Help to use N.S.

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

V1.8

Table of contents

1. Presentation

1.1. NS : Network Scanner

1.1.1. Introduction

NS : Network Scanner, Network Tools search for evidence and configuration items.

Coded in C/Win32 language with Codeblocks '(http://www.codeblocks.org/) and compiled with MinGW (http://www.mingw.org/).

License: GPLv3

For SSH connections: 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 of NS : http://code.google.com/p/omnia-projetcs/source/browse/#svn%2Ftrunk%2FNS

1.1.2. Goals

The purpose of this tool is to enable verification on a network fleet the presence of configuration items. It can be used as part of security investigations or acts of administration on Microsoft Windows, Linux or Mac machines.

1.1.3. Files

The application consists of the following files:

NS.exe
libgcrypt-11.dll
libgpg-error-0.dll
libssh2-1.dll
zlib1.dll
accounts.csv
conf_registry.csv
conf_registry_write.csv
conf_files.txt
conf_services.txt
conf_softwares.txt
conf_ssh.txt
conf_USB.txt
ip_test.txt
NS_log.txt
NS.ini

NS.exe: is the binary of the application to run.

The *. dll are needed and used for SSH connections.

accounts_list.csv: sample file of account list to load.

The ***.conf** files are the files used to configure the tests to perform.

ip_test.txt, **ip_test.csv**: an example of IP format supported.

NS_log.txt: The trace file of activities. This file reports the results of all tests.

NS.ini: automatic configuration file for setting up automatic scan when running NS.exe.

1.1.4. Dependencies

No external dependencies outside of the application files and system files required Microsoft native (no service pack is required).

The application was tested on 32/64bits environments:

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

1.2. Features

- Discover machines on a network (IPv4), based on ICMP, DNS and NetBIOS.
- Remote connection to the registry, the file system machines and NetBIOS to verify:
  - o The type of operation and its associated service pack system;
  - o The domain of the computer;
  - o The presence of null session (authorized remotely connection with an empty account and password);
  - o Enumeration user account SID.
  - o The list of shares;
  - o The time and date of the remote system;
  - o The list of files on the remote system with the last modification date and the SHA256 and MD5 hashes of the file;
  - o The list of keys, values and data of registry;
  - o The list of the services;
  - o The list of the software ;
  - o The USB drives already installed on the computer and the date of last attendance.

- Modifying registry values;
- Export remote registry and files;
- SSH remote command execution;
- Remote connection from the current account, an account set, a list of account or null session;
- Real-time logging of tests;
- Export in XML, HTML, CSV et TXT.

