ÉRIC BEAULIEU

Visibilité du Système d'Information

Degré de difficulté

Cet article présente les informations plus ou moins sensibles issues du réseau interne d'une entreprise et susceptibles d'être découvertes sur un ordinateur portable perdu ou volé. Il présentera également comment une personne malveillante découvre ces traces et mène une attaque contre le réseau de l'entreprise.

CET ARTICLE EXPLIQUE...

La prise de contrôle d'un ordinateur portable par une personne malveillante.

Les informations sur l'architecture de l'entreprise susceptibles d'être découvertes sur le système.

Les attaques pouvant être lancées par une personne malveillante à partir de ces informations.

Les contre-mesures destinées à limiter ces fuites d'informations.

CE QU'IL FAUT SAVOIR...

Connaître les systèmes Microsoft Windows.

Connaître les bases du système Linux.

Disposer des bases des Systèmes d'Information en entreprise.

De plus en plus d'entreprises mettent à la disposition de leurs employés des matériels nomades (ordinateur portable, PDA, BlackBerry…). Tous ces équipements leur permettent de travailler depuis n'importe quel endroit (en clientèle, dans un aéroport, de chez eux…). Parallèlement à leur démocratisation, ces équipements se miniaturisent de plus en plus et sont, par conséquent, facilement perdus ou volés.

Outre le prix du matériel, c'est la perte des données, le temps nécessaire pour les reconstituer et surtout, l'exploitation potentielle de ces données (par une personne malveillante) qui coûtent cher à une entreprise. Et malheureusement, toutes les protections réseau (firewall, antispam, antivirus, IPS…), traditionnellement mises en place, n'empêcheront pas la perte des nomades ni l'exploitation des données stockées. En partant du principe que la meilleure manière de se protéger des agressions est de les connaître, nous expliqueront comment une personne malveillante peut prendre le contrôle d'un nomade volé et comment elle peut découvrir des informations sensibles. Évidemment, les informations détaillées dans ces lignes sont destinées à élargir les connaissances des lecteurs et ne doivent pas être utilisées pour commettre des actes de malveillance…

Duplication du média de stockage

Avant toutes opérations, il faut commencer par réaliser une copie de sauvegarde du disque dur. Cette opération permettra de :

- conserver une sauvegarde des données,
- réaliser par la suite une recherche des fichiers effacés,
- restaurer le disque et le restituer sans laisser de trace.

Il est donc nécessaire de faire une copie bit à bit du média de stockage. Ce type de copie permet de conserver les fichiers supprimés dont des traces persistent sur le disque. Pour dupliquer le média, deux solutions sont disponibles, selon qu'il est possible d'accèder à la séquence de boot *Bios*, ou que le disque physique s'extrait facilement :

- la séquence de boot est accessible : faire démarrer le nomade sur un LiveCD Linux, par exemple Ubuntu, et brancher un disque dur externe au nomade,
- le disque dur est accessible : démonter ce dernier du nomade, le placer dans un adaptateur USB externe et le connecter à un PC sous Linux.

Une fois l'une des deux opérations réalisées, lancez la commande suivante : *dd if=/dev/sda of=/dev/hdb(/data/disk.iso)* ; *sda* représente le

disque du nomade dans le périphérique USB et hdb représente le disque de destination sur lequel la copie est réalisée (ici, le deuxième disque IDE de notre PC).

Lors de la copie des données, il arrive que des erreurs sur le média source ne permettent pas de réaliser la duplication. Pour que la copie ne soit pas sensible aux secteurs défectueux, le mieux est d'utiliser l'utilitaire *dd_rhelp* ou *dd_rescue* (pour plus de détails, voir le projet freshmeat *dd_rhelp*).

Pour éviter qu'une personne malveillante accède aux données du disque dur, il faut protéger le bios par un mot de passe, configurer la séquence de boot pour ne démarrer que sur le disque dur du nomade et interdire tous les autres modes de démarrage (CD, USB, réseau…). Mais la solution ultime qui reviendra tout au long de l'article est le chiffrement du disque dur.

Récupération des comptes et mots de passe

Nous commencerons par les comptes locaux. Pour obtenir la liste des comptes locaux ainsi que leurs mots de passe chiffrés, le Live CD BackTrack et l'utilitaire de brute force des mots de passe *John The Ripper* seront utilisés : démarrez le nomade sur cette distribution et tapez les commandes du Listing 1.

Si les hashs des mots de passe n'existent qu'au format NTHash, il faudra spécifier ce format à *John The Ripper*. Pour cela, modifiez la commande de découverte des mots de passe et tapez :

```
john /tmp/mdp-hash.txt -format
      NT -w:dictionnaire.txt
```

D'autres outils s'utilisent également pour découvrir les mots de passe Windows à partir de la base SAM : Ophtcrack, LCP5, Caïn & Abel…

Cette procédure de récupération des mots de passe ne fonctionne que si le système de fichier est accessible en clair. Par conséquent, si l'entreprise met en place un processus de chiffrement des partitions, un attaquant n'accèdera pas à la base SAM et n'obtiendra donc pas les mots de passe des comptes locaux.

Listing 1. *Récupération des comptes locaux*

```
# bkhive-linux /mnt/hda1/WINDOWS/system32/config/system /tmp/syskey.txt
# samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam /tmp/syskey.txt >
      /tmp/mdp-hash.txt
# john /tmp/mdp-hash.txt -w:dictionnaire.txt
```

Listing 2. *Extrait du journal de sécurité Microsoft*

```
10/31/2007 ADDomaine\francky nomade francky ADDomaine (0x0,0xAAAE8) 7 User32 Negotiate
      nomade {1c9fc19c-479e-dc6a-539e-e07de2a1987e}
11/1/2007 ADDomaine\admin1 nomade admin1 ADDomaine (0x0,0x653C8) 3 NtLmSsp NTLM
      PCAdmin {00000000-0000-0000-0000-000000000000}
11/9/2007 DOMINO\marie Nomade marie DOMINO (0x0,0x39608CB) 2
```

Listing 3. *Extrait du journal de sécurité Microsoft*

```
10/30/2007 N/A Nomade Votre ordinateur a perdu le bail de son adresse
      IP 192.168.100.163 sur la carte réseau d'adresse réseau 001C273DB7C7.
11/2/2007 N/A Nomade Le bail de l'adresse IP 192.168.240.11 pour la carte réseau dont
      l'adresse réseau est 000C293D77C7 a été refusé par le serveur DHCP 192.168.0.1
      (celui-ci a envoyé un message DHCPNACK).
10/30/2007 N/A nomade Le système de sécurité n'a pas pu établir une connexion
      sécurisée avec le serveur DNS/ns.domain.dom. Aucun protocole n'était disponible.
11/1/2007 N/A nomade Échec lors de la mise à jour et la suppression des
      enregistrements (RR) des ressources pointeurs (PTR) de la carte réseau ayant
      les paramètres : Nom de la carte : {4409FF5E-92A2-4D5A-BBC4-92090E51B8E9}
      Nom de l'hôte : nomade Suffixe du domaine spécifique à la carte : ADDomaine.dom
      Liste de serveurs DNS : 192.168.0.1, 192.168.0.2 Mise à jour envoyée
      au serveur :
      <?> Adresse(s) IP :192.168.100.41 L'ordinateur n'a pas pu supprimer ces RR PTR
      car la demande de mise à jour a dépassé le délai en attendant une réponse
      du serveur DNS. Ceci est probablement dû au fait que le serveur DNS d'autorité
      pour la zone qui nécessite la mise à jour ne fonctionne pas.
11/2/2007 N/A Nomade Le service de temps synchronise maintenant l'heure système avec
      la source de temps SRVAD.ADdomaine.dom (ntp.d|192.168.100.11:123->
      192.168.0.1:123).
```

Que peut faire un attaquant avec ces informations ? Si une personne malveillante obtient des logins / mots de passe locaux, elle disposera de comptes potentiels sur le réseau de l'entreprise. Il y a même de grandes chances pour que le compte administrateur de l'entreprise soit le même sur tous les ordinateurs de l'entreprise. Il dispose donc d'un accès potentiel à tous les postes de travail de l'entreprise. Le cas le plus désastreux pour une entreprise serait que le mot de passe administrateur local des serveurs soit le même que le mot de passe des stations de travail.

