



PingCastle Basic Edition

Version: 2.8.0



| | |
|--|----|
| About PingCastle | 4 |
| "For CISO, by CISO" | 4 |
| License | 4 |
| Methodology..... | 4 |
| How to use PingCastle | 5 |
| Requirements | 5 |
| How it works..... | 6 |
| Installation..... | 6 |
| Run the program..... | 7 |
| Getting help..... | 7 |
| Generating log file for support requests..... | 7 |
| Performing an Active Directory health check | 8 |
| Perform domain discovery | 13 |
| Option 1: performing multiple health check reports (recommended)..... | 13 |
| Option 2: when having existing health check reports..... | 14 |
| Option 3: perform a quick domain exploration (fastest but not scalable)..... | 14 |
| Maps..... | 15 |
| Full domain map | 15 |
| Simple domain map | 17 |
| Hilbert map..... | 17 |
| Deploying PingCastle | 19 |
| Involvement of the management | 19 |
| Deploying PingCastle in centralized locations | 21 |
| Updating PingCastle..... | 21 |
| Centralizing reports | 22 |
| Encryption | 22 |
| Email..... | 23 |
| API..... | 24 |



| | |
|---|----|
| Getting an overview with multiple reports | 25 |
| Scanners | 29 |
| Annex | 31 |
| Command line reference..... | 31 |
| Full command line options..... | 32 |
| List of open source software used..... | 36 |
| Scheduling PingCastle report..... | 37 |





About PingCastle

“For CISO, by CISO”

PingCastle was born based on a finding: security based only on technology does not work. That's why the company focuses on process and people rather than just technology. PingCastle does not sell products !

The company does not provide solutions to protect your infrastructure. Instead, it provides tools to discover what you have to protect, evaluate its security level and provide insights on if the budget you have provided has been successfully used.

PingCastle'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 !

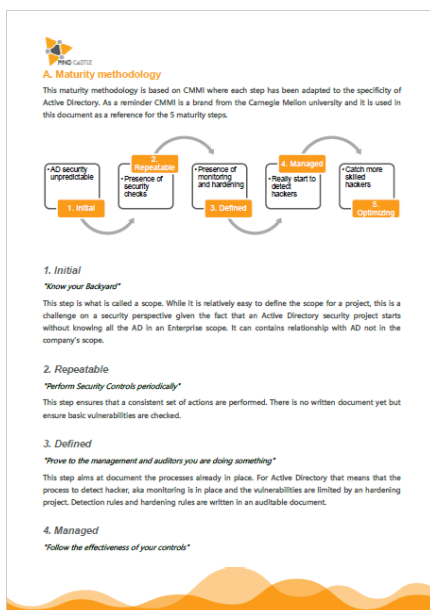
Vincent LE TOUX

License

The source code of the program is licensed to the Non-Profit Open Software License (“Non-Profit OSL”) 3.0.

Regarding the binary code, **Being part of a commercial package is forbidden** except if a license is purchased. Check the "our services" section on <https://www.pingcastle.com> for more information.

The program is allowed to run only during its support date. Support can be extended by purchasing additional support.



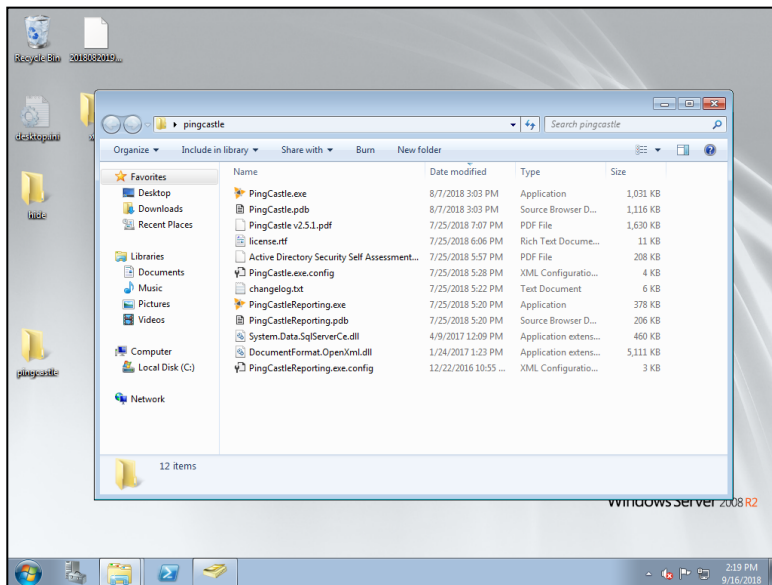
Methodology

The PingCastle tool is just one part of a global methodology aiming at securing Active Directories.

You can get more information about this methodology by visiting the website <https://www.pingcastle.com/methodology/>



How to use PingCastle



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.

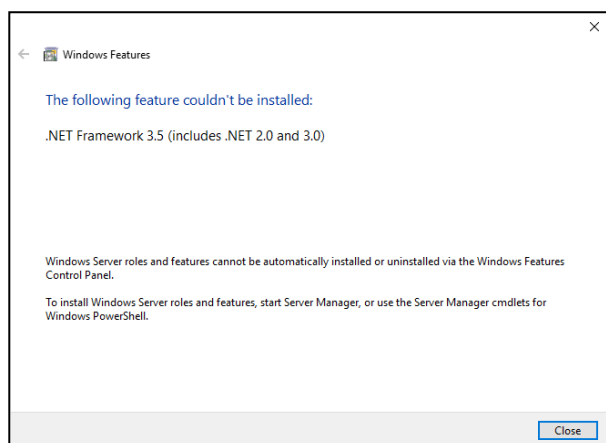
The analysis tool (PingCastle.exe) requires DotNet 3.0 (or next versions) which is available by default since Windows Vista. It can be run under DotNet 2.0 but with fewer functionalities.

The reporting tool (PingCastleReporting.exe) requires DotNet 3.5 (or next versions) which is available



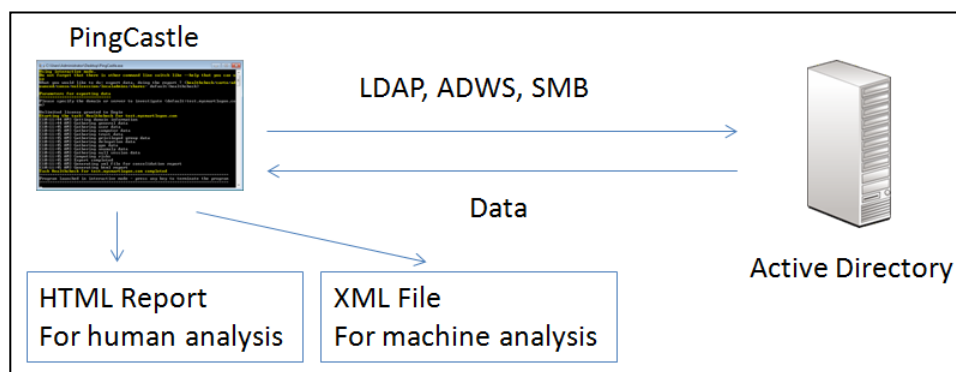
by default since Windows Seven. Files produced by the reporting tool are .xlsx and .pptx. To read them, you may install the [Excel Viewer](#) or the [PowerPoint Viewer](#) or any viewer compatible like [OpenOffice](#).

Starting from PingCastle 2.7, PingCastle.exe can be run without the .config file next to the program. But in this case, the program will be run under the .Net 3.5 framework (and not the .Net 4 which is installed by default on Windows 10). Windows does show a popup to suggest the installation of the missing framework.

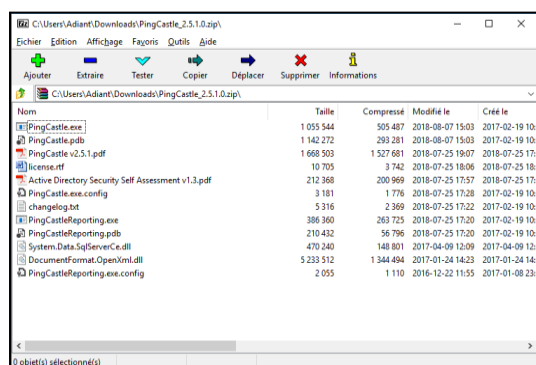


How it works

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.



Installation

PingCastle Basic Edition is provided in a zip file. You need a program such as 7zip or the native unzip program to decompress the file.

For the most operating systems, PingCastle does not need any more actions.

For Windows 2000, the dotnet framework 2.0, which is the last

supported version, need to be installed.



