



version 2.5.1.0



*Here at Ping Castle we think that **Security relies on Processes and People** rather than Technology. Here is the first Tool that check the security processes rather than a long list of known vulnerabilities.*

*Ping Castle's objective is not to reach a perfect security but to **impulse changes using the management**. And with low effort, I think you'll get support to change the situation !*

Vincent LE TOUX, CEO



About PingCastle.....	4
The philosophy of PingCastle	4
How it works	4
Requirements	5
Running PingCastle.....	6
Quick Launch.....	6
Running PingCastle in Interactive mode	7
Running PingCastle in Command line mode.....	7
Health check	7
Overview:	7
Advanced mode:	8
Other investigations:	8
Full command line options	8
PingCastle Methodology	12
Step1: perform domain discovery	13
Option 1: do the healthcheck on several domains (recommended)	13
Option 2: perform a quick domain exploration (fastest but not scalable)	14
Step2: Get the Active Directory risk level.....	18
Step3: Get reports for all domains	22
Step4: Getting an overview	26
Step5: Dashboard	28
Operations to perform.....	28
Configuration file.....	28
Generation of the Excel report.....	28
Generation of the PowerPoint report	29
Advanced	31
Compromise graphs	31
Null sessions.....	34
Scanners.....	35
Other	35
Annex: Scheduling the health check	37



About PingCastle

The philosophy of PingCastle

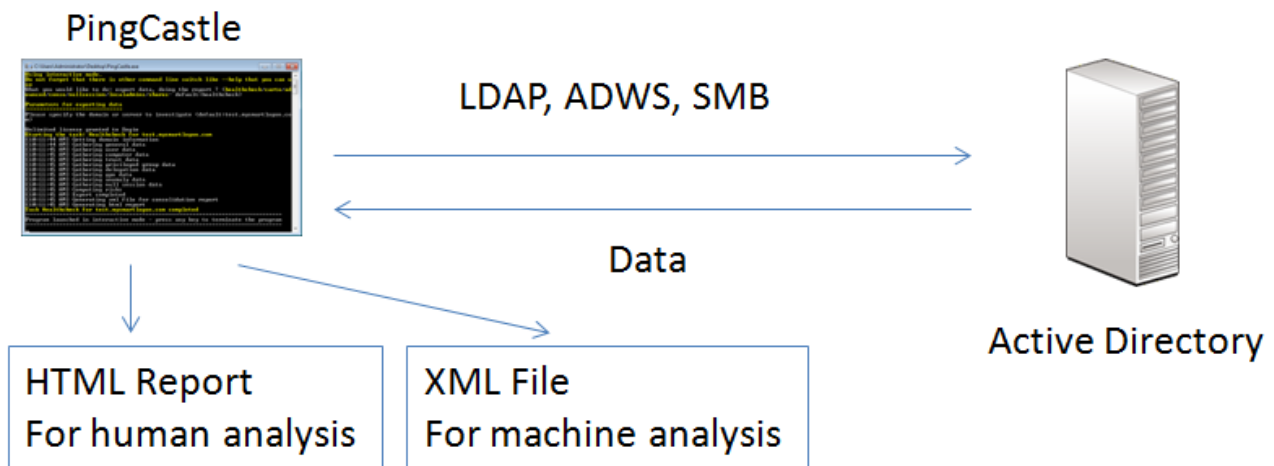
The philosophy of the tool is:

1. Minimize the requirements as much as possible
2. Use only AD native and supported protocols (LDAP, ADWS, SMB) without any “hack”
3. Be scalable

As a consequence the tool doesn't perform any check that requires administrator rights like the [non secure DNS update problem](#). It does not check problems which require a maintained list, like for example, checking for non applied patches.

How it works

PingCastle is a standalone program (not requiring installation) which produces reports for human or machine.



PingCastle reads its own machine readable reports to build analysis or dashboard.



Requirements

Active Directory Account

The PingCastle program **needs an Active Directory account to connect to the AD to audit**. No requirements is needed for this account. It can be an account without any privileges or even an account from a trusted domain. This account doesn't require to be part of the local administrators group.



Server Side

There is **no requirement on the server side**.

However it is **strongly recommended (but not mandatory) for performance reasons** to install on the server side a component named "Active Directory Web service" aka ADWS. It is installed by default on any domain where at least **one** domain controller has the OS **Windows 2008 R2** or later. Having this component installed can divide the time required to compute the report by a factor of 10.

ADWS can be installed manually on [Windows 2003 and Windows 2008](#) (require [.NET Framework 3.5 SP1](#)). The hot fix that may be needed for these OS is located [here](#).

Client side

The program is supported on every Operating System supported by Microsoft without the installation of any component nor any local privilege.

From Windows Vista to Windows 10 and Windows 2008 to Windows 2016 in both 32 and 64 bits.

In addition, the program is known to be working on Windows 2000 with the .net framework 2, Windows XP and Windows 2003.

The analysis tool (PingCastle.exe) requires DotNet 3.0 (or next versions) which is available by default since Windows Vista. It can be run under DotNet 2.0 but with fewer functionalities.

The reporting tool (PingCastleReporting.exe) requires DotNet 3.5 (or next versions) which is available by default since Windows Seven. Files produced by the reporting tool are .xlsx and .pptx. To read them, you may install the [Excel Viewer](#) or the [PowerPoint Viewer](#) or any viewer compatible like [OpenOffice](#).

The functionality to create the graph using Active Directory dumps may require the Sql Compact runtime (SqlCE). It is included by default by the .Net runtime but may not be present if executed on servers.

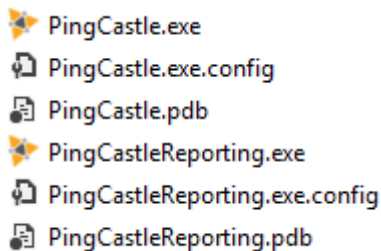


Running PingCastle

The program is a command line program. It can be run with switches to perform a specific work. It can be run without command line arguments to interact with the end user.

Quick Launch

Uncompress the files in a new directory.



Double click on PingCastle.exe.
Press Enter twice.

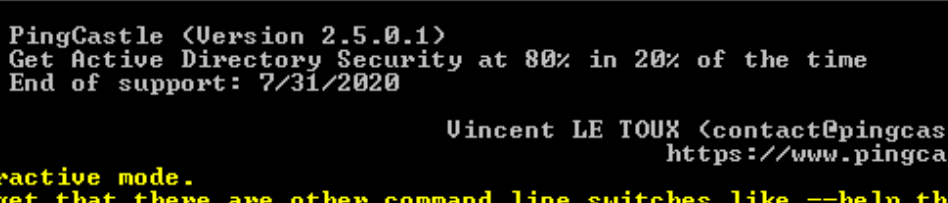
If you want to get a quick status of your infrastructure, run the healthcheck (enter) and enter as domain the asterisk (*). All reachable domains will be scanned, the reachable mode will be activated and the consolidation report will be made automatically.

If you need only the map, enter "carto" and press enter.

```
C:\Users\Administrator\Desktop\PingCastle.exe

!:.      PingCastle <Version 2.5.0.1>
! #:.    Get Active Directory Security at 80% in 20% of the time
# @@ >   End of support: 7/31/2020
! @@@:
! .#
! .#      Vincent LE TOUX <contact@pingcastle.com>
! .#      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
carto
PingCastle v2.5
Starting the task: Exploration
[5:29:02 PM] Exploring test.mysmartlogon.com <source:current domain>
List of domains that will be queried
test.mysmartlogon.com
Task Exploration completed
Starting the task: Examining all domains in parallele <this can take a few minutes>
[5:29:02 PM] Starting the analysis of test.mysmartlogon.com
[5:29:05 PM] Analysis of test.mysmartlogon.com failed
Task Examining all domains in parallele <this can take a few minutes> completed
Starting the task: Healthcheck consolidation
Simplified graph: automatic center on test.mysmartlogon.com <S-1-5-21-4005144719-3948538632-2546531719>
Simplified graph: you can change this with --center-on <domain>
Simplified graph: contains 3 nodes on a total of 3
Task Healthcheck consolidation completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```



```
C:\Users\Administrator\Desktop\PingCastle.exe

!:.      PingCastle <Version 2.5.0.1>
! #:.    Get Active Directory Security at 80% in 20% of the time
# ee >   End of support: 7/31/2020
! eee:
! .#
! .#      Vincent LE TOUX <contact@pingcastle.com>
! .#      https://www.pingcastle.com
:.
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
```

Here is a short description of the main tasks performed by the program.

- run the health check :

- run the consolidation of the health check reports:

- export rule list:

Overview:

- Built only a cartography without scores:

7



Advanced mode:

- run the export:

```
PingCastle --advanced-export --server mydomain.com
```

- build the reports:

```
PingCastle --advanced-report --database thegeneratedsdffile.sdf
```

Other investigations:

- Check the presence of null session:

```
PingCastle --nullsession --server servertotest
```

- Scan the domains for local administrators:

```
PingCastle --localadmins --server domainToExplore
```

- Scan the presence of local shares:

```
PingCastle --shares --server domainToExplore
```

- The available switches can be obtained using the “--help” switch.

