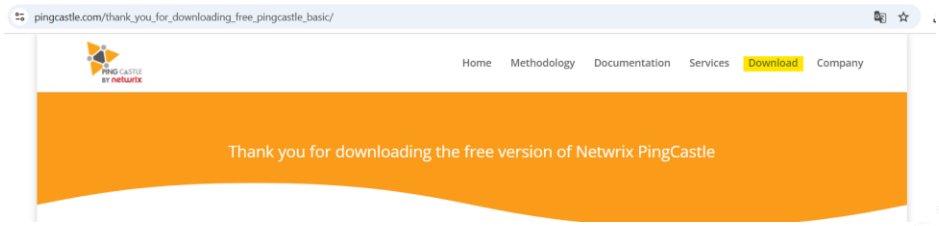
PINGCASTLE

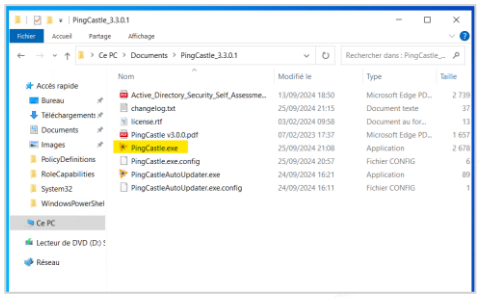
PingCastle est un outil d'audit de sécurité pour les environnements Active Directory (AD). Il permet d'évaluer rapidement le niveau de risque d'un domaine AD en identifiant les failles de configuration, les mauvaises pratiques et les vulnérabilités potentielles.

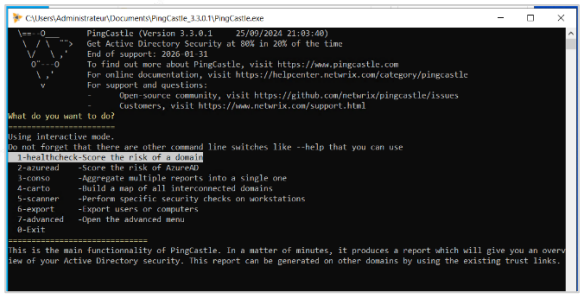
Tout d'abord, télécharger PingCastle sur le site :
https://www.pingcastle.com/thank_you_for_downloading_free_pingcastle_basic/



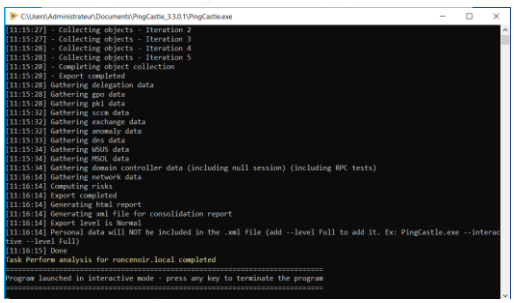
J'ai décidé de l'installer sur mon contrôleur de domaine principal ADsecure1 afin d'avoir un audit rapide.

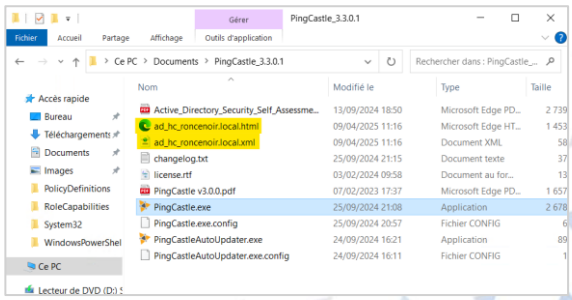
J'ai dézippé le fichier téléchargé **et je lance la programme pingcastle.exe. Pour lancer un audit, je sélectionne 1-healthcheck-score the risk of a domain.**



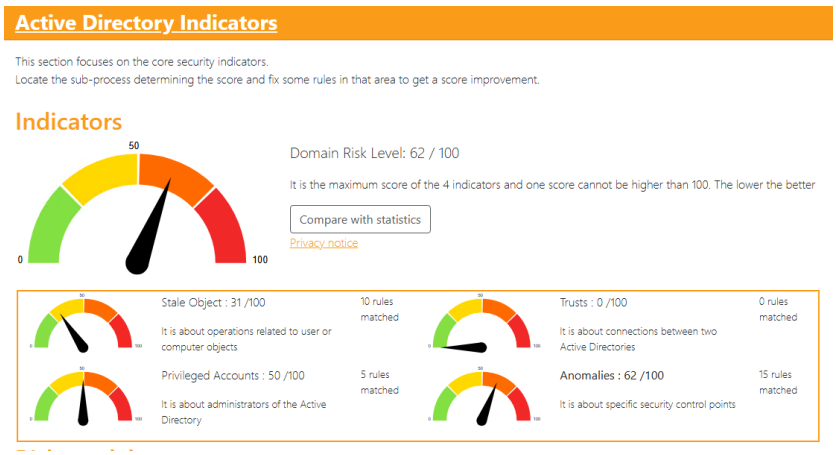


Je fais « **entrer** » car le domaine à auditer est bien mon domaine proposé par défaut. Une fois l'audit terminé, faire « **entrer** » pour fermer la fenêtre. On peut constater que **deux fichiers ont été créés.**





