Rump Session 09 : Projet IMA

Outil d'audit pour la gestion des identités et des habilitations

Yannick HAMON

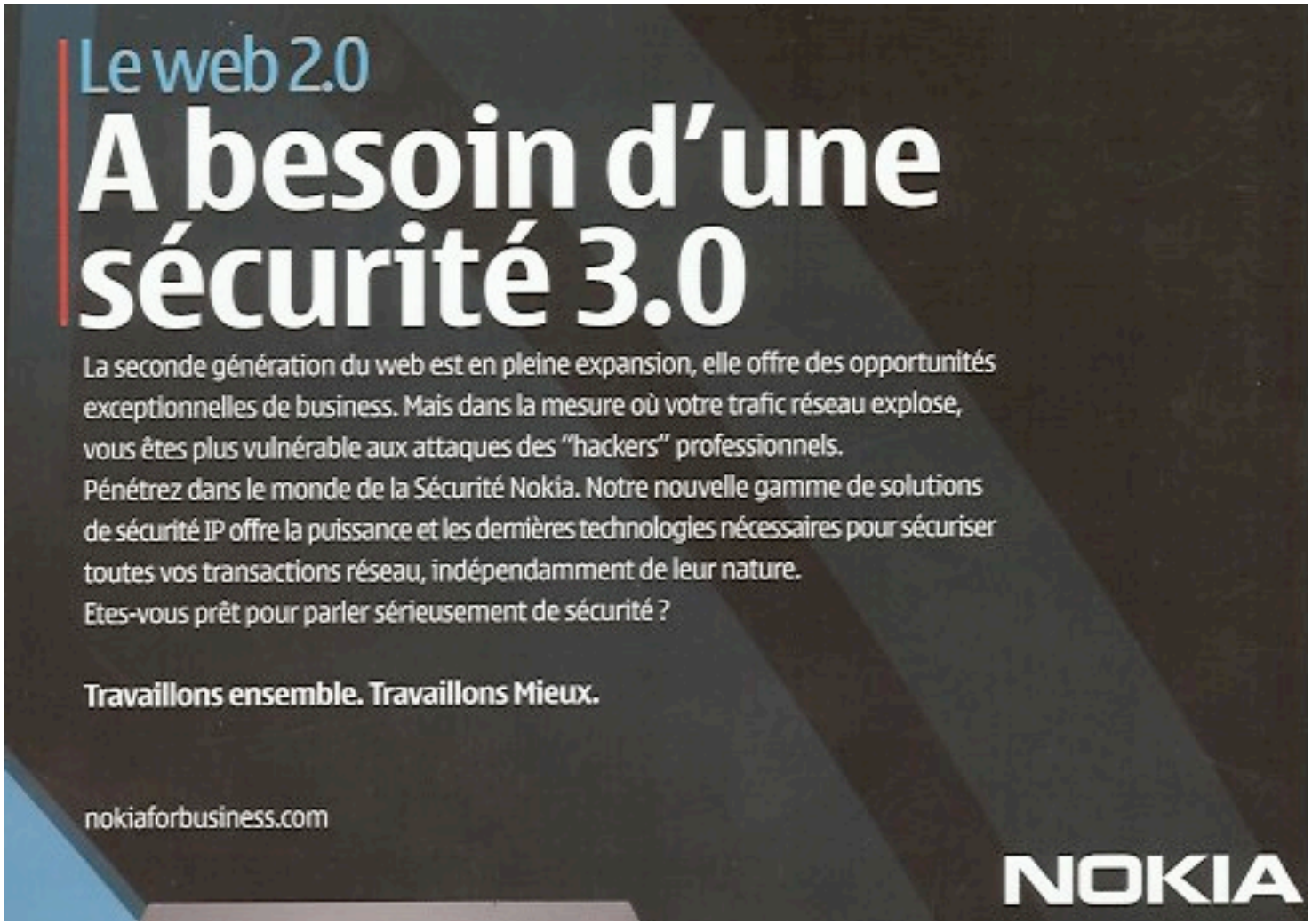
Date: 4 Juin 2009

xmco | Partners

AGENDA

- **Introduction**
- Le Projet IMA

SECURITE 3.0 ??