```
PingCastle --help
```

Full command line options

```
|:..    PingCastle (Version 2.5.1.0)
| #:..  Get Active Directory Security at 80% in 20% of the time
# @@ >  End of support: 7/31/2020
| @@@:
: .#                                Vincent LE TOUX (contact@pingcastle.com)
.:                                https://www.pingcastle.com

switch:
--help          : display this message
--interactive   : force the interactive mode
--log           : generate a log file
--log-console   : add log to the console

Common options when connecting to the AD
--server <server> : use this server (default: current domain controller)
                  the special value * or *.forest do the healthcheck for all domains
--adws-port <port> : use the port for ADWS (default: 9389)
```




```
--user <user>      : use this user (default: integrated authentication)
--password <pass>   : use this password (default: asked on a secure prompt)
--protocol <proto>  : selection the protocol to use among LDAP or ADWS (fastest)
                    : ADWSThenLDAP (default), ADWSOnly, LDAPOnly, LDAPThenADWS

--carto             : perform a quick cartography with domains surrounding

--healthcheck       : perform the healthcheck (step1)
  --api-endpoint <> : upload report via api call eg: http://server
  --api-key <key>   : and using the api key as registered
  --explore-trust    : on domains of a forest, after the healthcheck, do the hc on all
trusted domains except domains of the forest and forest trusts
  --explore-forest-trust : on root domain of a forest, after the healthcheck, do the hc
on all forest trusts discovered
  --explore-trust and --explore-forest-trust can be run together
  --explore-exception <domains> : comma separated values of domains that will not be
explored automatically

  --encrypt          : use an RSA key stored in the .config file to crypt the content of
the xml report
  --level <level>    : specify the amount of data found in the xml file
                    : level: Full, Normal, Light
  --no-enum-limit     : remove the max 100 users limitation in html report
  --reachable         : add reachable domains to the list of discovered domains
  --split-OU <level> : this is used to bypass the 30 minutes limit per ADWS request. Try
5 and increase 1 by 1.
  --sendXmlTo <emails>: send xml reports to a mailbox (comma separated email)
  --sendHtmlTo <emails>: send html reports to a mailbox
  --sendAllTo <emails>: send html reports to a mailbox
  --notifyMail <emails>: add email notification when the mail is received
  --smtplogin <user>: allow smtp credentials ...
  --smtppass <pass> : ... to be entered on the command line
  --smtptls          : enable TLS/SSL in SMTP if used on other port than 465 and 587
  --skip-null-session: do not test for null session
  --webdirectory <dir>: upload the xml report to a webdav server
  --webuser <user>    : optional user and password
  --webpassword <password>

--generate-key       : generate and display a new RSA key for encryption

--hc-conso           : consolidate multiple healthcheck xml reports (step2)
```



```
--center-on <domain> : center the simplified graph on this domain
                        default is the domain with the most links

--xmls <path>       : specify the path containing xml (default: current directory)

--filter-date <date>: filter report generated after the date.


--gen-hc-report <xml> : regenerate a html report based on a xml report
--reload-report <xml> : regenerate a xml report based on a xml report
                        any healthcheck switches (send email, ..) can be reused

--level <level>     : specify the amount of data found in the xml file
                        : level: Full, Normal, Light (default: Normal)

--encrypt           : use an RSA key stored in the .config file to crypt the content of
the xml report
                        the absence of this switch on an encrypted report will produce a
decrypted report


--advanced-live      : perform the compromise graph computation directly to the AD


--advanced-export    : perform the export of the AD data (step1)

--split-OU <level> : this is used to bypass the 30 minutes limit per ADWS request. Try
10 and increase 1 by 1.


--advanced-report    : generate the default reports (step2)
--max-depth          : maximum number of relation to explore (default:30)
--max-nodes          : maximum number of node to include (default:1000)
--auto-reports       : generate the default reports
--node <node>        : create a report based on a object
                        : example: "cn=name" or "name"
--nodes <file>       : create x report based on the nodes listed on a file
--rev-direction      : reverse the direction when exploring nodes
--database <file>    : specify the file to work on. Default: Ad-my.domain.com.sdf
--save-memory        : use optimization to save memory space. Can be slower by a factor
of 10
--json-only          : do not produce node map in html but in json (for external import)


--nullsession        : test for null session
--nslimit <number> : Limit the number of users to enumerate (default: 5)


--scanner <type>     : perform a scan on all computers of the domain (using --server)
localadmin
Enumerate the local administrators of a computer.
ms17-010
```



Check for the ms17-010 vulnerability without exploiting it. Beware that it may trigger AV response by closing the connection

replication

Search replication metadata for modification done in the past but recorded more than 1 day after the supposed modification

share

List all shares published on a computer and determine if the share can be accessed by anyone

smb

Scan a computer and determine the smb version available. Also if SMB signing is active.

startup

Get the last startup date of a computer. Can be used to determine if latest patches have been applied.

--nulltrusts : check if the trusts can be enumerated using null session

--enum inbound <sid> : Enumerate accounts from inbound trust using its FQDN or sids
Example of SID: S-1-5-21-4005144719-3948538632-2546531719

--upload-all-reports: use the API to upload all reports in the current directory

--api-endpoint <> : upload report via api call eg: http://server

--api-key <key> : and using the api key as registered

Note: do not forget to set --level Full to send all the information available



PingCastle Methodology

Acting on the processes of Active Directory security

The goal of the tool “PingCastle” is not to fix all the technical problems (for example [Microsoft Security Compliance Manager](#) allows to check the GPO compliance). It is not to do a one shoot audit but to put in place an organization and security processes.



The tool is an help regarding the implementation of an AD security standard. The tool follows two goals:

- For the local IT:
Make the AD administrators aware of their security level and help them detect potential security issues
- For the Corporate:
Gather a global view, especially the trust part, and be able to budget and prioritize security projects

Involve the management

The PingCastle methodology is based on 4 steps:

Domain discovery	Risk level	Deploy the tool	Report to the management
<ul style="list-style-type: none">• Get to know how much domains are under your responsibility	<ul style="list-style-type: none">• Get the Active Directory risk level of domains queried	<ul style="list-style-type: none">• Deploy the tool to get as many risk reports as possible	<ul style="list-style-type: none">• Consolidate the results and present them to the management

Then you can use the [advanced functionalities](#) of PingCastle to hunt specific weaknesses.

Improve your risk level

For a big corporation, having an Active Directory domain compromised may not be the only risk. You can have trusts with third party where you have no control or a trust with a domain you (and the company) know nothing about.

Our suggestion is to built a plan with the management support to improve the security:

1. Remove trusts with external companies, without control, or forgotten
2. Put in place SID Filtering to limit cross-domain contamination
3. Fix critical vulnerabilities like [passwords found in GPP](#)



Step1: perform domain discovery

Option 1: do the healthcheck on several domains (recommended)

If you want to get a quick status of your infrastructure, [run the program](#) with the "healthcheck" mode (just press enter) and enter as domain the asterisk (*). All reachable domains will be scanned, the reachable mode will be activated and the consolidation report will be made automatically. This takes from a few minutes to one hour.

```
C:\Users\Administrator\Desktop\pingcastle\PingCastle.exe

!:.      PingCastle <Version 2.5.1.0>
! #:.    Get Active Directory Security at 80% in 20% of the time
# ee >   End of support: 7/31/2020
! eee:
! :.#
! :.      Vincent LE TOUX <contact@pingcastle.com>
! :.      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>

Parameters for exporting data
=====
Please specify the domain or server to investigate <default:test.mysmartlogon.com>
*
PingCastle v2.5
Starting the task: Exploration
[5:31:50 PM] Exploring test.mysmartlogon.com <source:current domain>
List of domains that will be queried
test.mysmartlogon.com
Task Exploration completed

Starting the report for test.mysmartlogon.com <1/1>
=====
Starting the task: Healthcheck for test.mysmartlogon.com
[5:31:50 PM] Getting domain information
[5:31:50 PM] Gathering general data
[5:31:50 PM] Gathering user data
[5:31:50 PM] Gathering computer data
[5:31:50 PM] Gathering trust data
[5:31:53 PM] Gathering reachable domains data
[5:31:53 PM] Gathering privileged group data
[5:31:53 PM] Gathering delegation data
[5:31:53 PM] Gathering gpo data
[5:31:53 PM] Gathering anomaly data
[5:31:54 PM] Gathering domain controller data <including null session>
[5:31:54 PM] Gathering network data
[5:31:54 PM] Computing risks
[5:31:54 PM] Export completed
[5:31:54 PM] Generating xml file for consolidation report
[5:31:54 PM] Generating html report
Task Healthcheck for test.mysmartlogon.com completed
Starting the task: Healthcheck consolidation
Reports loaded: 1 - on a total of 1 valid files
Simplified graph: automatic center on test.mysmartlogon.com <S-1-5-21-4005144719-3948538632-2546531719>
Simplified graph: you can change this with --center-on <domain>
Simplified graph: contains 3 nodes on a total of 3
Task Healthcheck consolidation completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

Then open the cartography reports (see below).

Important: xml reports generated from multiple point of view can be used to have a consolidated map. Do not forget to check the [Getting an overview](#) or [dashboard](#) section.



Option 2: perform a quick domain exploration (fastest but not scalable)

