HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Solutions Linux

Extraction de données authentifiantes de la mémoire Windows

29 mai 2013

Steeve Barbeau
<steeve.barbeau@hsc.fr>

Hervé Schauer Consultants

- Société de conseil et d'expertise en sécurité des systèmes d'information
  - Depuis 1989
  - Indépendant
  - 30 consultants
- Domaines d'expertise
  - Expertise technique en sécurité : audit de sécurité, tests d'intrusion, etc.
  - Expertise organisationnelle : risk management, SMSI, etc.
  - Expertise juridique
  - Formation :
    - Securité applicative, sécurité des systèmes d'exploitation, réseau, organisation de la sécurité, etc.
- Certifications des consultants
  - CISSP, OSCP, PCI-DSS, GIAC, ISO2700x

Sommaire

- Introduction
- Processus d'authentification
- Extraction en mémoire
  - Windows NT & Windows 2000
  - Post Windows XP
- Outils réalisés
- Scénario d'attaque
- Recommandations
- Conclusion

Introduction

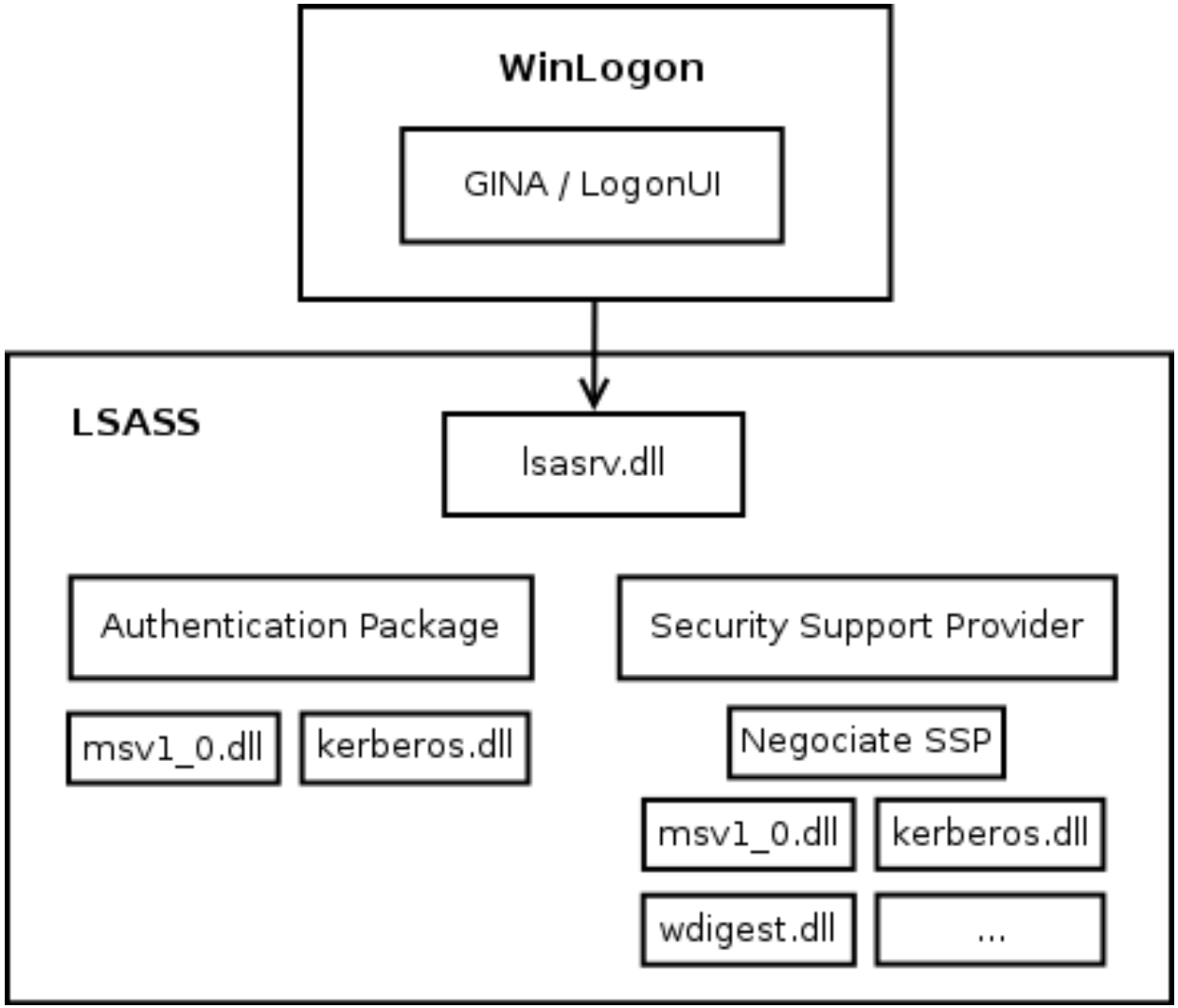
- *Objectif* : étudier le stockage des mots de passe Windows en mémoire
- *Contrainte* : ne pas affecter la stabilité du système
- *Intérêt* : permettre d'acquérir des privilèges supérieurs et de rebondir sur d'autres machines
- *Contexte* : prestations de type tests d'intrusion