1.3. Application GUI
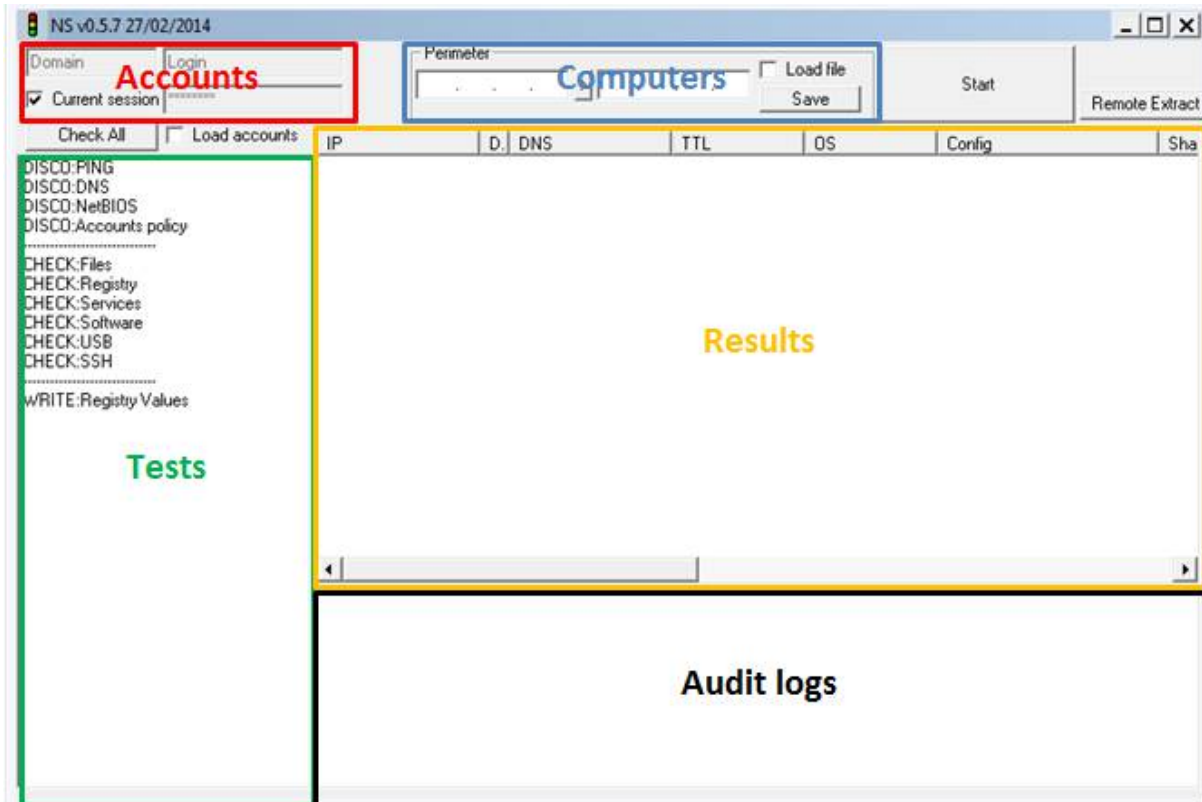
2. Restrictions

2.1. Remote connection

Access to network computers for testing is only possible if the filtering of these computers allow access. In case of active firewall on computers to check, it is necessary to disable or allow the IP address of the computer performing the tests.

2.2. Remote connection to registry

The remote access to the registry service must be enabled for the connection to the registry (Operation Microsoft Windows RPC is based on local service).

From the 0.5.7 version in case of failure of the database connection, the Remote Registry service is started and then turned off at the end of the tests if possible.

2.3. Execute permissions

The application does not require local administration right to function properly.

2.4. Authentication file

Be careful when using the file "CSV" containing multiple accounts and passwords. In case of multiple passwords for a single account, depending on political accounts on remote machines, it is possible to lock the account. So be careful not to put too many different passwords for the same account.

2.5. Restriction for data extracted

NS aims to provide a summary statement of configuration on remote machines. Returns orders are limited to a size of 16384 characters per category (register, service, software, USB, files, and SSH).N

Example: 16384 for a machine and the USB Returns + 16384 for software, etc..

3. The different types of remote authentication

The application authenticates via secure RPC channels, accounts and passwords are not transmitted in clear text over the network.

3.1. Using the current user

To use the current user trying to authenticate, it is necessary to check the "Current Session" box:

Note:

Some cases specific operation can cause problems when authenticating to a remote machine using the current user session. It is therefore strongly recommended to enter the authentication elements as described in the next section "User defined".

This failure has been detected in some particular cases, the application of machine running Windows 7 to a Windows 7 machine.

3.2. User defined

It is possible to use a domain and a different user to the current user by unchecking the "Current session" and filling in the following fields:

3.3. User list

When testing on a large network, it is always interesting to enter multiple accounts to connect for example to machines outside the domain.

These accounts must have sufficient privileges to be able to connect to administrative shares or remote registry.

Warning:

Loading account is made from a CSV file or usernames and passwords are filled in clear text.

In the advanced IP list, the accounts can be added.

File format:
```
"Domain";"user";"password";
"";"user2";"password";
```

The first parameter is the authentication domain. When connecting with a local account setting is not required.

The second parameter is the name of the user.

The third parameter is the password in plain text.

