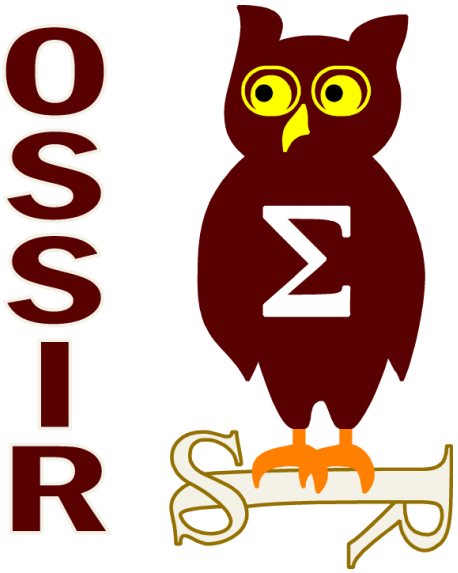
19 Mars 2013



JSSI 2013
Retour sur expérience de test d'intrusion sur domaine Windows

Ary Kokos – solucom management & IT consulting

Alain Schneider – COGICEO

Agenda

1. Introduction
2. Méthodologie d’attaque avec accès physique à un poste
3. Méthodologie d’attaque avec un accès au réseau
4. Post exploitation
5. Quelques pistes de contremesures

Le test d'intrusion : un domaine d'artisans

Des vulnérabilités connues

De techniques d'exploitations publiques

Des architectures qui se répètent

Comment articuler efficacement ces connaissances « simples » en un temps réduit, sans perturber le fonctionnement du SI ?

Ces techniques simples reposent sur des configurations par défaut et des erreurs d'administration… qui se retrouvent (mal)heureusement très souvent sur le terrain.

Les méthodologies utilisées sont en effet souvent considérées comme les « petits secrets » des entreprises du domaine et ne sont que rarement diffusées.

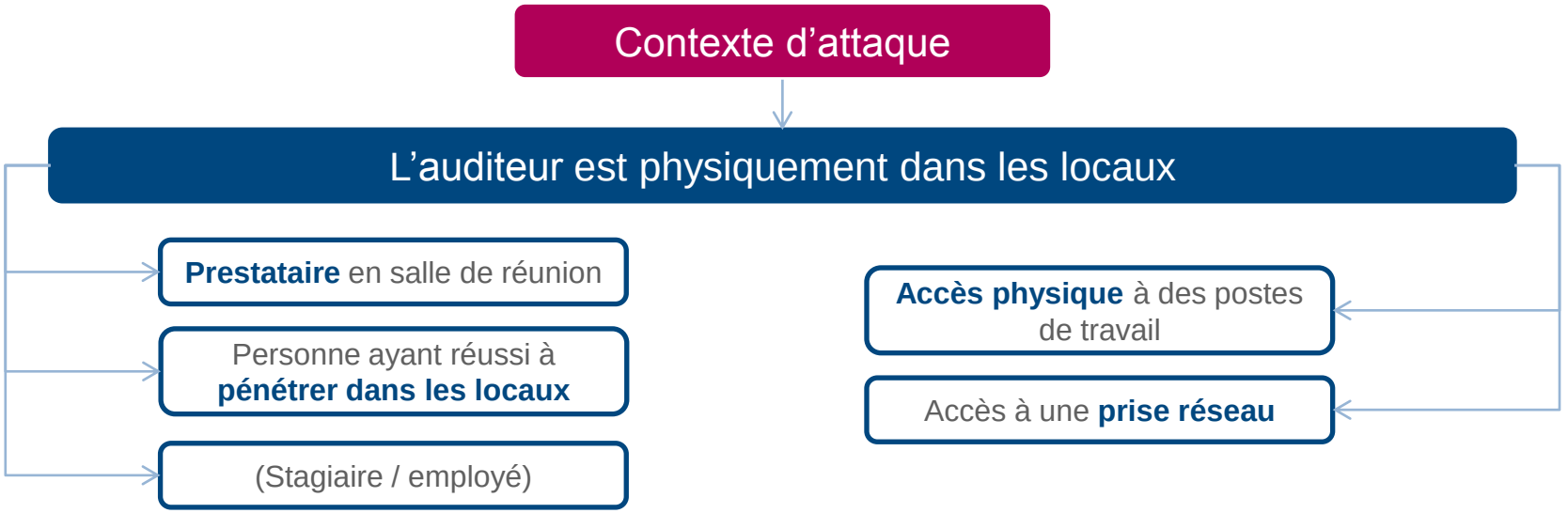
En dépit d'une « recette » de base composée d'ingrédients accessibles à tous, le test d'intrusion reste un domaine d'artisans spécialistes.

