification basé sur l'utilisation de « tickets »
- Désigné dans les 80's par le MIT
- Fonctionnement



None shall pass (the ticket) !

Pourquoi Kerberos ?

- On pouvait espérer se protéger du rejeu de hashs de mots de passe (attaque *Pass-the-hash*) via l'implémentation d'un domaine Windows full Kerberos, en désactivant totalement NTLM
- Très, très difficile à mettre en œuvre dans la réalité, nécessite un parc homogène (Win7/Server 2008 ou plus récent)

Mais ça, c'était avant

- Depuis janvier, l'outil Mimikatz permet de récupérer et de rejouer les tickets de session Kerberos (et WCE depuis 2 ans)
- Pour faire simple, si un administrateur de domaine se connecte sur un serveur, son TGT est stocké en mémoire du processus LSASS, et peut donc être volé puis réutilisé sur une autre machine
- Création de *Golden ticket (*TGT pour le service KRBTGT), valide 10 ans, permettant d'assurer la persistance dans un domaine compromis

A nouveau, un serveur compromis = compromission de tout le domaine

Agenda

1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
   - *2. 1 Back to Basics*
   - *2. 2 Les solutions "hype"*
   - *2. 3 Des mesures efficaces… si elles sont bien implémentées*
   - *2. 4 Windows 8.1 : des améliorations suffisantes ?*
3. La réalité du terrain : état des lieux et perspectives

Filtrage réseau

Filtrage : réduire la capacité de rebond d'un attaquant

Interfaces d'administration dédiées

VLAN d'administration

Filtrage réseau

Ne pas exposer les interfaces d'administration et en limiter l'accès depuis un nombre limités de postes (bastion)

Sauf cas particulier les ports SMB/RDP des postes de travail n'ont pas à être exposés

Segmenter les zones pour limiter la capacité de propagation d'un attaquant

La limite principale reste la nécessité pour les systèmes Windows d'un domaine de communiquer avec leur DC : si un attaquant parvient à récupérer sur un système un compte administrateur de domaine, il peut rebondir sur le DC puis de là, sur l'ensemble des systèmes du domaine

Back to basics

Postes dédiés d'administration

Règles de connexion

➔ Un administrateur de domaine ne devrait **jamais se connecter directement** avec son compte à privilèges sur son poste

1. En particulier, un compte d'administration du domaine ne doit pas être utilisée pour surfer sur Internet ou faire de la bureautique
2. L'usage du compte administrateur de domaine/forêt doit être restreint à l'administration du domaine/forêt

Règles sur les postes de travail

➔ Les postes sur lesquels des comptes d'administration du domaine sont utilisés **doivent être isolés**

1. Si possible disposés dans une salle dédiée
2. Sinon l'administrateur doit disposer de deux postes physiquement séparés (ou d'une isolation par VM avec un socle non Windows)
3. Ces postes doivent faire l'objet d'un durcissement avancé et ne doivent pas avoir de connectivité Internet

REX #Fail

Suite à un attaque ciblée une entreprise reconstruit son SI mais quelques semaines après le domaine Windows est de nouveau compromis

Les DC ont été réinstallés (deux forêts ont été créées, avec un trust unidirectionnel) et de nombreux serveurs ont été réinstallés… seulement les postes administrateurs initialement compromis ont simplement été remastérisés (et non changés physiquement)

Agenda

1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
   - *2. 1 Back to Basics*
   - *2. 2 Les solutions "hype"*
   - *2. 3 Des mesures efficaces… si elles sont bien implémentées*
   - *2. 4 Windows 8.1 : des améliorations suffisantes ?*
3. La réalité du terrain : état des lieux et perspectives

Cartes à puces : la crypto-parade absolue ?

Objectif : s'authentifier via des certificats stockés sur support physique afin d'empêcher la récupération de mots de passe / hash de mot de passe

La réalité

On évite les mots de passes faibles (SOCIETE123, deployment, changeme, etc.)