To load the file, just check the "Load accounts" box and select a file in CSV format matching:
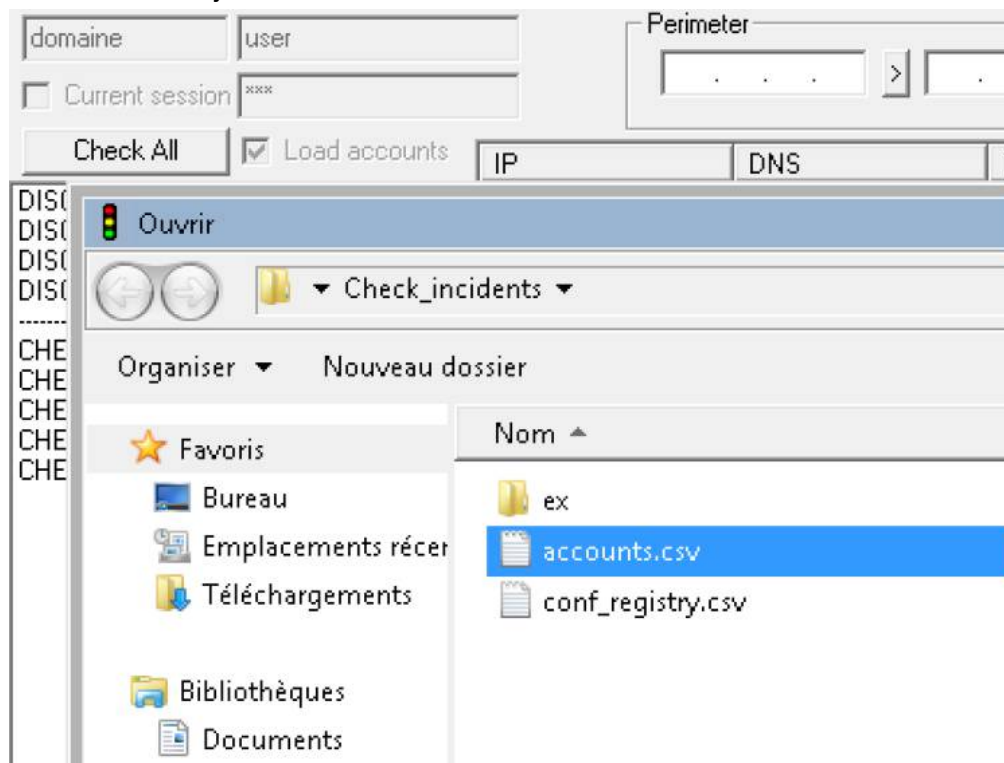
3.4. Traces of successful authentication

When the discovery of the machines is launched in case of successful authentication during the various tests, a warning message is generated in the "Config" column and in the audit console as:

```
[time] INFORMATION - Login (type of connection) in <remote IP> IP with <login (id login)>
account
```

Connection type:

- ScanReg:NET, represents a successful connection to the registry remotely through access to the IPC$ share of the remote machine;

- FileScan:NET, is described in a successful administrative share connection.

- Id login: is the ID of the account starting at 0 present in the CSV file loaded from the user authentication list.

Example:

Upon successful authentication with the account 'user2' file:

```
"Domain";"user";"password";
"";"user2";"password";
```

We have the following message in the event of detection:

```
[2013/11/30-14:00:00] LOGIN NET - with 192.168.0.1\user2 (01) account
```

4. Use

4.1. Network discovery

The discovery of the target can be configured through the direct interface:

Or by checking the "Load file" box and load a file in TXT or CSV format.

Example TXT format file allowed:
```
10.10.0.1-10.10.0.2
10.11.0.0/24
10.12.1.4
computername
```


Example CSV format file allowed:
```
"10.10.0.1-10.10.0.2";"lan1";
"10.11.0.0/24";"lan2";
"10.12.1.4";"lan3";
"computername";"lan2";
```


The second column is a comment that will be reported in the second column "DSC" visible on the interface.

The number of target machines is reported in the audit console at the beginning of the discovery of machines.

Advanced IP format with credentials by ip:

Example CSV format file allowed:
```
"#!";"10.10.0.1-10.10.0.2";"lan1";"domain";"login";"password";
"#!";"10.11.0.0/24";"lan2";"domain";"login";"password";
"#!";"10.12.1.4";"lan3";"domain";"login";"password";
"#!";"computername";"lan2";"domain";"login";"password";
```


The first column is for details the file format.

4.2. Files: Check if a file exist

Loading the list of files to check is automatically loaded during the start-up tests.

