Aide à l'utilisation de N.S.

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

V1.2

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/) et libssh2 (http://www.libssh2.org).

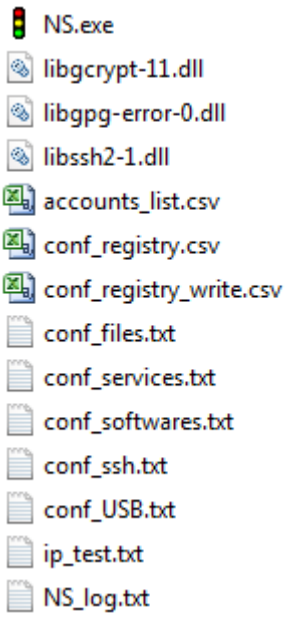
Sources de NS : http://code.google.com/p/omnia-projetcs/source/browse/#svn%2Ftrunk%2FNS

1.1.2. Objectifs

L'objectif de cet outil est de permettre de vérifier sur un parc réseau la présence d'éléments de configuration. Il peut donc être utilisé dans le cadre d'investigations sécurité ou d'actes d'administration.

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 : fichier d'exemple de chargement d'IP pour expliciter les formats des IP pris en comptes.

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

1.1.4. Dépendances

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

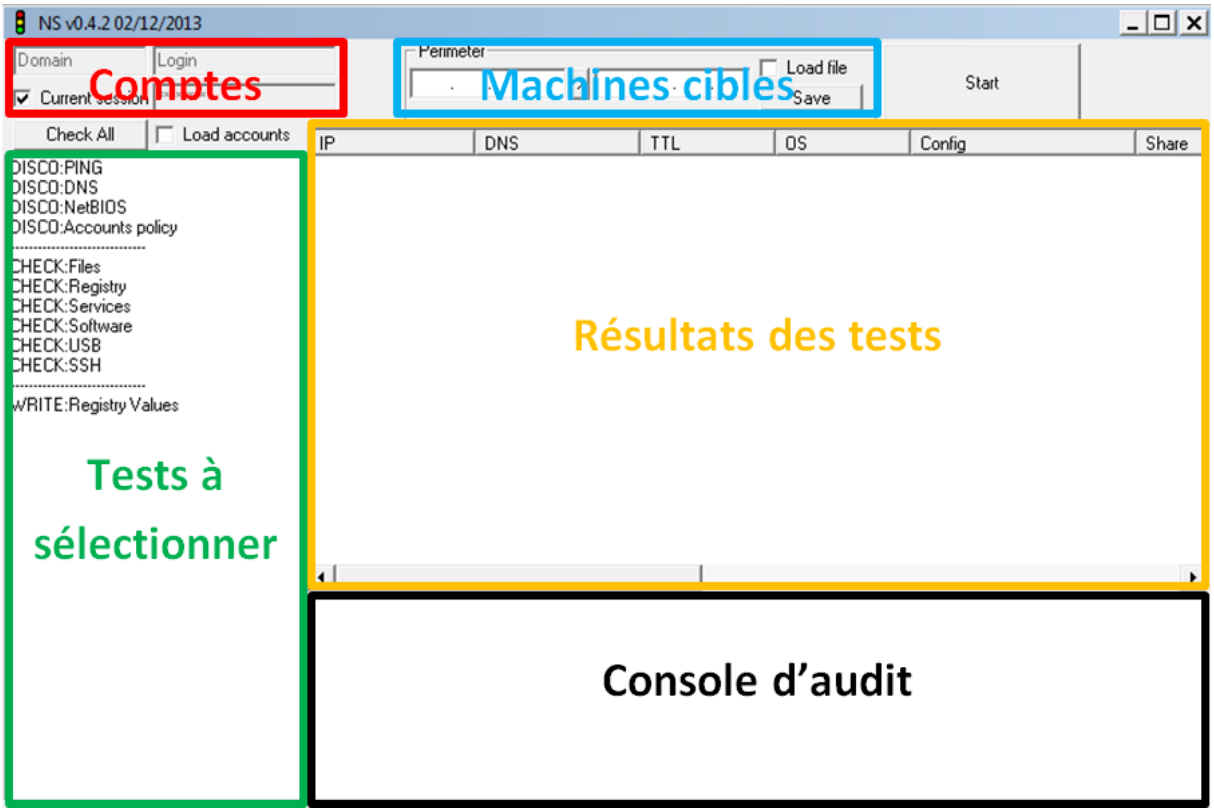
- Windows XP/2003
- Windows Vista/7/8/2008 32/64bits

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 et au système de fichier des machines et *via* 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 vides) ;
    - La possibilité d'effectuer à distance une énumération de compte au travers d'une énumération des SID.
    - 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 et date de dernière présence.

- La modification de valeurs de registre.
- 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, ou d'une liste de compte ;
- Journalisation en temps réel des tests ;
- Export des résultats en XML, HTML et CSV

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.