Réinitialisation du compte administrateur local

Une fois la base SAM obtenue et durant le processus de découverte des mots de passe, le compte administrateur local peut être réinitialisé avec l'outil Offline NT Password. Pour cela, téléchargez soit les binaires, soit l'ISO, placez-le ou les sur un CD ou une disquette et démarrez le portable sur ce dernier.

Après avoir démarré avec le média contenant Offline NT Password, indiquez-lui la partition contenant la base SAM et le fichier contenant la base SAM elle-même. Après avoir obtenu la liste des comptes locaux, il ne reste plus qu'à lui spécifier le compte administrateur et à lui indiquer le

Figure 1. *Connexion d'un disque dur externe au nomade*

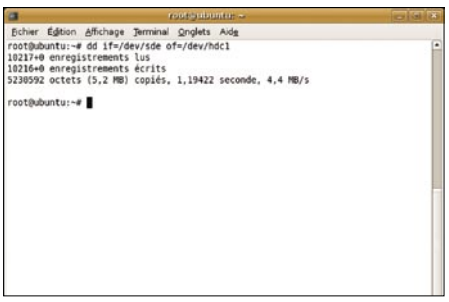

Figure 2. *Duplication du disque dur avec la commande dd*

mot de passe : * signifiant que le mot de passe sera vide.

Redémarrez à présent le portable et saisissez le nom du compte administrateur sans mot de passe pour obtenir l'accès à la station avec le maximum de privilèges.

Que peut faire un attaquant avec ces informations ? L'attaquant dispose maintenant d'un compte de plus haut niveau sur le nomade qui lui permet d'accéder à toutes les données du portable, de désactiver / arrêter des services (par exemple l'antivirus), d'avoir accès à la base de registre…

La réinitialisation du compte administrateur local ne se fait que si le disque du portable n'est pas chiffré ou si l'attaquant démarre sur un média autre que le disque dur interne ou modifie la séquence de démarrage.

Comptes Active Directory stockés en cache

Pour que l'utilisateur puisse se connecter à son portable, en utilisant son compte Active Directory, mais sans être connecté au réseau de l'entreprise, Windows intègre un système de cache des comptes Active Directory. Ainsi, l'attaquant, après avoir obtenu une session locale (administrateur local) et éventuellement désactivé l'antivirus, pourra tenter d'obtenir les comptes placés en cache sur le système d'exploitation. Pour obtenir la liste des comptes *Active Directory*, il faut utiliser l'utilitaire cachedump. Cet utilitaire permettra d'obtenir le nom des derniers comptes Active Directory qui se sont connectés sur le portable, le hash de leur mot de passe et les domaines Active Directory de connexion :

```
C:\ >cachedump.exe > mdp_cache.txt
francky:68A6B7098E54C6B525BD65C2151
      3B381:addomaine:domaine.dom
marie:38b9302918c9210ac45d39d1029a029:
      addomaine:domaine.dom
admin_support:3840329a12931ac23948201
      94832ac2:addomaine:domaine.dom
bob:39104928130ab3223acb302913da129:
      addomaine:domaine.dom
```

Après avoir obtenu les Hash des mots de passe des utilisateurs Active Directory, il faut les déchiffrer. Pour cela, le logiciel *John The Ripper* sera utilisé en lui spécifiant le format *mscash* (*-format=mscash*) :

```
C:\ >john.exe mdp_cache.txt
      -format=mscash
Loaded 4 password hashes with 4
      different salts (M$ Cache Hash
      [mscash])
password (bob)
hercule    (marie)
francky07 (francky)
admin_societe (admin_support)
```

Que peut faire un attaquant avec ces informations ? L'attaquant dispose maintenant de quatre comptes Active Directory sur le domaine de l'entreprise dont un compte appartenant probablement au support technique de l'entreprise et disposant potentiellement de droits avancés sur le réseau. Le format des mots de passe découvert laisse penser que, l'entreprise ne dispose pas de politique de mots de passe forts. Ainsi, il serait possible à notre attaquant de découvrir d'autres mots de passe utilisateur si ce dernier obtenait un accès au réseau de l'entreprise ou testait différents mots de passe sur des ressources extérieures de l'entreprise (extranet, webmail…)

L'entreprise devrait mettre en place une politique de mots de passe plus forte qui ne permettra pas à un attaquant de découvrir facilement les mots de passe de

