CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

GESTION DES COMPTES LOCAUX

GESTION DES COMPTES LOCAUX
Introduction

- Deux points majeurs pour la sécurité vont être abordés :
  - La gestion des comptes
  - Les mots de passe

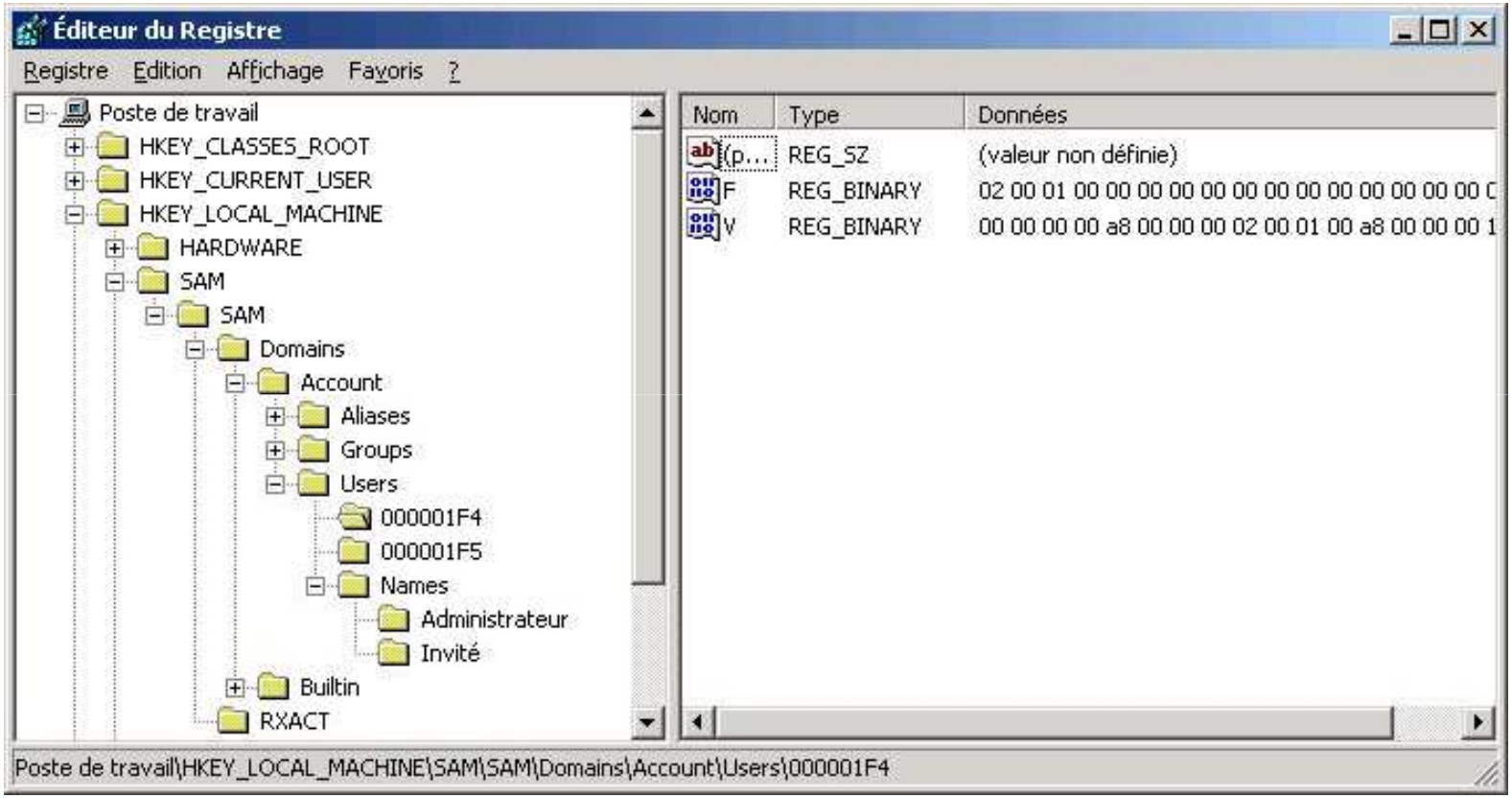
GESTION DES COMPTES LOCAUX

Les comptes locaux

- Windows utilise une base de données pour les comptes locaux appelé SAM (Security Account Manager)
- Stockage de la base SAM sur le système de fichiers: %SystemRoot%\system32\Config\SAM
- SAM est accessible au travers de la ruche de la base de registre : HKEY_LOCAL_MACHINE/SAM
- La base SAM n'est accessible que par le compte « SYSTEM » à travers le processus LSA (Local Security Authority Subsystem Service) qui est en charge des politiques de sécurité sous Windows

GESTION DES COMPTES LOCAUX

Exemple de contenu de la base SAM



GESTION DES COMPTES LOCAUX
SAM

- Elle contient 3 types de comptes :
  - Les utilisateurs
  - Les groupes
  - Les ordinateurs
- Chaque compte contient :
  - Identifiants : RID, Nom, Prénom, Commentaire, « Home dir »
  - Attributs : désactivé, délais d'expiration du mot de passe, …
  - Groupes : liste des groupes auxquels le compte appartient
  - Le mot de passe : haché dans différents formats NTLM, LM
- Sur un réseau Windows, les comptes sont stockés sur un serveur AD (Active Directory)

GESTION DES COMPTES LOCAUX

Les hashs de mot de passe

- Plusieurs formats de hash sont utilisés sous Windows pour protéger les mots de passe
- LM était le premier format de hash de Windows
  - 14 caractères (remplacés par des 0 si > et tronqués si <)
  - 2 hash de 7 caractères sans casse avec l'algo DES
  - Actif par défaut pour des raisons de compatibilité jusqu'à Windows XP SP2
