Aide à l'utilisation de N.S.

http://code.google.com/p/omnia-projetcs/

V1.9c

Table des matières

1. Présentation

1.1. NS : Network Scanner

1.1.1. Introduction

NS : Network Scanner pour la recherche d'évidences ou d'éléments de configuration sur des machines du réseau.

Codé en langage C Win32 avec Codeblocks '(http://www.codeblocks.org/) et compilé avec MinGW (http://www.mingw.org/).

Licence : GPLv3

Librairies pour les connexions SSH : libgpg (http://www.gnupg.org/related_software/libgpg-error/), libgcrypt (http://www.gnu.org/software/libgcrypt/), libssh2 (http://www.libssh2.org) et zlib (http://www.zlib.net/).

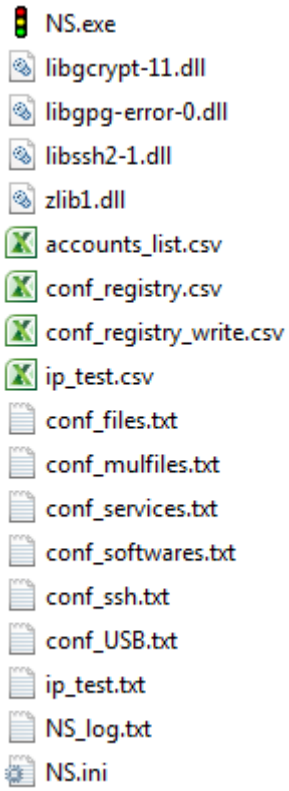
Sources de NS : http://code.google.com/p/omnia-projetcs/source/browse/#svn%2Ftrunk%2FNS

1.1.2. Objectifs

L'objectif de cet outil est de permettre la vérification sur un parc réseau de la présence d'éléments de configuration. Il peut donc être utilisé dans le cadre d'investigations sécurité ou d'actes d'administration sur des machines Microsoft Windows, Linux ou Mac.

1.1.3. Fichiers

L'application se compose des fichiers suivants :



NS.exe : représente le binaire de l'application à exécuté.

Les librairies en ***.dll** sont nécessaires et utilisées pour les connexions SSH.

accounts_list.csv : fichier d'exemple de liste de compte à charger.

Les fichiers **conf_*** représentent les fichiers utilisés pour configurer les tests à effectuer.

ip_test.txt, **ip_test.csv** : fichiers d'exemple de chargement d'IP pour expliciter les formats des IP pris en charge.

NS_log.txt : fichier de trace des activités. Ce fichier reporte les résultats positif de tous les tests configurables effectués.

NS.ini : fichier de configuration automatique permettant la mise en place de scan automatique lors de l'exécution de NS.exe.

1.1.4. Dépendances

Aucune dépendance externe hors des fichiers de l'application et des fichiers systèmes Microsoft natif requis (aucun service pack n'est nécessaire).
L'application est compatible et a été testée sur les environnements 32/64bits :

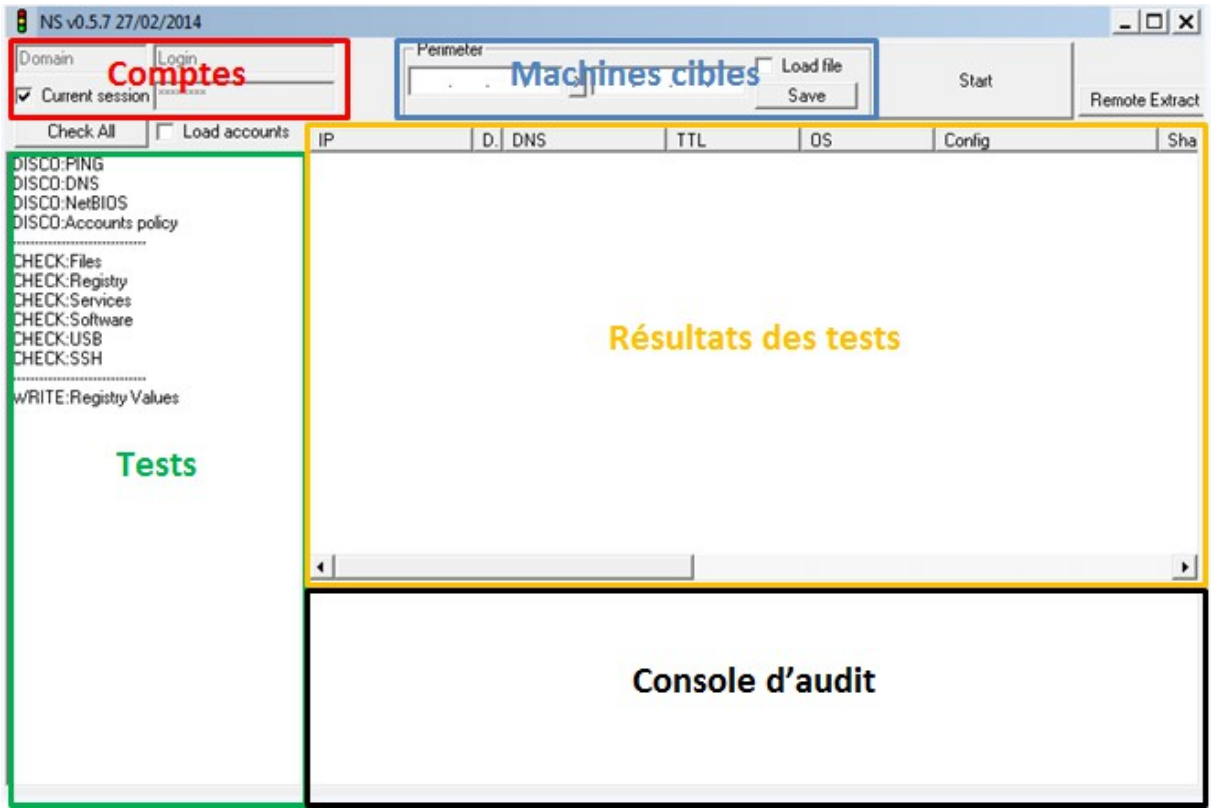
- Windows XP/2003
- Windows Vista/7/8/2008