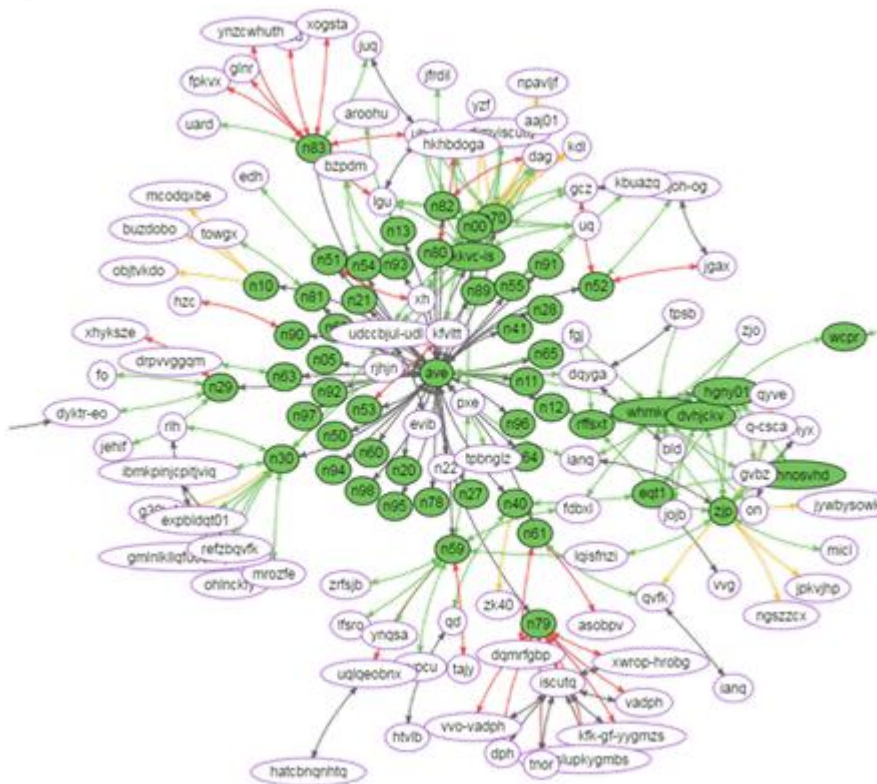
If you need only a quick map (< 5 minutes of execution), enter “carto” when using the interactive mode or run the program with the switch `--carto`.

```
C:\Users\Administrator\Desktop\PingCastle.exe

!:.      PingCastle <Version 2.5.0.1>
! #:.    Get Active Directory Security at 80% in 20% of the time
# @@ >   End of support: 7/31/2020
! @@@:
! .#
! .#      Vincent LE TOUX <contact@pingcastle.com>
! .#      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
carto
PingCastle v2.5
Starting the task: Exploration
[5:29:02 PM] Exploring test.mysmartlogon.com <source:current domain>
List of domains that will be queried
test.mysmartlogon.com
Task Exploration completed
Starting the task: Examining all domains in parallel <this can take a few minutes>
[5:29:02 PM] Starting the analysis of test.mysmartlogon.com
[5:29:05 PM] Analysis of test.mysmartlogon.com failed
Task Examining all domains in parallel <this can take a few minutes> completed
Starting the task: Healthcheck consolidation
Simplified graph: automatic center on test.mysmartlogon.com <S-1-5-21-4005144719-3948538632-2546531719>
Simplified graph: you can change this with --center-on <domain>
Simplified graph: contains 3 nodes on a total of 3
Task Healthcheck consolidation completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

The program discovers all the reachable domains, does a light scan and produce the same map than in the health check consolidation mode. The SID Filtering status is accurate but the individual scores are not available. Scans are performed in parallel. Cartography reports cannot be combined when run on more than one point of view. If you need to combine data from multiple AD, you should run the healthchecking reports and consolidate their reports.



Domain map

When the cartography has been performed, many files are generated. Two kinds of map exists. The full domain map is a cartography where each trust is represented. It is good when there is no much domains or trusts. The simple domain map is a simplified cartography. Each domain is present but not all trusts. This simplified map is computed to have a synthetic view when the number of trusts become too important.

Full domain map

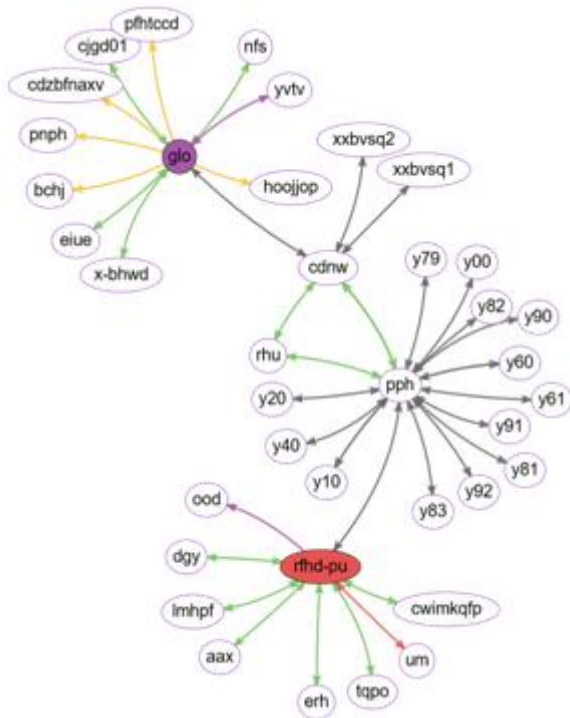
The full domain map is represented by the files xxx_full_node_map.html. Each map is a dynamic map. Each node can be moved.

These files embeds the [Ovali Tool](#) made by the ANSSI

Copyright (c) 2016, ANSSI All rights reserved.

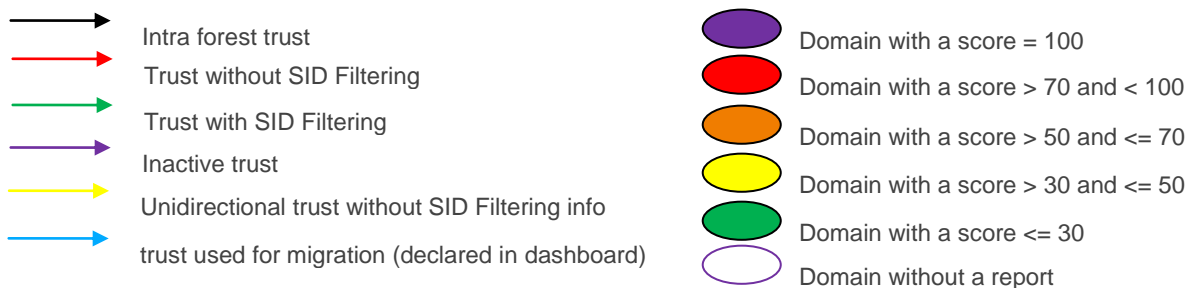
These file MUST be opened by Firefox or Chrome. Internet Explorer doesn't work.

Example of graph produced by the tool

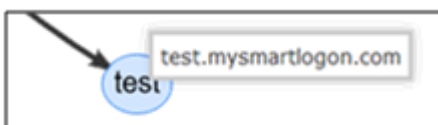


The colored circles are the domain on which the reports have been run. The color depends on the score. The purple bordered circles are the domains on which the script has not been run but that they program found using trust link.

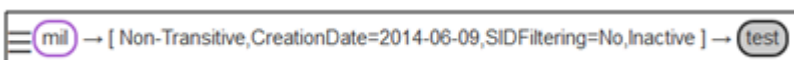
Legend:



When the mouse is on a circle, the full name of the domain appears:



If the mouse is hold on a trust, the detail is shown at the bottom right of the Windows:



Simple domain map

The simple domain map is represented by the files xxx_simple_node_map.html. It is a static map (domains cannot be rearranged). This file can be opened in Internet Explorer, Chrome or Firefox and some details can be obtained when the mouse is on a domain. Specifically if it has been generated with the BU/Entity information (advanced consolidation), the BU and Entity can be shown.

Methodology used to build the maps

1. The most reliable source is domain where the report has been generated.
2. Then the tool is using direct [trust data](#).
3. Then the tool is using forest trust information. This information is located in the [msDS-TrustForestTrustInfo](#) attribute of a forest trust and in the [partition element](#) of the configuration binding context.
4. The tool is using the information provided by the [domain locator service](#) when examining trusts. This information can add the Netbios name or the forest name of a trusted domain.
5. If the “reachable” option has been set when producing a report, the tool is using domain SID found (in [foreign security principals](#) or [sid history](#)) to query the [domain locator service](#) and guess forest trusts.



Step2: Get the Active Directory risk level

The report can be generated in the interactive mode by choosing “healthcheck” or just by pressing Enter. Indeed it is the default analysis mode.

```
C:\Users\Administrator\Desktop\pingcastle\PingCastle.exe

!:.      PingCastle <Version 2.5.1.0>
! #:.    Get Active Directory Security at 80% in 20% of the time
# @@ >   End of support: 7/31/2020
! @@@:
! .#
! .#      Vincent LE TOUX <contact@pingcastle.com>
! .#      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>

Parameters for exporting data
=====
Please specify the domain or server to investigate <default:test.mysmartlogon.com>
m)

PingCastle v2.5
Starting the task: Healthcheck for test.mysmartlogon.com
[5:32:48 PM] Getting domain information
[5:32:48 PM] Gathering general data
[5:32:48 PM] Gathering user data
[5:32:48 PM] Gathering computer data
[5:32:48 PM] Gathering trust data
[5:32:51 PM] Gathering privileged group data
[5:32:51 PM] Gathering delegation data
[5:32:51 PM] Gathering gpo data
[5:32:51 PM] Gathering anomaly data
[5:32:51 PM] Gathering domain controller data <including null session>
[5:32:51 PM] Gathering network data
[5:32:51 PM] Computing risks
[5:32:51 PM] Export completed
[5:32:51 PM] Generating xml file for consolidation report
[5:32:51 PM] Generating html report
Task Healthcheck for test.mysmartlogon.com completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

It can be run using the command:

```
PingCastle --healthcheck --server mydomain.com
```

Active Directory risk level analysis

When the health check is run, an html file and an xml file are generated. The html file represent the report of the active directory. It is designed for humans. The xml contains some of the data used to generate the html file and can be used to consolidate data on multiple active directories. It is designed to be computer read (PingCastle). **The xml file is required for all analysis, including global overview or cartography.**



test.mysmartlogon.com

Date: 2019-07-25 - Engine version: 2.5.1.0

This report has been generated on the basis of information provided by the Ping Castle tool. It is not intended to be used for legal purposes. The tool is not a security scanner and does not perform any security checks. It is only a tool for information gathering.

Active Directory Indicators

Indicators

Risk model

State Objects rule details [5 rules matched]

Trusts rule details [3 rules matched]

Privileged Accounts rule details [3 rules matched]

Anomalies rule details [9 rules matched]

Domain Information

User Information

SID History

Computer Information

Operating Systems

Domain controllers

Admin Groups

Admin Groups

Trusts

Discovered Domains

Reachable Domains

Examples

Backup

LAPS

Windows Event Forwarding (WEF)

krbtgt (Used for Golden ticket attacks)

AdminSDHolder (detect temporary elevated accounts)

NULL SESSION (anonymous access)

Login scripts

Logon scripts

Certificates

Password Policies

Screensaver policies

LSA settings

GPO

Obfuscated Passwords

Restricted Groups

Privileges

GPO Login script

The report is divided in 3 parts:

1) Scores

The Score is computed by the maximum of the 4 sub scores:

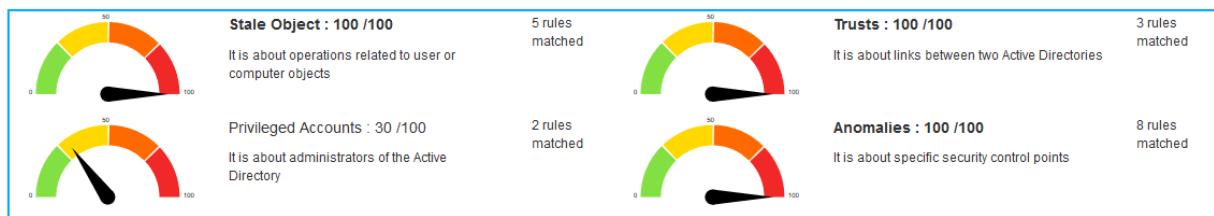
- Privileged accounts**
It is about administrators.
- Trusts**
It is about the links between Active Directories (reminder: one AD can compromise one other via trusts).
- Stale objects**
Stale objects represent everything about the AD objects and their life cycle: computer and user creation, delegation.



- **Security anomalies**

Everything that doesn't fit into the previous categories. For example the [krbtgt password change](#).

The details of the rules triggered is shown with some indication and the number of points calculated (the total cannot be above 100).



Stale Objects rule details [5 rules matched]

Number of DC vulnerable to MS17-010 = 1 (>0)	+ 100 points
Presence of wrong primary group = 1 (>0)	+ 15 points
Non admin users can add up to 10 computers to a domain	+ 10 points
Presence of Windows XP = 2	+ 10 points
SMB v1 activated on 1 DC	+ 1 points

When the button “solve it” is clicked, a short explanation of the rule is shown with some indication on how to solve the situation.