2.3. Droits d'exécution

L'application ne nécessite pas les droits d'administration locale pour fonctionner correctement.

2.4. Authentification par fichier

Attention en cas d'utilisation du fichier « CSV » contenant de multiples comptes et mots de passes. En cas de multiples mots de passes pour un même compte, en fonction des politiques de comptes locales 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 de commandes sont limités à une taille de 16384 caractères par catégorie (registre, services, logiciels, 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 en cas de certaine 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 pour 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.

Format du fichier :

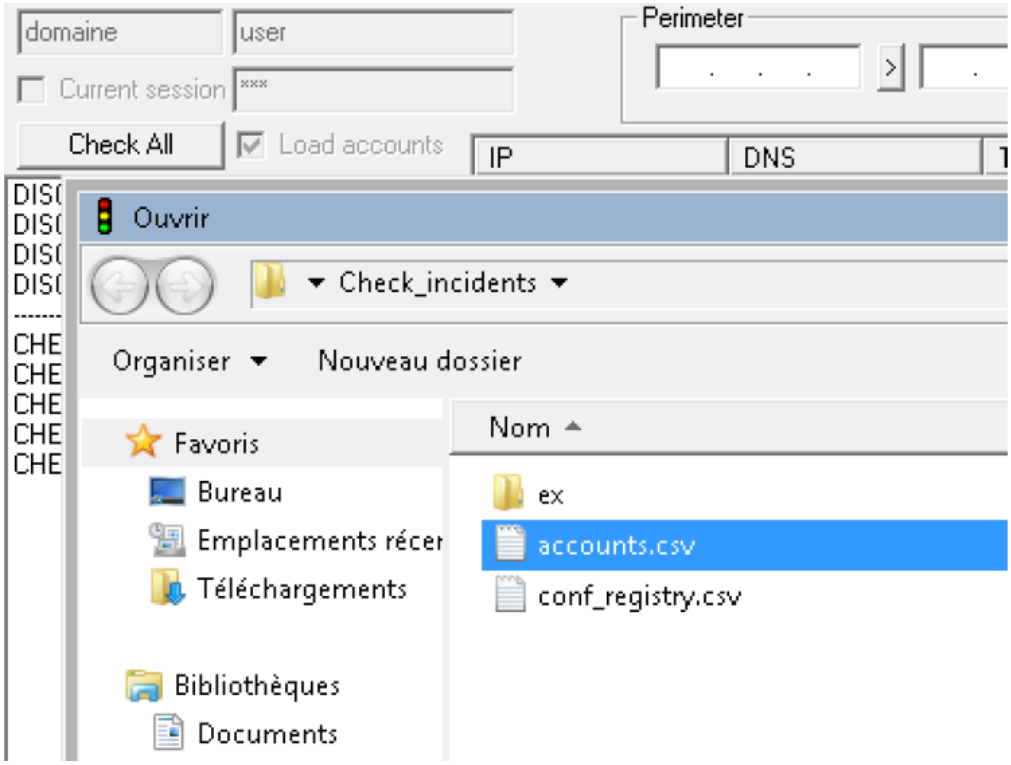
```
"Domaine";"Utilisateur";"Mot de passe";
"";"Utilisateur2";"Mot de passe";
```

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 via 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] INFORMATION - Login (ScanReg:NET) in 192.168.0.1 IP 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.

Exemple de format de fichier autorisé :

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

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

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.

Exemple de format de fichier autorisé :

```
IO.SYS
WINDOWS\explorer.exe
\WINDOWS\toot.zc
```

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];MD5;C124E332FE3F0E737B865EDA0E90D5BF;SHA256;df8f2
50ac6dba58c81d7eb697bd6b2860aba020de47a0fcc5661b39026818495
```

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

La liste des clés et valeurs à vérifiées 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\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=0
(Password complexity)
```

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 de service ou description.

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. Service : 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\Uninsta
llString="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 nom 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)

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 et libssh2.

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

Les commandes à exécutée 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 :

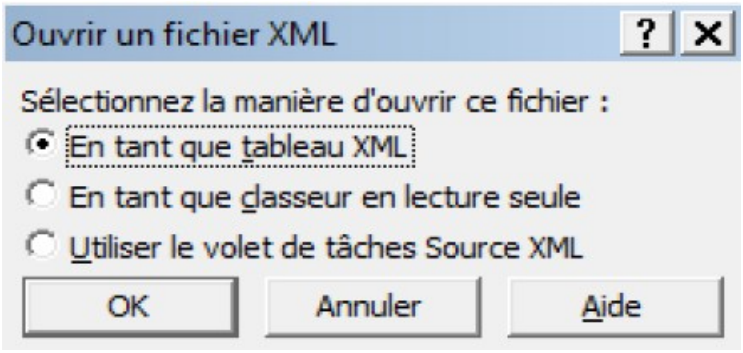
```
[2013/11/30-14:00:00] FOUND (SSH) [192.168.0.1\\uname -arv] Linux proxysvr 2.6.18
```

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.

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, 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.