



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

An advertisement for Nokia's security solutions. The background is dark with diagonal lines. At the top left, 'Le web 2.0' is written in light blue. Below it, the main headline 'A besoin d'une sécurité 3.0' is in large white font. The body text is in a smaller white font, discussing the risks of Web 2.0 and promoting Nokia's IP security solutions. At the bottom left is the URL 'nokiaforbusiness.com' and at the bottom right is the 'NOKIA' logo in white.

Le web 2.0

A besoin d'une sécurité 3.0

La seconde génération du web est en pleine expansion, elle offre des opportunités exceptionnelles de business. Mais dans la mesure où votre trafic réseau explose, vous êtes plus vulnérable aux attaques des "hackers" professionnels.

Pénétrez dans le monde de la Sécurité Nokia. Notre nouvelle gamme de solutions de sécurité IP offre la puissance et les dernières technologies nécessaires pour sécuriser toutes vos transactions réseau, indépendamment de leur nature.

Etes-vous prêt pour parler sérieusement de sécurité ?

Travaillons ensemble. Travaillons Mieux.

nokiaforbusiness.com

NOKIA

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**



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 !!!**

LE PROJET IMA



Systemes 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 travaux** 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

The screenshot displays the Password Auditor tool interface. At the top, there are tabs for 'Audit', 'Password', 'Report', and 'Logs'. The main area is a table with the following columns: Username, UID, PWDSTAT, LMPASSWD, NTPASSWD, LMHASH, and NTHASH. The table lists various system and user accounts, with their password status and hashes. Below the table, there are two panels: 'Quick Assessment' and 'Password Auditor'. The 'Quick Assessment' panel has radio buttons for 'Trivial Password Only (NULL, Login, Default...)' (selected) and 'Trivial / Weak Password'. A text box shows '# Weak Passwords' as 51082. There is a 'Check' button with a warning icon. The 'Password Auditor' panel has a checkbox for 'Included Default Password List' (checked) and a list box containing 'admin', 'Invité', 'password', and 'soleil'. There is also a checkbox for 'Hide Password Columns' (unchecked). Below these are dropdown menus for 'Audited Hashes' (set to 'LM & NT') and 'Seconds' (set to '10'). A 'Password Assessment' button with a gear icon is at the bottom right.

Username	UID	PWDSTAT	LMPASSWD	NTPASSWD	LMHASH	NTHASH
ADMEXCH	1282	WEAK	EXCHADM01	Exchadm01	404F335AFC45...	89A9A71C1A3...
ADMINWEB	21112	TRIVIAL	ADMINWEB	ADMINWEB	D8C356681684...	5297D621FC8...
ADMUNIX	5166	WEAK	PAUNIX01	Paunix01	758A7EEB858...	2A0E0AD0761...
ADMsql	1141	TRIVIAL	PASSWORD01	Password01	E52CAC67419...	7100A909C7FF...
AdmAntivirus	16956	STRONGD01	NOT CRACKED	85F6A9C3A091...	9E9CBD55D44...
Administrator	500	STRONG			B64C4A36CFE...	D7DA8046E61...
USER_1000	11455	WEAK	ANNAROSE	annarose	0622B12D20C...	371368ECB20...
USER_1003	11462	TRIVIAL	SOLEIL	soleil	78AEFB56EFE...	A721B8F115C...
USER_1004	11466	WEAK	SAHARA	sahara	E5D854DDC1...	84106758443C...
USER_1005	11467	WEAK	PRESTAS	prestas	2EA9D0B52C0...	33F57A32881C...
USER_1006	11471	WEAK	LOULOU	loulou	256C77A05FE...	7CF656F150E7...
USER_1010	11485	WEAK	DRAZUR	drazur	5FEB4CD7937...	19F7DD2FFE5...
USER_1013	11490	TRIVIAL	PASSWORD1	Password1	E52CAC67419...	64F12CDDAA8...
USER_1048	11645	WEAK	LAURENT	laurent	2F043D9346C1...	6640C7B1719...

Quick Assessment

Trivial Password Only (NULL, Login, Default...)

Trivial / Weak Password

Weak Passwords: 51082

Included Default Password List

admin
Invité
password
soleil

Check

Password Auditor

Hide Password Columns

Audited Hashes: LM & NT

Seconds: 10

Password Assessment

IMA : MODULE WINDOWS – Statistiques

Identity Management Auditor :: XMCO | Partners

File Tools ?