Lors de l'activation du smartcard logon, les mots de passe des utilisateurs restent les même et ne changent plus jamais… et restent utilisables sur certains composants (intranet, etc.)

Il est possible de récupérer en mémoire des tokens de délégation avec *incognito*, et ainsi d'usurper l'identité d'un administrateur

Hash NTLM et code PIN stockés en mémoire sur le serveur cible lors d'une connexion RDP

Domaine d'administration dédié et trust

Objectif : segmenter l'infrastructure AD pour limiter les possibilités de propagation de l'attaquant

La réalité

- ⚠ Trust bi-directionnel : pas de réel gain sécurité, l'attaquant peut rebondir vers le deuxième domaine
- ⚠ Trust unidirectionnel : les informations d'authentification du domaine 1 sont stockées en mémoire des serveurs du domaine 2 lorsqu'on s'y connecte
- ⚠ Et toujours, dans la réalité, des mots de passe partagés entre les deux domaines

Agenda

1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
   - *2. 1 Back to Basics*
   - *2. 2 Les solutions "hype"*
   - *2. 3 Des mesures efficaces… si elles sont bien implémentées*
   - *2. 4 Windows 8.1 : des améliorations suffisantes ?*
3. La réalité du terrain : état des lieux et perspectives

Des mesures efficaces… si elles sont bien implémentées

Mots de passes uniques pour les comptes administrateurs locaux

Limitation et segmentation des usages des comptes administrateurs

Utilisation de bastions d'administration

Sécurisation des frontaux Internet

Mise en place de mécanismes de détection

Mots de passes uniques pour les comptes administrateurs locaux

1. **L'une des méthodes les plus utilisée en pentest consiste à attaquer un système pour récupérer un compte administrateur local valide**
2. **Ce compte étant dans la plupart des cas le même sur tous les système** *(dans le master)***, il permet de rebondir** *(PTH ou autre)* **sur les autres machines**
3. **Puis sur chaque machine l'attaquant récupère les comptes présents** *(login/mot de passe en mémoire, dans le navigateur, etc.)*
4. **Il itère ainsi jusqu'à atteindre un système où compte à haut privilège est présent** *(par exemple un administrateur de domaine)*

Les mots de passe des comptes administrateurs locaux doivent être uniques à chaque système

Cette méthode est efficace, à condition qu'elle soit correctement implémentée…

REX #Fails

Les mots de passe des comptes administrateurs locaux doivent être uniques à chaque système

REX Audit #Fail n°1

Calculons le mot de passe administrateur local en fonction d'un algorithme

Dans le cas rencontré, le jour et le nom de l'ordinateur sont utilisés et un script change tous les soirs à minuit le mot de passe administrateur local

… en pratique

Il n'a fallu que peu de temps à l'auditeur pour trouver le script VBS et comprendre son fonctionnement

REX Audit #Fail n°2

Utilisons une tâche planifiée qui va récupérer le mot de passe du jour sur un serveur centralisé puis le redéfinir en local (implémentation « maison »)

… en pratique

Le mot de passe de l'administrateur du domaine est codé en dur dans le script local *(« pour changer le mot de passe administrateur local, il faut bien être administrateur »)*

REX #Fails (suite)

REX Audit #Fail n°3

Une autre implémentation « maison » d'un système générant chaque jour un mot de passe unique, le définit sur le système et en renvoie une version chiffrée sur un serveur centralisé

… en pratique

Après étude du binaire : le mot de passe est correctement généré (longueur suffisante, usage d'un PRNG) mais il est renvoyé via un appel à un web service (HTTP) chiffré en AES… avec une clef hardcodée dans le binaire

REX Audit #Fail n°4

On accepte de garder le même mot de passe administrateur local, mais il est changé plus plusieurs fois par jour via GPP

… en pratique

Outre les problèmes de performance / implémentation, il suffit de récupérer Groups.xml et de déchiffrer le mot de passe (Microsoft utilise une clef AES statique et publiquement disponible)

REX Audit #Fail n°5

Sans oublier les cas où le mot de passe administrateur local est correctement modifié pour être rendu unique à chaque poste…

… en pratique

…mais où les administrateurs ont oublié de faire de même avec les autres comptes administrateurs locaux
(backup, support, etc.)

