

PingCastle Para Auditorias de Active Directory

Misti Offensive

Nombre: Cristhian Chahuayo

Correo: info.mistioffensive@gmail.com

Peru, May 2025

CONTENTS

Contents	1
1 PingCastle Para Auditorias	2
1.1 ¿Que es PingCastle?	2
1.2 Diferencias frente a BloodHound y PowerView	2
2 Uso de la Herramienta	3
2.1 Instalacion	3
2.2 Generacion de reportes	3
3 Conclusion	7

PINGCASTLE PARA AUDITORIAS

1.1 ¿Que es PingCastle?

PingCastle es una herramienta útil que evalúa la postura de seguridad de un entorno AD y nos proporciona los resultados en varios mapas y gráficos diferentes e incluso nos puede brindar un inventario activo de los hosts de una red empresarial.

PingCastle puede ser de gran ayuda para reunir información del mapa del dominio legible y sea legible por el auditor y usuario.

1.2 Diferencias frente a BloodHound y PowerView

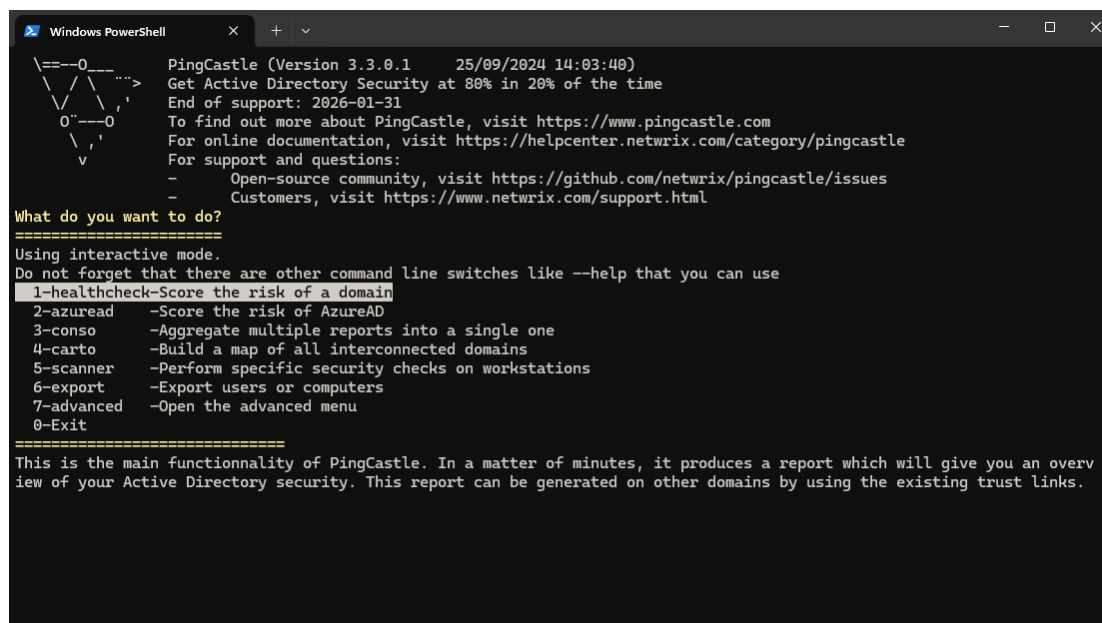
Además de proporcionar datos de enumeración que pueden informar nuestros ataques, muestra un informe detallado del nivel de seguridad de un dominio. Esto lo hace utilizando una metodología basada en un marco de evaluación de riesgos/madurez. Utilizando el Modelo de Integración de Madurez de Capacidades (CMMI).

USO DE LA HERRAMIENTA

2.1 Instalacion

Descargamos el archivo .exe desde la Pagina de **PingCastle** o de su repositorio de **GitHub**.