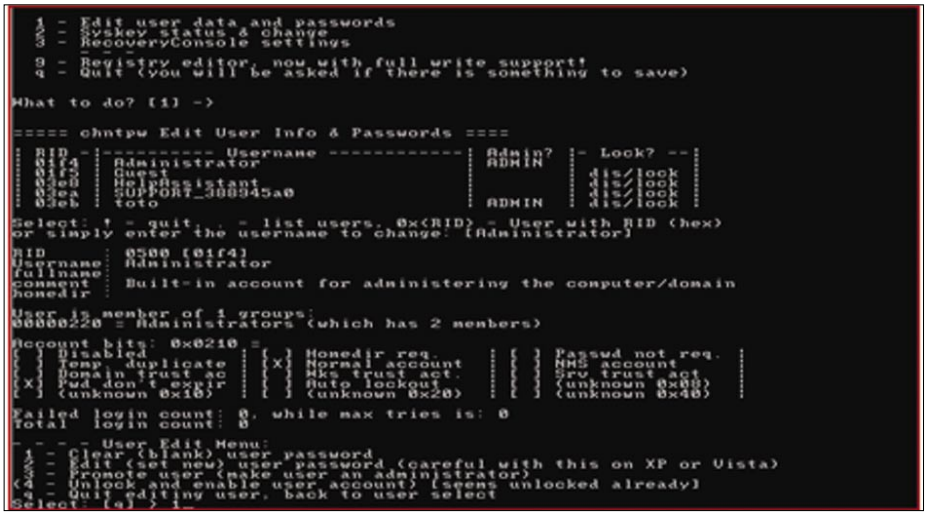

Figure 3. *Réinitialisation d'un compte administrateur local*

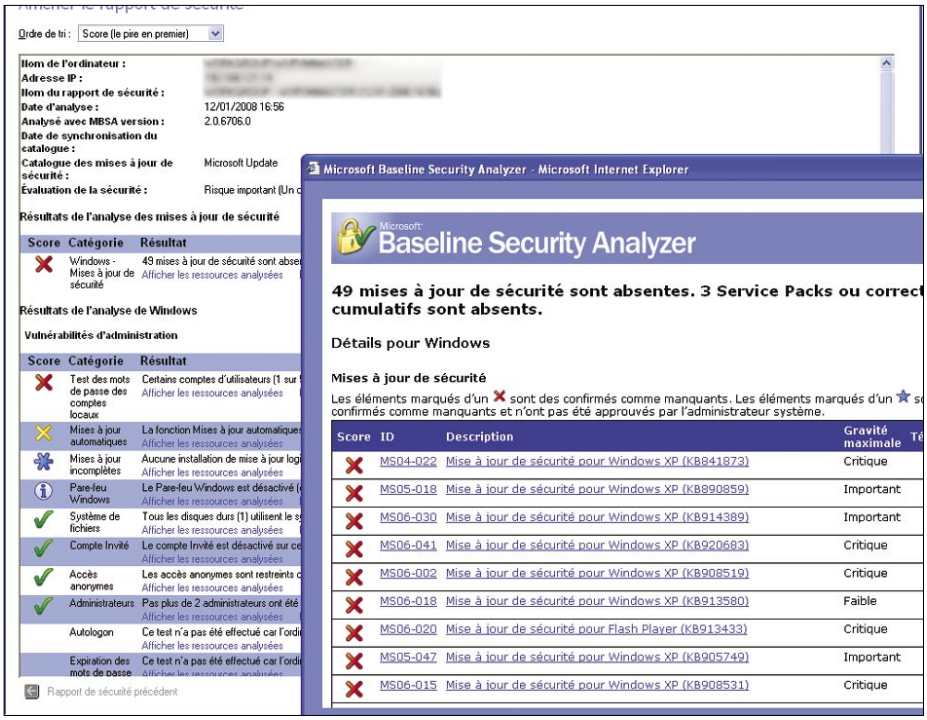

Figure 4. *Analyse du nomade avec MBSA*

ces utilisateurs. Il faut que les utilisateurs disposent de mots de passe d'au moins sept caractères avec des majuscules, minuscules, chiffres et/ou caractères spéciaux. Il faut également que ces mots de passe soient régulièrement changés et que l'utilisateur ne puisse pas réutiliser le même mot de passe plusieurs fois de suite.

Recherche des traces de l'infrastructure de l'entreprise

Après avoir pris la main sur la session administrateur local, l'attaquant recherche maintenant des traces laissées par le Système d'Information de l'entreprise. Pour les trouver, il n'a que l'embarras du choix : fichiers de journalisation d'évènements (application, système ou sécurité), fichiers de configuration…

Analyse des journaux d'évènements Windows

Pour simplifier la recherche d'informations, le mieux est d'exporter au format texte les fichiers d'évènements avec, par exemple, l'utilitaire dumpel de Microsoft :

```
dumpel.exe -l system -f log_
      system.txt -format ducs
dumpel.exe -l security -f log_
      security.txt -format ducs
dumpel.exe -l application -f log_
      application.txt -format ducs
```

Le Listing 2 représente un extrait du journal de sécurité. Voici les informations qui ressortent de ce dernier :

- le nom des domaines Active Directory présents sur le réseau de l'entreprise (ADDomaine et Domino),
- le nom des postes de travail qui se sont connectés à distance au nomade (PCAdmin),
- les utilisateurs qui se sont connectés à la station (en local ou à distance), dont les comptes administrateur (francky, admin1, marie).

Le Listing 3 représente un extrait du journal système. Voici les informations qui ressortent de ce dernier :

- les adresses IP utilisées sur le réseau de l'entreprise, ici avec l'erreur d'un renouvellement d'adresse DHCP (*192.16.100.163*),
- l'adresse IP du serveur DHCP (*192.168.0.1*),
- la liste des serveurs DNS de l'entreprise (ns.domaine.dom, *192.168.0.1* et *192.168.0.2*),
- le serveur NTP utilisé par les postes de travail (*SRVAD.ADdomaine.dom 192.168.0.1*).

Que peut faire un attaquant avec ces informations ? Grâce aux journaux d'évènements Windows, notre attaquant est en mesure de cartographier en partie le réseau interne. Il obtient ainsi une partie des noms des stations et des serveurs de l'entreprise (et donc, en conclure éventuellement le plan de nommage), le plan d'adressage interne (des serveurs et des postes de travail), le nom de certains

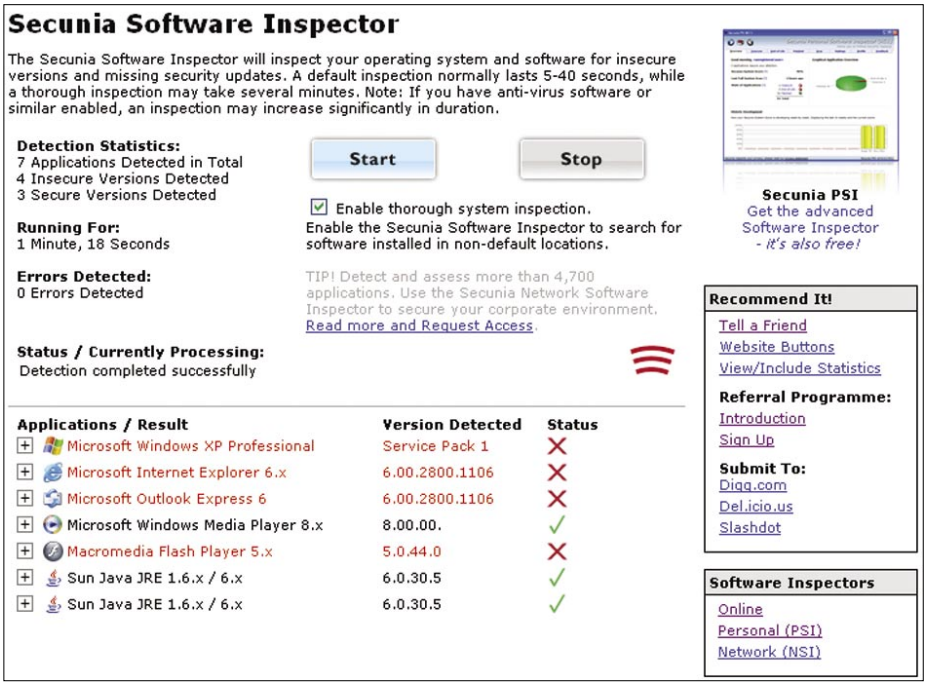

Figure 5. *Analyse en ligne avec Secunia Software Inspector*

Figure 6. *Logiciel Metasploit*

utilisateurs, etc… Toutes ces informations lui seront très utiles s'il parvient à disposer d'une connexion sur le réseau de l'entreprise (soit dans les locaux, soit à distance via le VPN de l'entreprise) : il sera à même de cibler les attaques vers les systèmes qu'il aura identifiés. Il disposera également d'une liste d'applications potentiellement vulnérables (par exemple, le service DNS de Microsoft avec la vulnérabilité MS07-029). Il paraît difficilement concevable pour une entreprise de supprimer les journaux d'évènements Microsoft. En effet, ces journaux permettent de trouver plus ou moins facilement l'origine de problèmes (applicatifs, systèmes ou réseaux). En cas d'investigation judiciaire, ils pourraient être demandés par le juge. Malheureusement, le chiffrement des fichiers n'est pas une solution ici. En effet, il est très difficile de chiffrer les fichiers système (et non les partitions), ces derniers devant être accessibles lors du démarrage de l'ordinateur, avant même que l'utilisateur ne se soit authentifié.

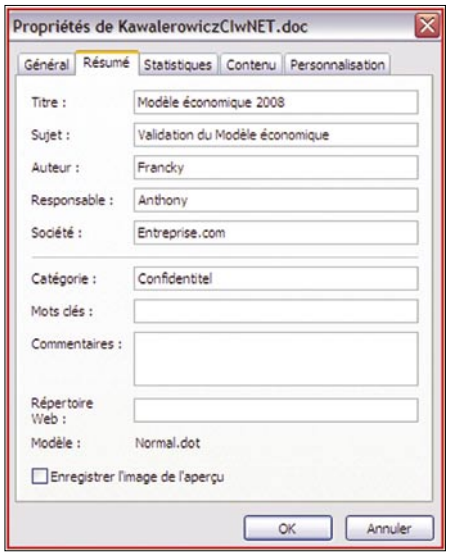

Figure 7. *Exemple de Meta donnée d'un fichier Word*

Analyse des journaux d'évènements ou de configuration des applications

Certains fichiers de log ou de configuration d'application contiennent des données très intéressantes. Un logiciel de filtrage d'URL, très renommé, lors de la première installation du logiciel se connecte à un serveur SQL. Constatez, après l'installation, que le fichier de log contient le mot de passe *SA* en clair utilisé par l'application.