The two files required to run scans are PingCastle.exe and PingCastle.exe.config

Run the program

The best way is just to double click on PingCastle.exe

```
C:\Users\Administrator\Desktop\PingCastle.exe
[.] PingCastle (Version 2.5.2.0)
[.] #:. Get Active Directory Security at 80% in 20% of the time
[.] #EE> End of support: 12/31/2018
[.] #EE: 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 would you like to do?
1-healthcheck-Score the risk of a domain
2-graph-Analyze admin groups and delegations
3-conco-Aggregate multiple reports into a single one
4-nullsession-Perform a specific security check
5-carto-Build a map of all interconnected domains
6-scanner-Perform specific security checks on workstations
```

This run the program in a mode called the "interactive mode.

The program can be run using a command line. A command line can be run by searching for "cmd" or "command line" in the start menu.

Then a drag and drop of the file "PingCastle.exe" automatically populates the command line with the binary. The same can be done with other files ending with ".exe"

Getting help

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>C:\Users\Administrator\Desktop\PingCastle.exe --help

[.] PingCastle (Version 2.5.2.0)
[.] #:. Get Active Directory Security at 80% in 20% of the time
[.] #EE> End of support: 12/31/2018
[.] #EE: 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 a
ll 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 (fastes
t)
                  : ADWSThenLDAP (default), ADWSOnly, LDAPOnly, LDAPThenADWS
```

PingCastle can display its help on a command line.

Indeed PingCastle has a lot of switches which can be displayed using the command line:

```
PingCastle.exe --help
```

Do not forget also to check the website <https://www.pingcastle.com> or on twitter @mysmartlogon

Generating log file for support requests

PingCastle can collect logs with the --log switch

However when a command line argument is submitted, the interactive mode is disabled and the module has to be launched manually. To avoid that, the "interactive mode" can be activated manually using the command:

```
PingCastle.exe --log --interactive
```



```
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)