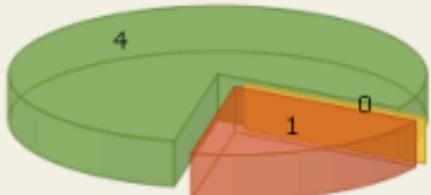
Microsoft Windows Linux / Unix Microsoft SQL Server

One Click Audit (1)
 192.168.106.128 (XMCO-YH)
 Users (5)
 Administrateur (ADM)
 HelpAssistant
 Invité
 MONITOR_USR (ADM)
 Locked : False
 Disabled : False
 memberOf
 Administrateurs
 Password Required
 Trusted Kerberos D
 Trusted Authentical
 UserFlags : 66113
 MaxStorage : -1
 PasswordAge : 205
 PasswordExpired : 1
 FullName : Monitor.
 BadPasswordAttem
 HomeDirectory :
 LoginScript :
 Profile :
 HomeDirDrive :
 Parameters :
 PrimaryGroupID : 5
 Name : MONITOR_
 MinPasswordLengt
 MaxPasswordAge :
 MinPasswordAge :

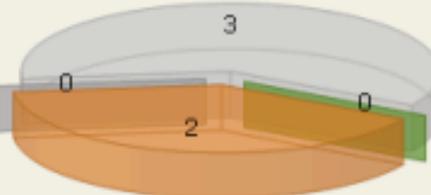
Audit Password Report Logs

Excel Report Graphs Matrix Groups

Password Assessment



Accounts



Last logons (Active Users Only)



Statistics	Results
# Accounts	5
# Active Administrators	2
# Active Users	3
# Disabled Accounts	3
# Locked Accounts	0
# Strong Passwords	4
# Trivial Passwords	0
# Weak Passwords	0
# Null Passwords	1
# Recent Logons	2
# Never Log	1
# More than 1 Year without logon	0
# More than 6 Months without logon	0
# More than 3 Months without logon	0

IMA : MODULE WINDOWS : Matrice des Groupes / Utilisateurs

The screenshot displays the Identity Management Auditor (IMA) interface for Windows. The main window title is "Identity Management Auditor :: XMCO | Partners". The interface is divided into several sections:

- Left Panel:** A tree view showing the hierarchy of the system. The selected path is "One Click Audit (1) > 192.168.106.128 (XMCO-YH) > Users (5)". Other visible items include "Groups (9)" and "Services (104)".
- Top Menu:** "File", "Tools", and "?".
- Sub-Menus:** "Microsoft Windows", "Linux / Unix", and "Microsoft SQL Server".
- Navigation Tabs:** "Audit", "Password", "Report", and "Logs".
- Report Options:** "Excel Report", "Graphs", and "Matrix Groups" (selected).
- Main Grid:** A matrix showing group membership. The columns represent user categories, and the rows represent specific groups.

Group	Administrateurs	Duplicateurs	Invités	Opérateurs de configuration réseau	Opérateurs de sauvegarde	Utilisateurs	Utilisateurs avec pouvoir	Utilisateurs du Bureau
Administrateur	Yes							
HelpAssistant								
Invité			Yes					
MONITOR_USR	Yes							
SUPPORT_388945a0								
Administrateurs	Yes							
Duplicateurs		Yes						
Invités			Yes					
Opérateurs de configuration				Yes				
Opérateurs de sauvegarde					Yes			
Utilisateurs						Yes		
Utilisateurs avec pouvoir							Yes	
Utilisateurs du Bureau à	0							Yes
HelpServicesGroup								

IMA : MODULE WINDOWS : Export XLS

The screenshot shows the Identity Management Auditor interface with a report window open. The report window displays a table with the following data:

Username	Groups	Password Assessment	# Logon	# Bad Password
Administrateur	Administrateurs	STRONG	0	0
HelpAssistant		STRONG	0	0
Invité	Invités	NULL	0	0
MONITOR_USR	Administrateurs	STRONG	0	0

The Excel window shows the same data in a spreadsheet format:

A	B	C	D	E	
1	Username	Groups	Password Assessment	# Logon	# Bad Password
2	Administrateur	Administrateurs	STRONG	0	0
3	HelpAssistant		STRONG	0	0
4	Invité	Invités	NULL	0	0
5	MONITOR_USR	Administrateurs	STRONG	0	0
6	SUPPORT_388945a0	HelpServicesGroup	STRONG	0	0

FIN

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



yannick.hamon@xmcopartners.com