Processus d'authentification

- Authentication Package (AP)
  - Bibliothèque appelée par LSASS pour valider les authentifications intéractives
- Security Support Provider (SSP)
  - Bibliothèque implémentant des protocoles d'authentification client/serveur pour les authentifications non-intéractives
- Session d'authentification
  - Créée lors de chaque connexion authentifiée
  - Différents types
    - Interactive (Type 2)
    - Network (Type 3)
    - Service (Type 5)
    - RemoteInteractive (Type 10)

Processus d'authentification

Composants intervenant lors de l'authentification



Processus d'authentification

- Windows 2000
  - Msv1_0
    - Protocole défi-réponse LM/NTLM
    - Authentification réseau (ex : SMB)
  - Kerberos
    - Protocole Kerberos v5
    - Utilisé par défaut pour s'authentifier sur un domaine Active Directory
  - Schannel
    - Certificats SSL/TLS
    - Utilisé pour des services Web, accès VPN
- Windows XP
  - Wdigest
    - Authentification « Digest »
    - Utilisé par certains sites internet (≠ authentification « Basic »)

Processus d'authentification

- Windows Vista
  - Tspkg
    - SSO pour Terminal Server
- Windows 7
  - Pku2u
    - Authentification pair à pair
      - Windows 7 Media
      - Échanges de fichiers (en dehors d'un domaine)
- Windows 8
  - LiveSSP
    - Authentification avec le Cloud « Live » de Microsoft
      - Office en ligne
      - Exchange en ligne

Extraction en mémoire - Windows NT & Windows 2000

- FindPass
  - Recherche du processus Winlogon.exe
    - Présence du module MsGina (interface graphique d'authentification)
  - Parcours de la mémoire de Winlogon à la recherche de
    - %USERNAME%
    - %USERDOMAIN% à l'offset 0x200 (Win NT), 0x400 (Win 2000)
  - Mot de passe présent à l'offset
    - 0x400 (Win NT)
    - 0x800 (Win 2000)
  - Désobfuscation du mot de passe à l'aide de RtlRunDecodeUnicodeString

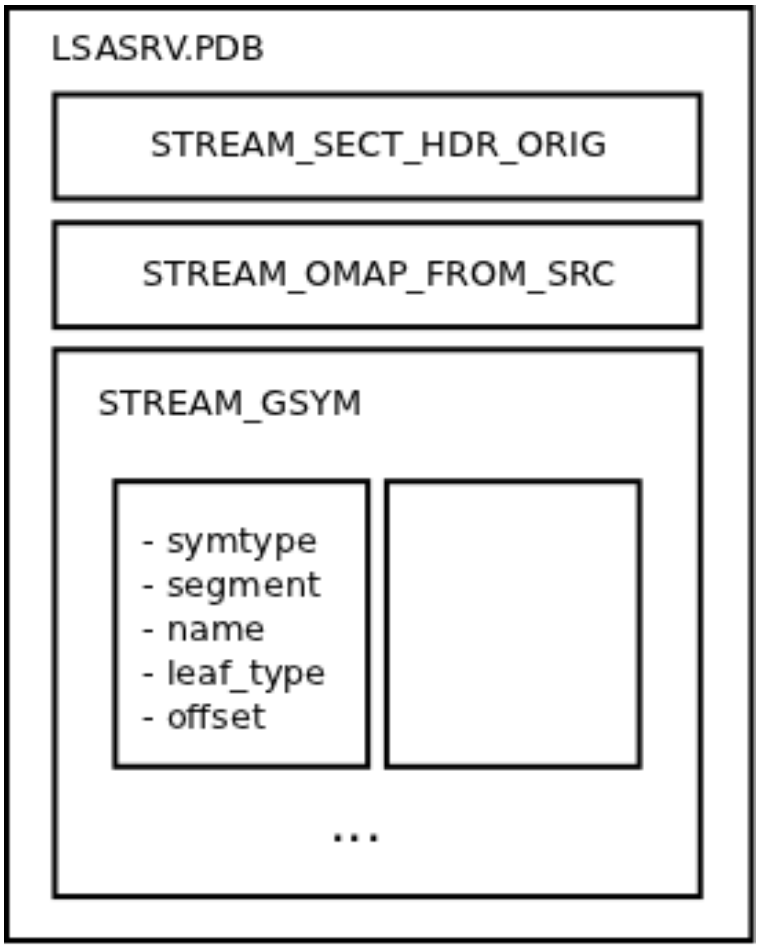
Extraction en mémoire – Post Windows XP
a) Pré-requis