En pratique…

En pratique les mots de passe administrateurs locaux n'ont pas besoin d'être changés tous les jours

Il est seulement nécessaire que ceux-ci soient uniques à chaque système

Et si possible, ce système doit…

- **Être non prévisible**
- **Assurer une traçabilité de l'utilisation de ce compte générique**
- **S'appliquer à tout compte disposant de droits d'administration locaux (ex. comptes de service)**
- **Éviter l'implémentation « maison », préférer une solution reconnue et la faire auditer**

Un tel système complique passablement le travail d'un attaquant visant à exploiter la réutilisation de comptes locaux

Limitation et segmentation des usages des comptes administrateurs

Un compte administrateur utilisé sur un système sera compromis à un moment ou un autre

Utiliser ce principe comme axiome

Un compte administrateur du domaine/forêt ne doit servir qu'à se connecter au DC pour l'administrer

Il ne doit jamais être utilisé pour se connecter sur un grand nombre de serveurs ou faire des tâches d'administration « courantes » et ne devrait être utilisé que sur des postes dédiés dans une bulle de sécurité

Limiter le nombre de comptes administrateurs du domaine/forêt (idéalement moins de 10)

Utiliser des comptes de domaine n'ayant des droits d'administration que sur un nombre limité de machines

Ainsi si un compte est compromis, un attaquant ne pourra pas s'en servir sur une autre partition

Exemple utiliser des comptes administrateurs pour l'application A disposant de droits administrateurs uniquement sur les 20 serveurs de cette application, mais ne permettant pas de se connecter par exemple sur le serveur Exchange

Bastions d'administration : la solution simplicité ?

Un administrateur de domaine ne devrait jamais se connecter directement avec son compte à haut privilège sur son poste de travail

Un compte administrateur utilisé sur un serveur sera à un moment ou un autre compromis

Les interfaces d'administration devraient être exposées le moins possible

Une bonne traçabilité des accès doit être assurée

Ces mesures sont difficiles à implémenter…

L'usage d'un bastion d'administration permet de répondre à une grande partie de ces besoins tout en facilitant l'usage pour les administrateurs

Bastions d'administration : intérêts et limites

Principe : décorréler une partie du système d'authentification, de gestion de compte et de contrôle d'accès de Windows à un système tiers plus robuste

- Authentification forte et indépendante de Windows pour la connexion au bastion
- Connexion aux systèmes par les administrateurs sans connaissance des mots de passe
- Gestion de comptes d'administration locaux uniques sur les serveurs
- Segmentation des comptes d'administration pour prévenir la réutilisation entre les systèmes
- Détection facilitée des comportements malveillants et amélioration de la traçabilité

L'usage d'un ou plusieurs bastions induit en soit un risque supplémentaire (SPOF)…

… mais il permet de réduire significativement les autres risques reposant sur des méthodes d'attaque ayant une forte probabilité d'occurrence

Si possible, utiliser **plusieurs bastions en fonction des niveaux de sensibilité**, les faire **auditer** et **renforcer leur surveillance**

Frontaux Internet

Les serveurs frontalement exposés sur Internet ne doivent pas faire partie du domaine cœur

Le risque de rebond sur le domaine par récupération de comptes est en effet très élevé

Si possible les mettre en WORKGROUP et implémenter un bastion d'administration dédié

Éviter autant que possible la délégation contrainte Kerberos sur un serveur frontal (ou pire la délégation non contrainte)