Extrait d'une publicité parue dans au sein de magazines informatiques

SECURITE 3.0 ??

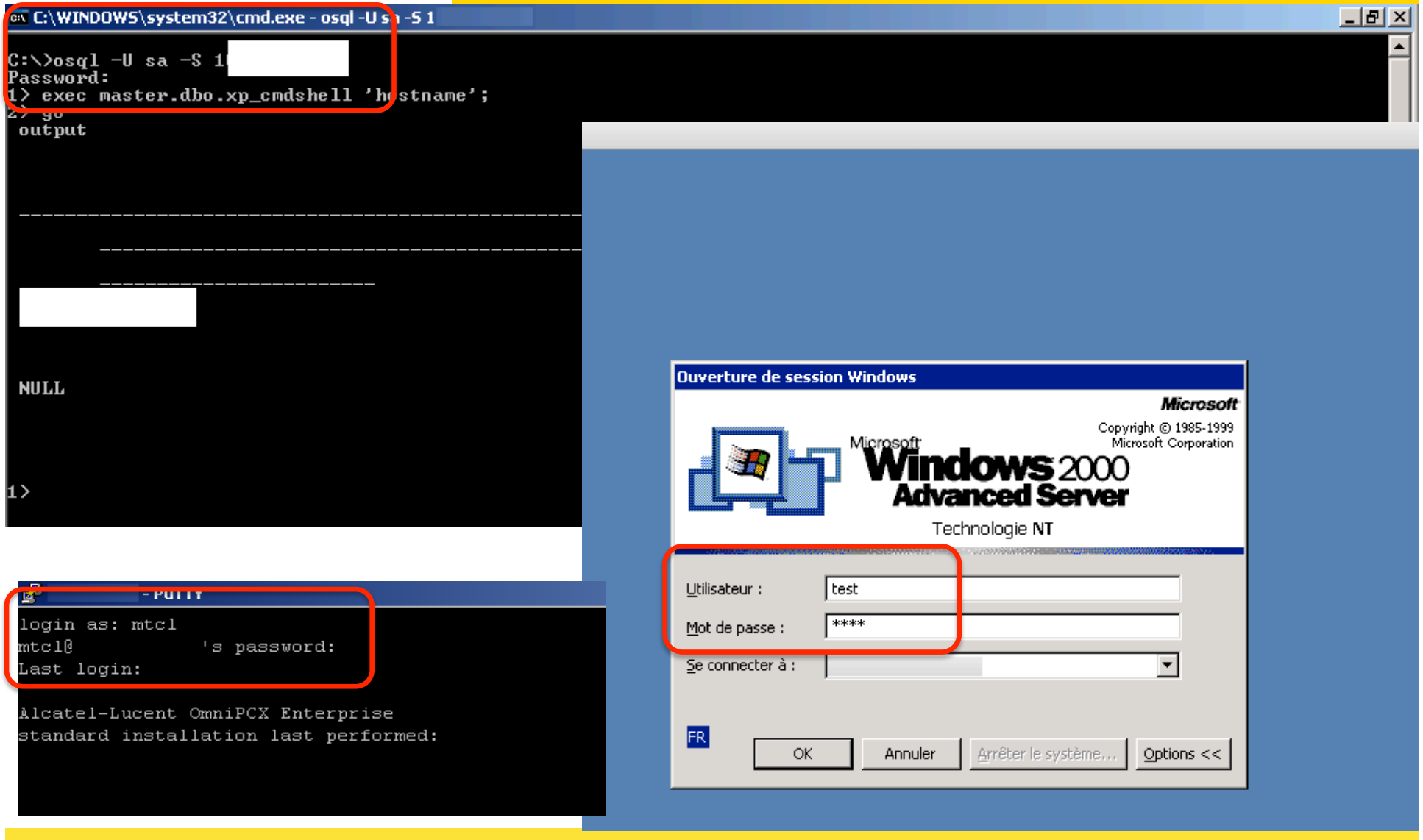
Imaginons que…

- Je mette de la **colle sur tous les ports PCI / FireWire**
- Il n'y ait plus **aucune vulnérabilité** au sein des OS / Logiciel… et le fuzzing ne trouve plus aucun bugs
- Mes équipement/logiciels de **sécurité 3.0 bloquent toutes les tentatives** de malversation
- **L'informatique de confiance est un fait réel**
- **…**