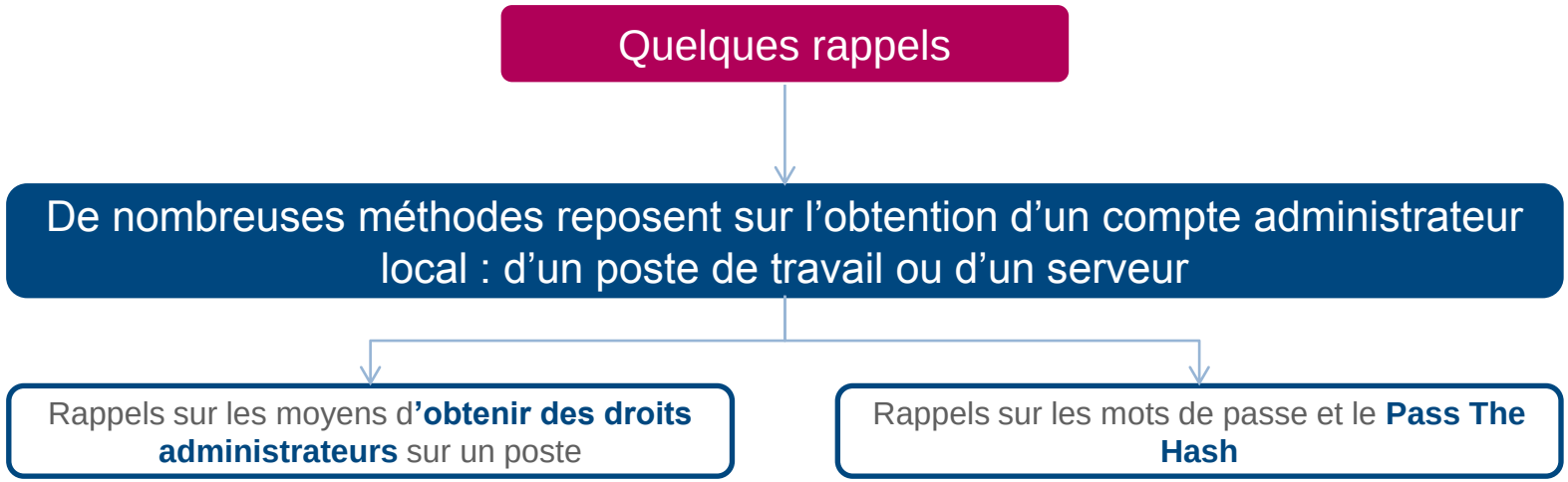
Cette intervention présente des **méthodes de tests d'intrusion sur domaine Windows** et vise à partager un retour sur expérience

Agenda

1. Introduction
2. Méthodologie d’attaque avec accès physique à un poste
3. Méthodologie d’attaque avec un accès au réseau
4. Post exploitation
5. Quelques pistes de contremesures

Contexte d'attaque et Quelques rappels





Rappels > Récupération de mots de passe avec accès physique

En théorie… (non exhaustif)

Sans chiffrement disque

- Boot sur un média alternatif puis récupération des hash ou utilman/Magnify

Restrictions sur le BIOS

- Retirer et lire le disque
- Comptes génériques /backdoors

Mot de passe disque

- Comptes génériques /backdoors
- Attaque orientée labo
- Possibilité de booter (mot de passe lié à la carte mère) : PXE boot, attaques DMA ou escalade de privilèges

Avec authentifiant utilisateur (FDE et Windows) : simulation du cas d'un utilisateur standard

Mot de passe

- Monter le disque sur un autre poste
- Certains logiciels de chiffrement ont un système de boot alternatif

TPM/Smartcard + PIN

- Élévation de privilèges
- Attaques DMA
- ➔ dump des hash ou génération d'une clef de recovery

Élévation de privilèges

- Mots de passe sur le poste/base de registre (si accessible)
- Droits d'écriture dans system32/Menu démarrer
- Partition de master / outil « maison de gestion des mots de passe admin »
- Insecurly registered executables
- Services/drivers, Taches planifiées
- Contournement de Applocker (DLL)
- Faille logicielle, etc

Attaques DMA

- Firewire/PCI/etc
- Connexion via le port série
- Cold boot, etc

Sans mot de passe

FDE

PC off et pas de mot de passe ?