- Nécessité de connaître
  - Structures internes
    - Liste chaînée
    - Structures imbriquées
    - Emplacement et type des différents champs
  - Adresses mémoire de certaines données
    - Emplacement de la liste des structures
    - Clefs de chiffrement
    - Vecteur d'initialisation
    - Fonction de déchiffrement

Extraction en mémoire – Post Windows XP
a) Pré-requis

- Identifiant unique
  - Lien entre DLL et fichier de débogage
  - DBG
    - Antérieur à Windows XP
  - PDB 2.0 (NB10)
    - 8 octets (DWORD) + 1
  - PDB 7.0 (RSDS)
    - 32 octets (GUID) + 1

Structure d'un fichier PDB

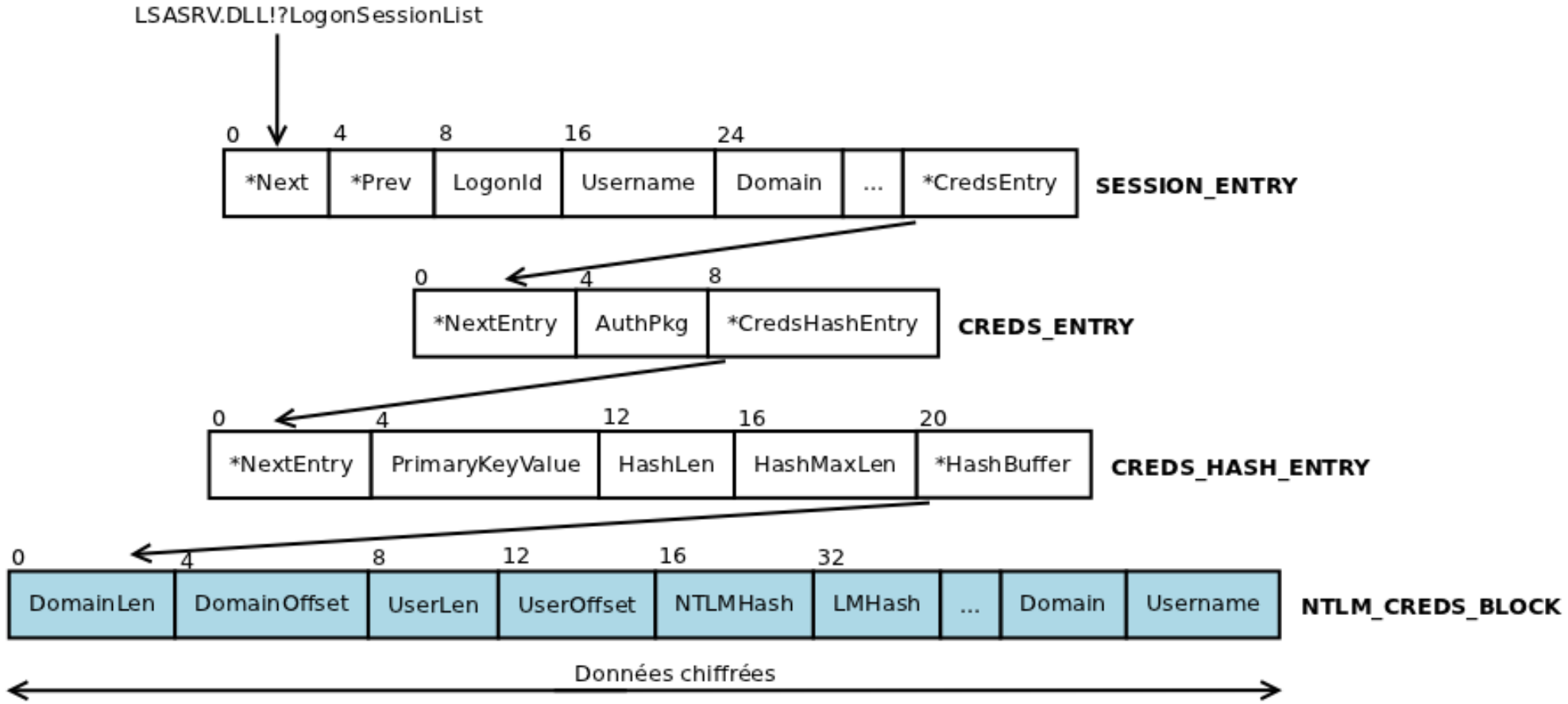


Extraction en mémoire – Post Windows XP
a) Pré-requis