It is done through the file "conf_files.txt" that must be present in the same directory as the application. This file is a simple list of file paths. In the paths specified, do not specify the drive letter. Indeed, all available readers with the file will be tested. The value '%' can be used for search in multiples directories.

A special search is possible by using the separator ":" used in the last line of the example. The first parameter is the file size in bytes (mandatory), the second the MD5 hash (optional) and the last footprint SHA256 (optional). This line begins and ends with a ":"

Example file format allowed:

```
IO.SYS
WINDOWS\explorer.exe
\WINDOWS\toot.zc
Windows\%\test.exe
:8000:C124E332FE3F0E737B865EDA0E90D5BF:df8f250ac6dba58c81d7eb697bd6b2860aba020de47a0fcc5661b39026818495:
```

Upon detection of a file on a machine, a trace is stored in the "Files" column as well as the audit console as:

```
[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;df8f250ac6dba58c81d7eb697bd6b2860ab
a020de47a0fcc5661b39026818495
```

A second search file was added to allow an optimized search.

Indeed, the first format is searchable by file or path for a limited number of file to get proper performance. For search on all drives of the machines, it is best to use the "conf_mulfiles, txt" file. Factors taken into account are:

Example file format allowed:

```
IO.SYS
test.txt
:8000:C124E332FE3F0E737B865EDA0E90D5BF:df8f250ac6dba58c81d7eb697bd6b2860aba020de47a0fcc5661b39026818495:
```

In this case, the search is done on the disc by checking each item. The performance impact of adding an item to be tested is almost zero, aside for MD5 fingerprinting / SHA256 / SHA1 involving calculating footprints all the files.
The ability to check fingerprints SHA1 was added by modifying the configuration file "NS.ini", see the related topic.

4.3. Registry: Check for keys or registry values

The list of keys and values to check is automatically loaded during the start-up tests.

It is done through the file "conf_registry.csv" that must be present in the same directory as the application.

Example file format allowed:

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

- The first data represents the registry key to check;

- The second, the registry value to obtain (not mandatory);

- Third, the expected data (not required);

- The fourth data format (DWORD and STRING allowed, not required);

- The fifth, the description of the key (for better readability of the results but not mandatory).

- The last parameter is the type of audit to be done. It accepts the following formats:

  o ***** No verification data;

  o **?** for the data type STRING can check if the value contained in the third parameter is contained in the data read;

  o **=** data must be identical;

  o **!** data must be different;

  o **<** for data type DWORD, to check if the value contained in the third parameter is less than the data read;

  o **>** for data type DWORD, to check if the value contained in the third parameter is greater than the data read.

Upon detection of a key, a track is recorded in the "Registry" and in the column of said console in the form:

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

Note:

The current version does not specify the hive in search of keys. By default, these hives are checked:

```
HKEY_LOCAL_MACHINE, HKEY_USERS et HKEY_CLASSES_ROOT.
```

4.4. Service: Check for service

Loading the list of services to check is automatically loaded during the start-up tests. It is done through the file "conf_services.txt" that must be present in the same directory as the application. This file is a simple list of names or service description.

Example file format allowed:
```
atapi
wmiapsrv
Google Update
```

Upon detection of a service on a machine, a trace is stored in the "Services" column as well as the audit console as:

```
[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: Check for software

Loading the list of software to check is automatically loaded during startup tests. It is done through the file "conf_softwares.txt" that must be present in the same directory as the application. This file is a simple list of name software.

Example file format allowed:
```
7-Zip
Notepad++
```

Upon detection of a software on a machine, a track is recorded in the "Plugin" and in the column of said console in the form:

```
[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: Check for evidence of the use of any USB storage device

Loading the list of USB devices to check is automatically loaded during startup tests. It is done through the "conf_USB.txt" file must be present in the same directory as the application.

This file is a simple list of ID or description of device registry keys that can be obtained in the registry paths to:

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

Example file format allowed:

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

Upon detection of a USB device on a machine, a trace is stored in the "USB" column as well as the audit console as:

```
[2013/11/30-14:00:00] FOUND (USB) –
192.168.0.1\SYSTEM\CurrentControlSet\Enum\USBSTOR\CdRom&Ven_BUFFALO&Prod_Virtual_Cdrom&Re
v_0.82\0010100704075C350&1 (Last Write Time 2013/11/30-14:00:00)
```

4.7. Extraction tests

Since Version 0.5.7, it is possible to carry out an extraction configuration on multiple machines remotely.