SMB v1 activated on 1 DC

+ 1 points

DC Vulnerability (SMB v1)

Description:

The purpose is to verify if Domain Controller are vulnerable to the SMB v1 vulnerability

Technical explanation:

The SMB downgrade attack is used to obtain credentials or executing commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed

Advised solution:

It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. **Do note that if you are still not following best practices regarding the usage of deprecated OS (Windows 2000, 2003, XP, CE), regarding Network printer using SMBv1 scan2shares functionalities, or regarding software accessing Windows share with a custom implementation relying on SMB v1, you should consider fixing this issues before disabling SMB v1, as it will generates additionnal errors.**

Points:

1 points if present

Documentation:

<https://github.com/lgandx/Responder-Windows>

<https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect>

<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>

Details:

Domain controller: WIN-PGAHI2ECI8E

2) General information

Contains the generated date, domain



3) Details

The Detail zone shows general information about users, computers, trusts, group policies, ...

User Information												
Nb User Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb Locked	Nb pwd never Expire	Nb SidHistory	Nb Bad PrimaryGroup	Nb Password not Req.	Nb Des enabled.	Nb Trusted delegation	Nb Reversible password
16	14	2	3	11	0	4	1	0	0	0	0	0
Inactive objects (Last usage > 6 months)												[11]
Objects with a password which never expires												[4]
Objects having the SidHistory populated												[1]
SID History												
SID History from domain					First date seen			Last date seen			Count	
test.mysmartlogon.com					2016-03-28 10:40:52Z			2016-03-28 10:40:52Z			1	

Some information can be seen in detail by clicking on the associated link. It contains data to help identify the underlying objects.

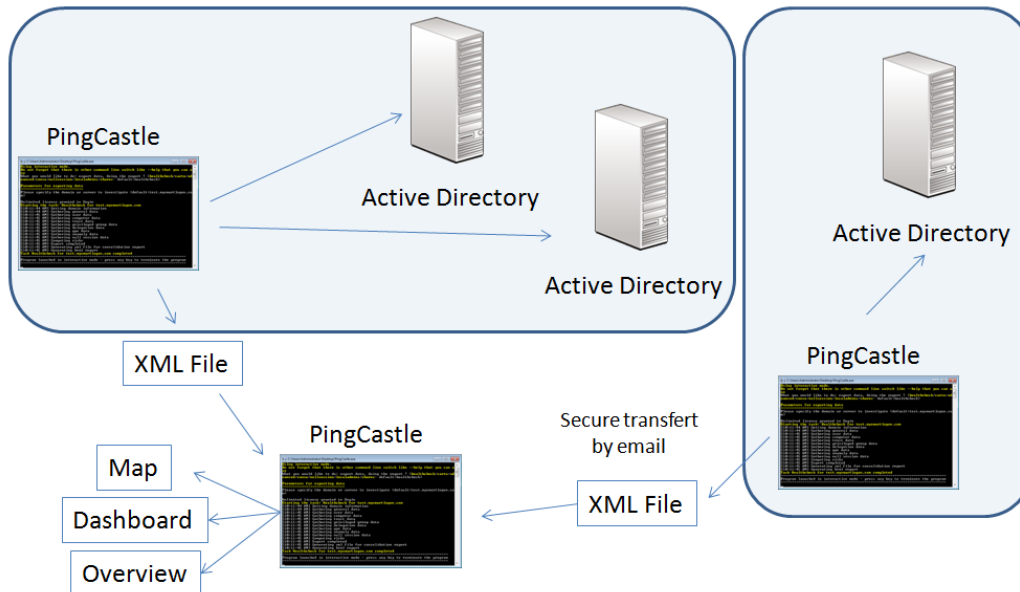
Inactive objects (Last usage > 6 months)				[11]
Name	Creation	Last logon	Distinguished name	
min	2014-06-21 21:19:29Z	2014-07-03 21:24:07Z	CN=min,CN=Users,DC=test,DC=mysmartlogon,DC=com	
HINSON	2014-11-30 16:02:50Z	Never	CN=Kimberly Hinson,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wrongAccount1	2015-06-26 10:20:33Z	Never	CN=wrongAccount1,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wrongAccount2	2015-06-26 10:20:48Z	Never	CN=wrongAccount2,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wrongaccount3	2015-06-26 11:13:15Z	Never	CN=wrongaccount3,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wronguser4	2015-06-26 15:21:03Z	2015-06-26 17:44:35Z	CN=wronguser4,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wrongAccount5	2015-06-26 15:47:18Z	Never	CN=wrongAccount5,OU=TestOU,DC=test,DC=mysmartlogon,DC=com	
wrongAccount6	2015-06-26 15:47:35Z	Never	CN=wrongAccount6,OU=TestOU,DC=test,DC=mysmartlogon,DC=com	
wrongAccount7	2015-06-27 07:26:05Z	2015-06-27 09:27:23Z	CN=wrongAccount7,OU=TestOU,DC=test,DC=mysmartlogon,DC=com	
wrongaccount8	2016-03-28 10:40:52Z	Never	CN=wrongaccount8,CN=Users,DC=test,DC=mysmartlogon,DC=com	
wrongaccount9	2016-03-30 13:02:35Z	Never	CN=wrongaccount9,OU=TestOU,DC=test,DC=mysmartlogon,DC=com	
Objects with a password which never expires				[4]
Objects having the SidHistory populated				[1]



Step3: Get reports for all domains

PingCastle has been designed to be **scalable** and used in a **decentralized architecture**.

To be the most effective, PingCastle needs to have the risk reports for all domains. Because **PingCastle doesn't need an account in the domain to audit**, you can take benefits of trusts to perform this task.



Management involvement

The management involvement is a critical factor of success. Here is how you can proceed.

You can start the project by running the tool without notifying the domain administrators to get a first overview. The healthcheck mode run on all trusted server (server set as “*”) or the carto mode can help [built a big picture of all domains involved](#).

Then you can **deploy officially in a small perimeter** and **use the report results to challenge the domain administrators**. Based on the risk indicators or on the delay required to fix the problems, you can take the opportunity to **involve the management here**.

Here some arguments which can help you involve the management about this kind of project:

- **Active Directory's security is crucial:** the probability that an auditor compromise an Active Directory is about 90%
- Management has to **prove to external auditors** that actions are being made on that topic
- The tool doesn't need any setup, installation, server, project, ... **Cost & effort are minimal**
- The risk indicators can be used to **prove that the situation has been improved** and it can be used for benchmarking (an effective management method)
- The tool returns anomalies which 80% of them **can be fixed within 5 minutes**

Decision to take

We recommend that the decision made by the management is about:

- **Deploy the tool on 100% of the domains**
For example set the initial deadline to 3 months and assign discovered trusted domain to the AD owner.
- **Request the implementation of SID Filtering on 100% of the trusts** except official migrations
For example set a list of critical domains and list the trusts linked to that domains without SID Filtering.
- **Follow the progress of these actions on the management meetings.**
For example set a monthly follow up meeting with the people involved.



Getting to 100%

Bellow is a list of reasons an entity can invoke (or remain silent) to be excepted:

- Minority share holding company
- Migration and removal of the domain in the upcoming months
- Regulations
- “Confidential information” included in the script

To handle the migration cases, PingCastleReporting **supports a “migration” status** for the domain auditing & a “migration” status for SID Filtering. In the SID Filtering case, an end date has to be defined. We recommend 3 to 12 months. Migration should be an excuse for removing anomalies, not running the script (a 5 minutes effort !).

For “confidential information”, the **xml report doesn’t include any personal information nor administrator accounts**. If the level of information included is too high, a configuration switch exists to lower the level of information. If the problem is about the transfer of the data in an unsafe channel, the tool can encrypt the xml report to solve this problem.

For other issues, we recommend to **insist if there are trusts to existing domains**. Indeed, a trust facilitates the attacker job because he knows that there is a domain via the trust information, that there can be credentials in memory (mimikatz) or that he can abuse network connection (LLMR spoofing with Python Responder). If you can’t get a report, we suggest to remove the trust to these domains.

Then for domains without a trust, you can **formally transfer the responsibility of the Active Directory compromise** and put the domain status to “Out Of Scope”.

Here is some template in [English](#) or [French](#) to transfer the responsibility.

Deploying PingCastle in decentralized locations

PingCastle **can be run on every domain of a company** using the command:

```
PingCastle --healthcheck
```

Reports can then be regrouped to produce a global view. See below for the technics (encryption, transfert by email) to centralize the reports.

Deploying PingCastle in centralized locations

PingCastle **can be run on a Bastion Active Directory**, generally used to perform administration tasks. In this case, all the domains will be scanned.

```
PingCastle --healthcheck --server *
```

The program **can be run on every forest root** and be limited to that perimeter

```
PingCastle --healthcheck --server *.forest.root
```

The tool **can be run on every forest child** and explore the child and its trusted domains. In this case the forest root is excluded.

```
PingCastle --healthcheck --explore-trust --server child.forest.root
```

PingCastle can explore all the domains of all the trusted forests from another forest. This is useful when the root and child doesn’t share the same name.

```
PingCastle --healthcheck --explore-forest-trust --server anotherforest.root
```

If needed, exceptions can be set to not scan domains. For example to not scan the Bastion domain multiple times. In this case use the option `--explore-exception <domains>` where domains are comma separated domain name.



Centralizing reports

Encryption

Sometimes, domains are unconnected or it is not possible to make the schedule tasks centralize in a single share all the reports. To deal with this case, **PingCastle can encrypt the reports to send them in an unsafe channel.**

A RSA key pair need to be generated and the public key needs to be shared with all the instance of the program. When producing risks reports and generating the .xml files, add the flag `--encrypt` to perform the encryption.