- Tous systèmes
  - Lsasrv.dll!**?LogonSessionList** — Liste chaînée des empreintes
  - Lsasrv.dll!**?LogonSessionListCount** — Nombre de listes
  - Lsasrv.dll!**?LogonSessionCount** — Nombre de listes
  - Wdigest.dll!**?l_LogSessList** — Liste chaînée des mots de passe
- Avant Vista SP1
  - Lsasrv.dll!**?g_Feedback** — Vecteur d'initialisation
  - Lsasrv.dll!**?g_pDESXKey** — Clé DESX
  - Lsasrv.dll!**?LsaEncryptMemory** — Fonction de déchiffrement
- Depuis Vista SP1
  - Lsasrv.dll!**?h3DesKey** — Clé 3DES
  - Lsasrv.dll!**?InitializationVector** — Vecteur d'initialisation

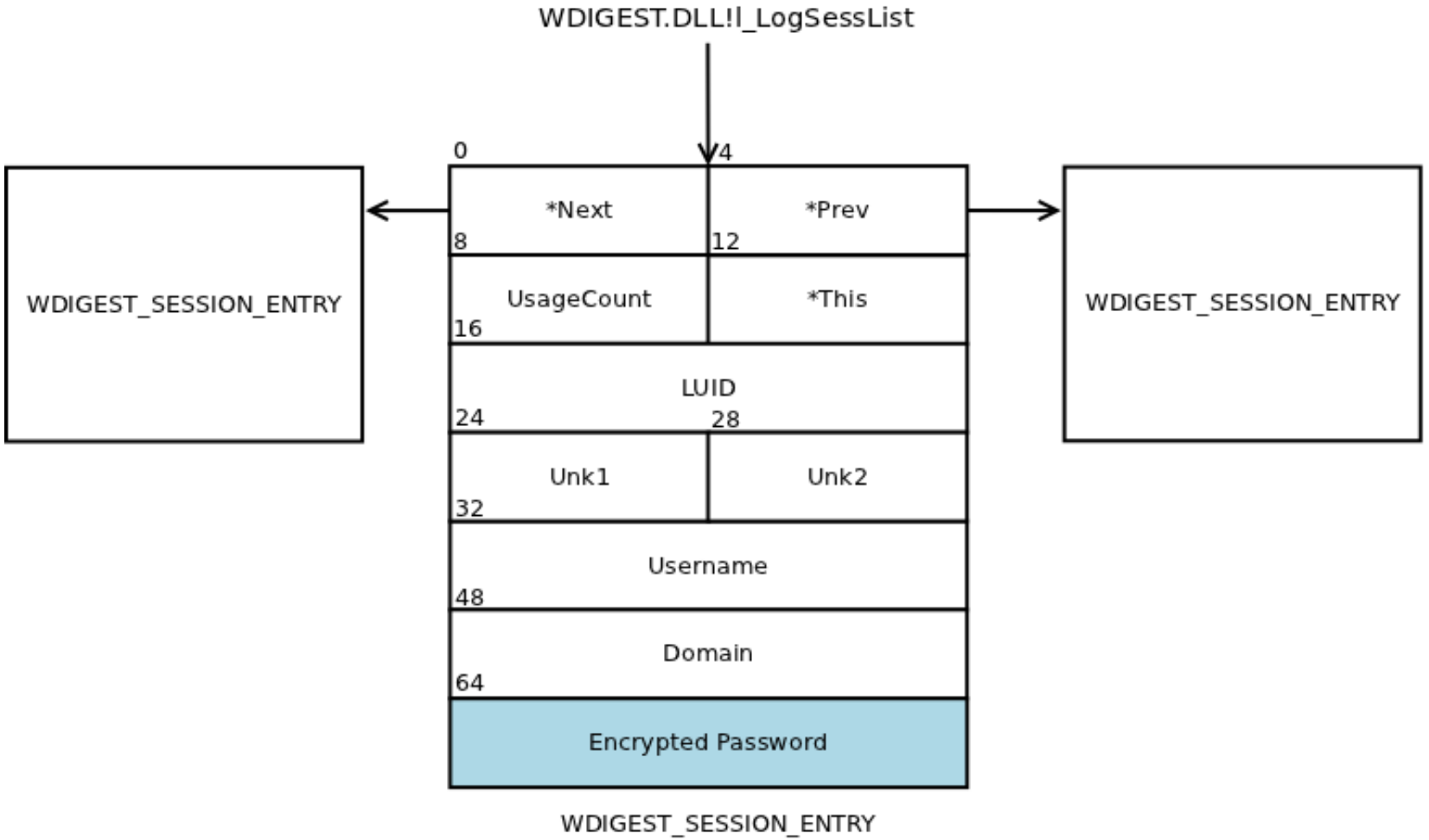
Extraction en mémoire – Post Windows XP
b) Extraction des empreintes