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
=====
```

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

Active Directory risk level analysis

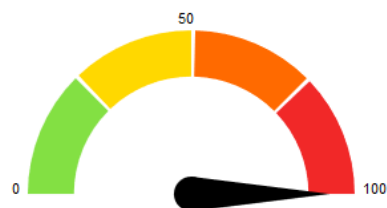
When the health check is run, an html file and an xml file are generated. The html file represent the report of the active directory. It is designed for humans. The xml contains some of the data used to generate the html file and can be used to consolidate date on multiple active directories. It is designed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

test.mysmartlogon.com

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

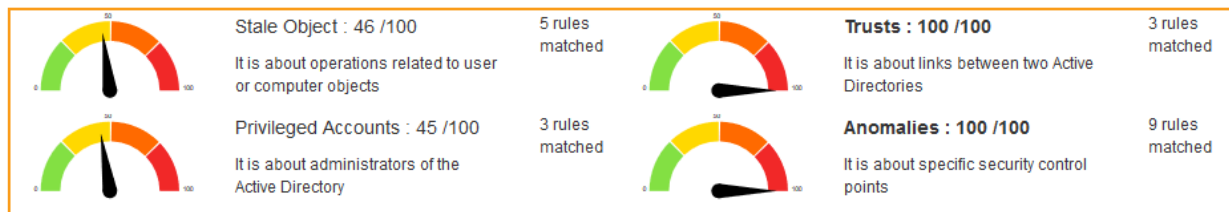
Active Directory Indicators

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



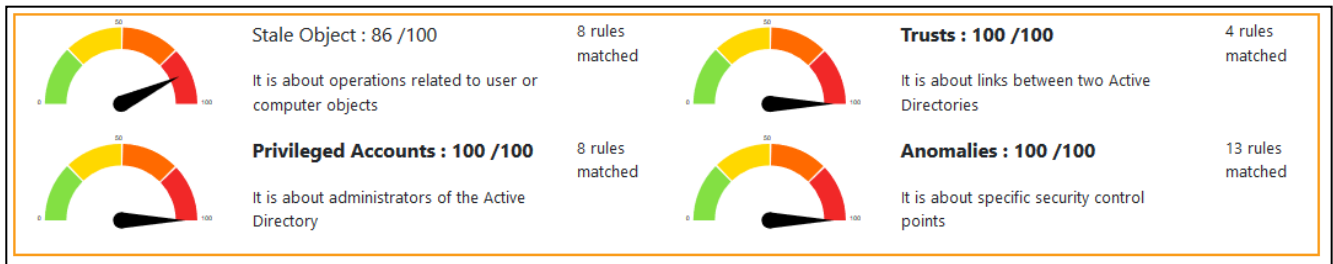
Risk model

The report is divided in 3 parts:

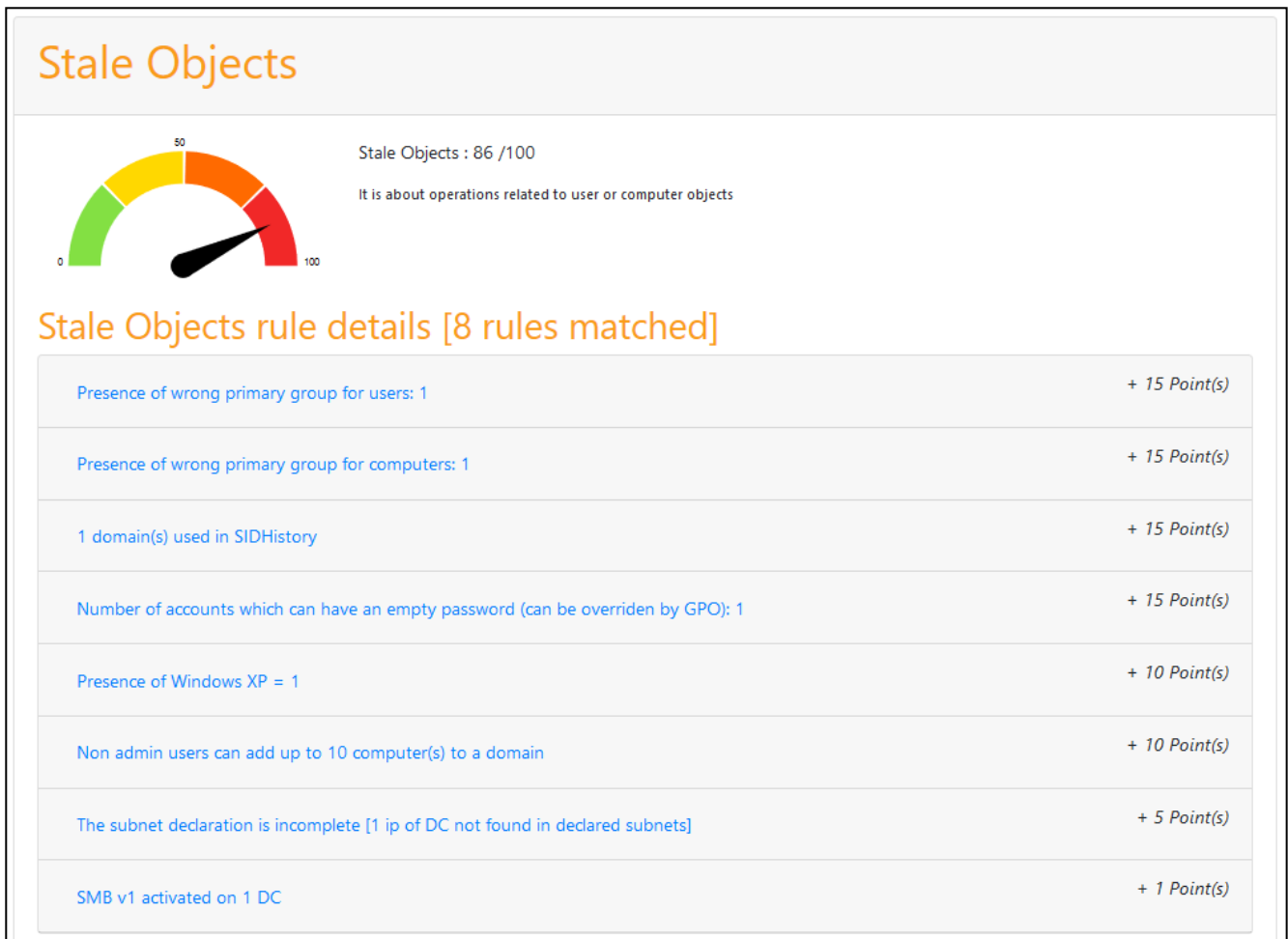
1) Scores

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 and related to security checks



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



When the rule 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 fonctionnalités, 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

Account analysis

| Nb User Accounts ↑↓ | Nb Enabled ? ↑↓ | Nb Disabled ? ↑↓ | Nb Active ? ↑↓ | Nb Inactive ? ↑↓ | Nb Locked ? ↑↓ | Nb pwd never Expire ? ↑↓ | Nb SidHistory ? ↑↓ | Nb Bad PrimaryGroup ? ↑↓ | Nb Passwor not Req. ? |
|---------------------|---|------------------|----------------|------------------|----------------|--------------------------|--------------------|--------------------------|-----------------------|
| | Indicates the number of accounts not set as disabled. | 4 | 4 | 14 | 0 | 4 | 3 | 1 | |

Showing 1 to 1 of 1 entries

| | |
|--|------|
| Inactive objects (Last usage > 6 months) | [14] |
| Objects with a password which never expires | [4] |
| Objects having the SIDHistory populated | [3] |
| Objects having the primary group attribute changed | [1] |
| Objects which can have an empty password | [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 \(Last usage > 6 months\)](#)

[14]

| Name ↑↓ | Creation ↑↓ | Last logon ↑↓ | Distinguished name ↑↓ |
|-----------------|----------------------|---------------|---|
| 123456789 | 2017-11-15 13:47:44Z | Never | CN=tata yoyo.123456789,CN=Users,DC=test,DC=mysmartlogon,DC=com |
| ADHealthCheck\$ | 2016-12-03 10:22:26Z | Never | CN=ADHealthCheck,CN=Managed Service Accounts,DC=test,DC=mysmartlogon,DC=com |
| BlueHat | 2018-01-19 15:23:37Z | Never | CN=BlueHat,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 |



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.

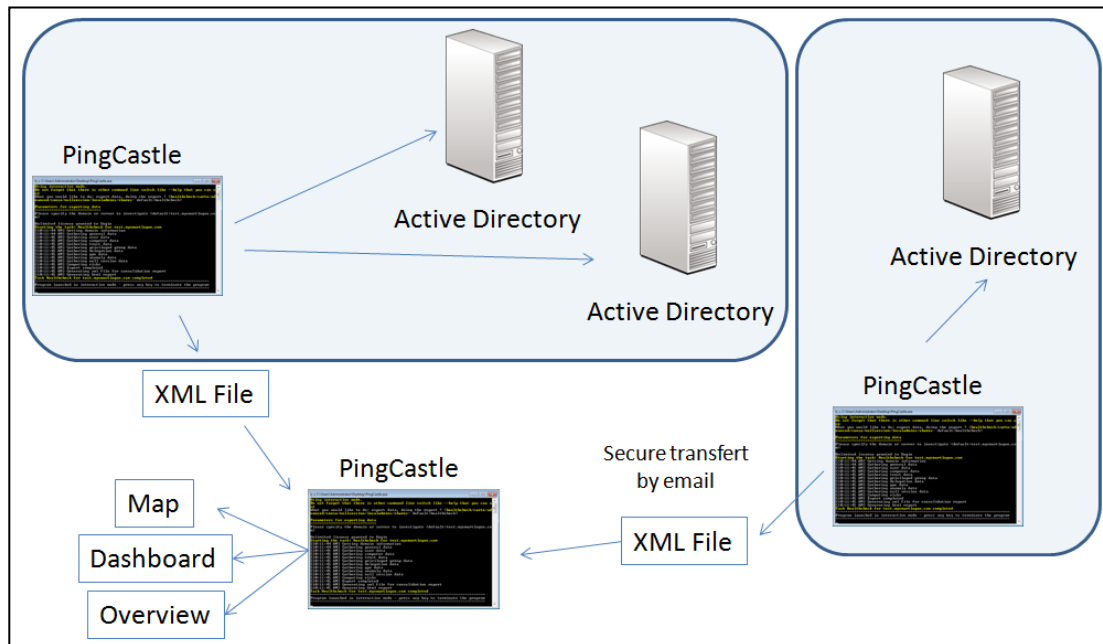
Important: xml reports generated from multiple point of view can be used to have a consolidated map.



Do not forget to check the [Getting an overview](#) or [dashboard](#) section.

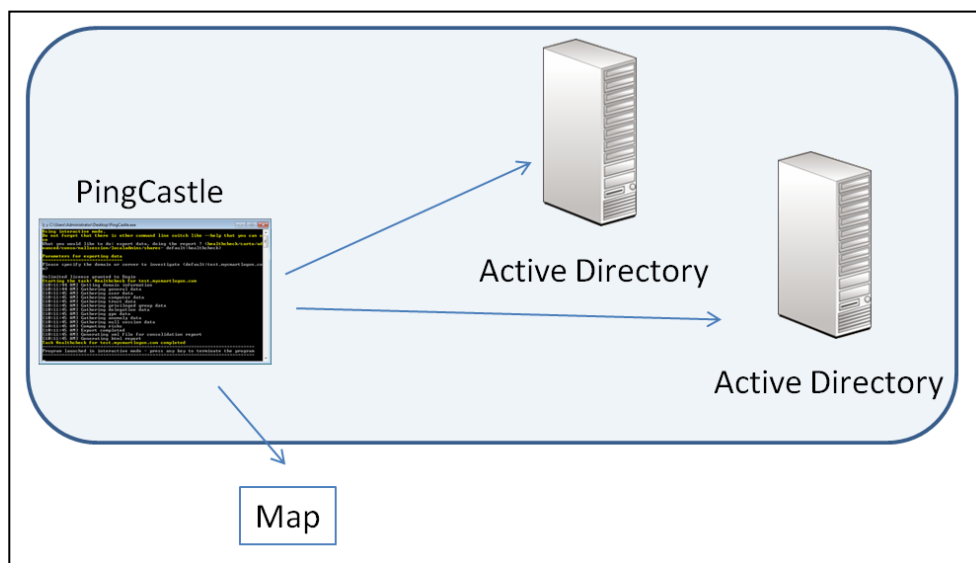
Option 2: when having existing health check reports

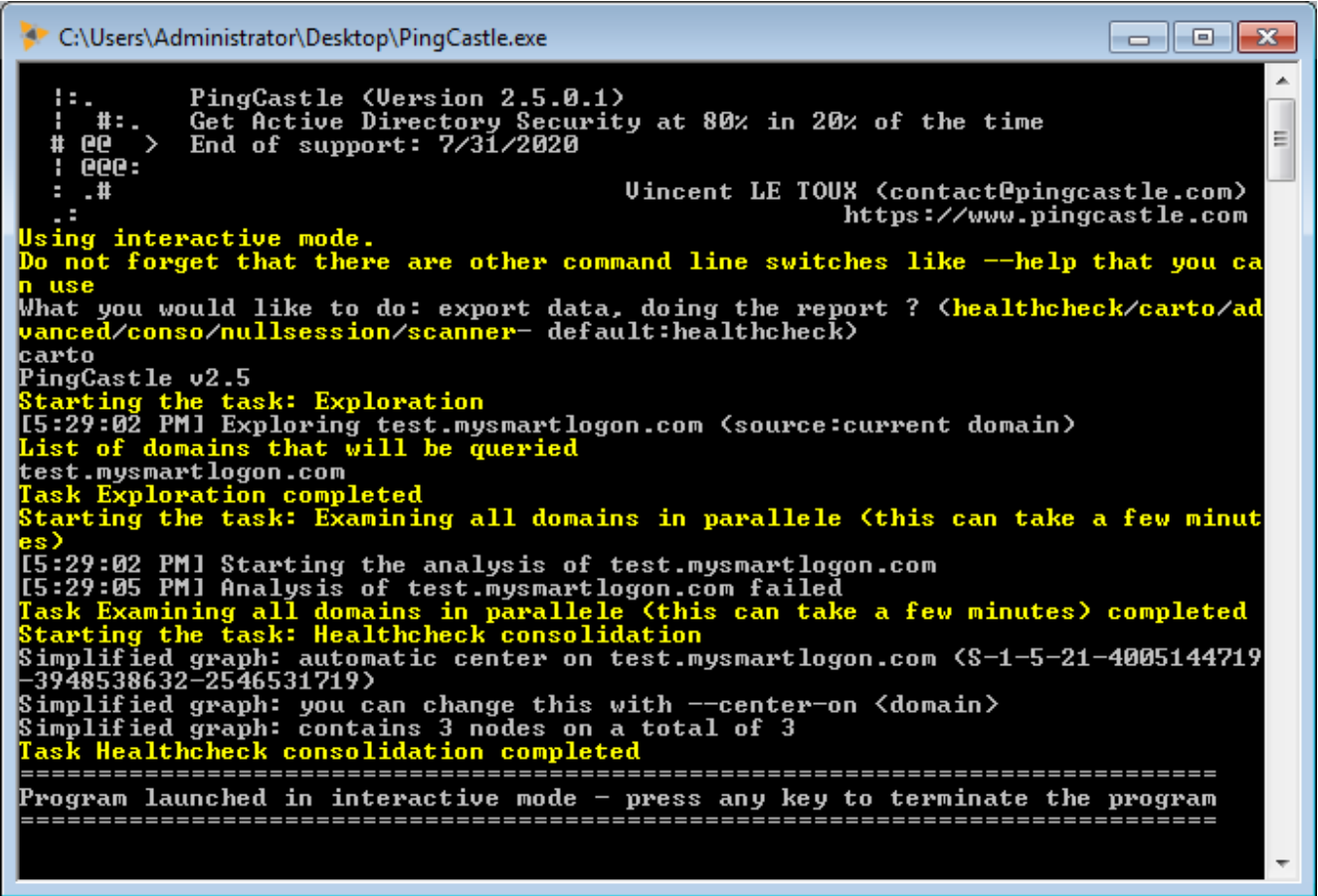
The map can be generated in the interactive mode by choosing “conso”. This mode performs the consolidation report and build the maps.



Option 3: 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.