1.2. Fonctionnalités

- Découverte de machines sur un réseau (IPv4), basé sur les protocoles ICMP, DNS et NetBios.
- Connexion à distance à la base de registre, au système de fichiers des machines et par NetBios afin de vérifier :
    - Le type de système d'exploitation et son service pack associé ;
    - Le domaine de la machine ;
    - La présence de session nulle (connexion autorisée à distance avec un compte et mot de passe qui sont vides) ;
    - La possibilité d'effectuer à distance une énumération de compte au travers d'une énumération des identifiants Windows uniques appelés SID ou Netbios.
    - La liste des partages réseaux accessibles ;
    - L'heure et la date du système distant ;
    - La liste des fichiers présents sur le système distant avec la date de dernière modification ainsi que les empreintes MD5 et SHA256 du fichier ;
    - La liste des clés, valeurs et données de registre présentes ;
    - La liste des services ainsi que la commande d'exécution du service ;
    - La liste des logiciels ainsi que le chemin et la date de dernière installation/mise à jour ;
    - La liste des clés USB déjà installées sur la machine ainsi que la date de dernière présence.

- La modification de valeurs de registre ;
- Export à distance de la base de registre et de fichiers ;
- L'exécution de commande au travers de connexions SSH ;
- La possibilité de se connecter à distance sur les machines à partir du compte courant, d'un compte définis, d'une liste de compte ou encore en session nulle ;
- Journalisation en temps réel des tests ;
- Export des résultats en XML, HTML, CSV et TXT.

1.3. Interface de l'application



2. Limitations

2.1. Connexion à distance

L'accès aux différentes machines du réseau à tester n'est possible que dans la mesure où aucun élément filtrant ne bloque la connexion entre la machine de test et les machines testées. En cas de pare-feu sur les machines à vérifier, il est nécessaire de le désactiver ou d'autoriser l'adresse IP de la machine effectuant les tests.

2.2. Connexion à distance à la base de registre

Pour que la connexion à la base de registre distance fonctionne il est nécessaire que le service d'accès à distance de la base de registre soit activé sur les machines à distance ainsi que sur la machine exécutant l'application (Le fonctionnement RPC Microsoft Windows se reposant sur le service local).

A partir de la version 0.5.7, en cas d'échec de connexion à la base, le service de registre à distance est démarré puis désactivé à la fin des tests si possible.

2.3. Droits d'exécution

L'application ne nécessite pas de droit d'administration locale pour fonctionner correctement.

2.4. Authentification par fichier

Attention en cas d'utilisation du fichier « CSV » contenant de multiple comptes et mots de passe. En cas de multiple mots de passe pour un même compte, en fonction des politiques de comptes sur la machines à distance, il est possible de verrouiller ce compte. Attention donc à ne pas mettre trop de mots de passes différents pour un même compte.

2.5. Limitation des données extraies

NS n'a pas pour objectif de permettre un relevé de configuration très long sur les machines à distance. Les retours des commandes sont limités à une taille de 16384 caractères par catégorie (registre, service, logiciel, USB, fichiers et SSH).

Exemple : 16384 pour une machine et pour les retours USB + 16384 pour les logiciels, etc.