- Chercher un poste allumé (pause de midi)
  - Élévation de privilèges
  - Attaques DMA

En pratique

Evilmade, cold boot, etc ?

En pratique des attaques moins élégantes mais plus efficaces

Rappels > Récupération de mots de passe avec accès physique

En pratique, il est rare de ne pas trouver au moins un poste non trivialement vulnérable en interne

Absence de restrictions ou mot de passe superviseur BIOS / Postes non chiffrés → **85%** →

En pratique il est rare de ne pas trouver en interne de postes non chiffrés. En général cela concerne les postes portables

Les **postes fixes et les postes en salle de réunion sont rarement chiffr**és

A la pause de midi les bureaux sont souvent vides, les postes allumés et de nombreuses sessions ouvertes

REX : Bitlocker Bypass

« je suis en déplacement loin, j'ai une réunion dans 2 heures, j'ai absolument besoin de mes supports sur mon PC mais il ne démarre plus qu'en mode sans échec et il demande la « clé de récupération bit-loqueurre ». Je mets quoi ? » (merci à Damien et Xavier)

Aucun poste non chiffré à proximité ? → **15%** →

- **Attaquer au niveau du réseau** (postes non patchés, poste de développeurs avec un tomcat, etc)
- **Keylogger** matériel /social engineering (peu élégant mais très efficace)
- Clef USB piégée
- Le BIOS est bloqué, mais qu'en est-il d'AMT ?
- Piéger le support (téléphone), demander à un administrateur de se connecter sur le poste à distance (pour récupérer ses authentifiants)

Si les postes sont bien protégés, il est plus rapide d'avoir recours à des méthodes moins élégantes mais rapides et efficaces (Attaque réseau, keylogger, social engineering, etc)

Rappels > Password dump & pass

Le monde merveilleux des mots de passe

Récolter des mots de passe

Dans l'OS
- **mimikatz**, taches planifiées, …

Dans les logiciels :
- navigateurs web, putty, ftp, …

Retrouver des mots de passe

Récupération des hash :
- gsecdump, creddump, …

Puis cassage des hashs :
- force brute, dictionnaires, rainbow tables (probabilistes !), …

Se passer des mots de passe

Le protocole d'authentification NTLM, copieusement utilisé dans l'univers microsoft, permet d'utiliser le hash d'un mot de passe à la place du mot de passe lui-même… (**Pass The Hash**)

La « fonctionnalité » n'est pas nouvelle et il est complexe de contrer cette technique, en particulier pour des raisons de rétrocompatibilité.

A ce sujet, voir une une conférence à la BlackHat 2012 : « Still Passing the Hash 15 Years Later? Using the Keys to the Kingdom to Access All Your Data »

Lucky auditor

Méthode « Lucky Auditor »

Tâches planifiées / Scripts (exemple : sauvegardes)

- Le **mot de passe est récupérable en clair**…
- …parfois c'est un compte du domaine qui est utilisé…
- …et c'est parfois un compte administrateur du domaine.

Compte administrateur local

- Parfois le même utilisateur avec le même mot de passe est aussi un compte administrateur du domaine

REX : #AuditorFail

Passer 3 jours à contourner les différents antivirus en place dans le réseau afin et rebondir de bastion en bastion pour finalement se rendre compte qu'un script en tâche planifiée contenait un mot de passe administrateur du domaine.

Lucky auditor

Méthode « Lucky Auditor »

Group Policy Preference

- Windows 2008 permet de créer des comptes via GPP…,
- …en spécifiant le mot de passe associé…
- Malheureusement tout utilisateur peut accéder au Groups.xml qui contient le **mot de passe chiffré** en AES… avec une **clef statique et publiquement disponible** :)

REX : #AuditorFail

Une journée entière à tenter de passer le hash de l'administrateur local sans succès (à ce jour nous ignorons encore pourquoi cela n'a pas marché) avant de tenter le brute force classique et de découvrir que le mot de passe domain admin est « Password123 ».