Problème PERSISTENT

- … ce n'est pas un programme parfait qui utilise l'informatique mais des hommes
- … cette **faille** est **exploitable sans aucune connaissance technique**

SECURITE 3.0…


C:\WINDOWS\system32\cmd.exe - osql -U sa -S 1
C:\>osql -U sa -S 1
Password:
1> exec master.dbo.xp_cmdshell 'hostname';
2> go
output
NULL
1>
- PuTTY
login as: mtcl
mtcl@ 's password:
Last login:
Alcatel-Lucent OmniPCX Enterprise
standard installation last performed:
Ouverture de session Windows
Microsoft
Copyright © 1985-1999
Microsoft Corporation
Microsoft Windows 2000
Advanced Server
Technologie NT
Utilisateur :
test
Mot de passe :
****
Se connecter à :
FR
OK
Annuler
Arrêter le système...
Options <<

SECURITE 3.0…

Source du Problème

- **Pas une faille** purement **technique/informatique**

- Turn-Over des entreprises (mutation interne, multiplication des prestataires)

(Utilisateurs jamais connectés ou depuis plus d'un an…)

- **Même si la politique de sécurité est renforcée,** elle n'est pas **forcément** appliquée sur tous les comptes systématiquement (VIP, départ de salariés…)

- **…**

AGENDA

- Introduction
- **Le Projet IMA**

Description

- **Faciliter l'audit interne de la gestion des utilisateurs et de leurs habilitations**
- **Outil d'audit et d'administration**… et non pas de *hacking*
- **Gratuit**, pas encore Open-Source… enfin presque (Application C# .NET)
- Obtenir une **corrélation** entre les informations suivantes
  - **Utilisateurs** (actif, dernière connexion, privilèges, âge du mot de passe…)
  - **Groupes** (membres, héritage)
  - **Solidité** des Mots de passe (NULL / Trivial / Faible / Solide)
- Automatisation de l'audit
- **Export des résultats** sous la forme d'un **classeur XLS**
- **Version BETA :** développé le soir sur le peu de temps libre donc… **soyez indulgent !!!**

Systèmes cibles

- **Microsoft Windows** (2000, XP, 2003,…)
- Modules Linux, HP-UX, IBM AIX et MS SQL **en cours de développement**.
- Prochainement : Modules Oracle, MySQL, Routeurs/Switchs Cisco et Alcatel

Téléchargement

- Version Béta v0.1 :

http://www.xmcopartners.com/ima/IMA_Beta_v0.1.zip

IMA : MODULE WINDOWS

Description

- Audit de **serveurs/postes de travails** ou de **contrôleurs de domaine**
- **Pas de magie** : utilisation d'outils d'audit / d'administration *fiable*
- **Utilisation de l'API Windows** pour se connecter et support de la session courante
- Deux types d'audit de **solidité des mots de passe** :
  - **Rapide :** Mots de passe triviaux, importation d'un fichier JOHN POT
  - **Complète :** Utilisation d'un outil externe durant un délai fixé

Limitations

- **Dump des mots de passe peut être bloqué par les antivirus**
- **Réservé aux administrateurs :** Privilèges *Administrateur local* du poste cible/audité