3. Les différents modes d'authentification à distance

L'application s'authentifie au travers de canaux sécurisés RPC, les comptes et mots de passe utilisés ne sont pas transmis en clair sur le réseau.

3.1. Utilisation de l'utilisateur courant

Pour utiliser l'utilisateur courant pour tenter de s'authentifier, il est nécessaire de cocher la case « Current session » :

Remarque :

Certains cas de fonctionnement particuliers peuvent poser problème lors de l'authentification sur une machine à distance en utilisant la session de l'utilisateur courant. Il est donc fortement recommandé de saisir les éléments d'authentification comme décrit dans la section suivante « Utilisateur définis ».

Cette défaillance a notamment été détectée dans certains cas, de machine exécutant l'application sous Windows 7 vers une machine en Windows 7.

3.2. Utilisateur définis

Il est possible d'utiliser un domaine et un utilisateur différent de l'utilisateur courant en décochant la case « Current session » et en renseignant les champs suivants :

3.3. Liste d'utilisateurs

En cas de test sur un large réseau, il est toujours intéressant de pouvoir saisir plusieurs comptes pour se connecter par exemple à des machines hors du domaine.

Ces comptes devront avoir suffisamment de privilèges afin de pouvoir se connecter au registre à distance ou aux partages administratifs.

Attention :

Le chargement de compte est effectué à partir d'un fichier CSV ou les identifiants et mots de passe sont renseignés en **clair**. Il est possible d'ajouter dans la liste avancée des IP les identifiants et mots de passe.

Format du fichier :

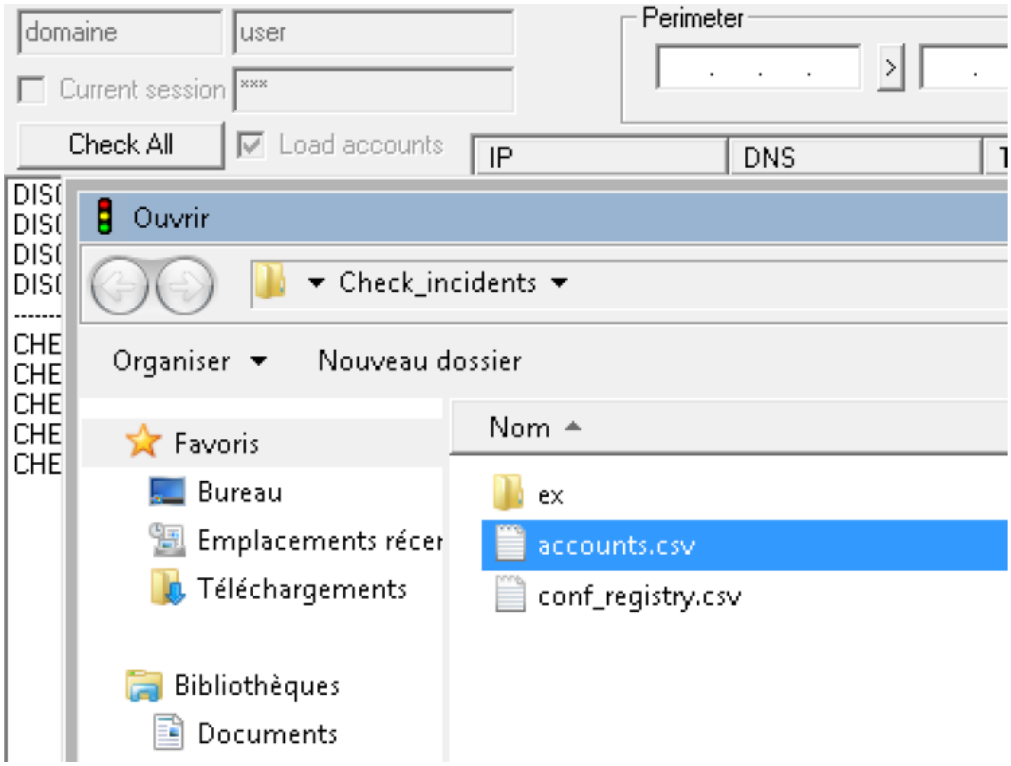
```
"Domaine";"Utilisateur";"Mot de passe";
"";"Utilisateur2";"Mot de passe";
```

Le premier paramètre correspond au domaine. En cas de connexion avec un compte local se paramètre n'est pas obligatoire.

Le second paramètre correspond au nom de l'utilisateur.

Le troisième paramètre est le mot de passe en clair.