Structures internes de Lsasrv.dll



Extraction en mémoire – Post Windows XP
c) Extraction des mots de passe

Structures internes de Wdigest.dll

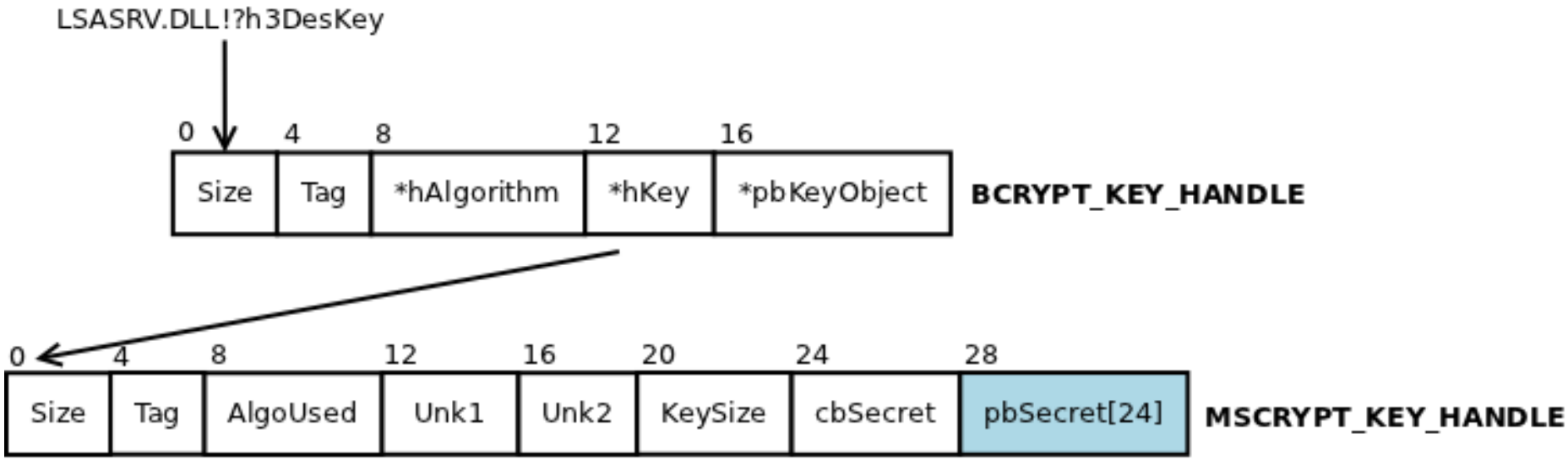


Extraction en mémoire – Post Windows XP
d) Déchiffrement des données en mémoire

- Avant Windows Vista SP1
  - Bibliothèque Lsasrv.dll
  - Chiffrement **DESX / RC4**
    - g_FeedBack (vecteur d'initialisation)
    - g_pDESXKey (clé de chiffrement)
    - LsaEncryptMemory (fonction de déchiffrement)
- Depuis Windows Vista SP1
  - Cryptography Next Generation (CNG)
    - Bibliothèque BCrypt.dll
  - Chiffrement **3DES / AES**
    - h3DesKey (clé de chiffrement)
    - InitializationVector (vecteur d'initialisation)

Extraction en mémoire – Post Windows XP
d) Déchiffrement des données en mémoire

Structures internes de BCrypt.dll



Extraction en mémoire – Post Windows XP
d) Déchiffrement des données en mémoire

Processus de déchiffrement avec Bcrypt

```
BCryptOpenAlgorithmProvider(..., BCRYPT_3DES_ALGORITHM, ...);
BCryptGetProperty(..., BCRYPT_OBJECT_LENGTH, ...);
BCryptGetProperty(..., BCRYPT_BLOCK_LENGTH, ...);
BCryptSetProperty(..., BCRYPT_CHAINING_MODE, BCRYPT_CHAIN_MODE_CBC, ...);
BCryptImportKey(..., BCRYPT_KEY_DATA_BLOB, ...);
BCryptDecrypt(...);
BCryptCloseAlgorithmProvider(...);
BCryptDestroyKey(...);
```

Outils réalisés
a) Findpass

- Intégré à Metasploit
  - Sous la forme d'une extension Meterpreter (module post-exploitation)