Posterior a ello, ejecutamos el archivo descargado mediante la CMD.



```
Windows PowerShell
PingCastle (Version 3.3.0.1 25/09/2024 14:03:40)
Get Active Directory Security at 80% in 20% of the time
End of support: 2026-01-31
To find out more about PingCastle, visit https://www.pingcastle.com
For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
For support and questions:
- Open-source community, visit https://github.com/netwrix/pingcastle/issues
- Customers, visit https://www.netwrix.com/support.html

What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-azuread -Score the risk of AzureAD
3-conso -Aggregate multiple reports into a single one
4-carto -Build a map of all interconnected domains
5-scanner -Perform specific security checks on workstations
6-export -Export users or computers
7-advanced -Open the advanced menu
0-Exit
=====

This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overv
iew of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

Figure 2.1: PingCastle

2.2 Generacion de reportes

Para este ejemplo solo usaremos la opcion por defecto nos dara una visión general de la línea base del dominio, y nos proporcionará información relacionada a las malas configuraciones y vulnerabilidades.

PingCastle puede informar sobre vulnerabilidades recientes, nuestros recursos compartidos, confianzas, la delegación de permisos y mucho más sobre los estados de nuestros usuarios y ordenadores. En la opción Scanner, podemos encontrar la mayoría de estas comprobaciones.

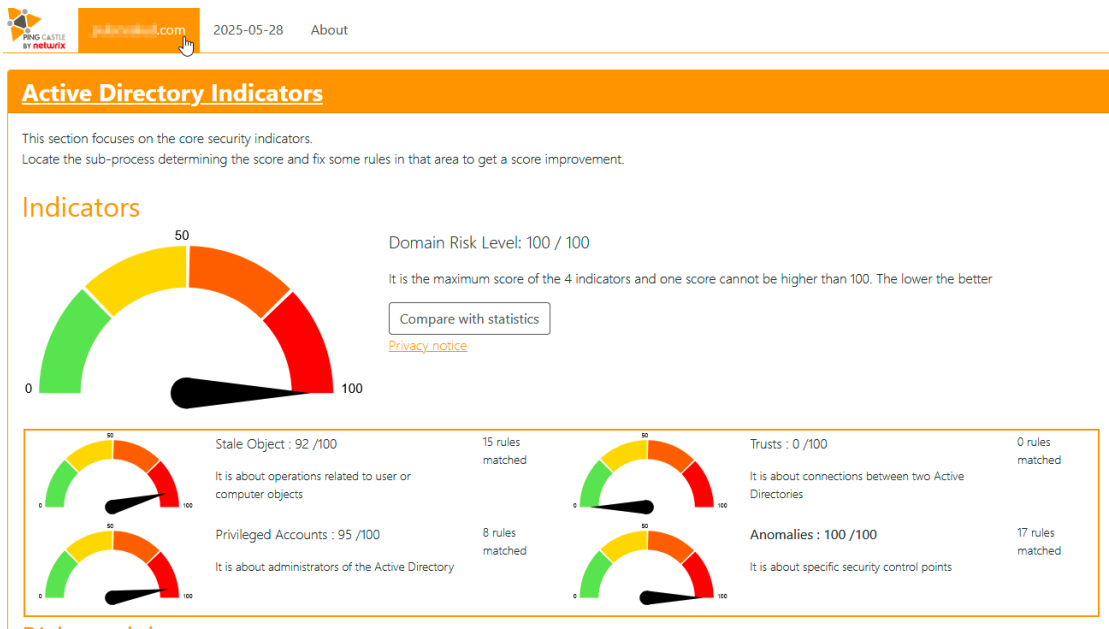


Figure 2.2: Indicadores

Risk model ⓘ

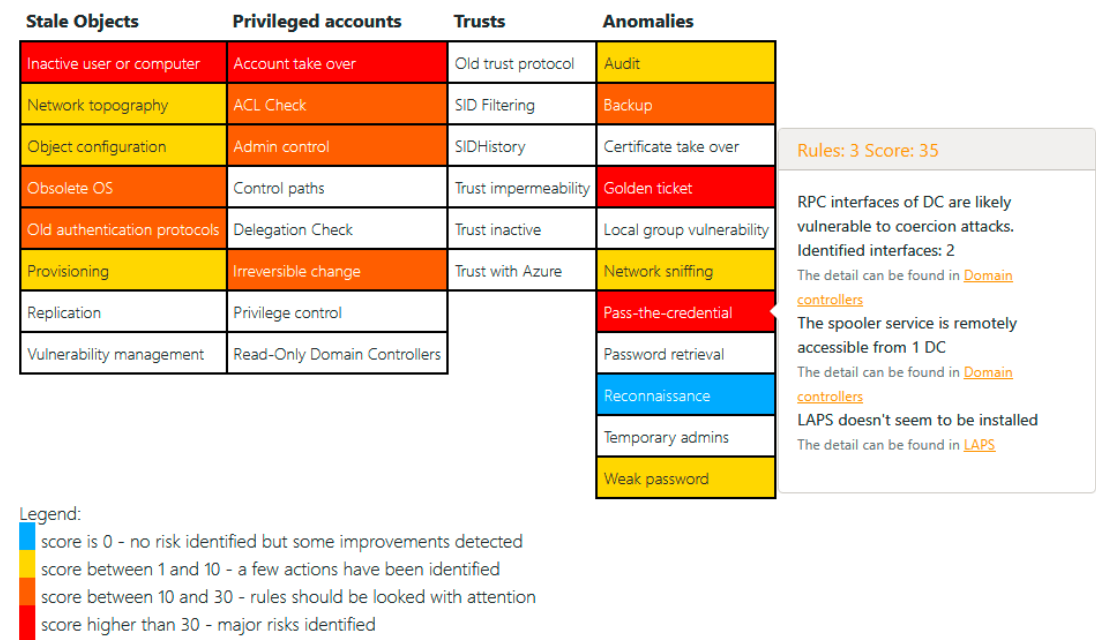


Figure 2.3: Modelo de Riesgo

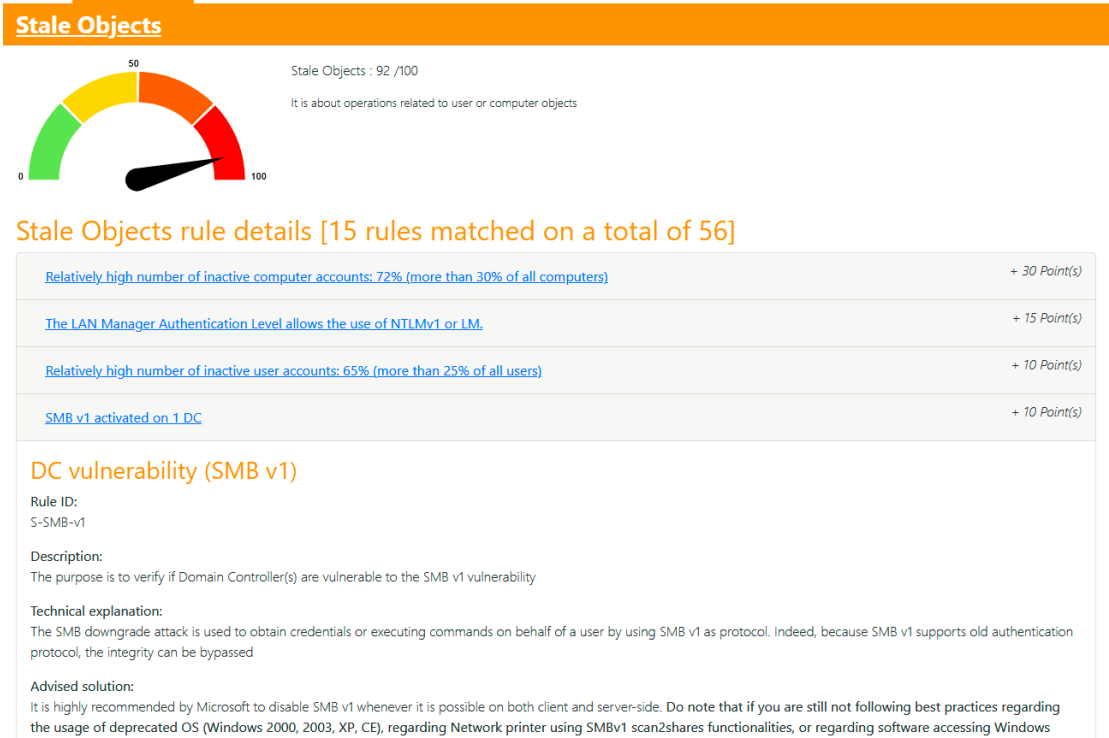