REX : #AuditorFail

Après 3 jours de tentatives pour forcer un mot de passe administrateur local des postes de travail, l'auditeur se rappelle de tester les GPP… heureusement le mot de passe faisait 18 caractères aléatoires…

Balayage de stations de travail (1/4) > Méthode

L'objectif est de moissonner des éléments d'authentification jusqu'à trouver ceux d'un administrateur du domaine.

Accès distant aux systèmes	Obtention d'authentifiants
$Shares	Hashs LM/NT & mots de passe en clair (Mimikatz, gsecdump, …)
RDP	Tokens (Incognito)
VNC/Applicatifs métier spécifiques	Hashs MSCache (cachedump, …)
« Down To OS » depuis l'applicatif	Mots de passe applicatifs stockés

Deux approches en temps restreint

Méthode « Texane » [Dangereuse]

Targets = nmap(quick scan, 139, 445)
For i in Targets do PTH+Mimikatz

Cibler les machines

Connexion à l'AD et recherche des domain admins

Balayage de stations de travail (2/4) > Pièges

Quelques pièges à éviter

Antivirus	Focus slide suivante
IDS	Attaque « manuelle »
Lorsque MSF Psexec ne fonctionne pas	Mimikatz (très fiable), SMBexec
Risque Social/Légal	Attention aux données personnelles
Lorsque l'administrateur utilise un bastion (ex : RDP)	Keylogger

Deux comportements sont en général détectés :
Scan & l'utilisation abusive de compte domain admin (itération sur un grand nombre de machines)

- Cibler un nombre limité de machines
- Générer un incident sur un serveur compromis pour pousser le domain admin à se connecter

REX

REX : #AuditorFail

Devoir repasser sur une centaine de machine pour effacer le password dumper maison…

Balayage de stations de travail (3/4) > Focus Antivirus

Désactivation

La méthode la plus simple est de le désactiver, en utilisant les **fonctions intégrées** :)

Abus / altération de la configuration

Identifier les répertoires avec des exceptions (**C:\dontscan**, D:\Oracle, etc)

Désactivation « forcée »
- Suppression des hooks SSDT (32bits) et kill des process
- Suppression des drivers / arrêt des services watchdogs
- Suppression des bases de signature, etc

Autres méthodes classiques

S'il est nécessaire de redémarrer le serveur ou en cas d'itération en masse :
- Packer les binaires / modifier le code source d'un outil
- Meterpreter modifié : loader détectant la sandbox de l'AV (timer, tentative de création de socket, etc) + payload encodé

Sans contourner l'AV

La prochaine version de mimikatz permettra d'analyse un dump mémoire :)

REX : #AuditorFail

Plus de 3h à outrepasser SEP en évitant de rebooter le serveur alors qu'il suffisait d'aller dans le panneau de configuration et de cliquer sur désinstaller…

Balayage de stations de travail (4/4) > Outils

La liste des outils de dump de mots de passes est disponible dans le rapport Mandiant APT1 (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)...

…dans le tableau des outils publics utilisés par les « pentesters » de l'armée chinoise

TABLE 6: Publicly available privilege escalation tools that APT1 has used

Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lslsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

Mimikatz, l'outil préféré du pentester

Pour le Pass The Hash, Mimikatz est de loin l'outil le plus fiable (éviter WCE !).
D'autre part le code source est disponible publiquement ;)

Agenda

1. Introduction
2. Méthodologie d’attaque avec accès physique à un poste
3. Méthodologie d’attaque avec un accès au réseau
4. Post exploitation
5. Quelques pistes de contremesures

Server attack !

Gold targets

- **JBOSS, tomcat**
- SQL Server
- **MS08-067** (oui, on en trouve encore)
- MS06-040 (oui…ça aussi on en trouve encore)

Silver targets

- Imprimantes (contenant des comptes admins ou utilisateurs pour le scan-to-folder)
- Systèmes de gestion de packages maison
- Partages anonymes (SMB, FTP)
- Le wiki des admins (mots de passes dans la doc)
- Systèmes de backups (share).
- Les environnements de dév/préprod /ntégration

Bronze targets

- Webapp avec code exec
- SNMP (parfois on y trouve des informations intéressantes),

UN CAS PARTICULIER

Un **boot PXE** est disponible sur le réseau afin de reformater simplement les machines et de leur appliquer le patron interne de l'entreprise. Ce patron est appliqué à toutes les machines utilisateur de l'entreprise, et le mot de passe de l'administrateur local n'est pas changé ➔ Un simple démarrage de VM suffit à obtenir le hash de ce mot de passe.