- Le remplaçant de LM est la fonction de hash du protocole NTLM (NT Lan Manager) qui réalise l'authentification, l'intégrité et la confidentialité dans un réseau Windows

GESTION DES COMPTES LOCAUX
NTLMv2

- NTLMv1 est apparu à partir de NT 3.1 et a été remplacé par NTLMv2 lors de mises à jour de Windows car peu robuste
- C'est l'algorithme md4 qui est utilisé pour hasher les mots de passe stockés dans une base SAM sans restriction de casse ni de longueur
- Le principal défaut est le manque de grain de sel :
  - Un mot de passe identique à deux utilisateurs génère le même hash
  - On peut pré-calculer l'ensemble des combinaisons possibles et générer des tables « Rainbow »

GESTION DES COMPTES LOCAUX

Crackage de mot de passe NTLM

- « Brute-force » avec 1 carte graphique haut de gamme

Character set	Password length	Password sample	Time to crack
A .. Z	5	CRUEL	instantly
A .. Z	6	SECRET	instantly
A .. Z	7	MONSTER	instantly
A .. Z	8	COOLGIRL	22s
A .. Z	9	LETMEKNOW	~ 10m
A .. Z, 0 .. 9	5	COOL3	instantly
A .. Z, 0 .. 9	6	BANG13	instantly
A .. Z, 0 .. 9	7	POKER00	8s
A .. Z, 0 .. 9	8	LETMEBE4	~ 5m
A .. Z, 0 .. 9	9	COOLGIRL1	~ 3h
A .. Z, a .. z, 0 .. 9	5	P0k3r	instantly
A .. Z, a .. z, 0 .. 9	6	S3cr31	10s
A .. Z, a .. z, 0 .. 9	7	DidIt13	~ 6m
A .. Z, a .. z, 0 .. 9	8	GoAway99	~ 6h
A .. Z, a .. z, 0 .. 9	9	19Sample3	~ 16d

GESTION DES COMPTES LOCAUX

Ce qu'il faut retenir pour la suite

- La base SAM contient toutes les données de sécurité de Windows NT (surtout les comptes utilisateurs)
- L'ancien format de hashage des mots de passe LM est à désactiver sur les vieilles versions de Windows
- Le format actuel de hashage NTLM permet le pré-calcul de toutes les combinaisons car il manque un grain de sel
- La sécurité des mots de passe dans Windows est insuffisante