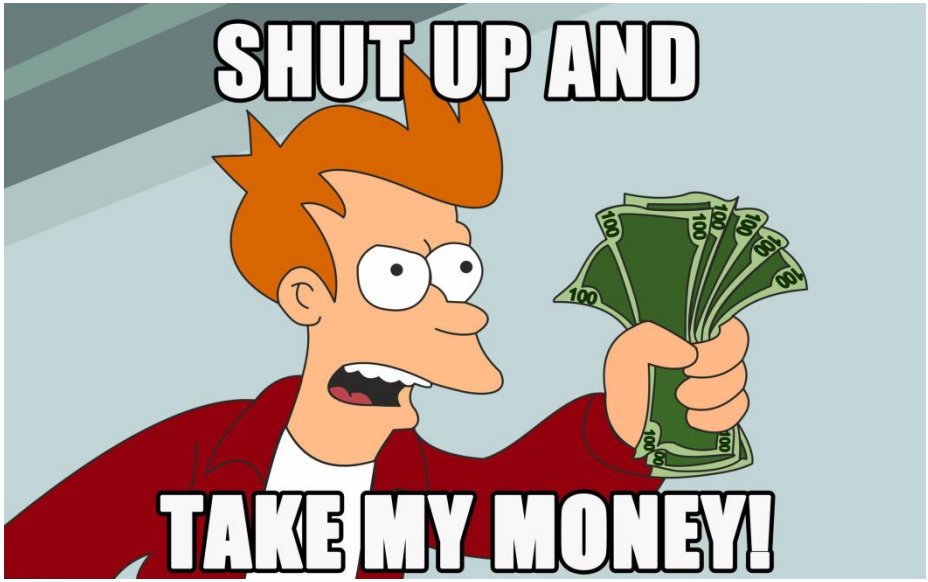
REX Audit #Fail

Le serveur frontal exposé sur Internet est placé dans un WORKGROUP, cependant un compte administrateur local partagé (lié au système de backup) est réutilisé entre les systèmes (même login et mot de passe)

Couplé à un cloisonnement réseau peu efficace, le compte a permis de rebondir entre les serveurs au sein de la DMZ puis sur le domaine interne

Détection des événements

- La détection doit se reposer sur les événement redoutés
- La meilleure détection n'est pas celle que l'on achète mais celle que l'on crée
- Des scripts VBS/PowerShell/Python sont souvent plus efficaces que des solutions commerciales non personnalisées (avec des règles adaptées au contexte)
- Nécessite une réelle compétence sécurité et une bonne connaissance du SI …



REX Forensic #Fail

Bloquer les connexions vers les serveurs C&C n'est pas facile quand on n'est pas capable de lister ses points de sortie Internet …