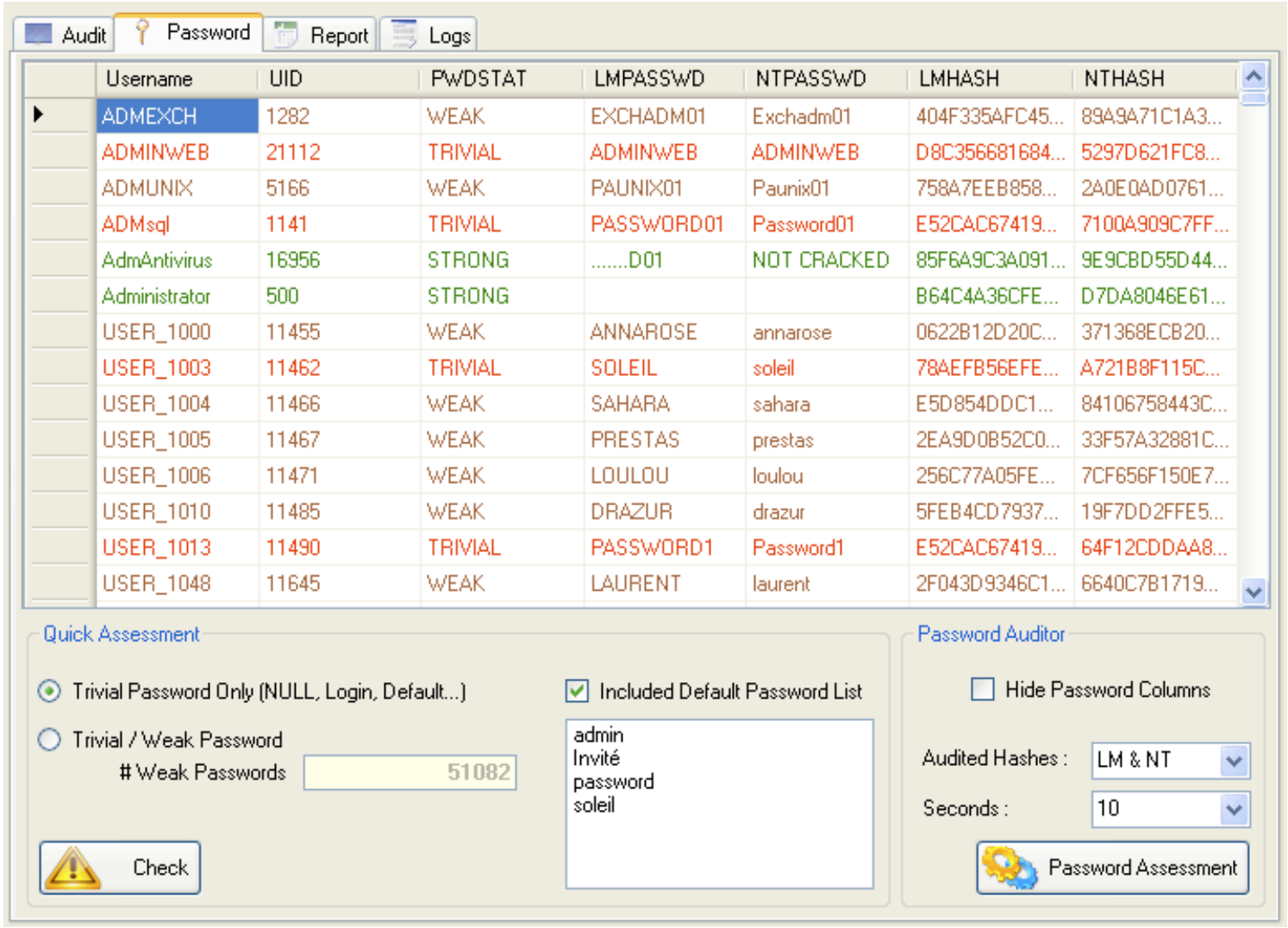
IMA : MODULE WINDOWS

Démonstration