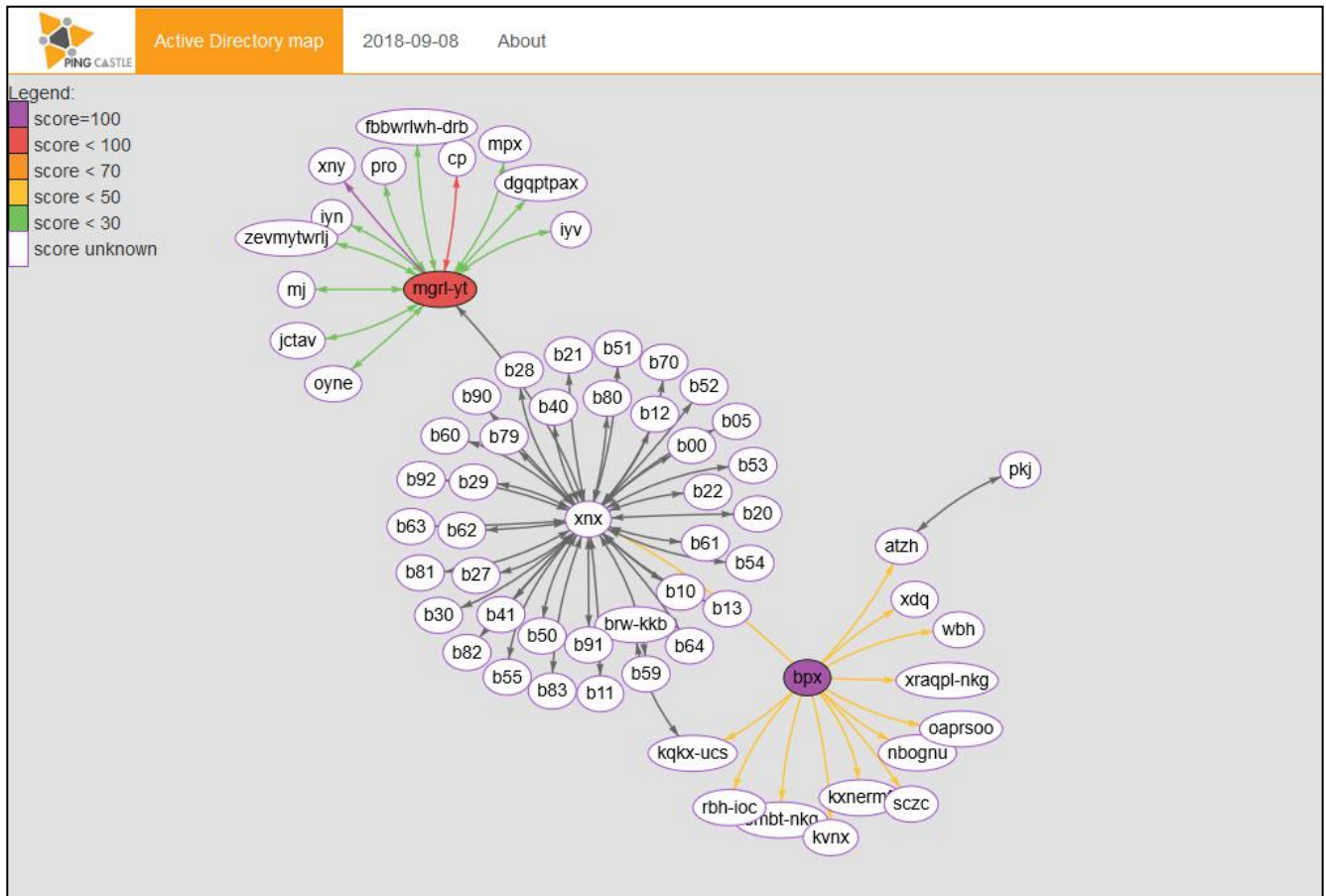




Maps

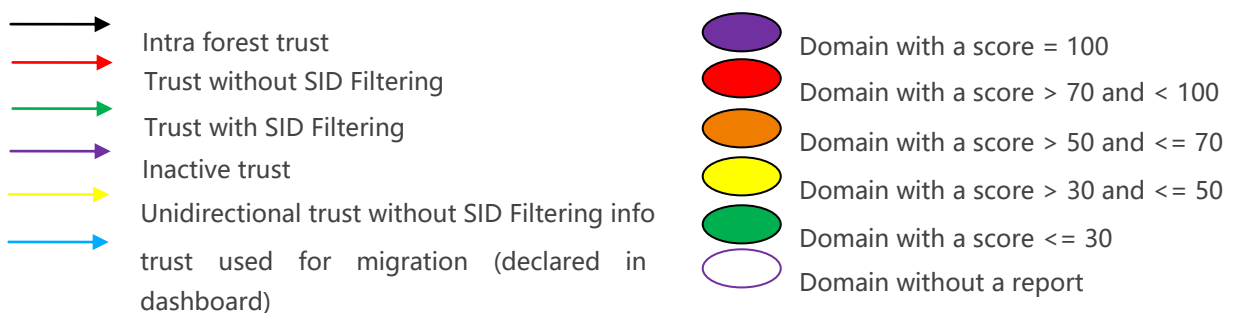
When available, the Active Directory health check score is displayed and colored by on it. Trusts are also colored based on the SID Filtering state.

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.

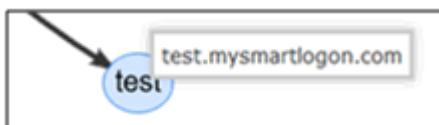


The colored circles are the domain on which the reports have been run. The color depends on the score. The purple bordered circles are the domains on which the script has not been run but that they program found using trust link.

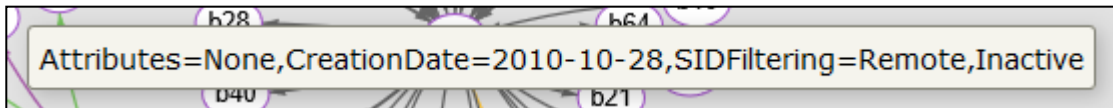
Legend:



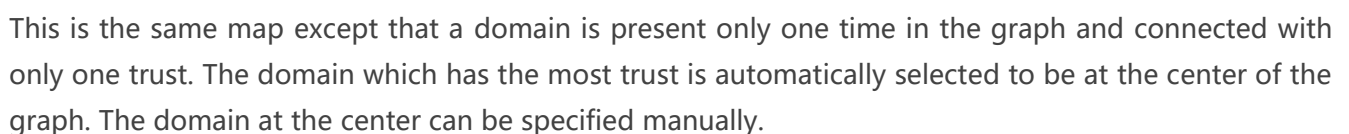
When the mouse is on a circle, the full name of the domain appears:



If the mouse is hold on a trust, the detail is shown in a popup:



The simple domain map is represented by the files `xxx_simple_node_map.html`.



The simple domain map is represented by the files `xxx hilbert map.html`.

This report is divided into 4 areas:


- the first one give an overview of all the networks
- the second one zoom deeper into the selected network
- the first one displays the list of networks



- the last one show the list of domain controllers identified

On the viewer Window, sources can be selected to avoid an overlapping with two sources.

There is a mouse over popup which gives you detail about a select IP (and the networks where it does belong) and a search function can be use to find a specific IP address.

 [Network map](#) [2019-07-05](#) [About](#)

Network map

Date: 2019-07-05 - Engine version: 2.7.0.0 Beta

[Overview](#) [Viewer](#) [Network list](#) [DC list](#)

Viewer

Viewing network 10.0.0.0/8

[Show Legend](#) [Select Sources](#)

Scale: 1 pixel is 16 ip(s)

Locate ip

Example: 10.0.1.0

Network:
test.local
France-TATAYOYO
10.0.0.0/16
assigned to: t2.root.local

10.8.0.0/16

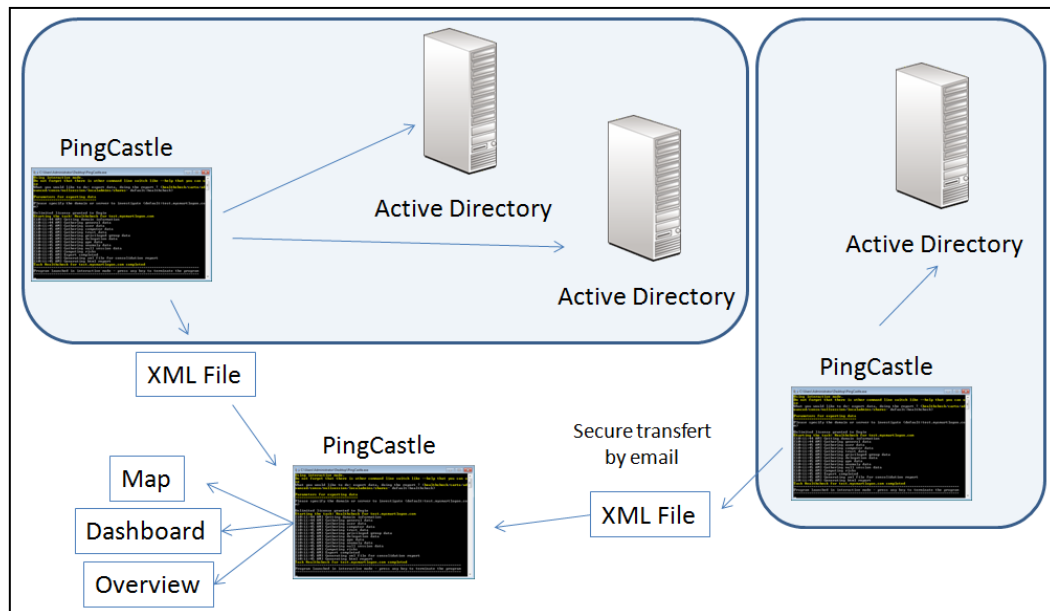
| | | | | | | | | | | | | | | | |
|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| 10.16.0.0/16 | 10.17.0.0/16 | 10.18.0.0/16 | 10.19.0.0/16 | 10.20.0.0/16 | 10.21.0.0/16 | 10.22.0.0/16 | 10.23.0.0/16 | 10.24.0.0/16 | 10.25.0.0/16 | 10.26.0.0/16 | 10.27.0.0/16 | 10.28.0.0/16 | 10.29.0.0/16 | 10.30.0.0/16 | 10.31.0.0/16 |
| 10.32.0.0/16 | 10.33.0.0/16 | 10.34.0.0/16 | 10.35.0.0/16 | 10.36.0.0/16 | 10.37.0.0/16 | 10.38.0.0/16 | 10.39.0.0/16 | 10.40.0.0/16 | 10.41.0.0/16 | 10.42.0.0/16 | 10.43.0.0/16 | 10.44.0.0/16 | 10.45.0.0/16 | 10.46.0.0/16 | 10.47.0.0/16 |
| 10.48.0.0/16 | 10.49.0.0/16 | 10.50.0.0/16 | 10.51.0.0/16 | 10.52.0.0/16 | 10.53.0.0/16 | 10.54.0.0/16 | 10.55.0.0/16 | 10.56.0.0/16 | 10.57.0.0/16 | 10.58.0.0/16 | 10.59.0.0/16 | 10.60.0.0/16 | 10.61.0.0/16 | 10.62.0.0/16 | 10.63.0.0/16 |
| 10.64.0.0/16 | 10.65.0.0/16 | 10.66.0.0/16 | 10.67.0.0/16 | 10.68.0.0/16 | 10.69.0.0/16 | 10.70.0.0/16 | 10.71.0.0/16 | 10.72.0.0/16 | 10.73.0.0/16 | 10.74.0.0/16 | 10.75.0.0/16 | 10.76.0.0/16 | 10.77.0.0/16 | 10.78.0.0/16 | 10.79.0.0/16 |
| 10.80.0.0/16 | 10.81.0.0/16 | 10.82.0.0/16 | 10.83.0.0/16 | 10.84.0.0/16 | 10.85.0.0/16 | 10.86.0.0/16 | 10.87.0.0/16 | 10.88.0.0/16 | 10.89.0.0/16 | 10.90.0.0/16 | 10.91.0.0/16 | 10.92.0.0/16 | 10.93.0.0/16 | 10.94.0.0/16 | 10.95.0.0/16 |