You can generate a keypair using the following command and copy the public key in the .config file to be deployed.

```
PingCastle.exe --generate-key
```

Starting the task: Generate Key

Public Key (used on the encryption side):

```
<encryptionSettings encryptionKey="default">
  <RSAKeys>
    <!-- encryption key -->
    <KeySettings name="default" publicKey="&lt;RSAKeyValue&gt;&lt;Modulus&gt;h
4smrLAZZ30QwWXHcT1oNz3hH3Ax2R9T75DlioGFCIdLb0QhUn3N8NWgJ2ZgyUNXn4qU1b0Ds10IhK+Cq
oqCPvXuHjK6TGrMyphtcbZvvgbLxfyalJemczx1+pOuBlqqVdalE94rnnnBr761WIJJnkJdZ0rzYsebn
DwGuk9kiw8=&lt;/Modulus&gt;&lt;Exponent&gt;AQAB&lt;/Exponent&gt;&lt;RSAKeyValue
&gt;"/>
    <!-- end -->
  </RSAKeys>
</encryptionSettings>
```

Private Key (used on the decryption side):

```
<encryptionSettings encryptionKey="default">
  <RSAKeys>
    <!-- decryption key -->
    <KeySettings name="39b5d076-17be-4999-b43e-b894a55446a1" privateKey="&lt;R
SAKeyValue&gt;&lt;Modulus&gt;h4smrLAZZ30QwWXHcT1oNz3hH3Ax2R9T75DlioGFCIdLb0QhUn3
N8NWgJ2ZgyUNXn4qU1b0Ds10IhK+CqoqCPvXuHjK6TGrMyphtcbZvvgbLxfyalJemczx1+pOuBlqqVda
lE94rnnnBr761WIJJnkJdZ0rzYsebnDwGuk9kiw8=&lt;/Modulus&gt;&lt;Exponent&gt;AQAB&lt;
;/Exponent&gt;&lt;P&gt;uwgX794pe703vIiQR5v03WK3Ug5LUAbXpPF6Xq4qGb3TGprZaJQq5rZ2u
J4qwRanOa5pI/zv7RhG/4ItesBuAw==&lt;/P&gt;&lt;Q&gt;uYanLEp9Vh8F29tSH+M4z+OjxPl+UL
LRjLrssFLTTnsdnrHgAtdJ11xfIm/gTUa0qPLa9Y/xkUb1khK/+tV3BQ==&lt;/Q&gt;&lt;DP&gt;Fd
feI8+IfMACH2xTnWljca+jxVuSBCioasUhC4m/tP3sd8D5/zK+x+8rcmhWifKBWUU7V6mHsS1FhY4BY
wPzQ==&lt;/DP&gt;&lt;DQ&gt;gzfwh8AT0CLXEP6ZomYi2571ST8xoUAoyEG5gKjEPJrJ42Fp0HiXB
9+Dhibc3atBwjEqvv5VXGx06iEK2g27RQ==&lt;/DQ&gt;&lt;InverseQ&gt;HRKFjYwrXqgO4v8Q+J
SOqR61SvQ15Z6V4AE23i4xfeuIYWwVf0t8AwgkDfFRQnEyh24byuh5PPzUbDOsUY+eYg==&lt;/Inver
```




```
seQ&gt;&lt;D&gt;QQ6pIXnkt6dvw2P2to0i4eDxjQVs56oBv5rske5YzB8kNeOdmqHXnEqzb519iQ8  
incZuP1gKNevTwBu1yxkFuFh0dzjS3iBjHvYGtDo5mARiZ1nN8QNI2zKE+Q6qXF8Z+wN3Fv3oBDQXATI  
6IQbgkAxLTMo4CUmtUQ6GvjwFwE=&lt;/D&gt;&lt;/RSAKeyValue&gt;"/>  
<!-- end -->  
</RSAKeys>  
</encryptionSettings>  
Done  
Task Generate Key completed
```

Then copy the private key section in the PingCastle and PingCastleReporting configuration file (.config) used to consolidate the results. PingCastle will perform the decryption automatically.

The program can generate an encrypted copy of a report (public key needed) and a decrypted copy of a report (private key needed) using the following commands:

```
PingCastle --reload-report report.xml --encrypt  
PingCastle --reload-report encrypted-report.xml
```

Note: Only one key can be specified for encryption but multiple keys can be used for decryption. Their selection is automatic.

Email

PingCastle can contact if specified a SMTP server to **send the reports by email**. If the encryption is set, the program will encrypt the reports. Use `--sendXmlTo <email>` to send only the xml report, `--sendHtmlTo <email>` to send only the html report and `--sendAllTo <email>` to send both html and xml report. Email addresses are comma separated ones and the previous flags can be combined.



Step4: Getting an overview

How much users or computers do you have ? Should you purchase additional support for Windows XP or Windows 2003 ? Should you plan an administrator cleanup ? Are the requirements for a 8 characters password enforced ?

This is the kind of questions you can answer with the simplest consolidation. Indeed, the program can be used to aggregate the report results.

Operations to perform

The consolidation process is working on the xml files generated by the consolidation report. By default, the files are picked in the directory (or sub directory) where the program is run. If there are duplicate reports, only the most recent is used.

To generate the report, enter “conso” in the interactive mode.

```
C:\Users\Administrator\Desktop\pingcastle\PingCastle.exe

!:.      PingCastle <Version 2.5.1.0>
! #:.    Get Active Directory Security at 80% in 20% of the time
# @@ >   End of support: 7/31/2020
! @@@:
! :.#
! :      Vincent LE TOUX <contact@pingcastle.com>
! :      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
conso
PingCastle v2.5
Starting the task: Healthcheck consolidation
Reports loaded: 1 - on a total of 1 valid files
Simplified graph: automatic center on test.mysmartlogon.com <S-1-5-21-4005144719-3948538632-2546531719>
Simplified graph: you can change this with --center-on <domain>
Simplified graph: contains 3 nodes on a total of 3
Task Healthcheck consolidation completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

Or type the following command line:

```
PingCastle --hc-conso
```

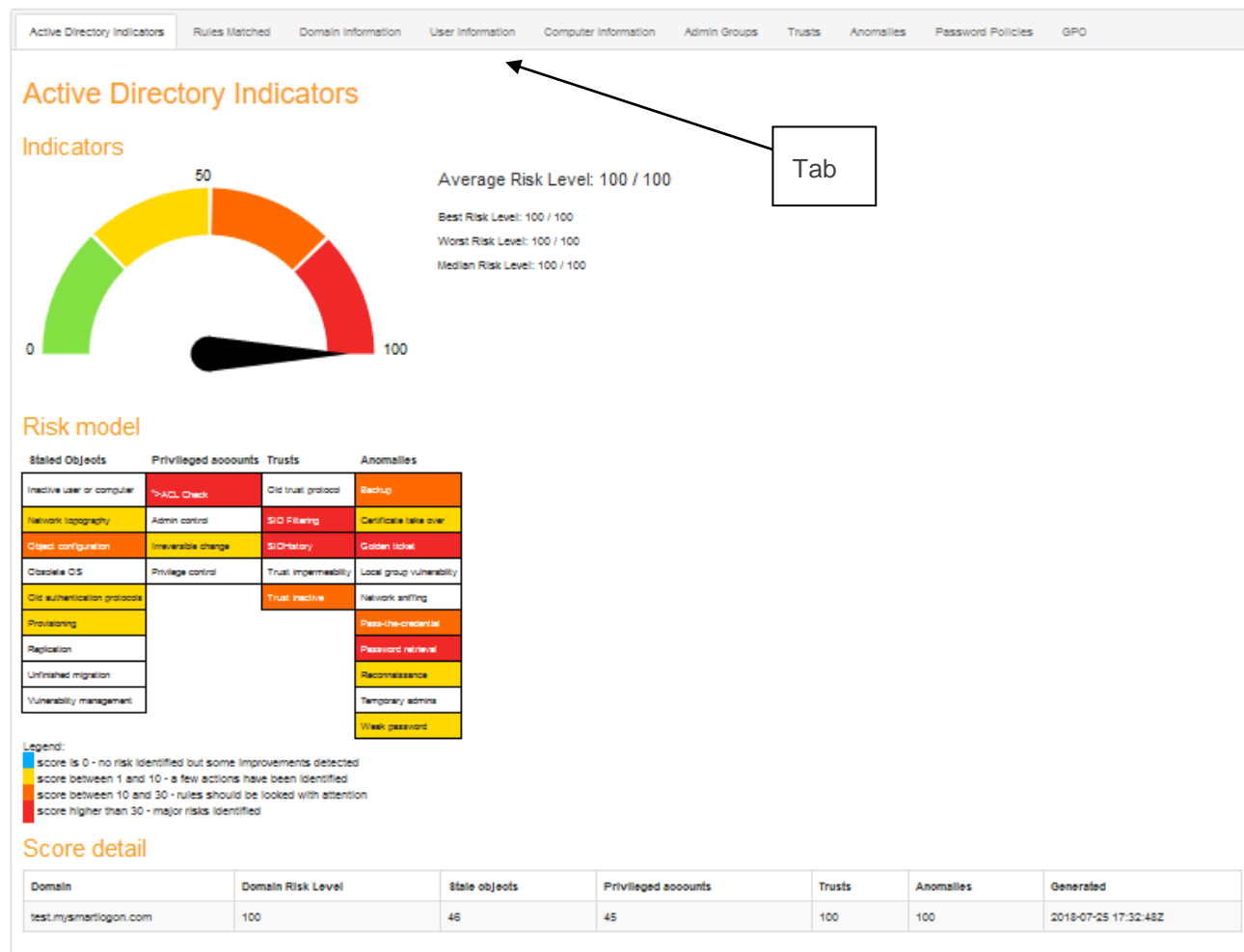
Note: This report is generated automatically when the healthcheck is performed with the server “*”

Consolidation report

The consolidation report is a concatenation of all data contained in the report, without the detail. It follows the same plan than a simple report.

Consolidation

Date: 2018-07-25 - Engine version: 2.5.1.0



When the consolidation is made, 3 html files are generated.

File ad_hc_summary.html

The first one contains the summary of all the reports: It keeps the same structure than the detailed reports but with a higher level of detail.

[Example](#)

ad_hc_summary_full_node_map.html

The second file is a map build on all trusts. See [domain discovery](#).

[Example](#)

ad_hc_summary_simple_node_map.html

The third file is a map build on all trusts. See [domain discovery](#).

[Example](#)



Step5: Dashboard

Operations to perform

This step requires in input a file describing the organization of the Active Directory domains. This information can be an empty file at the start and this file can be completed after each run. The procedure to create it is described below.

In summary:

1. Create an empty configuration file
2. Run the advanced consolidation to create the Excel report
3. Use the information provided in the report to complete the configuration file
4. Iterate to the 2nd step until all domains have been assigned to an owner
5. Produce the PowerPoint report

Configuration file

Run the program **PingCastleReporting** and enter “**template**” in the interactive mode. An empty `ad_gc_entitymap.xlsx` will be created. As an alternative, run the command:

```
PingCastleReporting --gc-template
```

	A	B	C	D	E
1	BU	Entity	Domain	Status	Contact
2	SuperHeroes	SUPER	superman.heros.com	1-Active	
3	SuperHeroes	BAT	batman.heros.com	1-Active	
4	SuperHeroes	SUPER	supergirl.com	1-Active	
5	BadGuys	ARKAM	joker.badguys.com	1-Active	
6	BadGuys	ARKAM	otherbadguys.com	2-Removed	
7	BadGuys	OTHER	otherdomain.com	1-Active	

The configuration file contains 3 sheets:

1. The sheet “Domains” making the link with a domain and its owner
The 2 mandatory columns are : BU and Domain. Entity, Contact or Comment can be left blank.
2. The sheet “Migrations” to not impact the score of an AD being officially migrated
3. The sheet “Exceptions” to deal with false positive or with situation whose risks have been accepted

The **individual** scores of the domains will be recomputed to take the information of the sheet “**Migrations**” and “**Exceptions**” into account. For example the rules about SID Filtering or SID History.

Generation of the Excel report

Run the program **PingCastleReporting** and enter in the interactive mode “**conso**”. As an alternative, run the command:

```
PingCastleReporting --gc-conso
```



```
e:\Documents\programmation\PingCastle\bin\Debug\dem...
Using interactive mode.
Do not forget that there is other command line switch like --help that you can use
What you would like to do: export data, doing the report ? (template/conso/history/overview/all- default:all)
conso
Starting the task: Group consolidation
Reports loaded: 2 - on a total of 2 valid files
Loading ad_gc_entitymap.xlsx
source domain souredomain.com not found in Domains sheet
target domain souredomain.com not found in Domains sheet
Generating ad_gc_summary_group.xlsx
Generating ad_gc_summary_full_node_map.html
Generating ad_gc_summary_simple_node_map.html
Simplified graph: automatic center on xnx.zjmaj (5-1-5-21-1206779787-896296972-1300041293)
Simplified graph: you can change this with --center-on <domain>
Simplified graph: contains 65 nodes on a total of 65
Done
Task Group consolidation completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

The program will load the file `ad_gc_entitymap.xlsx` in the current path and produce the Excel file `ad_gc_summary_group.xlsx`. It will also produce the maps described [at the previous chapter](#).

The file `ad_gc_summary_group.xlsx` is an Excel file composed by many sheets:

1. The sheet BU and entity contains information related to the BU level or the Entity level.

	A	B	C	D	E	F	G	H
1	BU	Domain Number	% of script deployment	Average Risk Level	Trust Number	% of safe trust	Last update date	First update date
2	SuperHeroes	15	0%	0	0	100%		
3	BadGuys	9	11%	61	2	100%	23/08/2016 12:48	23/08/2016 12:48

2. The sheet Domains contains the detailed information related to the domains' scores combined with the information specified in the configuration file.
3. The sheet Trusts contains the detailed information related to the trusts.
4. The sheet Discovered AD displays the domains found and their probable assignment. **This information can be used to complete the configuration file.**
5. The sheet Migrations summarize the migration of users or computers between domains. It helps setup the Migrations sheet of the configuration file to be able to tune the configuration and adjusts the score in consequence.

Generation of the PowerPoint report

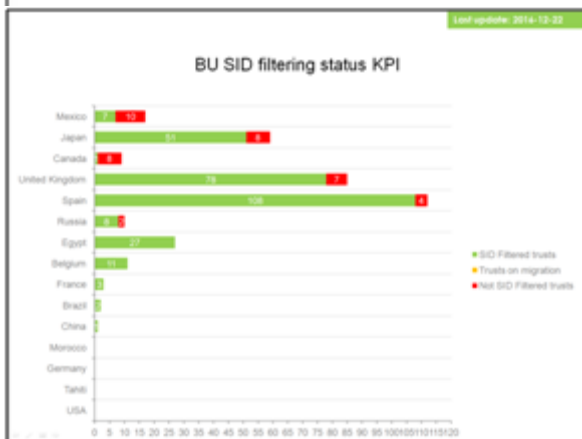
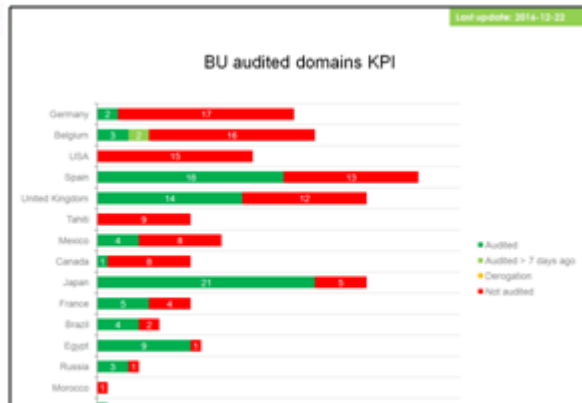
Run the program **PingCastleReporting** and enter in the interactive mode **"overview"**. As an alternative, run the command:

```
PingCastleReporting --gc-overview
```

The program will load the file `ad_gc_entitymap.xlsx` in the current path and produce the Powerpoint file `ad_gc_overview.pptx`.

The template used to generate can be exported with the flag `--export-pptx-template`, modified, then loaded using the flag `--use-pptx-template`. Only slides with special notes will be altered.

[Example of dashboard](#)





PingCastle can be used to make quick security analysis like:

- Who can get the control of the CEO account or the domain ?
- Can an auditor enumerate all the users of the domain without an account ?
- How much local administrators are there ?
- How much public shares are published on local computers ?

The tool can be used to build compromise graph analysis (thanks to [AD-control-paths](#)), check null sessions, local admins or local share.

Compromise graphs

Compromise graphs are networks where user, groups, computer are connected. They explain how a user can take the control of another account. **It can be used to answer the question: Who can get the control of the CEO account or the domain ?**

```
C:\Users\Administrator\Desktop\pingcastle\PingCastle.exe

:~.      PingCastle (Version 2.5.1.0)
: #~.    Get Active Directory Security at 80% in 20% of the time
# @@ >   End of support: 7/31/2020
! @@@:
:~.      Vincent LE TOUX <contact@pingcastle.com>
:~.      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
advanced
Parameters for advanced mode
=====
Would you like to open an existing dump, create one or work on the AD in live mode ?
Enter a dump file name (*.sdf) or the name of a domain previously used to query it. Enter "new" to create a new dump file. Enter "live" to enable the live mode and query the server directly.
Note: The live mode is faster for one shot investigation but cannot perform all the reports
Default: live

Parameters for exporting data
=====
Please specify the domain or server to investigate (default:test.mysmartlogon.com)

Parameters for advanced report
=====
Please specify the user to investigate (sAMAccountName, display name):
If no user is selected, the program will make the default reports

PingCastle v2.5
Starting the task: Advanced live export & report
[15:48:29 PM] Doing the export
[15:48:29 PM] Getting domain informations
[15:48:30 PM] Exporting objects from Active Directory
[15:48:30 PM] Inserting relations between nodes in the database
[15:48:30 PM] Export completed
[15:48:30 PM] Doing the report
Report for dom_cmp_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for dom_gue_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for dom_usr_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for guests_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for guest_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for usr_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
Report for waac_from_short ignored because this is a live analysis (live analysis doesn't support reverse direction analysis)
[15:48:30 PM] Done
Task Advanced live export & report completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

Requirements

Except from live reports, SQL CE must be installed ([download](#)). This component is installed by default in most of the OS but may not be installed on servers.

Overview

The advanced mode is a two steps process:

1. collect the data from the AD



2. run an analysis to find links between a target and all AD objects.

PingCastle supports 2 modes:

- live mode where all the queries are made online (**recommended**)
Pro: quick **Con:** no archive and no reverse direction analysis
- dump mode where the data is stored in a SqlCE database
Pro: offline analysis, reverse direction analysis **Con:** more time required to export data

This process can be run quickly using the interactive mode or manually using the command line:

- Using the live mode

```
PingCastle --advanced-live--server mydomain.com
```

- Using the dump mode
 - Run the export:

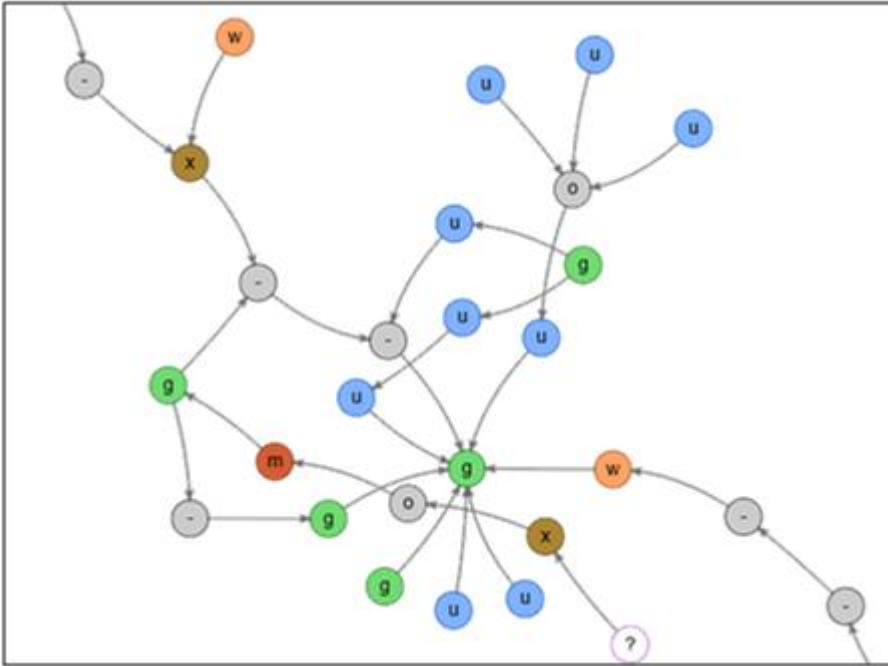
```
PingCastle --advanced-export --server mydomain.com
```

- Build the reports:

```
PingCastle --advanced-report --database thegeneratedsdf file.sdf
```

In the case of the interactive mode, the .html for the most common reports are generated automatically.

- ad_cp_test.mysmartlogon.com_accop_to_short.html
- ad_cp_test.mysmartlogon.com_adm_dom_to_short.html
- ad_cp_test.mysmartlogon.com_adm_ent_to_short.html
- ad_cp_test.mysmartlogon.com_adm_sch_to_short.html
- ad_cp_test.mysmartlogon.com_adm_to_short.html
- ad_cp_test.mysmartlogon.com_adms_to_short.html
- ad_cp_test.mysmartlogon.com_backup_to_short.html
- ad_cp_test.mysmartlogon.com_certpub_to_short.html
- ad_cp_test.mysmartlogon.com_cryptop_to_short.html
- ad_cp_test.mysmartlogon.com_dc_to_short.html
- ad_cp_test.mysmartlogon.com_dom_cmp_from_short.html
- ad_cp_test.mysmartlogon.com_dom_gue_from_short.html
- ad_cp_test.mysmartlogon.com_dom_usr_from_short.html
- ad_cp_test.mysmartlogon.com_erodc_to_short.html
- ad_cp_test.mysmartlogon.com_gpoco_to_short.html
- ad_cp_test.mysmartlogon.com_guest_from_short.html
- ad_cp_test.mysmartlogon.com_guests_from_short.html
- ad_cp_test.mysmartlogon.com_incftb_to_short.html
- ad_cp_test.mysmartlogon.com_krbtgt_to_short.html

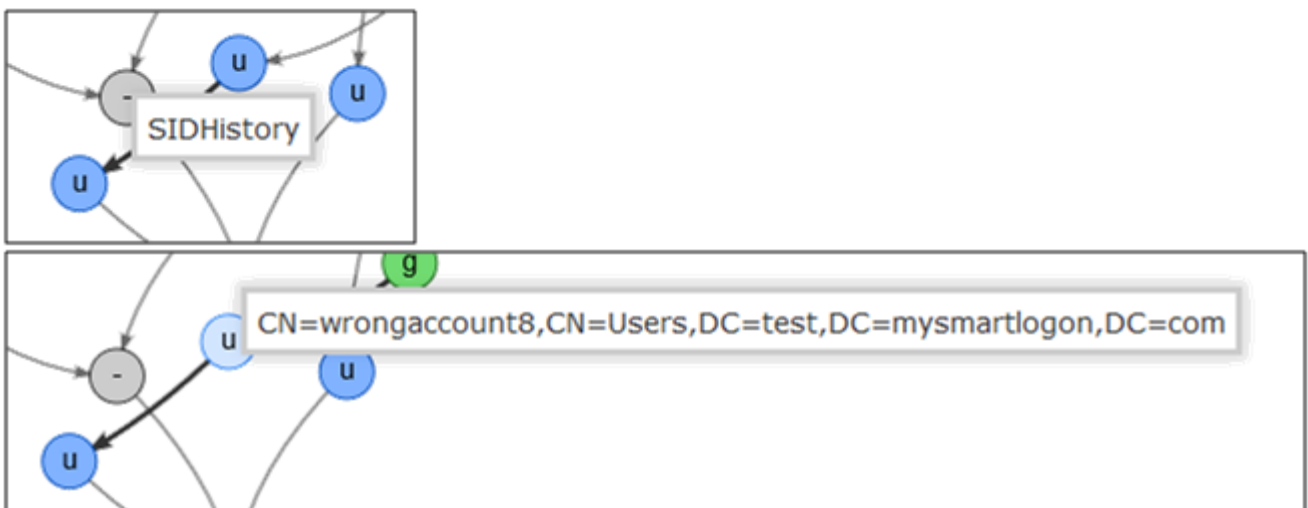


A graph is shown on the window.

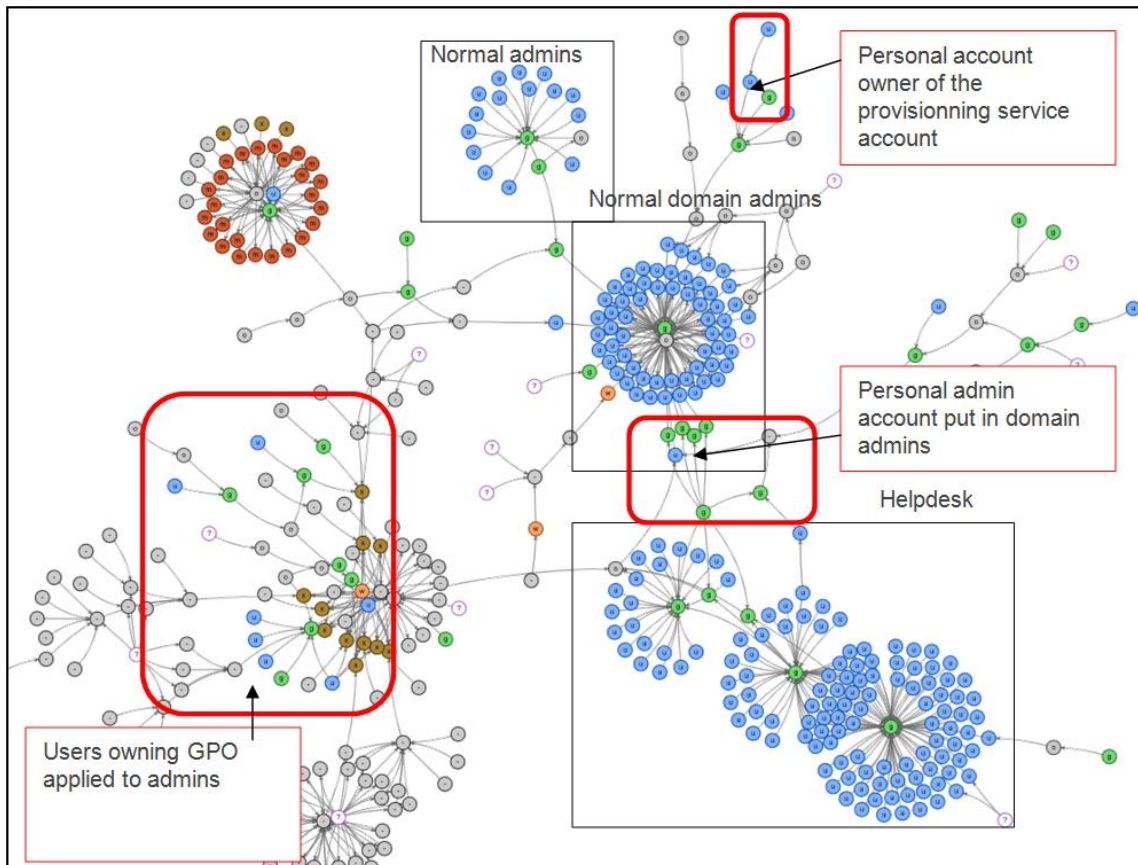
Some explanation about the nodes:

- u: user
- g: group
- o: OU
- w: well known security principals
- -: other common type like domain, built-in, ...
- ?: the program was not able to get more information. Typically SID not resolved or account from other domains

In this example, a path can be found using the SID History and the name of the account can be displayed.



A real life example:



Null sessions

Null sessions are an old Windows NT4 problem. It should have been disappeared but is still present on 20-30% of the domains. When it is enabled, an auditor with no account on the domain can use this to enumerate all the accounts of the domain. Then this list can be used to generate wrong authentication attempts and lock the accounts. Or perform brute-force attacks.

You can use PingCastle to attempt to extract a list of user accounts using this functionality. Run the following command:

```
PingCastle --nullsession --server <servertotest>
```



Scanners

```
C:\Users\Administrator\Desktop\pingcastle\PingCastle.exe

!:.      PingCastle <Version 2.5.1.0>
! #:..   Get Active Directory Security at 80% in 20% of the time
! @@ >   End of support: 7/31/2020
! @@@:
! :#
! :#      Vincent LE TOUX <contact@pingcastle.com>
! :#      https://www.pingcastle.com

Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do: export data, doing the report ? <healthcheck/carto/advanced/conso/nullsession/scanner- default:healthcheck>
scanner
WARNING
Checking a lot of workstation in a short time using tcp/445 can raise alerts to a SOC. Be sure to have warned your security team.
Parameters for advanced mode
=====
What scanner would you like to run ?
localadmin
Enumerate the local administrators of a computer.
ms17-010
Check for the ms17-010 vulnerability without exploiting it. Beware that it may trigger AU response by closing the connection
replication
Search replication metadata for modification done in the past but recorded more than 1 day after the supposed modification
share
List all shares published on a computer and determine if the share can be accessed by anyone
smb
Scan a computer and determine the smb version available. Also if SMB signing is active.
startup
Get the last startup date of a computer. Can be used to determine if latest patches have been applied.
```

Local administrators

The local administrator accounts can be used in an attack to recover passwords in memory with tools like mimikatz. You can enumerate most of them without any privilege with PingCastle with the following command:

```
PingCastle --scanner localadmin --server <domainToExplore>
```

Local shares

Local shares can be opened to everyone and be storing confidential information like login and passwords or backups. PingCastle can do a quick scan without any privilege and locate open share using the following command:

```
PingCastle --scanner share --server <domainToExplore>
```

Start time

Any authenticated users can get the start time of a computer in the domain and even unauthenticated ones if SMB v2 is activated. PingCastle can do a quick scan without any privilege and gather the start time of all computers of the domain:

```
PingCastle --scanner startup --server <domainToExplore>
```

SMB version

PingCastle can do a quick scan without any privilege to know which version is supported as server for each computer of a domain:

```
PingCastle --scanner smb --server <domainToExplore>
```

Other

Exploit inbound trust to get the user list

An inbound trust (an unidirectional trust) is understood as a diode. Nothing is supposed to be extracted. But this is not true. PingCastle can extract the list of users from an inbound trust via a MS-LSAT enumeration:



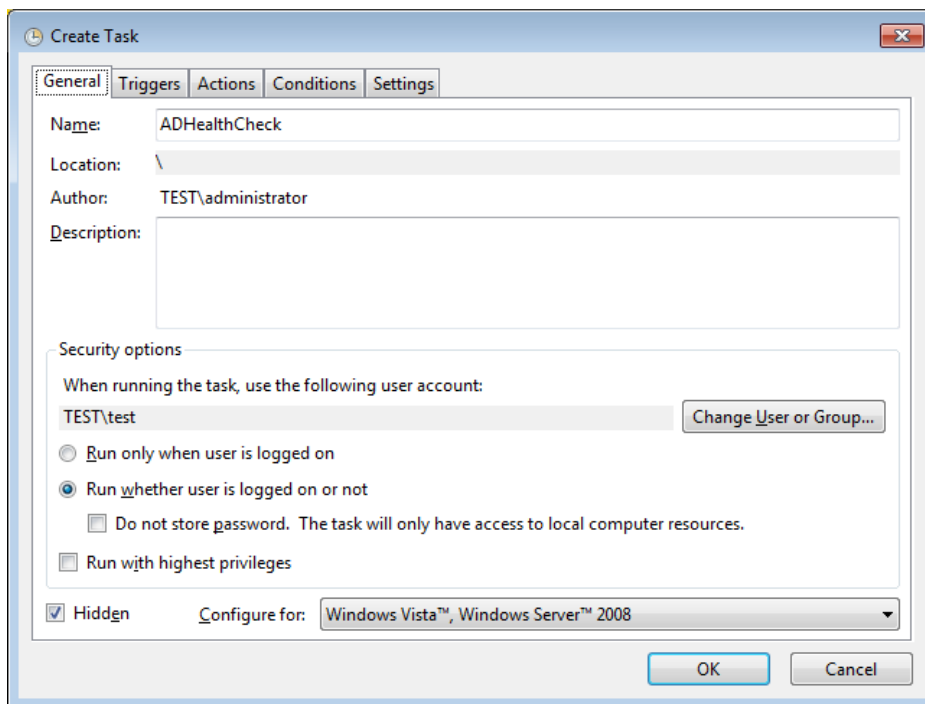
```
PingCastle --enum inbound <remote domain or sid> --server <domainToExplore>
```



Annex: Scheduling the health check

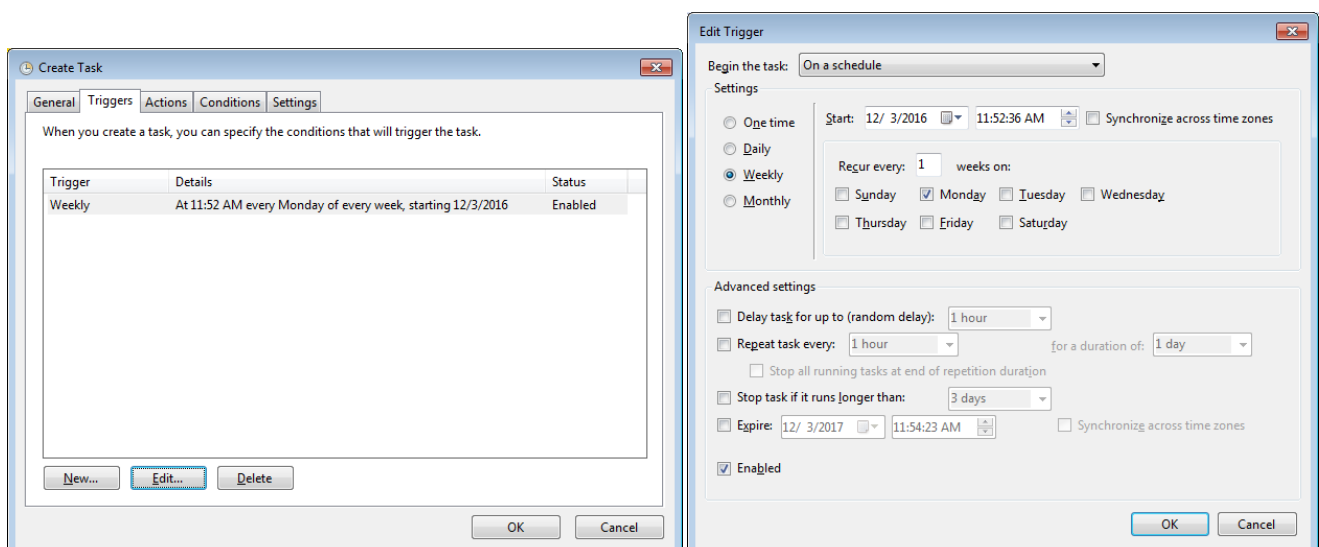
The program is compatible with the "managed service account" available since Windows 2008 R2 and if the scheduled task is run on Windows 2012.

Important setting: check "run whether user is logged on or not" and choose a service account running under the domain (not a local account). Check hidden to hide the console.



The "Create Task" dialog box is shown with the "General" tab selected. The "Name" field is "ADHealthCheck", "Location" is "\", "Author" is "TEST\administrator", and "Description" is empty. Under "Security options", "When running the task, use the following user account:" is "TEST\test". The radio button "Run whether user is logged on or not" is selected. The checkbox "Do not store password. The task will only have access to local computer resources." is checked. The checkbox "Run with highest privileges" is unchecked. The checkbox "Hidden" is checked. The "Configure for:" dropdown is set to "Windows Vista™, Windows Server™ 2008".

Set the schedule:

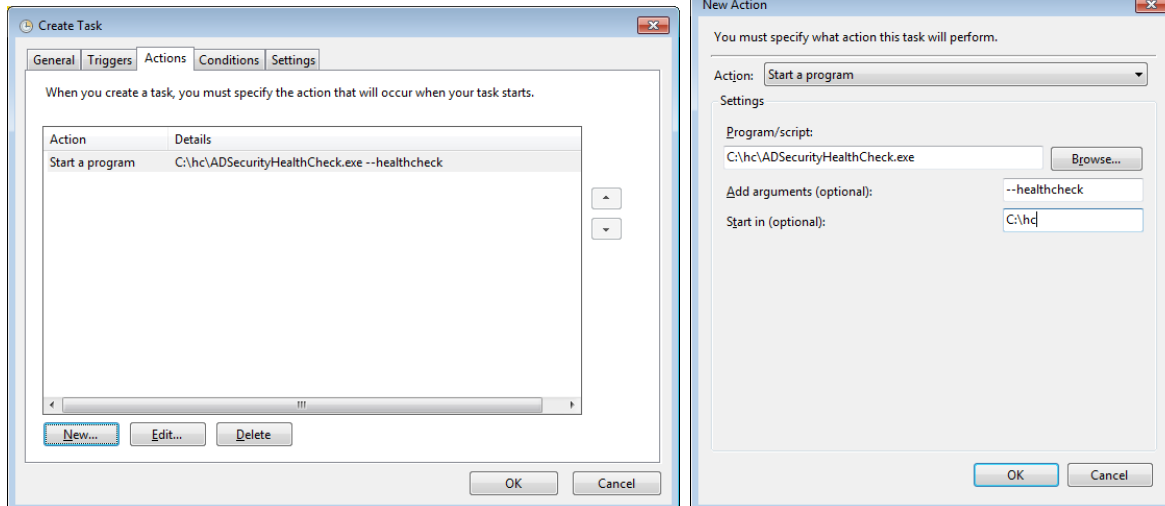


The "Create Task" dialog box is shown with the "Triggers" tab selected. The "Trigger" table is as follows:

Trigger	Details	Status
Weekly	At 11:52 AM every Monday of every week, starting 12/3/2016	Enabled

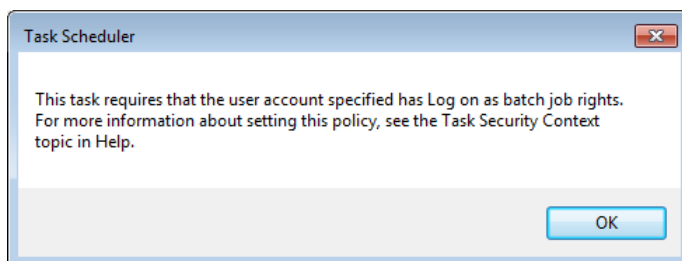
The "Edit Trigger" dialog box is shown with the "Settings" tab selected. The "Begin the task:" dropdown is "On a schedule". The "Settings" section has "One time" selected. The "Start:" date is "12/ 3/2016" and time is "11:52:36 AM". The "Synchronize across time zones" checkbox is checked. The "Recur every:" is "1" weeks on: "Monday". The "Advanced settings" section has "Repeat task every:" "1 hour" for a duration of "1 day". The "Stop task if it runs longer than:" is "3 days". The "Egpire:" is "12/ 3/2017" and time is "11:54:23 AM". The "Synchronizg across time zones" checkbox is checked. The "Enabled" checkbox is checked.

Set the command line:

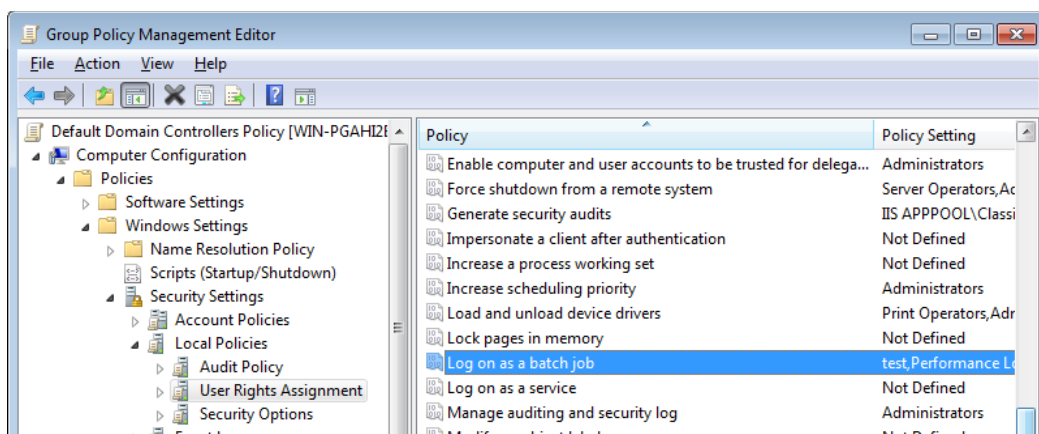


Be sure that the service account has the right to write the report in the current directory.

If you get the following message, be sure that the user as the right to logon as batch job.



This can be modified in the security policies:

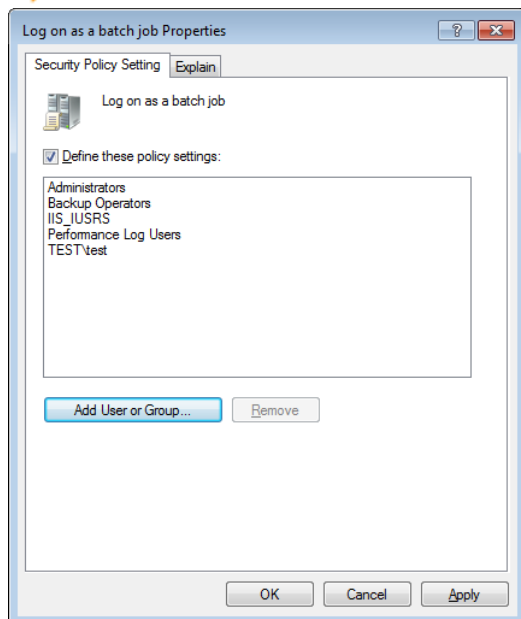


Select "Local Policies" in MSC snap in

Select "User Rights Assignment"

Right click on "Log on as batch job" and select Properties

Click "Add User or Group", and include the relevant user.



If the button "Add User or Group" is grayed, that means that the setting is overridden by a GPO (by default, the Domain Controller Policy). You can find the GPO by running `rsop.msc`, locate the setting and look at the "Policy" sheet.