Agenda

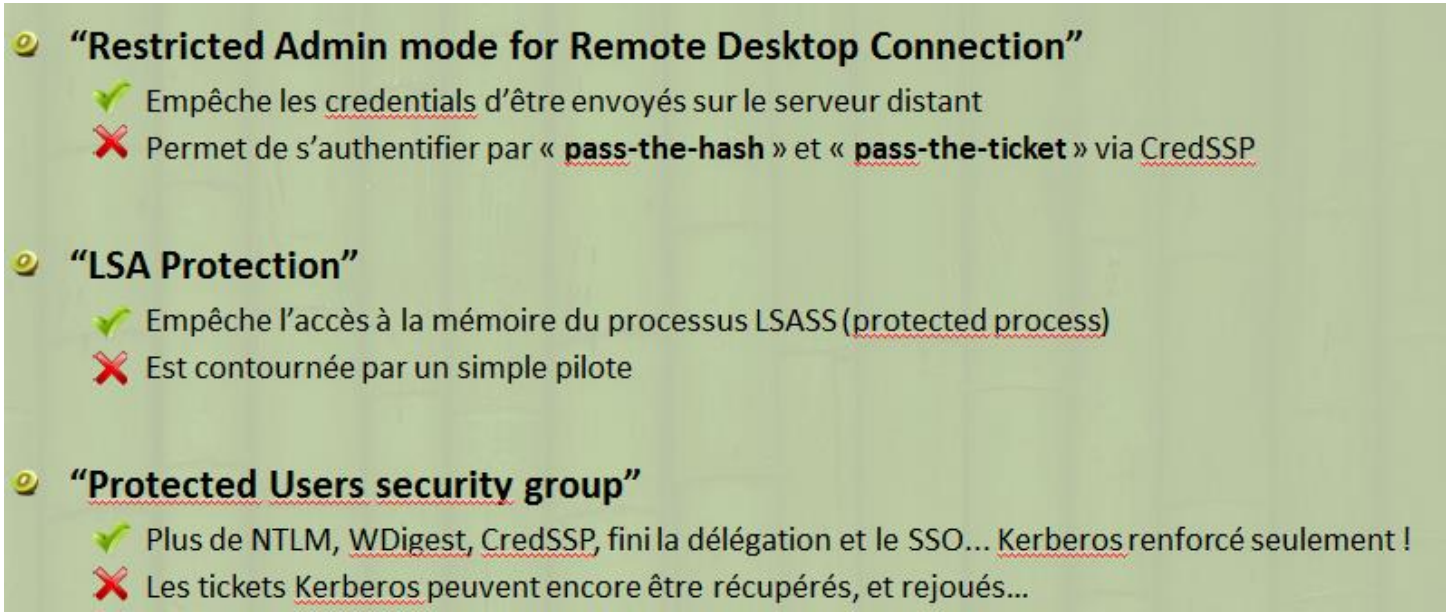
1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
   - *2. 1 Back to Basics*
   - *2. 2 Les solutions "hype"*
   - *2. 3 Des mesures efficaces… si elles sont bien implémentées*
   - *2. 4 Windows 8.1 : des améliorations suffisantes ?*
3. La réalité du terrain : état des lieux et perspectives

Windows 8.1/2012R2 : des améliorations suffisantes ?

Microsoft a fait un certain travail de réduction d'exposition des authentifiants en mémoire, mais est-ce suffisant ?

Des contres mesures non encore rencontrées sur le terrain ➔ à évaluer

Un sujet étudié par Benjamin Delpy dans son (excellente) présentation à ST HACK 2014



Extrait de la présentation, slides complets sur : http://fr.slideshare.net/gentilkiwi/mimikatz-sthack

Agenda

1. Du besoin de sécuriser les domaines Windows
2. Mesures et limites
3. La réalité du terrain : état des lieux et perspectives

REX de pentest

Est-il possible de sécuriser un domaine Windows ?

Réponse courte : NON

Pas en cherchant à s'appuyer uniquement sur les fonctionnalités de Windows

En particulier à cause de failles de conception inhérentes à la technologie utilisée, des pratiques d'administration et de la complexité (souvent historique) des systèmes

REX de pentest : Back to basics ?

Les techniques les plus efficaces ne sont pas forcément les plus complexes techniquement

Il s'agit avant tout de **bonne pratiques « old school »** d'administration, de cloisonnement et de supervision plutôt que de l'achat de produit et de mise en place d'architectures complexes

La mise en place de ces mesures à grande échelle n'est pas simple et induisent un coût important en particulier dans un environnement complexe et historique

Cependant la maturité de certaines solutions de gestion d'identité et de bastion permet d'en faciliter la mise en place
➔ la facilité d'usage étant une des principales clef de réussite !

REX terrain

Ces mesures sont rarement mises en place et l'infrastructure Windows reste une cible rarement correctement protégée

La plupart des entreprises ayant mis en place des mesures de ce type l'ont fait suite à la **prise de conscience induite par une attaque ciblée**

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contacts

Ary KOKOS
Arnaud SOULLIE
Florent DAQUET

Auditeurs

Mail : prenom (dot) nom (at) solucom.fr