| 10.96.0.0/16 | 10.97.0.0/16 | 10.98.0.0/16 | 10.99.0.0/16 | 10.100.0.0/16 | 10.101.0.0/16 | 10.102.0.0/16 | 10.103.0.0/16 | 10.104.0.0/16 | 10.105.0.0/16 | 10.106.0.0/16 | 10.107.0.0/16 | 10.108.0.0/16 | 10.109.0.0/16 | 10.110.0.0/16 | 10.111.0.0/16 |
| 10.112.0.0/16 | 10.113.0.0/16 | 10.114.0.0/16 | 10.115.0.0/16 | 10.116.0.0/16 | 10.117.0.0/16 | 10.118.0.0/16 | 10.119.0.0/16 | 10.120.0.0/16 | 10.121.0.0/16 | 10.122.0.0/16 | 10.123.0.0/16 | 10.124.0.0/16 | 10.125.0.0/16 | 10.126.0.0/16 | 10.127.0.0/16 |
| 10.128.0.0/16 | 10.129.0.0/16 | 10.130.0.0/16 | 10.131.0.0/16 | 10.132.0.0/16 | 10.133.0.0/16 | 10.134.0.0/16 | 10.135.0.0/16 | 10.136.0.0/16 | 10.137.0.0/16 | 10.138.0.0/16 | 10.139.0.0/16 | 10.140.0.0/16 | 10.141.0.0/16 | 10.142.0.0/16 | 10.143.0.0/16 |
| 10.144.0.0/16 | 10.145.0.0/16 | 10.146.0.0/16 | 10.147.0.0/16 | 10.148.0.0/16 | 10.149.0.0/16 | 10.150.0.0/16 | 10.151.0.0/16 | 10.152.0.0/16 | 10.153.0.0/16 | 10.154.0.0/16 | 10.155.0.0/16 | 10.156.0.0/16 | 10.157.0.0/16 | 10.158.0.0/16 | 10.159.0.0/16 |
| 10.160.0.0/16 | 10.161.0.0/16 | 10.162.0.0/16 | 10.163.0.0/16 | 10.164.0.0/16 | 10.165.0.0/16 | 10.166.0.0/16 | 10.167.0.0/16 | 10.168.0.0/16 | 10.169.0.0/16 | 10.170.0.0/16 | 10.171.0.0/16 | 10.172.0.0/16 | 10.173.0.0/16 | 10.174.0.0/16 | 10.175.0.0/16 |
| 10.176.0.0/16 | 10.177.0.0/16 | 10.178.0.0/16 | 10.179.0.0/16 | 10.180.0.0/16 | 10.181.0.0/16 | 10.182.0.0/16 | 10.183.0.0/16 | 10.184.0.0/16 | 10.185.0.0/16 | 10.186.0.0/16 | 10.187.0.0/16 | 10.188.0.0/16 | 10.189.0.0/16 | 10.190.0.0/16 | 10.191.0.0/16 |
| 10.192.0.0/16 | 10.193.0.0/16 | 10.194.0.0/16 | 10.195.0.0/16 | 10.196.0.0/16 | 10.197.0.0/16 | 10.198.0.0/16 | 10.199.0.0/16 | 10.200.0.0/16 | 10.201.0.0/16 | 10.202.0.0/16 | 10.203.0.0/16 | 10.204.0.0/16 | 10.205.0.0/16 | 10.206.0.0/16 | 10.207.0.0/16 |
| 10.208.0.0/16 | 10.209.0.0/16 | 10.210.0.0/16 | 10.211.0.0/16 | 10.212.0.0/16 | 10.213.0.0/16 | 10.214.0.0/16 | 10.215.0.0/16 | 10.216.0.0/16 | 10.217.0.0/16 | 10.218.0.0/16 | 10.219.0.0/16 | 10.220.0.0/16 | 10.221.0.0/16 | 10.222.0.0/16 | 10.223.0.0/16 |
| 10.224.0.0/16 | 10.225.0.0/16 | 10.226.0.0/16 | 10.227.0.0/16 | 10.228.0.0/16 | 10.229.0.0/16 | 10.230.0.0/16 | 10.231.0.0/16 | 10.232.0.0/16 | 10.233.0.0/16 | 10.234.0.0/16 | 10.235.0.0/16 | 10.236.0.0/16 | 10.237.0.0/16 | 10.238.0.0/16 | 10.239.0.0/16 |
| 10.240.0.0/16 | 10.241.0.0/16 | 10.242.0.0/16 | 10.243.0.0/16 | 10.244.0.0/16 | 10.245.0.0/16 | 10.246.0.0/16 | 10.247.0.0/16 | 10.248.0.0/16 | 10.249.0.0/16 | 10.250.0.0/16 | 10.251.0.0/16 | 10.252.0.0/16 | 10.253.0.0/16 | 10.254.0.0/16 | 10.255.0.0/16 |



Deploying PingCastle

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.



Involvement of the management

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%

Below 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” .

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.

Updating PingCastle

Since PingCastle 2.7, a new update program is delivered. It downloads the latest release from the github official releases. In option, it can download the beta release or wait that the release has reached a specific age.

Here is the options available:

```
--api-url http://xx : use an alternative url for checking for updates
--force-download      : download the latest release even if it is not the most recent.
Useful for tests
--use-preview         : download preview release if it is the most recent
--wait-for-days 30    : ensure the releases has been made public for at least X days
```



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
4smrLAZZ30QwWXHcT1oNz3hH3Ax2R9T75D1ioGFCIdLb0QhUn3N8NWgJ2ZgyUNXn4qU1b0Ds10IhK+Cq
oqCPvXuHjK6TGrMyphtcbZvvgbLxfyalJemczx1+pOuBlqqVda1E94rnnnBr761WIJJnkJdZ0rzYsebn
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;h4smrLAZZ30QwWXHcT1oNz3hH3Ax2R9T75D1ioGFCIdLb0QhUn3
N8NWgJ2ZgyUNXn4qU1b0Ds10IhK+CqoqCPvXuHjK6TGrMyphtcbZvvgbLxfyalJemczx1+pOuBlqqVda
1E94rnnnBr761WIJJnkJdZ0rzYsebnDwGuk9kiw8=&lt;/Modulus&gt;&lt;Exponent&gt;AQAB&lt
;/Exponent&gt;&lt;P&gt;uwgX794pe703vIiQR5v03WK3Ug5LUAbXpPF6Xq4qGb3TGprZaJQq5rZ2u
J4qwRan0a5pI/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+8rcmhWifKBWUU7Vk6mHsSlFhY4BY
wPzQ==&lt;/DP&gt;&lt;DQ&gt;gzfwh8AT0CLXEP6ZomYi2571ST8xoUAoyEG5gKjEPJrJ42Fp0HiXB
9+Dhibc3atBwjEqvv5VVGx06iEK2g27RQ==&lt;/DQ&gt;&lt;InverseQ&gt;HRKFjYwrXqg04v8Q+J
SOqR6lSvQ15Z6V4AE23i4xfeuIYWwVf0t8AwgkDfFRQnEyh24byuh5PPzUbD0sUY+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.



API

A screenshot of the Swagger UI for the PingCastle API V1. The interface has a green header bar with the "swagger" logo and a dropdown menu labeled "Select a spec" showing "PingCastle API V1". Below the header, the title "PingCastle API" is displayed with a "v1" badge and a link to "/swagger/v1/swagger.json". The main content area is divided into sections. The "Agent" section, indicated by a dropdown arrow, contains two endpoints: a POST method for "/api/Agent/Login" with the description "Login and get a token for API", and another POST method for "/api/Agent/SendReport" with the description "Import a report". Below this is the "Models" section, also with a dropdown arrow, which lists two data models: "LoginData" and "ReportData", each with a right-pointing arrow to expand its details.

PingCastle can send the report (encrypted or not) using an API.

You can query a PingCastle API server or build a client or server from [Swagger](#).

The description of the API in swagger format can be found [here](#).



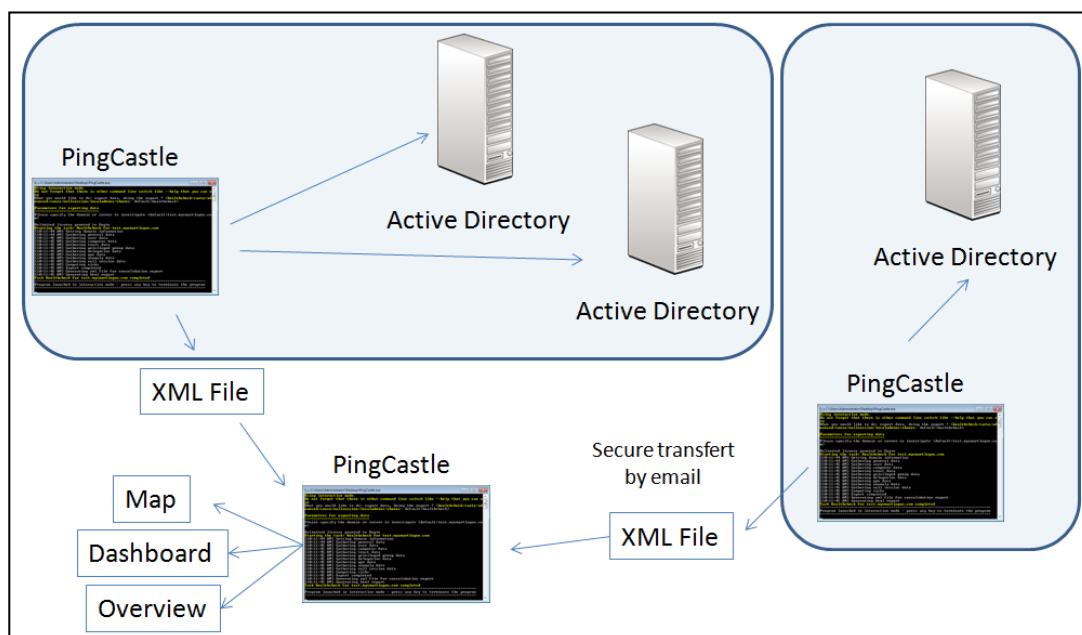
Getting an overview with multiple reports

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

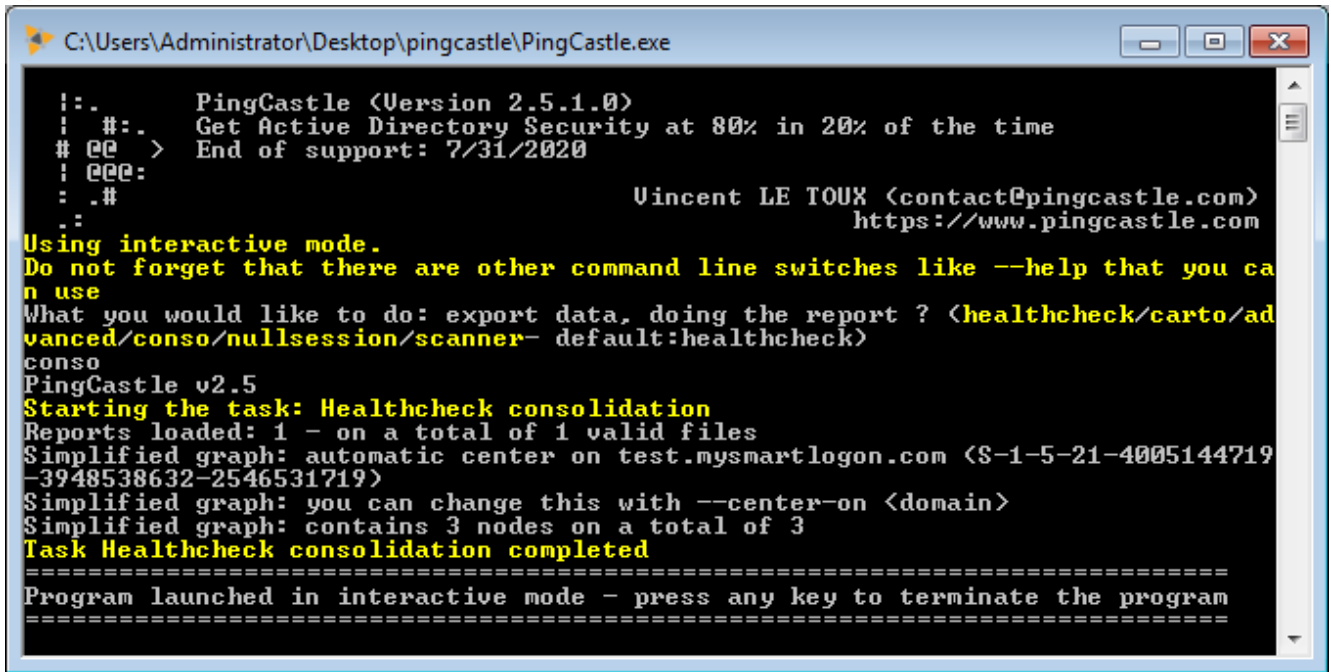
This is the kind of questions you can answer with the simplest consolidation. Indeed, the program can be used to aggregate the report results.

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.

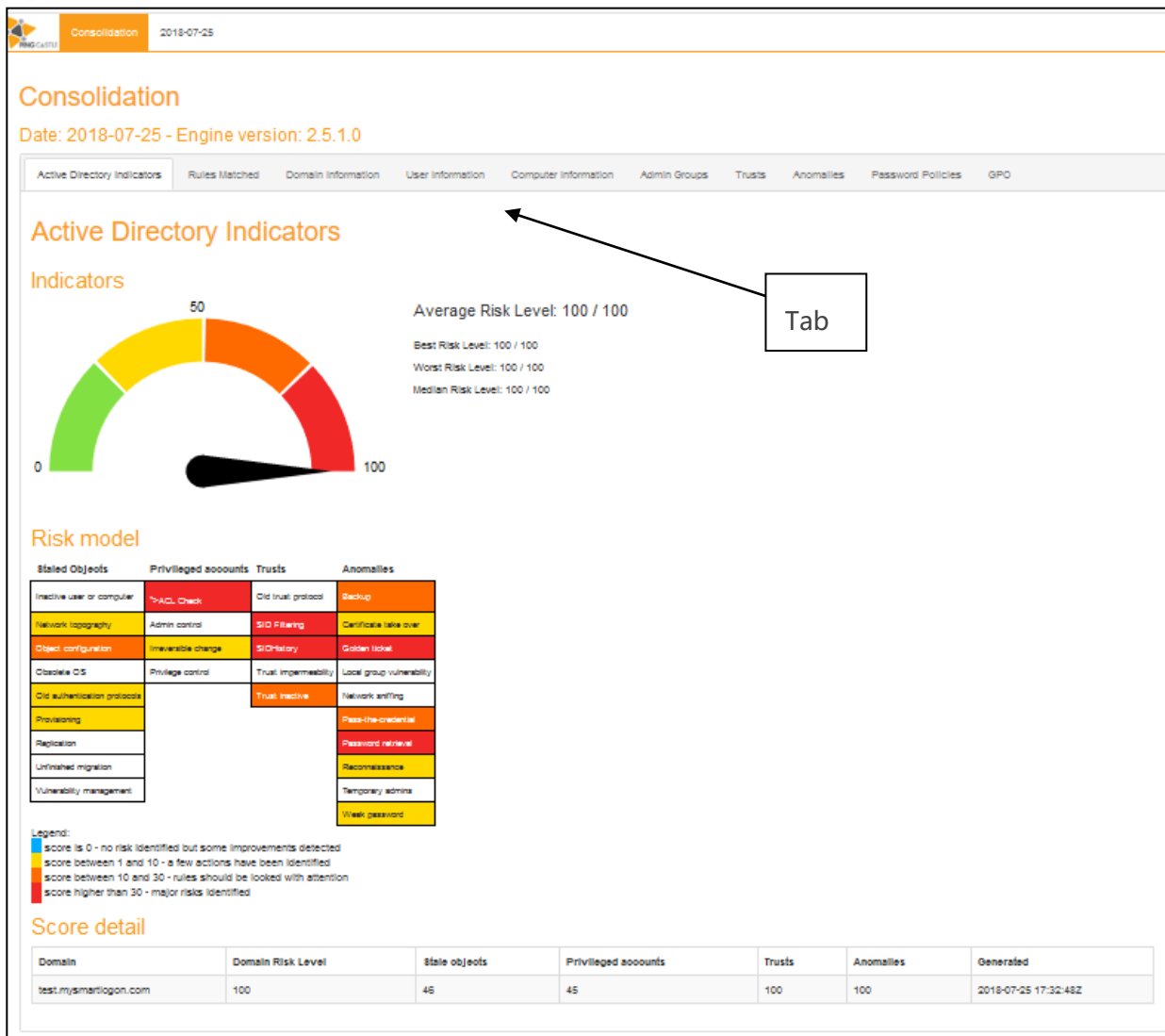


To generate the report, enter "conso" in the interactive mode.



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

Consolidation report



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](#)

File `ad_hc_summary_full_node_map.html`

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

[Example](#)

File `ad_hc_summary_simple_node_map.html`

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

[Example](#)

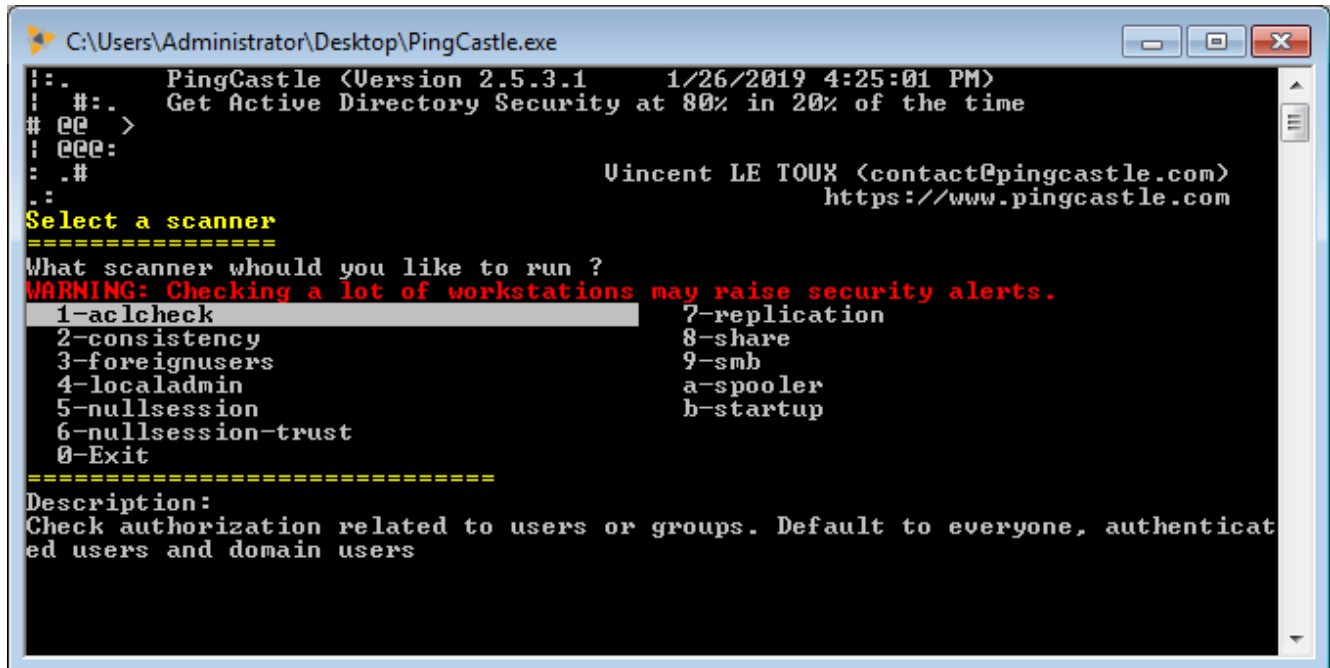




Scanners

PingCastle has some builtin program to check for specific features. These programs are called "scanners" and are accessible from the "scanner" item on the main menu.

When selected, a menu is displayed to select the program. At the bottom, a scanner description is shown.