Figure 2.4: Objetos Antiguos u obsoletos

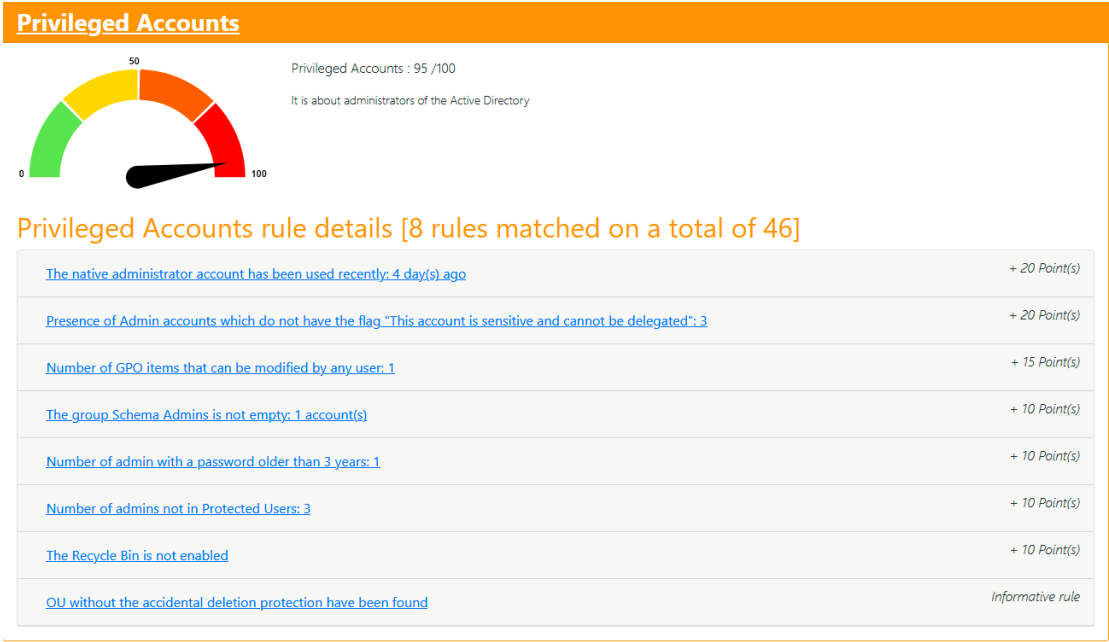


Figure 2.5: Cuentas Privilegiadas

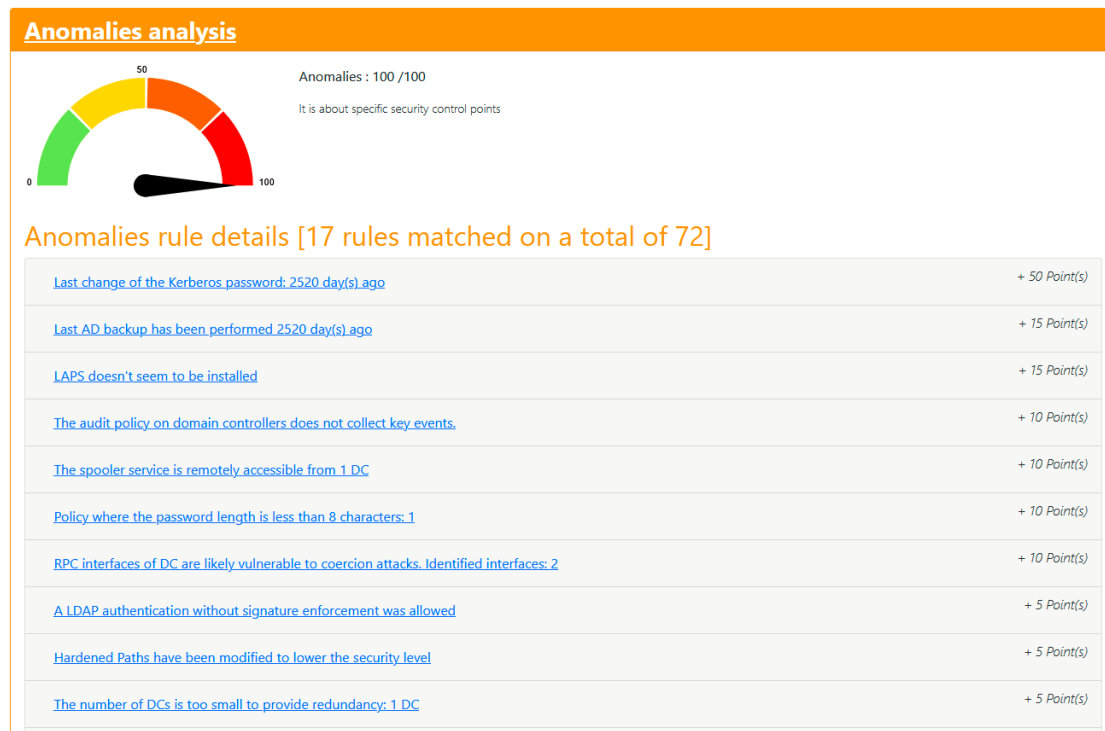


Figure 2.6: Analisis de Anomalias

Groups

This section is focused on the groups which are critical for admin activities. If the report has been saved which the full details, each group can be zoomed with its members. If it is not the case, for privacy reasons, only general statistics are available.

Group Name	Nb Admins	Nb Enabled	Nb Disabled	Nb Inactive	Nb PWD never expire	Nb Smart Card required
Account Operators	0	0	0	0	0	0
Administrators	3	3	0	2	0	0
Backup Operators	0	0	0	0	0	0
Certificate Operators	0	0	0	0	0	0
Certificate Publishers	0	0	0	0	0	0
Dns Admins	0	0	0	0	0	0
Domain Administrators	2	2	0	1	0	0
Enterprise Administrators	1	1	0	0	0	0
Enterprise Key Administrators	0	0	0	0	0	0
Key Administrators	0	0	0	0	0	0

Figure 2.7: Grupos

CONCLUSION

Sin duda alguna, esta herramienta podría ser bastante útil en entornos de directorio activo, para realizar auditorías, ya que nos puede dar una visión detallada de enumeración para técnicas de ataque y explotación de vulnerabilidades, todo esto de manera ética y profesional.

Cuando realizamos una auditoría en un entorno de AD, es recomendable usar varias herramientas que nos puedan ser útiles para el tema de enumeración y darnos una visión general de cómo está constituido un entorno AD dentro de una red empresarial y una de ellas es esta.

Personalmente, me impresionó la claridad de los reportes HTML que genera, ideales para mostrar hallazgos tanto a equipos técnicos como a gerencia, todo esto con la finalidad de mitigar o corregir dichas vulnerabilidades que se puedan hallar.

Gracias
Misti Offensive.