L'analyse du fichier de journalisation du client antivirus local (Listing 4) fournit un second exemple. Le fichier *c:\windows\debug\netsetup.log* qui contient les informations d'adhésion aux domaines Active Directory ou aux Workgroups (Listing 5). Vous y retrouvez le ou les serveurs Active Directory ainsi que le compte qui a effectué l'adhésion au domaine.

Il est donc facile de trouver dans ces fichiers des informations telles que :

- des logins / noms d'employés / adresses e-mail,
- des mots de passe,
- des noms de serveurs et leurs adresses IP,
- des technologies / protocoles mis en place dans l'entreprise.

Que peut faire un attaquant avec ces informations ? L'attaquant se servira de ces données pour obtenir encore plus d'informations sur l'entreprise. Il pourra ainsi lancer des attaques ciblées contre l'entreprise et ses employés.

Deux solutions sont disponibles pour éviter la fuite d'informations via les logs des applications : soit régulièrement auditer les stations de travail pour supprimer ces fichiers, soit empêcher la personne malveillante d'accéder aux données en mettant en place une solution de chiffrement.

Analyse du fichier Host

Le fichier Host local contient les adresses IP et noms de domaine qui ne sont pas à résoudre par les serveurs DNS, ou qui ne pourraient pas l'être. Par exemple, pour accéder à des serveurs internes sans utiliser le service DNS (soit les adresses IP internes ne sont pas renseignées sur les DNS Internet, soit les flux Internet ne passent pas à l'intérieur du tunnel VPN).

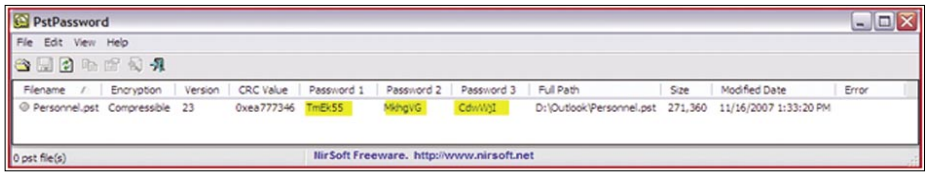

Figure 8. *Découverte du mot de passe protégeant une archive PST avec PstPassword*

Figure 9. *Découverte des clefs Wifi avec WirelessKeyView*

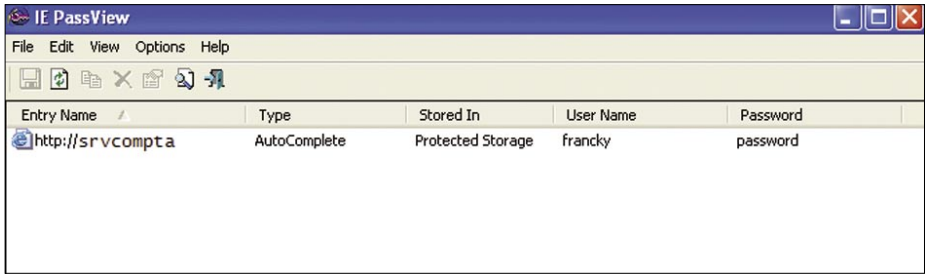

Figure 10. *Exportation des mots de passe préenregistrés dans Internet Explorer*

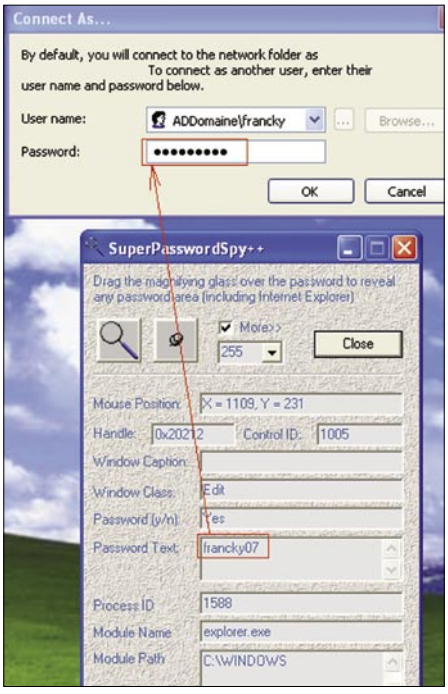

Figure 11. *Visualisation d'un mot de passe caché derrière des étoiles*

Le fichier *Host* se trouve à l'adresse : *C:\Windows\System32\drivers\etc\hosts*. Le Listing 6 montre un exemple de fichier *Host*.

Analyse de la table de routage

Il est possible que certaines entreprises indiquent en dur sur chaque nomade des routes statiques (sous Windows XP : `route -p add`). Cela permet d'obtenir une liste des réseaux internes à l'entreprise, ainsi que différentes passerelles par défaut.

Le Listing 7 montre l'exemple d'une table de routage avec des routes statiques. Cette table de routage indique que d'autres réseaux autres que le *192.168.x.x* sont disponibles dans l'entreprise, que les plages IP *10.100.10.x* et *10.10.10.x* sont également utilisées et que la passerelle par défaut de ces réseaux est : *192.168.100.10*.

Analyse des variables d'environnement

L'attaquant pourra se connecter aux différentes sessions Windows des utilisateurs qu'il a précédemment découvertes (utilisateur Active Directory en cache). Il lui est donc également possible d'obtenir la liste des variables d'environnement de chaque utilisateur. Le Listing 8 montre un extrait des variables d'environnement d'un utilisateur. Cet extrait des variables d'environnement indique clairement :

- le serveur Active Directory (SRVAD),
- le nom du domaine Active Directory (noms Netbios et FQDN).

Analyse des logiciels installés

L'analyse des différents programmes installés sur le nomade permettra à la personne malveillante de rechercher différents points d'accès au réseau de l'entreprise. Par exemple, si le pirate constate la présence du logiciel Acrobat Reader en version 7, il pourra envoyer un mailing aux employés en exploitant la vulnérabilité de type XSS affectant cette version. Pour rappel, cette vulnérabilité a été découverte en janvier 2007, elle permet à une personne d'exécuter sur le PC de la victime un JavaScript malveillant à partir d'un simple fichier PDF. Autre exemple : la présence d'un softphone installé sur le nomade trahira la présence d'un système de communication de VoIP interne. De même, un logiciel d'accès à distance, de type client VPN, pourrait être préconfiguré et ne demander aucune authentification supplémentaire à l'utilisateur (authentification basée sur un certificat installé dans le magasin local, basé sur le compte ActiveDirectory ou dont le mot de passe aurait été préenregistré

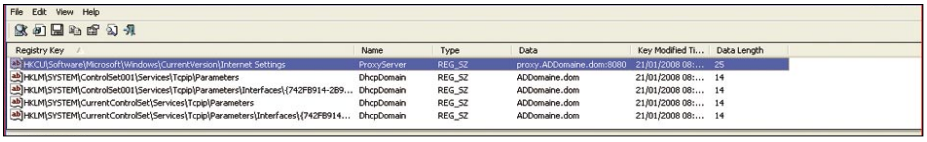

Figure 12. *Recherche de la chaîne ADDomaine.dom dans la base de registre*

Listing 4. *Exemple de log antivirus*

```
======================================================================
* Date Time:[20071030 11:05:36]
* Server Information:
 Server Name:[antivirus.domaine.dom] IP:[192.168.0.12] Port:[88]
* Client Information:
 Computer Name:[nomade] Port:[8888]
 Client IP:[192.168.100.163 ]
 GUID:[fE40fabf-4f70-4a2d-a36d-1ff66be56954]
* Action: Realtime Scan
* Result: Started.
======================================================================
* Date Time:[20071030 11:14:34]
* Server Information:
 Server Name:[antivirus.domaine.dom] IP:[192.168.0.12] Port:[88]
* Client Information:
 Computer Name:[nomade] Port:[8888]
 Client IP:[192.168.100.163 ]
 GUID:[fE40fabf-4f70-4a2d-a36d-1ff66be56954]
* Action: Realtime Scan
* Result: Stopped
======================================================================
```