Pour charger le fichier, il suffit de cocher la case « Load accounts » et de sélectionner un fichier au format CSV correspondant :



3.4. Traces de la réussite de l'authentification

Lorsque la découverte des machines est lancée, en cas d'authentification réussie pendant les différents tests, un message d'avertissement est généré dans la colonne « Config » ainsi que dans la console d'audit sous la forme :

[Date et heure] INFORMATION - Login (type de connexion) in <IP distante> IP with <login (id login)> account

Type de connexion :

- ScanReg:NET, correspond à une connexion réussie à la base de registre à distance au travers d'un accès au partage IPC$ de la machine à distance ;
- FileScan:NET, correspond à une connexion réussie au partage administratif décrit.
- Id login : correspond à l'ID commençant à 0 du compte présent dans le fichier CSV chargé en cas d'authentification avec une liste d'utilisateur.

Exemple :

En cas de réussite de l'authentification avec le compte « Utilisateur2 » du fichier :

```
"Domaine";"Utilisateur";"Mot de passe";
"";"Utilisateur2";"Mot de passe";
```

Nous aurons le message suivant en cas de détection :

[2013/11/30-14:00:00] LOGIN NET - with 192.168.0.1\Utilisateur2 (01) account

4. Utilisation

4.1. Découverte réseau

Les cibles de la découverte peuvent être configurées au travers de l'interface directe :

Ou en cochant la case « Load file » et en chargeant un fichier au format TXT ou CSV.

Exemple de format de fichier TXT autorisé :

```
10.10.0.1-10.10.0.2
10.11.0.0/24
10.12.1.4
nomdemachine
```

Exemple de format de fichier CSV autorisé :

```
"10.10.0.1-10.10.0.2";"réseau1";
"10.11.0.0/24";"réseau2";
"10.12.1.4";"réseau3";
"nomdemachine";"réseau4";
```

La seconde colonne représente un commentaire qui sera reporté dans la seconde colonne « DSC » visible sur l'interface.

Le nombre de machines ciblé est reporté dans la console d'audit lors du début de la découverte des machines.

Format avancé de fichier d'IP avec les identifiants et mots de passe :

Exemple de format de fichier CSV autorisé :

```
"#!";"10.10.0.1-10.10.0.2";"réseau1";"domaine";"utilisateur";"mdp";
"#!";"10.11.0.0/24";"réseau2";"domaine";"utilisateur";"mdp";
"#!";"10.12.1.4";"réseau3";"domaine";"utilisateur";"mdp";
"#!";"nomdemachine";"réseau2";"domaine";"utilisateur";"mdp";
```

La première colonne permet de définir le format du fichier.

4.2. Fichiers : Vérifier la présence d'un fichier

Le chargement de la liste des fichiers à vérifier est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_files.txt » qui doit être présent dans le même répertoire que l'application. Ce fichier est une simple liste de chemins de fichiers. Dans les chemins précisés, il ne faut pas préciser la lettre du lecteur. En effet, la totalité des lecteurs accessibles seront testés avec les fichiers. L'utilisation du caractère '%' permet de faire les recherches dans l'arborescence des fichiers et répertoires à la suite.

Une recherche spéciale est possible en utilisant le séparateur « : » utilisé en dernière ligne de l'exemple. Le premier paramètre correspond à la taille du fichier en octet (facultatif, peut être désactivé avec la valeur -1), le second l'empreinte MD5 (facultatif) et le dernier l'empreinte SHA256 (facultatif). Cette ligne commence et termine par un « : ».

Une seconde recherche spéciale permet des recherches de zones de texte dans un fichier texte (sans prise en compte de la casse). Il utilise le séparateur « ; ». Son premier paramètre ets le chemin du fichier et le second la chaîne à rechercher.

Le dernier format permet une recherche par mot dans le nom d'un fichier en utilisant en début de ligne le caractère « * ».

Exemple de format de fichier autorisé :

```
IO.SYS
WINDOWS\explorer.exe
\WINDOWS\toot.zc
Windows\%\test.txt
:8000:C124E332FE3F0E737B865EDA0E90D5BF:df8f250ac6dba58c81d7eb697bd6b2860aba020de47a0fcc5661b39026818495:
;Windows\System32\drivers\etc\hosts;127.0.0.1;
*.dll
```

Lors de la détection d'un fichier sur une machine, une trace est enregistrée dans la colonne « Files » ainsi que dans la console d'audit sous la forme :

```
[2013/11/30-14:00:00] FOUND (File) - \\192.168.0.1\C$\Windows\win.ini
[Last_modification:2013/11/30-
14:00:00,10o];MD5;C124E332FE3F0E737B865EDA0E90D5BF;SHA256;df8f250ac6dba58c81d7eb697bd6b28
60aba020de47a0fcc5661b39026818495
```

Un second fichier de recherche a été ajouté afin de permettre une recherche optimisée.

En effet, le premier format permet une recherche par fichier/chemin pour un nombre limité de fichier afin d'obtenir des performances correctes.