  - Ecrit en C et Ruby
- Uniquement compatible Windows 2000

- Commande unique
  - Findpass

- Disponible sur http://www.hsc.fr/ressources/outils/findpass/index.html.en

Outils réalisés

b) Scripts Python

- dll_download.py
  - Parse les pages des bulletins de sécurité de Microsoft
  - Télécharge les correctifs
  - Extrait les bibliothèques de ces correctifs
- dll_parser.py
  - Télécharge les fichiers PDB
  - Extrait les symboles de ces fichiers
  - Sauvegarde les offsets dans un fichier CSV
- get_input_offset.py
  - Génère l'entrée nécessaire pour fournir les offsets aux commandes Meterpreter à la volée

Outils réalisés

c) Sessiondump

- Intégré à Metasploit
  - Sous la forme d'une extension Meterpreter (module post-exploitation)
  - Ecrit en C et Ruby
- Compatible 32 bits et 64 bits
  - De Windows XP/2003 à Windows 8/2012
- Offsets des différentes versions des bibliothèques
  - metasploit-framework/data/sessiondump_lsasrv_offsets.csv
    - dll_version, architecture, encryptmemory, logon_session_list_addr, logon_session_list_count, feedback_addr, deskey_ptr_addr, 3deskey_ptr_addr, iv_addr
  - metasploit-framework/data/sessiondump_wdigest_offsets.csv
    - dll_version, architecture, wdigest_session_list

Outils réalisés
c) Sessiondump

- Requiert les droits systèmes
- Commandes
  - GetLsasrvVer
  - GetWdigestVer
  - SetLsasrvOffsetsFile
  - SetWdigestOffsetsFile
  - GetHashes
  - GetWdigestPasswords