Listing 5. *Extrait du fichier NetSetup.log*

```
10/31 15:52:40 NetpDoDomainJoin
10/31 15:52:40 NetpMachineValidToJoin: 'nomade'
10/31 15:52:40 NetpGetLsaPrimaryDomain: status: 0x0
10/31 15:52:40 NetpMachineValidToJoin: status: 0x0
10/31 15:52:40 NetpJoinDomain
10/31 15:52:40 Machine: nomade
10/31 15:52:40 Domain: ADDomaine
10/31 15:52:40 MachineAccountOU: (NULL)
10/31 15:52:40 Account: ADDomain\administrateur
10/31 15:52:40 Options: 0x25
10/31 15:52:40 OS Version: 5.1
10/31 15:52:40 Build number: 2600
10/31 15:52:40 ServicePack: Service Pack 2
10/31 15:52:40 NetpValidateName: checking to see if 'ADDomaine' is valid as type
      3 name
10/31 15:52:40 NetpCheckDomainNameIsValid [ Exists ] for 'ADDomaine' returned 0x0
10/31 15:52:40 NetpValidateName: name 'ADDomaine' is valid for type 3
10/31 15:52:40 NetpDsGetDcName: trying to find DC in domain 'ADDomaine', flags: 0x1020
10/31 15:52:40 NetpDsGetDcName: found DC '\\SRVAD' in the specified domain
10/31 15:52:40 NetpJoinDomain: status of connecting to dc '\\SRVAD': 0x0
```

Listing 6. *Exemple de fichier Host*

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
…
127.0.0.1 localhost
192.168.0.25 mail mail.ADdomaine.dom
192.168.0.80 intranet intranet.ADdomaine.dom
192.168.0.1 srvad srvad.ADdomaine.dom
```

par l'utilisateur). Pour réaliser l'inventaire des logiciels installés, il suffit d'utiliser un logiciel comme Aida32 ou Everest. Que peut faire un attaquant avec ces informations ? Après avoir analysé l'inventaire des logiciels installés sur le nomade (Listing 9), notre attaquant pourra envisager plusieurs possibilités d'attaque :

- le plugin flash player n'est pas à jour. L'attaquant pourra créer un site web malveillant mettant à disposition des utilisateurs une animation flash qui exploite la vulnérabilité de cette version. Il devra trouver un moyen pour que les employés de l'entreprise visitent son site Internet,
- le cas du client Acrobat Reader et celui de la connexion au VPN IPsec Netscreen ont été abordés précédemment,
- la présence du client Citrix Presentation Web indique que l'utilisateur a déjà eu l'occasion de se connecter à une ressource Citrix. L'attaquant recherchera donc la présence de service Citrix accessible à distance,
- la version des lecteurs QuickTime et VideoLan semble également être vulnérable aux récentes failles touchant le protocole RTSP (découverte respectivement fin 2007 et début 2008) qui permettraient à notre attaquant de prendre le contrôle du poste à distance.

Listing 7. *Exemple de table de routage*

```
C:\>route print
…
Itinéraires persistants :
   Adresse réseau Masque réseau Adresse passerelle Métrique
   192.168.0.0 255.255.255.0 192.168.100.254 1
   10.10.10.0 255.255.255.0 192.168.100.10 1
   10.100.10.0 255.255.255.0 192.168.100.10 1
```

Listing 8. *Extrait des variables d'environnement d'un utilisateur*

```
COMPUTERNAME=nomade
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\francky
LOGONSERVER=\\SRVAD
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\
      QuickTime\QTSystem\
QTJAVA=C:\Program Files\QuickTime\QTSystem\QTJava.zip
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\E6A68~1.BEA\LOCALS~1\Temp
USERDNSDOMAIN=domaine.dom
USERDOMAIN=ADDomaine
USERNAME=francky
USERPROFILE=C:\Documents and Settings\francky
windir=C:\WINDOWS
```

Listing 9. *Extrait de l'inventaire logiciel du nomade*

```
-------[ Programmes installés ]------------------------------------------------------
   Adobe Flash Player Plugin 8.0.22.0
   Adobe Reader 7.0 - Français [français (france)] 7.0
   Citrix Presentation Server Web Client for Win32 Inconnu
   FileZilla Client 3.0.1 3.0.1
   IZArc 3.81 3.81 Build 1550
   Java 2 Runtime Environment, SE v1.4.2_03 1.4.2_03
   Microsoft Office Enterprise 2003 12.0.4518.1014
   Mozilla Firefox (2.0.0.11) 2.0.0.11 (fr)
   Netscreen RemoteAccess 6.0.3
   QuickTime [français (france)] 7.2.0.240
   RealPlayer Inconnu
   Symentec Client Security 3.0.1
   VideoLAN VLC media player 0.8.6c 0.8.6c
```

Les entreprises souhaitant limiter l'impact que pourraient provoquer d'éventuelles failles de sécurité doivent en permanence déployer les mises à jour. Mais il s'agit d'un processus lourd qui demande énormément de ressources internes pour identifier, qualifer, valider et déployer à l'ensemble des parcs informatiques.

Analyse des mises à jour de sécurité des systèmes d'exploitation

Puisque le niveau de mise à jour est homogène dans la plupart des entreprises, nous en déduisons que la présence des mises à jour installées sur le nomade seront également installées sur les autres ordinateurs de l'entreprise. Inversement, il est très probable que l'absence de certaines mises à jour sur notre nomade se retrouve sur les autres ordinateurs. En effet, déployer des mises à jour de sécurité demande des efforts plus ou moins importants pour les entreprises : validations de bon fonctionnement de toutes les applications, tests de non-régression, mises à jour de la documentation… Microsoft a mis à disposition un outil très utile pour facilement découvrir les mises à jour nécessaires sur ses systèmes d'exploitation : MBSA (*Microsoft Baseline Security Analyzer*) – Figure 4 et Listing 10.

Toutefois, les mises à jour ne s'arrêtent pas à l'installation des patches Microsoft. Il faut également déployer les mises à jour des autres applications, telles que : JAVA, QuickTime, Acrobat Reader, RealPlayer, Flash, ShockWave. Pour faire le tour des différentes applications, la personne malveillante recherchera les applications installées dans le menu *ajout/suppression de programmes* et comparer avec la dernière version de l'éditeur, ou alors elle utilisera le logiciel d'analyse en ligne Secunia Software Inspector. Un attaquant obtiendra très facilement l'état de mise à jour du parc de l'entreprise. Il tentera de découvrir une vulnérabilité non corrigée et son exploitation probable. Il consultera ensuite les principaux sites Internet qui mettent à disposition des exploits, ou

il utilisera le *Framework metasploit* qui répertorie un certain nombre de scripts pouvant lui être utiles. Il est très important pour les entreprises de déployer les mises à jour de sécurité de leurs systèmes d'exploitation (aussi bien Microsoft que les autres) mais comme expliqué au chapitre précédent, il faut également installer les mises à jour des autres applications.

Analyse des données personnelles des utilisateurs locaux

Après avoir obtenu les identifiants de connexion des utilisateurs locaux, la personne malveillante fera l'inventaire de toutes les données personnelles présentes sur le nomade. Il inventoriera les fichiers bureautiques, les différentes réplications locales des boîtes de messagerie Outlook…

Analyse des fichiers bureautique

Les fichiers bureautiques contiennent des métadonnées qui sont exploitables par l'attaquant (Figure 7). Ce dernier trouvera facilement :

- les imprimantes,
- les URL où ont été stockés les fichiers sur les serveurs distants,
- les noms des créateurs et des différents auteurs.

Analyse des messageries utilisateur

Afin de pouvoir consulter les messageries sans être connecté au réseau de l'entreprise, Outlook intègre un cache des boîtes aux lettres. Un utilisateur, ou notre attaquant, aura accès à ces messages sans être connecté au serveur de messagerie interne. L'analyse des boîtes aux lettres des utilisateurs révélera à notre utilisateur :

- des adresses e-mail,
- des listes de diffusion,
- des noms, prénoms, coordonnées (dont les numéros de téléphone dans les signatures des messages)…

Analyse des réplications locales des messageries (archive)

Pour libérer de la place sur les serveurs de messagerie et conserver tous leurs messages, les utilisateurs archiveront les messages les plus anciens. Pour sécuriser ces archives (fichier **.pst*), ils peuvent les protéger par des mots de passe. Malheureusement, ces mots de passe procurent une fausse impression de sécurité. En effet, les mots de passe sur les archives pst sont facilement contournables. L'utilisation du logiciel *PstPassword* de l'éditeur NirSoft le prouve : la Figure 8 montre que le logiciel *PstPassword* a été capable de découvrir

Listing 10. *Analyse des mises à jour de sécurité manquantes avec MBSA*