Pour une recherche systématique sur l'ensemble des lecteurs des machines, il est préférable d'utiliser le fichier «conf_mulfiles,txt ». Le format est identique au fichier « conf_files.txt ».

Dans le cas présent, la recherche s'effectuera sur tout le disque en vérifiant chacun des éléments. L'impact de performance de l'ajout d'un élément à tester est quasiment nul, mise à part pour les empreintes MD5/SHA256/SHA1 qui implique le calcul des empreintes de tous les fichiers présents.

La possibilité de vérifier les empreintes SHA1 (en remplacement de la vérification sha256) a été ajoutée en modifiant le fichier de configuration « NS.ini », voir dans la rubrique associée.

4.3. Registre : Vérifier la présence de clés ou de valeurs de registre

La liste des clés et valeurs à vérifier est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_registry.csv » qui doit être présent dans le même répertoire que l'application.

Exemple de format de fichier autorisé :

```
"Software\Microsoft\Windows\CurrentVersion\policies\Explorer\";"NoDriveTypeAutorun";
"";"DWORD";"Disable autorun = 255";"*";
```

- La première donnée représente la clé de registre à vérifier;
- La seconde, la valeur de registre à obtenir (non obligatoire) ;
- La troisième, les données attendues (non obligatoire) ;
- La quatrième, le format de donnée (DWORD et STRING autorisés, non obligatoire) ;
- La cinquième, la description de la clé (pour une meilleure lisibilité des résultats mais non obligatoire).
- Le dernier paramètre correspond au type de vérification à faire. Il accepte les formats suivants :
    - ***** aucune vérification de donnée ;
    - **?** pour les données de type STRING, permet de vérifier si la valeur contenu dans le troisième paramètre est contenu dans la donnée lue ;
    - **=** les données doivent être identiques ;
    - **!** les données doivent être différentes ;
    - **<** pour les données de type DWORD, permet de vérifier si la valeur contenu dans le troisième paramètre est inférieure à la donnée lue ;
    - **>** pour les données de type DWORD, permet de vérifier si la valeur contenu dans le troisième paramètre est supérieure à la donnée lue.

Lors de la détection d'une clé, une trace est enregistrée dans la colonne « Registry » ainsi que dans la console d'audit sous la forme :

```
[2013/11/30-14:00:00] FOUND (Registry) –
192.168.0.1\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutoru
n=0 (Disable autorun = 255)
```

Remarque :

La version actuelle ne permet pas de préciser la ruche lors des recherches de clés. Par défaut, les ruches suivantes sont vérifiées : `HKEY_LOCAL_MACHINE, HKEY_USERS et HKEY_CLASSES_ROOT.`

4.4. Service : Vérifier la présence d'un service

Le chargement de la liste des services à vérifier est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_services.txt » qui doit être présent dans le même répertoire que l'application. Ce fichier est une simple liste de nom ou description de service.

Exemple de format de fichier autorisé :

```
atapi
wmiapsrv
Google Update
```

Lors de la détection d'un service sur une machine, une trace est enregistrée dans la colonne « Services » ainsi que dans la console d'audit sous la forme :

```
[2013/11/30-14:00:00] FOUND (Service) –
192.168.0.1\SYSTEM\CurrentControlSet\Services\WmiApSrv\ImagePath=C:\WINDOWS\system32\wbem
\wmiapsrv.exe wmiapsrv
```

4.5. Software : Vérifier la présence d'un logiciel

Le chargement de la liste des logiciels à vérifier est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_softwares.txt » qui doit être présent dans le même répertoire que l'application. Ce fichier est une simple liste de nom de logiciels.

Exemple de format de fichier autorisé :

```
7-Zip
Notepad++
```

Lors de la détection d'un logiciel sur une machine, une trace est enregistrée dans la colonne « Softwares » ainsi que dans la console d'audit sous la forme :

```
[2013/11/30-14:00:00] FOUND (Software) –
192.168.0.1\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\7-
Zip\UninstallString="C:\Program Files (x86)\7-Zip\Uninstall.exe" (Last Write Time
2013/11/30-14:00:00) 7-zip
```

4.6. USB : Vérifier la présence de trace de l'utilisation de tout périphérique de stockage USB

Le chargement de la liste des périphériques USB à vérifier est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_USB.txt » qui doit être présent dans le même répertoire que l'application. Ce fichier est une simple liste d'ID ou de description de périphérique de clés de registre qui peuvent être obtenues dans la base de registre aux chemins :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\<description périphérique>\<ID>

Exemple de format de fichier autorisé :

```
CdRom&Ven_BUFFALO&Prod_Virtual_Cdrom&Rev_0.82
0010100704075C350&1
```

Lors de la détection d'un périphérique USB sur une machine, une trace est enregistrée dans la colonne « USB » ainsi que dans la console d'audit sous la forme :

[2013/11/30-14:00:00] FOUND (USB) – 192.168.0.1\SYSTEM\CurrentControlSet\Enum\USBSTOR\CdRom&Ven_BUFFALO&Prod_Virtual_Cdrom&Rev_0.82\0010100704075C350&1 (Last Write Time 2013/11/30-14:00:00)

4.7. Tests d'extraction

Depuis la version 0.5.7, il est possible d'effectuer une extraction de configuration sur plusieurs machines à distance.