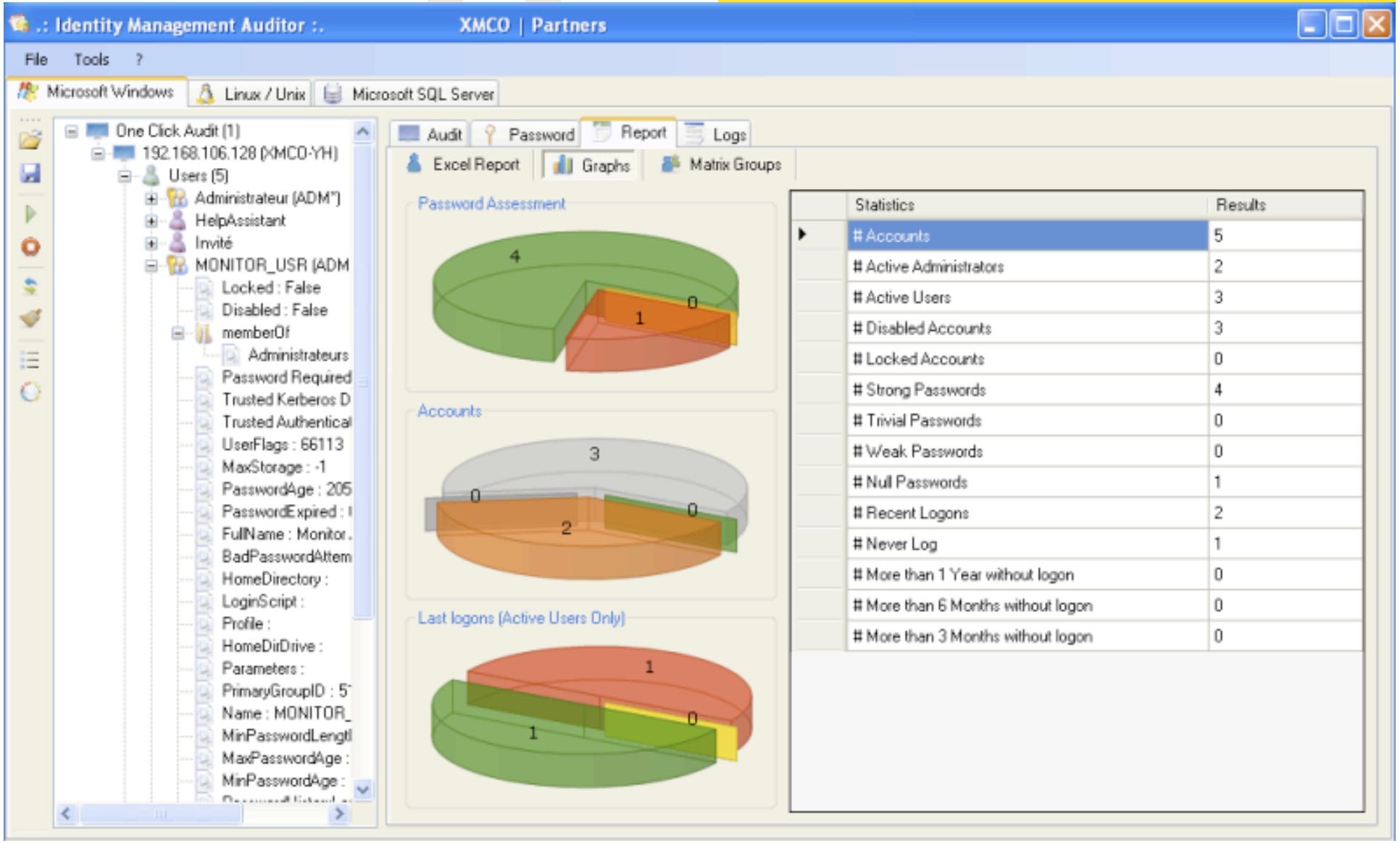
Vidéo disponible (compatible QuickTime/VLC):