```
C:\Program Files\Microsoft Baseline Security Analyzer 2>mbsacli.exe /n OS
Microsoft Baseline Security Analyzer
Version 2.0.1 (2.0.6706.0)
(C) Copyright 2002-2006 Microsoft Corporation. Tous droits réservés.
Analyse terminée.
Nom de l'ordinateur : ADDomaine\nomade
Adresse IP : 192.168.0.14
   Résultats de l'analyse des mises à jour de sécurité
   Catégorie : Windows - Mises à jour de sécurité
   Score : Le test a échoué (critique)
   Résultat : 48 mises à jour de sécurité sont absentes. 3 Service Packs
         ou correctifs cumulatifs sont absents.
Mises à jour de sécurité
MS04-022 | Manquant | Mise à jour de sécurité pour Windows XP (KB841873) | Critique |
MS05-018 | Manquant | Mise à jour de sécurité pour Windows XP (KB890859) | Important |
MS06-030 | Manquant | Mise à jour de sécurité pour Windows XP (KB914389) | Important |
MS06-041 | Manquant | Mise à jour de sécurité pour Windows XP (KB920683) | Critique |
MS06-002 | Manquant | Mise à jour de sécurité pour Windows XP (KB908519) | Critique |
MS06-018 | Manquant | Mise à jour de sécurité pour Windows XP (KB913580) | Faible |
MS05-047 | Manquant | Mise à jour de sécurité pour Windows XP (KB905749) | Important |
MS06-015 | Manquant | Mise à jour de sécurité pour Windows XP (KB908531) | Critique |
MS06-042 | Manquant | Mise à jour de sécurité cumulative pour IE6 SP1 (KB918899) |
      Critique |
MS06-001 | Manquant | Mise à jour de sécurité pour Windows XP (KB912919) | Critique |
MS05-049 | Manquant | Mise à jour de sécurité pour Windows XP (KB900725) | Important |
MS05-017 | Manquant | Mise à jour de sécurité pour Windows XP (KB892944) | Important |
MS06-051 | Manquant | Mise à jour de sécurité pour Windows XP (KB917422) | Critique |
MS06-057 | Manquant | Mise à jour de sécurité pour Windows XP (KB923191) | Critique |
MS05-036 | Manquant | Mise à jour de sécurité pour Windows XP (KB901214) | Critique |
MS06-032 | Manquant | Mise à jour de sécurité pour Windows XP (KB917953) | Important |
```

Listing 11. *En-tête SMTP d'un message électronique*

```
Received: from mx.entreprise.com (192.16.200.25) by smtp.entreprise.com
      (192.168.0.25) with Microsoft SMTPSVC(6.0.3790.3959);;
      Tue, 25 Sep 2007 19:36:46 +0200
Received: from smtp.expediteur.com (194.16.24.3) by barracuda.entreprise.com
      (192.168.200.102) with ESMTP id 3382F70035; Tue, 25 Sep 2007
      19:36:46 +0200
Received: from smtp.expediteur.com (unknown [10.10.0.1]) by
      mx.entreprise.com with ESMTP id 3382F70035 for
      <francky@entreprise.com>; Tue, 25 Sep 2007 19:39:37 +0200 (CEST)
X-MimeOLE: Produced By Microsoft Exchange V6.5
X-IronPort-AV: E=Sophos;i="4.24,287,1196636400";
      d="doc'145?scan'145,208,217,145";a="750902"
Content-Class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: multipart/related;
      boundary="----_=_NextPart_001_01C7FF9A.A3B1DE3A";
      type="multipart/alternative"
Subject: négociation de contrat
Date: Tue, 25 Sep 2007 19:36:42 +0200
Message-ID: <D2520599FC71E140B9B34A4A5F4CFE4E01826530@expediteur.com>
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: négociation de contrat
Thread-Index: Acf/mqMTSuq7E3OTS0aPc4t54Mq7yw==
From: contact <contact@expediteur.com>
To: <francky@entreprise.com>
Return-Path: contact@expediteur.com
```

trois mots de passe qui permettent d'ouvrir l'archive précédemment protégée.

Par ailleurs, c'est ce qui ne se voit pas du premier coup d'œil qui intéressera notre attaquant : les en-têtes des messages

```
[root @knoppix]# rifiuti /mnt/disk/RECYCLER/S-1-5-21-14544/1165-141/001333-725345543-1003/INFO2
INFO2 File: /mnt/disk/RECYCLER/S-1-5-21-1454471165-1417001333-725345543-1003/INFO2

INDEX   DELETED TIME    DRIVE NUMBER    PATH    SIZE
1       Mon Jan 21 00:32:01 2008        2       C:\Documents and Settings\toto\Desktop\liste des mots de passe.txt       4096
```

Figure 13. *Analyse de l'une des corbeilles locales avec l'outil Rifiuti*

Listing 12. *Contenu de la clef «Exécuter» de Windows*

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]
      "a"="mstsc /v SRVDRH\\1"
      "MRUList"="bcafkdihglje"
      "b"="cmd\\1"
      "c"="notepad\\1"
      "d"="calc\\1"
      "e"="\\\\ADDmaine\\ \\1"
      "f"="mstsc /console /v SRVCompta\\1"
      "g"="explorer\\1"
      "h"="ping 192.168.0.1 -t\\1"
      "i"="ping srvdocumentation\\1"
      "j"="ping 192.168.0.2\\1"
      "k"="ping 192.168.0.254\\1"
      "l"="\\\\SRVDocumentation\\1"
```

Listing 13. *Contenu de la clef indiquant les derniers fichiers ouverts*

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\
      OpenSavePidlMRU\doc]
"0"=hex:14,00,1f,50,e0,4f,d0,20,ea,3a,69,10,a2,d8,08,00,2b,30,30,9d,19,00,2f,\
      5a,3a,5c,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,54,00,31,\
…
"MRUListEx"=hex:09,00,00,00,08,00,00,00,07,00,00,00,06,00,00,00,05,00,00,00,04,\
      00,00,00,03,00,00,00,02,00,00,00,01,00,00,00,00,00,00,00,ff,ff,ff,ff
"1"=hex:a6,00,32,00,00,00,00,00,00,00,00,00,80,00,44,4f,53,53,49,45,52,20,44,\
      45,20,44,45,4d,41,4e,44,45,20,44,45,20,53,55,42,56,45,4e,54,49,4f,4e,2e,64,\
…
"2"=hex:14,00,1f,50,e0,4f,d0,20,ea,3a,69,10,a2,d8,08,00,2b,30,30,9d,19,00,2f,\
      5a,3a,5c,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,54,00,31,\
```

Listing 14. *Contenu de la clef indiquant les derniers montages réseau*

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network
      Drive MRU]
      "a"=\\\\192.168.0.1\\c$
      "b"="\\\\SRVDocumentation\\Private$"
      "c"="\\\\SRVDRH\\Fiches_Employes"
      "MRUList"="abc"
```