La phase de découverte prend en compte la découverte par requêtes ICMP et requêtes DNS. Le système d'exploitation est récupéré si possible au travers de la connexion à la base de registre à distance et SSH.

Les tests présents sont :

- Extraction des ruches de base de registre : HKEY_LOCAL_MACHINE SOFTWARE et SYSTEM, ainsi que HKEY_USERS sous forme de fichier CSV ;
- Copie des fichiers détaillés dans le fichier « conf_files.txt » ;
- Sauvegarde du résultat des tests en CSV et XML.
- Commandes SSH (sans limite de retour).

4.8. Automatisation de test

Depuis la version 0.4.13, il est possible d'effectuer des tests automatiques en créant un fichier « NS.ini » dans le répertoire de l'application.

Exemple de format de fichier autorisé :

```
[SCAN]
IP_FILE="fichier_ip.txt"
ACCOUNT_FILE="accounts.csv"
TYPE="DISABLE"
DISCO_ICMP="YES"
DISCO_DNS="YES"
DNS_DISCOVERY="NO"
SHA1_ONLY="NO"
NO_HASH_CHECK="NO"
DISCO_NETBIOS="YES"
DISCO_NETBIOS_POLICY="YES"
DISCO_NETBIOS_USERS="YES"
DISCO_CHECK_FILES="YES"
DISCO_CHECK_REGISTRY="YES"
DISCO_CHECK_SERVICES="YES"
DISCO_CHECK_SOFTWARE="YES"
DISCO_CHECK_USB="YES"
DISCO_CHECK_SSH="YES"
DISCO_WRITE_KEY="YES"

[LOG]
LOG="ENABLE"

[SAVE]
CSV="OK"
XML="OK"
HTML="OK"

[CHECK]
M_SEC="OK"
WSUS_WORKS="OK"
PATCH_UPDATED="OK"
MCAFEE_INSTALLED="OK"
MCAFEE_UPDATED="OK"
MCAFEE_SCAN="OK"
PASSWORD_POLICY="OK"
ADMIN_ACOUNT="OK"
NULL_SESSION="OK"
REVERS_SID="OK"
AUTORUN="OK"
SHARE_ACCESS="OK"
DISCO_NETBIOS_USERS="NO"
DISCO_CHECK_SSH="NO"

[CHECK_OPTIONS]
MSEC_REG_PATH=""
MSEC_REG_VALUE=""
MCAFEE_UPDATE_DAYS_INTERVAL="5"
MCAFEE_SCAN_DAYS_INTERVAL="7"
ADMIN_ACOUNT="administrator"
PASSWORD_POLICY_MIN_AGE="1"
PASSWORD_POLICY_MAX_AGE="90"
PASSWORD_POLICY_MIN_LEN="7"
PASSWORD_POLICY_LOCKOUT_COUNT="5"
PASSWORD_POLICY_COMPLEXITY_ENABLE="OK"
PASSWORD_POLICY_HISTORY="10"
```

4.8.1. Section du fichier NS.ini [SCAN]

La section « **[SCAN]** » correspond aux différents éléments de configuration initiale.

- **IP_FILE:** fichier au format TXT comprenant la liste des adresses IP, intervalles IP ou noms de machines à cibler.
- **ACCOUNT_FILE** : fichier au format CSV à prendre en compte pour s'authentifier sur les machines à tester.
- **TYPE** : peut prendre trois valeurs différentes :
  - *AUTO* : exécution des tests configurés dans les parties « [CHECK] » et « [CHECK_OPTIONS] » en sauvegardant les résultats à la fin en fonction des formats activés dans « [SAVE] ».
  - *SIMPLE* : ce mode permet de prendre en compte la liste des paramètres en DISCO_* qui correspondent aux différents tests à activer et de lancer les tests dés l'exécution du programme.
  - MANUAL : ce mode permet de sélectionner l'ensemble des tests sans lancer le scan.
  - *DISABLE* : mode de test automatique désactivé.
- **DISCO_*** : représente pour le scan de type « SIMPLE » la liste des tests à activer.
- **DNS_DISCOVERY** : par défaut l'ICMP et la résolution DNS sont utilisés pour découvrir des machines. Pour désactiver la résolution DNS comme moyen de détection tout en gardant la résolution DNS de chaque IP, il suffit de mettre se paramètre à « NO ».
- **SHA1_ONLY** : si activée, cette option désactiver la gestion des empreintes SHA256 pour utiliser les empreintes SHA1.
- **NO_HASH_CHECK** : si YES, désactive la génération d'empreintes MD5 et SHA1/SHA256.