It allows the discovery by ICMP and DNS queries. The operating system is recovered through the connection to the remote registry and SSH.

Existing tests are:

- Copying registry hives: HKEY_LOCAL_MACHINE SOFTWARE, SYSTEM and HKEY_USERS as a CSV file;
- Detailed copy files in the "conf_files.txt";
- SSH remote commands (unlimited return);
- Saving test results in CSV and XML.

4.8. Tests automation

Since the 0.4.13 version, it is possible to perform automatic tests by creating a "NS.ini" file in the application directory.

Example file format allowed:

```
[SCAN]
IP_FILE="file_ip.txt"
ACCOUNT_FILE="accounts.csv"
TYPE="DISABLE"
DISCO_ICMP="YES"
DISCO_DNS="YES"
DNS_DISCOVERY="NO"
DISCO_NETBIOS="YES"
DISCO_NETBIOS_POLICY="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"

[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 NS.ini file [SCAN]

The "[SCAN]" corresponds to different elements of initial configuration.

- **IP_FILE:** TXT file containing the list of IP , IP ranges or hostnames target addresses.

- **ACCOUNT_FILE** : CSV to take into account to authenticate to the machine test format.

- **TYPE** : can take three different values:

  - *AUTO* : execution configured in the parties' [CHECK] "and" [CHECK_OPTIONS] "saving the results at the end depending activated in" [SAVE] "formats tests.

  - *SIMPLE*: this mode allows you to take into account the list of parameters DISCO_ * that correspond to different tests to activate.

  - *DISABLE* : automatic test mode disabled.

- **DISCO_*** : represents for the scan type "SIMPLE" list of tests to be activated.

- **DNS_DISCOVERY** : default ICMP and DNS resolution are used to discover machines. To disable DNS resolution as a means of detection while keeping the DNS resolution for each IP, just put parameter is "NO".

4.8.2. Section NS.ini file [SAVE]

The "[SAVE]" to specify what format backup should be used when test type "AUTO" set in the "[SCAN]" section.

The type of response formats allowed are:

- YES : save
- NO : disable

4.8.3. Section NS.ini file [LOG]

This section allows you to disable the auto login of the operation in the "NS_LOG.txt".

The following settings can be enabled with the value OK:

- **LOG**: allows you to disable the auto login file with the value "DISABLE".

4.8.4. Section NS.ini file [CHECK]

This section allows you to enable the tests to be performed when selecting the type of test "AUTO."

The following settings can be enabled with the value OK:

- **M_SEC**: allows you to check for a value of registry key in the HKEY_LOCAL_MACHINE hive of the remote machine.

  The path and the value in the hive can be configured in the "[CHECK_OPTIONS]" section with MSEC_REG_PATH and MSEC_REG_VALUE parameters.

- **WSUS_WORKS**: check if a server WSUS update is configured and running on the computer.

- **PATCH_UPDATED**: check that the machine is up to date for less than a month.

- **MCAFEE_INSTALLED**: check if McAfee Antivirus is installed on the machine.

- **MCAFEE_UPDATED**: verify that McAfee Antivirus is up to date for less than X days. The reference number of days is set in the " [CHECK_OPTIONS]" section with MCAFEE_UPDATE_DAYS_INTERVAL parameter

- **MCAFEE_SCAN**: Check that a total test machine with McAfee Antivirus has been made for less than X days. The reference number of days is set in the " [CHECK_OPTIONS]" section with MCAFEE_SCAN_DAYS_INTERVAL parameter.

- **PASSWORD_POLICY**: allows verification of compliance with the management policy statements. The configuration can be done in the " [CHECK_OPTIONS]" section with PASSWORD_POLICY_* settings.

- **ADMIN_ACOUNT**: check for an account on the machine. The checking account can be configured in the "[CHECK_OPTIONS]" section with ADMIN_ACOUNT parameter.

- **NULL_SESSION**: check for null session (authentication with username and null passwords) on the machine.

- **REVERS_SID**: ability to enumerate user accounts without being logged on the machine.

- **AUTORUN**: check autorun program when inserting into the machine external media has been deactivated (CDROM, USB, etc. .).

- **SHARE_ACCESS**: retrieve the list of network shares accessible without authentication.

4.8.5. Section NS.ini file [CHECK_OPTIONS]

This section details the configuration elements operated by the activation of tests "[CHECK]" section.

Check for a registry value. Here HKLM \ Software \ test:

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

Check the configuration of McAfee Antivirus:

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

Check the security policy of passwords:

```
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"
```

Check that the account (by administrator):

```
ADMIN_ACOUNT="administrator"
```

5. Changing the Remote Setup

5.1. Register: Changing registry value

The application is designed to allow the modification or creation of registry value remotely.

The list of values to be written is loaded automatically during startup tests.

It is done through the file "conf_registry_write.csv" that must be present in the same directory as the application.

Example file format allowed:

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

- The first figure represents the registry key to check;
- The second, the registry value or write;
- The third, data write;
- The fourth data format (DWORD and STRING allowed);
- The fifth, the registry hive impacted. Different formats included:
  - o **HKLM pour HKEY_LOCAL_MACHINE**
  - o **HKU pour HKEY_USERS**
  - o **HKCR pour HKEY_CLASSES_ROOT**
- The sixth parameter is the content of the current data expected towards operators seventh parameter.
- The seventh parameter is the type of audit to be done. It accepts the following formats:
  - o ***** no audit;
  - o **?** for the data type STRING can check if the value contained in the sixth parameter is contained in the current data;
  - o **=** data must be identical;
  - o **!** data must be different;
  - o **<** for data type DWORD, to check if the value contained in the sixth parameter is smaller than the current data;
  - o **>** for data type DWORD, to check if the value contained in the sixth parameter is greater than the current data.

When writing a value is successful, a trace is recorded in the audit console as:

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

Warning:

If the access to the registry value path does not exist, it will be created.

5.2. SSH: command execution

SSH module in the application through DLL libgcrypt, libgpg, libssh2 and zlib.

It allows execution of commands through SSH connection with username and password.

Commands to be executed must be present (one per line) in the file "conf_ssh.txt" that must be present in the same directory as the application.

Example file format allowed:
```
uname -a
ifconfig -a
```

When writing a value is successful, a trace is recorded in the audit console in the form (in case of very large response, it can be split across multiple lines):
```
[2013/11/30-14:00:00] FOUND (SSH) [192.168.0.1\\uname -arv] Linux proxysvr 2.6.18
```

6. Export results

Export results ("Save" button) can be done during or after the tests to CSV, XML and HTML formats. CSV format can be opened by spreadsheet allowing data including line breaks (like LibreOffice) with separator semicolon and quotation marks as the delimiter (Microsoft Excel does not correctly load these files).

XML can be opened by spreadsheet as XML table (Excel):
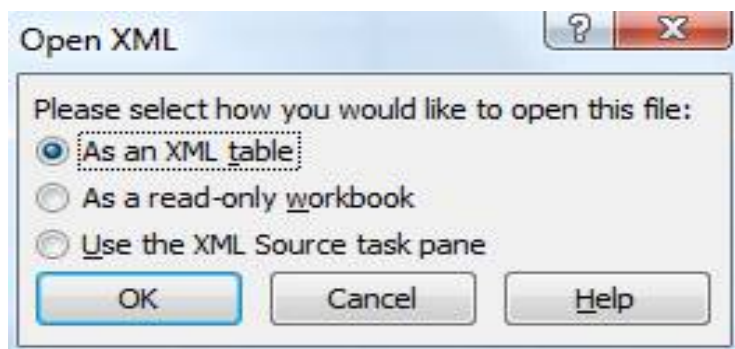
By default, an audit file shares (Content audit console) is generated in the application directory under text "NS_log.txt" form. Even in case of a crash, this file is accessible and writing being generated in real time.

This document contains the date and results as well as global statistical data such as:
- The number of computers available.
- The number of computers allowing connections to the registry or file system remotely.
- The number of computers in a Microsoft Windows operating system.