http://www.xmcopartners.com/ima/XMCO_IMA_ModuleWindows.mov

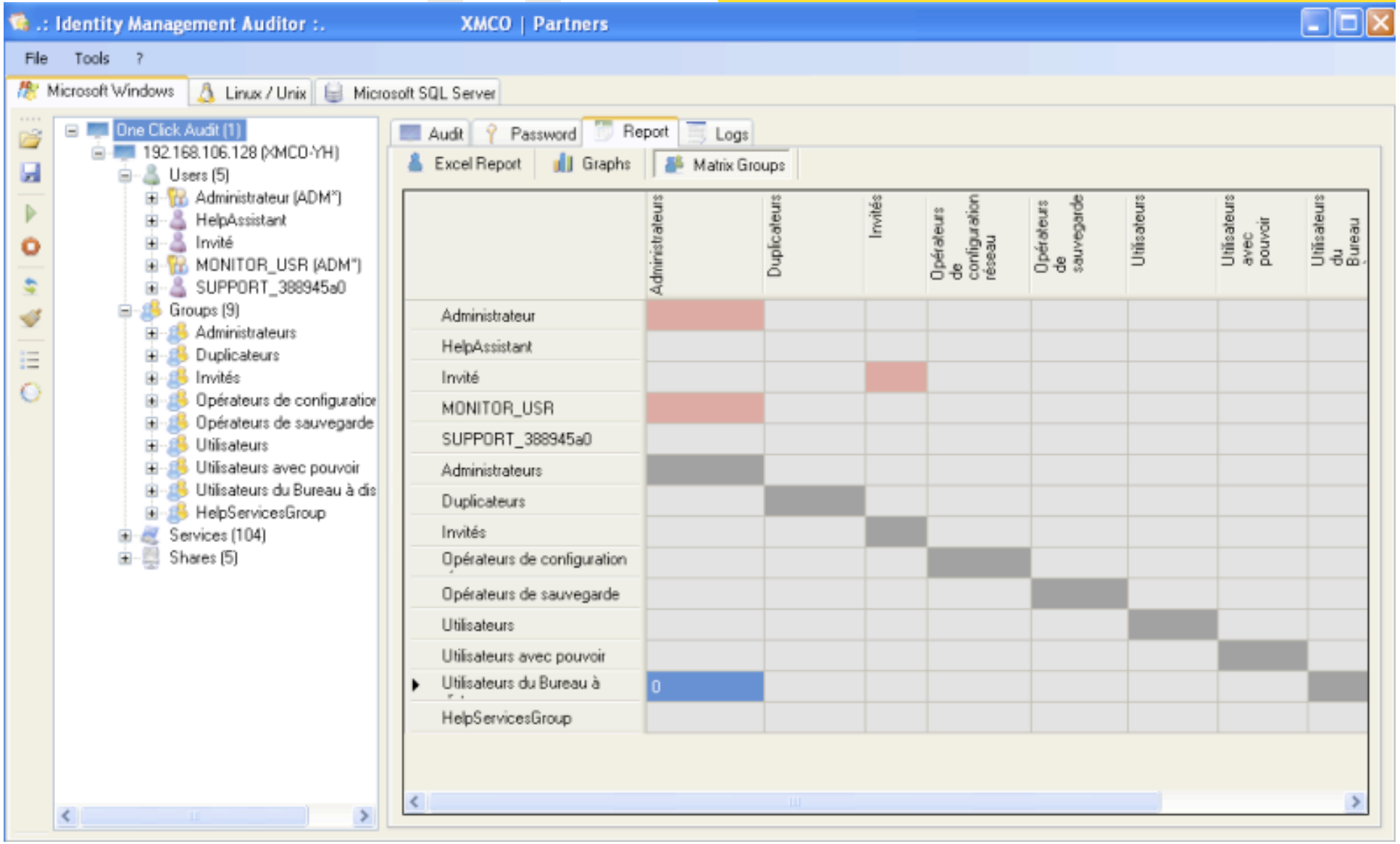
IMA : MODULE WINDOWS – Audit des mots de passe