4.8.2. Section du fichier NS.ini [SAVE]

La section « **[SAVE]** » permet de spécifier quel format de sauvegarde doit être utilisé en cas de type de test « AUTO » configuré dans la section « [SCAN] ».

Les type de réponse autorisées pour les formats sont :

- YES : sauvegarde dans le format activée
- NO : format désactivé

4.8.3. Section du fichier NS.ini [CHECK]

Cette section permet d'activer les tests à effectuer en cas de sélection du type de test en « AUTO ».

Les paramètres suivant peuvent être activés avec la valeur OK :

- **M_SEC** : permet de vérifier la présence d'une valeur de clé de registre dans la ruche HKEY_LOCAL_MACHINE de la machine à distance.

  Le chemin et la valeur dans la ruche peuvent être configurés dans la section « [CHECK_OPTIONS] » avec les paramètres MSEC_REG_PATH et MSEC_REG_VALUE.
- **WSUS_WORKS** : vérifier si un serveur de mise à jour WSUS est configuré sur la machine et fonctionne.
- **PATCH_UPDATED** : vérifier que la machine est à jour depuis moins d'un mois.
- **MCAFEE_INSTALLED** : vérifier si l'Antivirus McAfee est installé sur la machine.
- **MCAFEE_UPDATED** : vérifier que l'Antivirus McAfee est à jour depuis moins de X jours. Le

nombre de jours de référence est configurée dans dans la section « [CHECK_OPTIONS] » avec le paramètre MCAFEE_UPDATE_DAYS_INTERVAL.

- **MCAFEE_SCAN** : vérifier qu'un test total de la machine avec l'Antivirus McAfee a été fait depuis moins de X jours. Le nombre de jours de référence est configurée dans dans la section « [CHECK_OPTIONS] » avec le paramètre MCAFEE_SCAN_DAYS_INTERVAL.
- **PASSWORD_POLICY** : permet la vérification de conformité avec la politique de gestion des comptes. La configuration peut être effectuée dans la section « [CHECK_OPTIONS] » avec les paramètres PASSWORD_POLICY_*.
- **ADMIN_ACOUNT** : vérifier la présence d'un compte sur la machine. Le compte à vérifier peut être configuré dans la section « [CHECK_OPTIONS] » avec le paramètre ADMIN_ACOUNT.
- **NULL_SESSION** : vérifier la présence de session nulle (authentification avec identifiant et mots de passe nuls) sur la machine.
- **REVERS_SID** : possibilité d'énumérer les comptes des utilisateurs sans être authentifier sur la machine.
- **AUTORUN** : vérifier que l'exécution automatique de programme lors de l'insertion dans la machine de supports externe est bien désactivé (CDROM, clé USB, etc.).
- **SHARE_ACCESS** : extraire la liste des partages réseaux accessibles sans authentification.
- **DISCO_NETBIOS_USER** : extraire la liste utilisateurs (Revers SID ou Netbios).
- **DISCO_CHECK_SSH** : exécution de commandes SSH.

4.8.4. Section du fichier NS.ini [CHECK_OPTIONS]

Cette section détail les éléments de configuration exploités par l'activation des tests de la section « [CHECK] ».

Vérifier la présence d'une valeur de registre. Ici HKLM\Software\test :

```
MSEC_REG_PATH="SOFTWARE\"
MSEC_REG_VALUE="test"
```

Verifier la configuration de l'Antivirus McAfee :

```
MCAFEE_UPDATE_DAYS_INTERVAL="5"
MCAFEE_SCAN_DAYS_INTERVAL="7"
```

Vérifier la politique de sécurité des mots de passe :

```
PASSWORD_POLICY_MIN_AGE="1"
PASSWORD_POLICY_MAX_AGE="90"
PASSWORD_POLICY_MIN_LEN="7"
PASSWORD_POLICY_LOCKOUT_COUNT="5"
PASSWORD_POLICY_COMPLEXITY_ENABLE="OK"
PASSWORD_POLICY_HISTORY="10"
MCAFEE_SCAN_DAYS_INTERVAL="7"
```

Vérifier la présence du compte (ici administrator) :

```
ADMIN_ACOUNT="administrator"
```

5. Modification de la configuration à distance

5.1. Registre : Modification de valeur de registre

L'application est prévue pour permettre la modification ou création de valeur de registre à distance.