Rappels de quelques élévations de privilèges

- Serveur sweeping
- Keepass / Fichier Excel
- Smart Lock sur la machine de l'admin
- Droits sur les binaires de services

REX : #AuditorFail

Un dump des hashs est déjà présent sur le système de fichier…Auditeur précédent peu scrupuleux ou intrusion ?

Interception réseau « Old school »

Une bonne vieille interception réseau sur les utilisateurs

Récupération de mots de passe transmis en clairs, challenge NTLM, … du grand classique

REX

Old school mais assez efficace, surtout lorsque les utilisateurs s'authentifient avec des comptes du domaine sur des sites internes en HTTP avec Firefox.

Être particulièrement prudent si l'interception est effectuée depuis un serveur, il doit être en mesure de supporter la charge

REX : #AuditorFail

Cette opération n'est pas sans risque surtout lorsque le réseau utilisateur contient des serveurs critiques… et que la carte réseau de l'auditeur « grille » durant l'interception…

REX

Fonctionne sans problèmes dans 70% des cas
Contremesures techniques dans 20% des cas
Déni de service dans 10% des cas

REX : #AuditorFail

Record actuel : Déni de service sur deux étages

Statistiques

Statistiques issues de 30 tests d'intrusion sur domaine Windows durant les 18 dernier mois

96% des domaines sont compromis en moins d'une semaine (5JH)*

Environ **85% des mots de passes tombent**

100% des entreprises avaient au moins un mot de passe trivial ou ne respectant pas la complexité mise en place.

Plus de **la moitié des domaines tombent en deux jours**.

Des **systèmes obsolètes sur un tiers des réseaux.**

Morale : Et oui…la sécurité des domaines Windows est un échec ;)

* Parfois, ça ne marche pas…pour information ça fait 29/30.

Note (Solucom) : sans pouvoir communiquer sur les chiffres, nos statistiques sont sensiblement identiques :)

Agenda

1. Introduction
2. Méthodologie d’attaque avec accès physique à un poste
3. Méthodologie d’attaque avec un accès au réseau
4. Post exploitation
5. Quelques pistes de contremesures

Post Exploitation

On a un compte d'administrateur du domaine, et après ?

Les privilèges d'administration du domaine, bien que « Sésame » quasi universel, reste limité. Il ne permettent en effet pas forcément d'accéder à toutes les systèmes (ex : site web tiers, systèmes unix, réseau, etc).

Récupérer sur le DC l'ensemble des mots de passe utilisés dans l'entreprise permet d'élargir sa vision du SI client et de revendiquer une « prise de contrôle totale du domaine ».

Méthode « brutale »	Méthode « propre »	Méthode « curieuse »
Injection en mémoire dans des processus à privilèges puis dump des hashs. Des outils spécialisés existent : gsecdump, etc.	Copie des fichiers contenants les hashs, puis extraction. La copie peut être faite par le service de « Shadow Copy » ou en accédant directement au périphérique de stockage.	Créer une VM Windows, la promouvoir en tant que contrôleur de domaine, attendre la fin de la synchronisation puis extraire tranquillement les hashs de sa propre VM sans interférence d'antivirus.

Cassage des mots de passe

Dictionnaires	GPU	Rainbow Tables	Force Brute	etc…

Plus de 80% des mots de passe sont en général « cassé » à la fin d'un pentest

Post Exploitation

On a prit la main sur le domaine. Et après ?