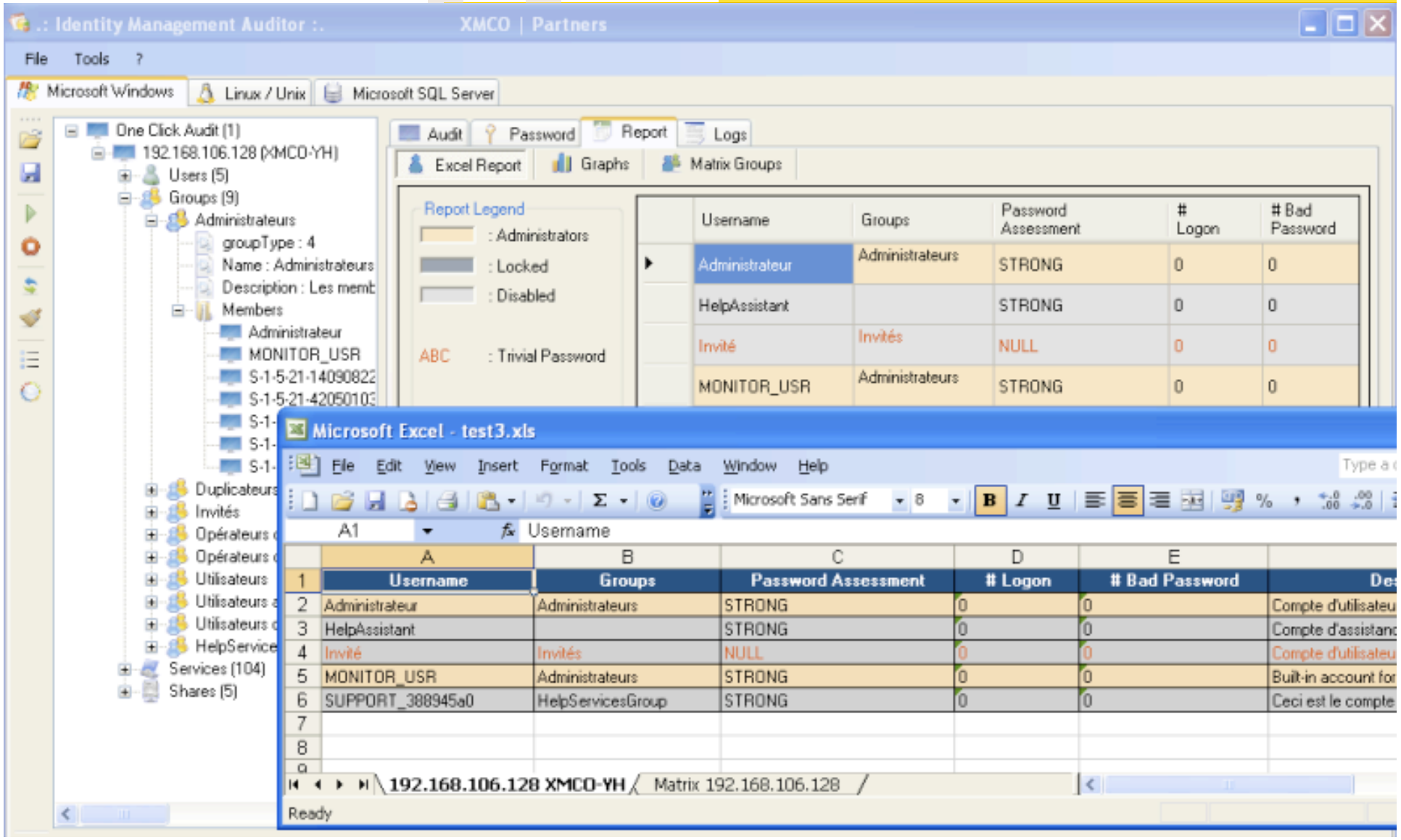
IMA : MODULE WINDOWS – Statistiques



IMA : MODULE WINDOWS : Matrice des Groupes / Utilisateurs



IMA : MODULE WINDOWS : Export XLS



FIN

http://www.xmcopartners.com/ima/index.html

yannick.hamon@xmcopartners.com