Listing 15. *Contenu des clefs indiquant les dernières recherches effectuées*

```
[HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru\5603]
      "000"="*.pst"
      "001"="Bulletin"
      "002"="password"
[HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMru\5604]
      "000"="password"
      "001"="Francky"
      "002"="mot de passe"
```

Listing 16. *Inventaire des fichiers effacés avec le kit d'analyse Sleuthkit*

```
#fls -f ntfs -ldr -o 63 -i raw /dev/hda > analyse.txt
r/r * 15337-128-1(realloc): Documents and Settings/francky/Cookies/toto@www.msn[1].txt
      2005.08.26 04:14:08 (MDT) 2007.09.07 08:00:49 (MDT) 2007.09.06 01:59:57
      (MDT) 68 0 0
r/- * 0: Documents and Settings/ francky /Desktop/Topologie réseau.vsd 0000.00.00 00:
      00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0000.00.00 00:00:00 (GMT) 0 0 0
r/r * 10148-128-1(realloc): Documents and Settings/ francky /Local Settings/Temporary
      Internet Files/Content.IE5/964IR6UM/pipe[1].gif 2008.01.16 08:45:54
      (MST) 2008.01.16 08:45:54 (MST) 2008.01.16 08:45:54 (MST) 43 0 0
…
```

SMTP. Ceux-ci lui révéleront partiellement ou intégralement l'architecture de messagerie interne. Le Listing 11 montre un exemple d'en-tête SMTP que la victime a reçu. L'attaquant peut en conclure les éléments suivants :

- il existe deux serveurs de messagerie : *smtp.entreprise.com* et *barracuda.entreprise.com*,
- le serveur *barracuda.entreprise.com* constitue probablement un relais anti-spam de type Barracuda Network,
- la présence d'un moteur antivirus sophos.

L'attaquant croisera ces informations avec d'autres messages pour obtenir les différentes versions des clients de messagerie utilisés au sein de l'entreprise, les adresses des serveurs de messagerie présents dans les autres filiales…

L'attaquant vérifiera si l'interface d'administration du relais antispam est accessible à partir d'Internet avec les mots de passe par défaut, et si la version installée est concernée par les dernières failles de sécurité présentes dans ce logiciel (injection de code via le composant *syslog*, attaque Cross Site Scripting…). Les informations contenues dans les en-têtes des messages *SMTP* sont très rarement nettoyées par les entreprises (aussi bien les messages entrant que sortant). Actuellement, peu de produits proposent l'anonymisation des messages électroniques. Une architecture qui fonctionne consiste à configurer, sur le dernier relais *SMTP*, un serveur postfix qui, en jouant avec les expressions régulières, réécrit les en-têtes des messages électroniques.

Recherche des données préenregistrées sur le système

Chaque utilisateur accumule dans l'ordinateur des informations personnelles qui pourraient être exploitées par notre attaquant. Il peut s'agir des documents qu'il a rédigés ou stockés sur le disque dur, des données enregistrées dans son profil (adresses internet consultées, mots de passe enregistrés, clef de connexion Wifi, etc.).

Découverte des clefs de connexion Wifi

L'éditeur NirSoft met à disposition l'outil *WirelessKeyView* qui permet d'exporter

les clefs Wifi préenregistrées (Figure 9). L'attaquant découvrira ainsi les clefs Wifi utilisées à l'intérieur de l'entreprise. Il pourra tenter une attaque de type WarDriving pour se connecter au réseau interne de l'entreprise via une borne Wifi. Afin de limiter l'effet de la découverte des clefs WEP ou WPA, les entreprises devraient interdire ces protocoles de connexion au profit du protocole *802.1x* permettant d'authentifier les utilisateurs. Si des accès de ce type sont encore implémenter, les entreprises devraient isoler le plus possible les réseaux wifi des autres ressources de l'entreprise.

Découverte des mots de passe préenregistrés dans le navigateur Internet

Beaucoup d'utilisateurs préenregistrent leurs mots de passe d'accès aux serveurs Internet ou Intranet. Notre attaquant pourra alors exporter la base des mots de passe soit en affichant ces derniers dans le menu adéquat de Firefox, soit en utilisan l'outil de NirSoft *IE PassView* (Figure 10). Ainsi, notre attaquant obtiendra facilement plusieurs couples login/mot de passe qu'il pourra exploiter.

Découverte des mots de passe cachés derrière des étoiles

Il est possible de découvrir les mots de passe préenregistrés et cachés par des étoiles. Un logiciel comme *SuperPasswordSpy++* (Figure 11) permet de visualiser facilement ces derniers. L'attaquant aura ainsi la possibilité de découvrir les mots de passe préenregistrés, le code PIN d'une éventuelle carte GPRS installé, etc.

Analyse des informations présentes dans la base de registre

La base de registre constitue une véritable ruche d'informations pour notre attaquant. L'outil de NirSoft *RegScanner* permet de rechercher une chaîne de caractères dans l'ensemble de la base de registre (Figure 12). Cette simple recherche a permis de découvrir la présence d'un proxy HTTP à l'intérieur de l'entreprise (*proxy.ADDomaine.dom*). Il est également possible de consulter directement certaines clefs de registres utiles. Par exemple, l'ensemble des commandes lancées par la fenêtre *exécuter* de Windows est stocké dans la clef suivante :

```
HKCU \Software\Microsoft\Windows\
     CurrentVersion\Explorer\RunMRU
```

Le Listing 12 montre le contenu de la clef Run pour l'un de nos utilisateurs ; y apparaît, par exemple que l'utilisateur a ouvert des sessions Terminal Server sur le serveur SRVCompta et SRVDRH.

Plusieurs clefs permettent d'obtenir des informations sur les fichiers récemment ouverts ou enregistrés :

```
HKCU \Software\Microsoft\Windows\
     CurrentVersion\Explorer\
     ComDlg32\OpenSaveMRU
HKCU \Software\Microsoft\Windows\
```

Tableau 1. *Synthèse des informations découvertes sur l'architecture interne de l'entreprise*

Nom du domaine Active Directory	ADDomaine (domaine.dom), Domino
Serveur DNS	192.168.0.1 et 192.168.0.2
Serveur DHCP	192.168.0.1
Serveur NTP	192.168.0.1
Plage d'adresse IP des utilisateurs	192.168.100.0/24, 10.10.10.0/24, 10.100.10.0/24
Login	Fancky, marie, bob, admin_support, administrateur
Serveur AntiVirus	Antivirus.domaine.dom (192.168.0.12) – Symantec AntiVirus AntiVirus de messagerie : Sophos
Serveur AntiSpam	mx.entreprise.com – 192.168.200.25
Serveur de messagerie	Mail.ADdomaine.dom – 192.168.0.25 mx.entreprise.com – 192.168.200.25
Adresses e-mail	Plusieurs adresses de messagerie trouvée lors de l'analyse des boîtes des utilisateurs
Serveur Intranet	Intranet.ADDomaine.dom – 192.168.0.80
Passerelle des postes de travail	192.168.100.254 et 192.168.100.10
Analyse applicative	Plusieurs logiciels ne sont pas à jour Il manque des mises à jour du système d'exploitation
Inventaire des clefs Wifi	Des clefs Wifi ont été découvertes
Mots de passe	Plusieurs mots de passe ont été découverts. Il s'agit de mots de passe Active Directory (découverts par BruteForce) ou de mots de passe applicatifs (découverts dans les données préenregistrées)
Fichiers sensibles	L'analyse des fichiers présents sur le disque et récemment supprimés a révélé plusieurs fichiers contenant des infirmations sensibles
Serveur Proxy	Proxy.ADDomaine.dom : 8080