```
C:\Users\Administrator\Desktop\PingCastle.exe
PingCastle <Version 2.5.3.1 1/26/2019 4:25:01 PM>
# #:. Get Active Directory Security at 80% in 20% of the time
# @@ >
# @@@:
# .#
# Vincent LE TOUX <contact@pingcastle.com>
# https://www.pingcastle.com

Select a scanner
=====
What scanner would you like to run ?
WARNING: Checking a lot of workstations may raise security alerts.
1-aclcheck 7-replication
2-consistency 8-share
3-foreignusers 9-smb
4-localadmin a-spooler
5-nullsession b-startup
6-nullsession-trust
0-Exit
=====
Description:
Check authorization related to users or groups. Default to everyone, authenticated users and domain users
```

Here are the main scanners

Check for specific user in global permissions

The AclCheck scanner is used to hunt for write permission given to objects on a domain. It is default to the "authenticated users", "domain users", "everyone" groups.

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

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>
```

Null sessions

Null sessions are an old Windows NT4 problem. It should have been disappears 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 account of the domain. Then this list can be used to generated wrong authentication attempts and lock the accounts. Or perform brute-force attacks.

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

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

foreignusers

A 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.

First, enter the domain to enumerate (eg: the bastion or a domain which is very far)

```
C:\Users\Administrator\Desktop\PingCastle.exe
!-: PingCastle <Version 2.5.3.1 1/26/2019 4:25:01 PM>
!-: Get Active Directory Security at 80% in 20% of the time
!-:
!-: @@@:
!-: .# Vincent LE TOUX <contact@pingcastle.com>
!-: .# https://www.pingcastle.com
!-:
!-: Select the targeted domain
!-: =====
!-: This scanner enumerate all the users of a trusted domain. Typically it can be a
!-: domain trusted by a domain you trust or an inbound trust such as a bastion.
!-: The server for the pivot will be asked next.
!-:
!-: Please enter the foreign domain targeted using its FQDN or sids
!-: Example of SID: S-1-5-21-4005144719-3948538632-2546531719
!-: Example of FQDN: bastion.local
!-:
!-: -
```

Then enter the domain which will be used as a pivot

```
PingCastle --scanner foreignusers --foreigndomain <remote domain or sid> --server <pivot domain>
```



Command line reference

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

Health check

- run the health check :

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

- run the consolidation of the health check reports:

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

- export rule list:

```
PingCastle --export-hc-rule
```

Overview:

- Run the report on all reachable domains and built a cartography:

```
PingCastle --healthcheck --server * --reachable --hc-conso
```

- Built only a cartography without scores:

```
PingCastle --carto
```

Advanced mode:

- run the export:

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

- build the reports:

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

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
--port <port>      : the port to use for ADWS or LDPA (default: 9389 or 389)
--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

--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>

--rules              : Generate an html containing all the rules used by PingCastle. Do
not forget PingCastleReporting includes a similar option but for .xlsx

--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.