La liste des valeurs à écrire est chargée automatique lors du démarrage des tests.

Il est effectué au travers du fichier « conf_registry_write.csv » qui doit être présent dans le même répertoire que l'application.

Exemple de format de fichier autorisé :

```
"SOFTWARE\Microsoft\Windows
NT\CurrentVersion\";"valeur";"données";"STRING";"HKLM";"valeure attendue";"*";
```

- La première, donnée représente la clé de registre à vérifier;
- La seconde, la valeur de registre ou écrire ;
- La troisième, les données à écrire ;
- La quatrième, le format de donnée (DWORD et STRING autorisés) ;
- La cinquième, la ruche de registre impactée. Les différents formats pris en compte :
  - **HKLM pour HKEY_LOCAL_MACHINE**
  - **HKU pour HKEY_USERS**
  - **HKCR pour HKEY_CLASSES_ROOT**
- Le sixième paramètre correspond au contenu de la donnée actuelle attendu vis à vis des opérateurs du septième paramètre.
- Le septième paramètre correspond au type de vérification à faire. Il accepte les formats suivants :
  - ***** aucune vérification ;
  - **?** pour les données de type STRING, permet de vérifier si la valeur contenu dans le sixième paramètre est contenu dans la donnée actuelle ;
  - **=** les données doivent être identiques ;
  - **!** les données doivent être différentes ;
  - **<** pour les données de type DWORD, permet de vérifier si la valeur contenu dans le sixième paramètre est inférieure à la donnée actuelle;
  - **>** pour les données de type DWORD, permet de vérifier si la valeur contenu dans le sixième paramètre est supérieure à la donnée actuelle.

Lorsque l'écriture d'une valeur est réussie, une trace est enregistrée dans la console d'audit sous la forme :

```
[2013/11/30-14:00:00] WRITE (Registry) - 192.168.0.1\HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\valeur(STRING)=données
```

Attention:

Dans le cas ou le chemin d'accès à la valeur de registre n'existe pas, il est créé.

5.2. SSH : exécution de commandes

Un module SSH est présent dans l'application au travers des DLL libgcrypt, libgpg, libssh2 et zlib.

Il permet l'exécution de commandes au travers de connexion SSH avec identifiant et mot de passe.

Les commandes à exécuter doivent être présentes (une commande par ligne) dans le fichier « conf_ssh.txt » qui doit être présent dans le même répertoire que l'application.

Exemple de format de fichier autorisé :

```
uname -a
ifconfig -a
```

Lorsque l'écriture d'une valeur est réussie, une trace est enregistrée dans la console d'audit sous la forme (en cas de réponse très importante, elle peut être divisée sur plusieurs lignes) :

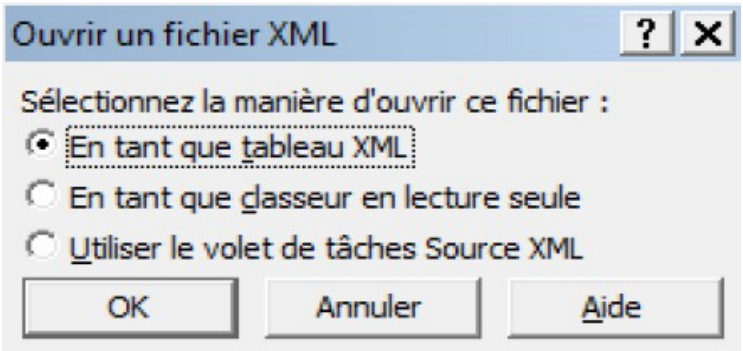
```
[2013/11/30-14:00:00] FOUND (SSH) [192.168.0.1\\uname -arv] Linux proxysvr 2.6.18
```

6. Export des résultats

L'export des résultats (bouton « Save ») peut être effectué pendant ou après les tests aux formats CSV, XML et HTML.

Le format CSV peut être ouvert par les tableurs autorisant les données comprenant des retours à la ligne (comme LibreOffice) avec comme séparateur le point-virgule et les guillemets comme délimiteur de texte (Microsoft Excel ne charge pas correctement ces fichiers).

Le format XML peut être ouvert par les tableurs en tant que tableau XML (Excel) :



Par défaut, un fichier d'audit des actions (Contenu de la console d'audit) est généré dans le répertoire de l'application sous forme texte « NS_log.txt ». Même en cas de plantage, ce fichier est accessible et écrit, étant généré en temps réel.

Ce document contient les heures et résultats obtenus ainsi que les éléments statistiques globaux tels que :

- Le nombre de machine accessible.
- Le nombre de machine autorisant les connexions à la base de registre ou au système de fichier à distance.
- Le nombre de machine sous un système d'exploitation Microsoft Windows.