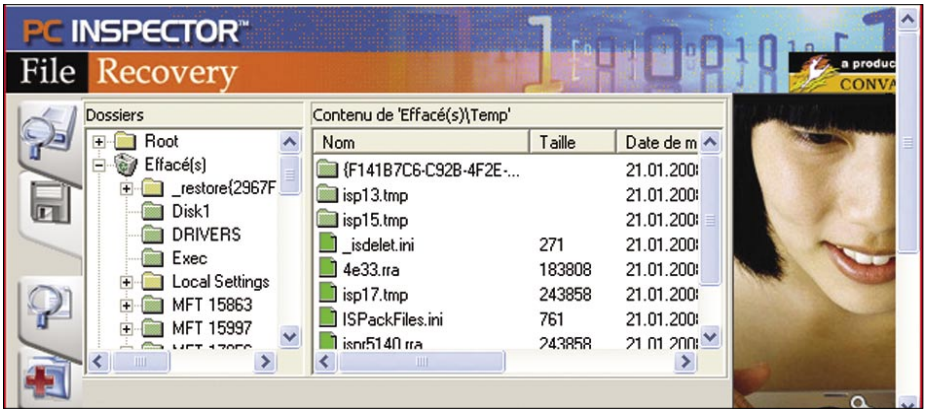

Figure 14. *Restauration de fichier avec File Recovery*

```
      CurrentVersion\Explorer\
      ComDlg32\LastVisitedMRU
HKCU\Software\Microsoft\Windows\
      CurrentVersion\Explorer\
      RecentDocs
```

Le Listing 13 indique le contenu de la clef de registre des derniers fichiers ouverts. Les données sont inscrites en hexadécimal. Il faut donc décoder la valeur des clefs pour obtenir les noms des fichiers. Les trois clefs de registre suivantes indiquent les dernières connexions réseau, le Listing 14 indique le contenu d'une de ces clefs :

```
HKLM \SYSTEM\MountedDevices
HKCU\Software\Microsoft\Windows\
      CurrentVersion\Explorer\
      MountPoints2\CPC\Volume
HKCU \Software\Microsoft\Windows\
      CurrentVersion\Explorer\
      Map Network Drive MRU
```

Il est également possible de visualiser les dernières recherches effectuées par des utilisateurs avec la fonction *Rechercher* de Windows, soit les noms des fichiers, soit le texte à l'intérieur des fichiers, en consultant les clefs suivantes (Listing 15) :

```
HKCU\Software\Microsoft\
      Search Assistant\ACMru\5603
HKCU \Software\Microsoft\
      Search Assistant\ACMru\5604
```

Analyse et restauration des données effacées

Après avoir réalisé toutes les opérations citées précédemment, notre attaquant va maintenant pouvoir restaurer la sauvegarde qu'il avait effectuée (voir le chapitre : duplication du média de stockage). En effet, s'il effectuait la recherche des fichiers effacés à ce stade, il trouverait moins d'informations intéressantes. Cela est dû au fait que toutes les opérations effectuées précédemment ont enregistré sur le disque dur des fichiers qui ont potentiellement pris la place de fichiers effacés. C'est pourquoi la restauration de la sauvegarde, effectuée en mode bit à bit (contenant les fichiers effacés), est si importante à cette étape.

Analyse des corbeilles des utilisateurs

La corbeille des utilisateurs locaux peut également apporter des informations à notre attaquant. L'une des nombreuses méthodes pour analyser la corbeille sans en altérer le contenu consiste à démarrer le nomade avec un LiveCD de Forensic (par exemple Helix) et d'utiliser l'outil *Rifiuti* (Figure 13).

Analyse des fichiers effacés

Un fichier, bien qu'effacé par l'utilisateur, ne disparaît pas réellement du disque dur. Inventorier les fichiers supprimés s'effectue avec le kit d'analyse post-mortem *Sleuthkit* (Listing 16). De même, il est possible de rechercher des bribes de fichiers dans les emplacements non alloués du disque dur avec `dls` et `srch _ strings`.

Restauration des fichiers effacés

Il existe des dizaines d'outils de restauration de fichiers, plus ou moins efficaces, suivant les situations, tels que File Recovery de PC Inspector, qui permet d'analyser et de récupérer facilement les fichiers effacés (Figure 14). Que peut faire un attaquant avec ces informations ? L'attaquant retrouvera facilement les fichiers effacés pouvant contenir des données confidentielles de l'entreprise ou des informations sur l'architecture du Système d'Information. Pour se protéger d'une telle attaque, la seule manière efficace consiste à chiffrer les partitions du nomade. De même, lorsque les nomades (postes fixes ou serveurs) arrivent en fin de vie, les disques durs devraient être effacés par surcharge (réécriture aléatoire de bit 0 et 1 au lieu d'un simple formatage), ce qui rendra plus difficile, et même impossible, la reconstruction des données effacées.

Conclusion

L'attaquant a, comme nous l'avons vu, de multiples possibilités pour attaquer l'entreprise. Il n'est maintenant limité que par son imagination et par ses compétences techniques :

- s'il dispose de connaissances pointues en matière de développement, il créera un virus adapté aux faiblesses de l'entreprise et de ses applications,
- s'il est bon menteur, il tentera une attaque de type social engineering en s'appuyant sur les noms, adresses de messagerie et téléphones qu'il a précédemment découverts,
- il disposera de suffisamment d'indications sur les ressources accessibles de l'extérieur pour tenter des attaques systèmes et/ou applicatives.

Comme nous l'avons présenté au fil de l'article, il n'existe pas de solution ultime qui permette de protéger une entreprise contre les fuites d'informations dues au vol ou à la perte d'un nomade. Toutefois, le chiffrement des données (des partitions et des fichiers) constitue un moyen d'empêcher la majorité des pirates d'accéder à celles-ci. De même, la mise à jour du système d'exploitation et des applications est une étape importante dans la protection des matériels mobiles, que les entreprises ne doivent jamais négliger.

Sur Internet

- *http://freshmeat.net/projects/dd_rhelp/* – Site officiel du projet freashmeat dd_rhelp,
- *http://www.remote-exploit.org/backtrack.html* – Site officiel du projet BackTrack,
- *http://www.openwall.com/john/* – Site officiel de John The Ripper,
- *http://ophcrack.sourceforge.net/* – Site officiel de Ophcrack,
- *http://www.lcpsoft.com/* – Site officiel de LCP,
- *http://www.oxid.it/cain.html* – Site officiel de Caïn & Abel,
- *http://home.eunet.no/%7Epnordahl/ntpasswd/* – Site officiel de Offline NT Password,
- *http://support.microsoft.com/kb/927229* – Outil Dumpel de Microsoft,
- *http://www.metasploit.com/* – Site officiel du projet Metaploit,
- *http://secunia.com/software_inspector/* – Lien vers Secunia Software Inspector,
- *http://www.nirsoft.net/* – Site internet de NirSoft,
- *http://www.e-fense.com/helix/* – Site internet du projet Helix,
- *http://www.sleuthkit.org/* – Site officiel du projet SleuthKit,
- *http://www.pcinspector.de/* – Site de l'éditeur du logiciel File Recovery.

Éric Beaulieu
L'auteur a travaillé pendant cinq ans en tant que Consultant en Sécurité des Systèmes d'Information dans une SSII parisienne. Il est maintenant Ingénieur réseau et sécurité pour une société développant des solutions technologiques intégrées dans la région de Bordeaux. Vous pouvez contacter l'auteur à l'adresse : *eric.beaulieu@gmail.com*.