--regen-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

--graph              : perform the light compromise graph computation directly to the AD

  --encrypt            : use an RSA key stored in the .config file to crypt the content of
the xml report
```



```
--max-depth      : maximum number of relation to explore (default:30)
--max-nodes      : maximum number of node to include (default:1000)
--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
```

```
--scanner <type> : perform a scan on one of all computers of the domain (using --server)
```

aclcheck

Check authorization related to users or groups. Default to everyone, authenticated users and domain users

antivirus

Check for computers without known antivirus installed. It is used to detect unprotected computers but may also report computers with unknown antivirus.

corruptADDatabase

Try to detect corrupted AD database. To run only when requested by PingCastle support.

foreignusers

Use trusts to enumerate users located in domain denied such as bastion or domains too far away.

laps_bitlocker

Check on the AD if LAPS and/or BitLocker has been enabled for all computers on the domain.

localadmin

Enumerate the local administrators of a computer.

nullsession

Check if null sessions are enabled and provide example(s).

nullsession-trust

Dump the trusts of a domain via null session if possible

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.

spooler

Check if the spooler service is remotely active. The spooler can be abused to get computer tokens when unconstrained delegations are exploited.

startup

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

options for scanners:

```
--scmode-single : force scanner to check one single computer
--nslimit <number>: Limit the number of users to enumerate (default: 5)
```



--foreigndomain <sid> : foreign domain targeted 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



List of open source software used

PingCastle uses a set of open source components to perform its job.

The list of components used by PingCastle, but not limited to, is:

- [Bootstrap](#) licensed under the [MIT license](#)
- [DataTables](#) licensed under the [MIT license](#)
- [Popper.js](#) licensed under the [MIT license](#)
- [jQuery](#) licensed under the [MIT license](#)
- [vis.js](#) licensed under the [MIT license](#)



Scheduling PingCastle report

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'. The 'Location' is '\'. The 'Author' is 'TEST\administrator'. The 'Description' field is empty. Under 'Security options', the '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'. The 'OK' and 'Cancel' buttons are at the bottom right.

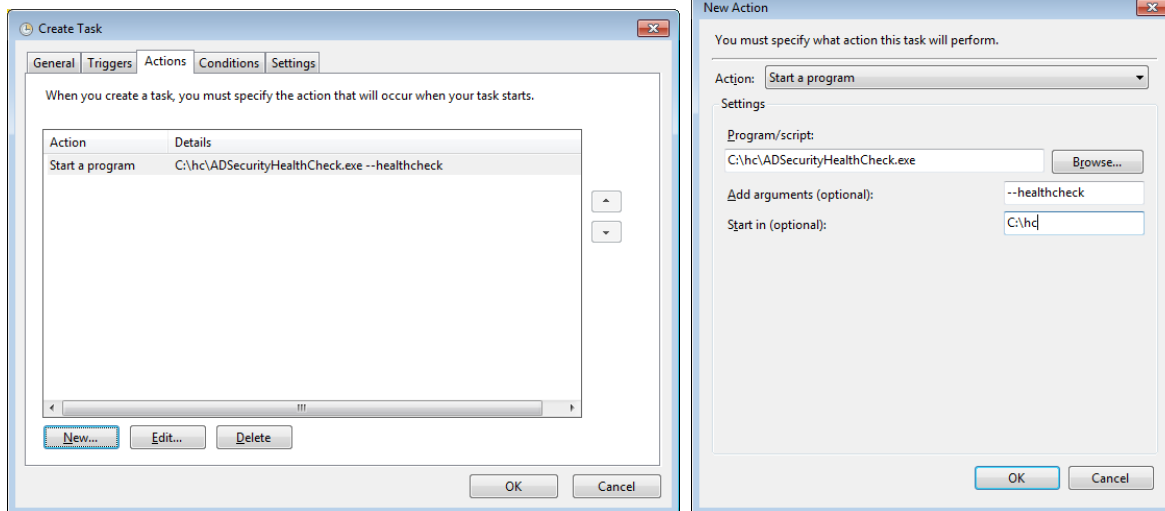
Set the schedule:

The 'Create Task' dialog box is shown with the 'Triggers' tab selected. The 'When you create a task, you can specify the conditions that will trigger the task.' section contains a table with one row: 'Weekly' trigger, 'At 11:52 AM every Monday of every week, starting 12/3/2016', and 'Enabled' status. The 'New...', 'Edit...', and 'Delete' buttons are at the bottom left. The 'OK' and 'Cancel' buttons are at the bottom right.

The 'Edit Trigger' dialog box is shown with the 'Settings' tab selected. The 'Begin the task:' dropdown is set to 'On a schedule'. The 'Settings' section has the 'Weekly' radio button selected. The 'Start' date is '12/ 3/2016' and the 'Time' is '11:52:36 AM'. The 'Repeat every:' is '1' week on 'Monday'. The 'Advanced settings' section has the 'Repeat task every:' set to '1 hour' for a duration of '1 day'. The 'Stop task if it runs longer than:' is '3 days'. The 'Expire:' date is '12/ 3/2017' and the 'Time' is '11:54:23 AM'. The 'Enabled' checkbox is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

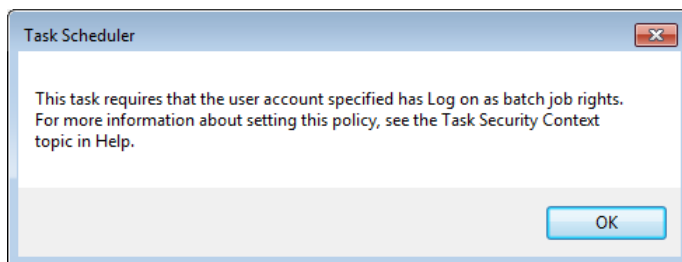


Set the command line:

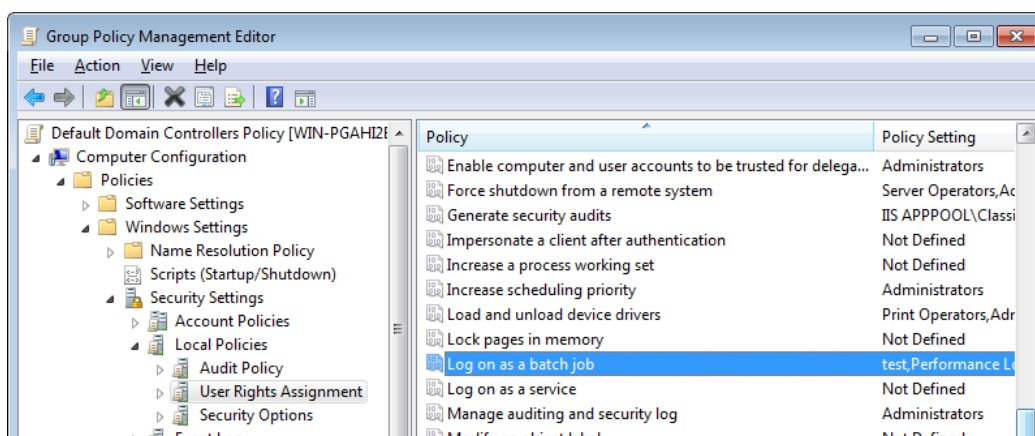


Be sure that the service account has the right to write the report in the current directory.

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:



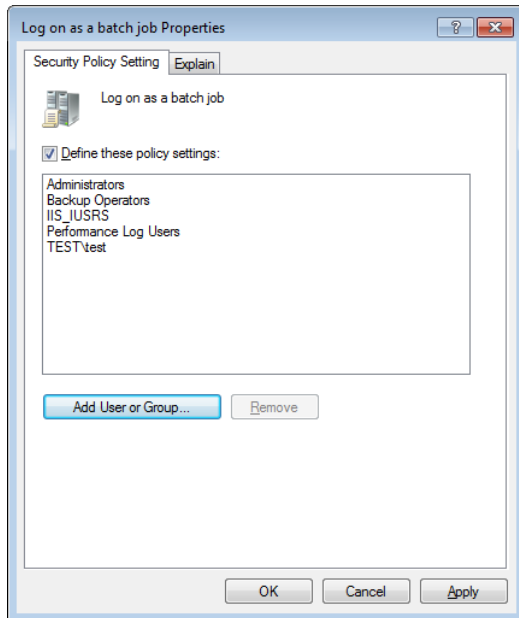
Select "Local Policies" in MSC snap in



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.