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getHashes
STEEVEXP\steeve::28de0fd8b9df404aaad3b435b51404ee:326b6bed3dbac2a86dd3008e0d40e078:::
WORKGROUP\STEEVEXP$::aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > getWdigestPasswords
STEEVEXP\steeve : steeve
meterpreter >
```

- Options de getHashes et getWdigestPasswords
  - « -i » : utilisation d'offsets « à la volée »
  - « -o » : enregistrement des données dans des fichiers

http://www.hsc.fr/ressources/outils/sessiondump/index.html.en

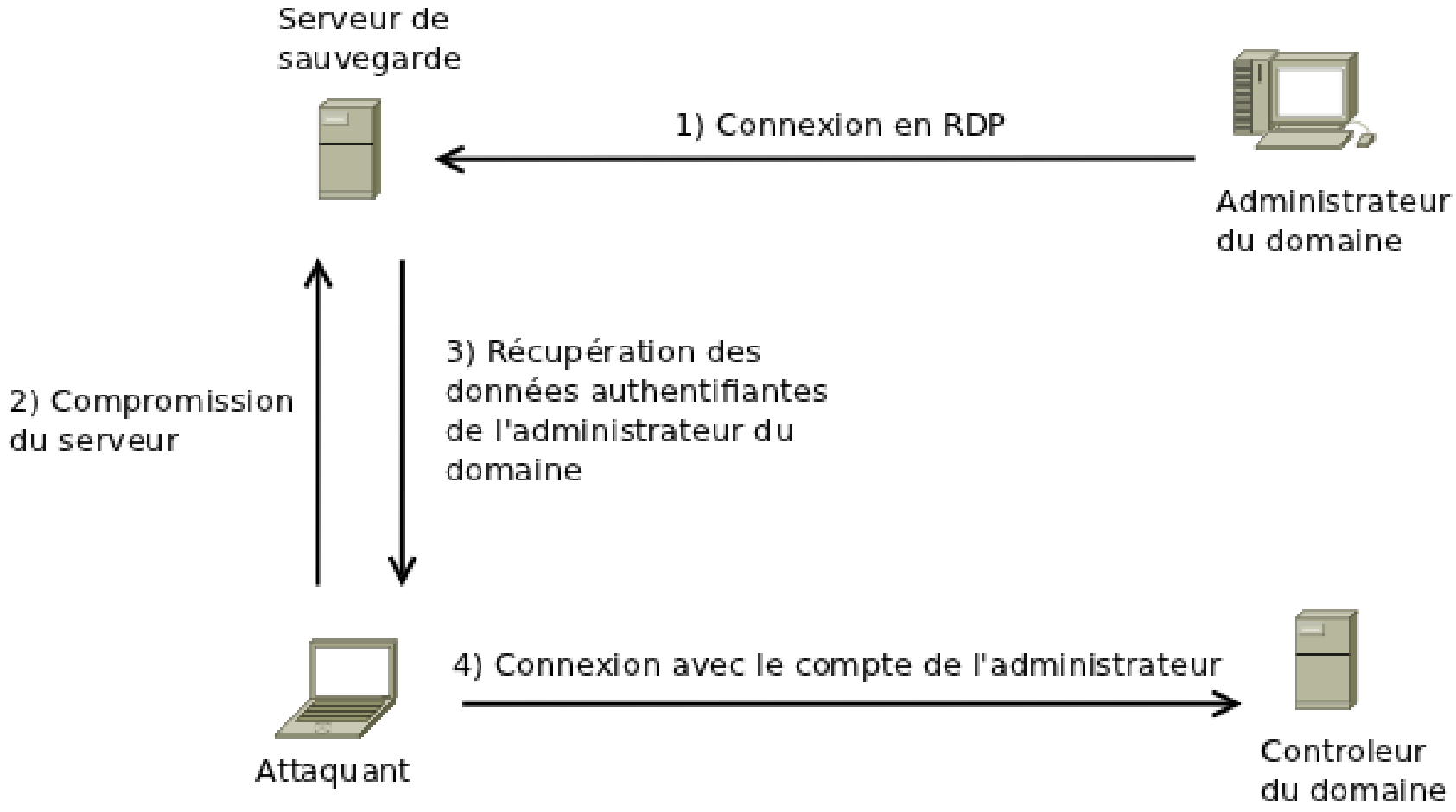
Outils réalisés

c) Sessiondump

Démonstration

Scénario d'attaque

Exemple de compromission du controleur du domaine avec sessiondump



Recommandations

- Désactivation des packages d'authentification non utilisés
  - HKLM\System\CurrentControlSet\Control\Lsa\Security Packages
- Certains sont indipensables à Windows
  - Kerberos
  - Msv1_0
  - Schannel
- Limiter l'utilisation des comptes privilégiés
- Ne pas laisser de sessions actives

Conclusion

- Empreintes et mots de passe toujours présent en mémoire
- Outil très pratique en test d'intrusion
  - Pas d'outil spécifique à uploader
  - Pas d'impact sur la stabilité de la machine

Merci de votre attention

Questions ?