Présenter une capture d'écran d'un contrôleur de domaine avec une accès administrateur n'est pas forcément parlant lors d'une présentation à des responsables métiers ou des tops manageurs

Cibler des données marquant les participants, en particulier si le but de l'audit est de sensibiliser aux risques encourus

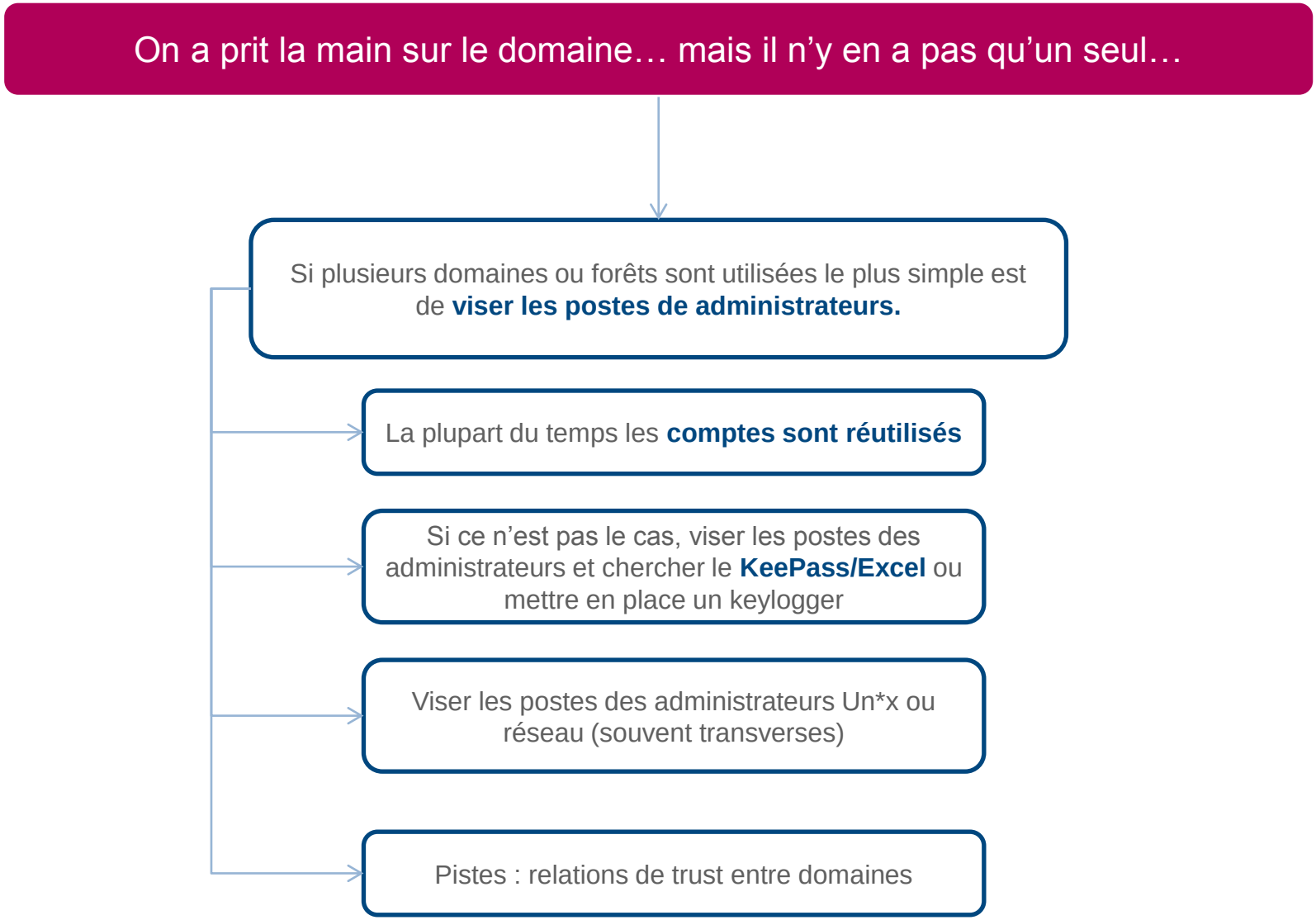
Récolte d'informations

- Identifier le serveur contenant **le home des utilisateurs** (via l'AD ou l'annuaire interne)
- Identifier le **serveur de partage** de fichiers (via poste utilisateur)
- Utiliser **l'AD pour cibler les actifs critiques**
- Wiki internes ou **SharePoint, Applications métier** / Fichiers créés par des VIP / recherche par mots clefs
- **OpenDLP** sur les postes
- **Attention au contexte légal et social dans l'entreprise**

Cibler des données « marquantes »

- **Données métier** (applicatifs métiers, partages métier)
- Le dossier **Syndicats** dans le **répertoire RH**
- Répertoire de la **direction générale**
- Serveur de **messagerie** / Serveur **BES** / Call Manager (pour récupérer les SMS (BES) ou les historiques d'appel)
- **Données personnelles** (paye, santé), serveur de scan de Fax, etc

Post Exploitation



Agenda

1. Introduction
2. Méthodologie d’attaque avec accès physique à un poste
3. Méthodologie d’attaque avec un accès au réseau
4. Post exploitation
5. Quelques pistes de contremesures

Contremesures > REX

S'il est la plupart du temps possible de prendre la main rapidement sur le domaine…

… le taux de réussite n'est pas toujours de 100%

La clef d'une prise rapide (~ 2 jours) d'un domaine repose avant tout sur l'exploitation de vulnérabilités inhérentes à Windows et de défauts d'administration (en particulier la réutilisation de mots de passe ou l'usage abusif de comptes admins du domaine)

- Compte tenu du **coût et de la difficulté de mettre en œuvre les contremesures**… et surtout de les maintenir dans le temps (éviter la réutilisation de mots de passe, interdire aux administrateurs de domaine de se connecter sur des serveurs directement avec le compte domain admin, etc est particulièrement complexe)
- des besoins de **rétrocompatibilité sous Windows** (essayez de désactiver complètement l'authentification NTLM… bon courage)

Ces vecteurs d'attaques devraient encore être exploitables durant une période de temps importante

Cependant dès lors que certaines contremesures sont appliquées, l'attaque reste réalisable, mais demande beaucoup plus de temps et d'efforts (5 jours, 10 jours voir plus)

Un attaquant motivé réussira toujours à prendre la main sur le SI
mais en appliquant certaines contremesures il est possible de lui compliquer la tâche, et d'augmenter la probabilité de détecter l'attaque et ainsi de pouvoir réagir plus rapidement

Contremesures > Limiter la propagation

Réutilisation des mots de passe

Ne pas réutiliser les mêmes mots de passe pour les comptes **administrateurs locaux** (mener l'étude pour les comptes de service). Jamais !

Utiliser des mots de passe admin locaux uniques pour chaque serveurs (par exemple via des outils de PIM)

Usage des comptes administrateurs

Interdire la **connexion** directe sur des serveurs avec des **comptes administrateurs de domaine**.

Les comptes administrateurs de domaine servent à administrer le domaine et ne doivent être utiliser pour des tâches d'administration courantes sur tous les serveurs.

C'est également valable pour les équipes de forensics (#ForensicsFail)

Filtrage réseau

Segmenter le réseau

Filtrer les ports **SMB/RDP** sur les postes de travail, même en interne

Frontaux internet

Éviter d'exposer des **serveurs du domaine frontalement sur internet** (workstation ou plusieurs domaines)

Éviter la délégation de contrainte sur des serveurs frontalement exposés sur internet (ou pire la délégation non contrainte)

Idéalement :

- L'administrateur de domaine ne doit pas ouvrir de session sur son poste de travail en domain admin, mais avec un simple utilisateur
- N'utiliser les comptes domain admin que pour se connecter sur les DC (dans les autres cas on préfèrera un compte du domain avec des droits d'administrateur sur un nombre limité de machines)
- Limiter le nombre de comptes domain admin (idéalement moins de 10) et ne les utiliser que sur des postes dédiés dans une bulle de sécurité
- Si possible utiliser plusieurs forêts avec une forêt d'administration et des trust unidirectionnels.
- Note : voir le guide de Microsoft sur le PTH
- Autre :
  - Sur des postes de travail limiter les sessions simultanées autorisées

Contremesures > Détecter, piéger et agir sur l'information

Détecter

Surveiller les accès administrateur :

- Un administrateur local qui se connecte consécutivement sur 300 postes de travail est rarement un cas d'usage normal
- Création de nouveaux comptes d'administration du domaine

Corréler les logs, y compris ceux des IPS/IDS/Antivirus

Utiliser des **HIPS** en plus des NIDS

Piéger l'attaquant

Honeypots

Agir sur l'information

Au-delà des mesures techniques et en particulier dans le cas d'une attaque ciblée, contre intelligence au niveau de l'information

REX : #AuditorFail

Piégé par un honeypot ;)

Questions ?

Remerciements :

Kevin Guerin
Florent Daquet
Damien Godard

Contact

Ary.Kokos@solucom.fr

Alain.Schneider@cogiceo.fr