Etudions le **rapport html.**



On peut voir que PingCastle a attribué une note à mon niveau de sécurité concernant mon active directory. Plus la note est élevée, moins notre installation est sécurisée. La note obtenue correspond au pire score enregistré parmi 4 indicateurs :

- **Stale Object :** points de sécurité liés aux utilisateurs ou aux ordinateurs
- **Privileged Accounts :** points de sécurité liés aux comptes avec des privilèges élevés (Administrateurs) du domaine Active Directory
- **Trusts :** points de sécurité liés aux relations d'approbations entre les domaines Active Directory
- **Anomalies :** points de sécurité liés à d'autres aspects de la configuration qui peuvent impacter la sécurité de votre annuaire

Ici, mon score le moins bon correspond au facteur « anomalies ».

Un tableau suit ces graphiques, permettant d'en savoir un peu plus sur les risques que j'encoure avec la configuration actuelle de mon annuaire Active Directory.

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:
score is 0 - no risk identified but some improvements detected
score between 1 and 10 - a few actions have been identified
score between 10 and 30 - rules should be looked with attention
score higher than 30 - major risks identified

S'en suit une liste de points aggravant et à améliorer pour que notre note de risque redescende et que notre active directory soit d'avantage sécurisé.

Stale Objects

Stale Objects : 31 /100

It is about operations related to user or computer objects

Stale Objects rule details [10 rules matched on a total of 56]

The LAN Manager Authentication Level allows the use of NTLMv1 or LM.	+ 15 Point(s)
Non-admin users can add up to 10 computer(s) to a domain	+ 10 Point(s)
The subnet declaration is incomplete [2 IP of DC not found in declared subnets]	+ 5 Point(s)
Number of accounts which have never expiring passwords: 3	+ 1 Point(s)
Verify Kerberos Armoring is enabled on DCs and the domain functional level is at least Windows Server 2012	Informative rule
Verify Kerberos Armoring is enabled on clients and the domain functional level is at least Windows Server 2012	Informative rule
Some script extensions, used in phishing, can be directly run by double clicking on it	Informative rule
Not all possible Defender ASR mitigations are in Block or Warn mode	Informative rule
It is possible for scripts engine used by hackers to connect directly to the Internet	Informative rule
The GPO are not pushing recommended configuration for Terminal Services	Informative rule

Privileged Accounts

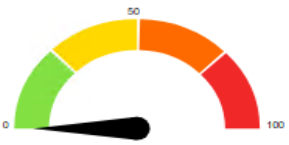
Privileged Accounts : 50 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [5 rules matched on a total of 46]

Presence of Admin accounts which do not have the flag "This account is sensitive and cannot be delegated": 2	+ 20 Point(s)
The group Schema Admins is not empty: 1 account(s)	+ 10 Point(s)
The Recycle Bin is not enabled	+ 10 Point(s)
Number of admins not in Protected Users: 2	+ 10 Point(s)
OU without the accidental deletion protection have been found	Informative rule

Trusts



Trusts : 0 /100

It is about links between two Active Directories

Trusts rule details [0 rules matched on a total of 12]

No rule matched

Anomalies analysis

Anomalies : 62 /100

It is about specific security control points

Anomalies rule details [15 rules matched on a total of 72]

Last AD backup has been performed 8 day(s) ago	+ 15 Point(s)
The audit policy on domain controllers does not collect key events.	+ 10 Point(s)
The spooler service is remotely accessible from 2 DC	+ 10 Point(s)
RPC interfaces of DC are likely vulnerable to coercion attacks. Identified interfaces: 2	+ 10 Point(s)
Policy where the password length is less than 8 characters: 1	+ 10 Point(s)
Hardened Paths have been modified to lower the security level	+ 5 Point(s)
At least one user, computer or group has been added as a member to the PreWin2000 compatible group	+ 2 Point(s)
No GPO has been found which disables LLMNR or at least one GPO does enable it explicitly	Informative rule
No password policy for service accounts found (MinimumPasswordLength>=20)	Informative rule
No GPO has been found which implements NetCease	Informative rule
The PreWin2000 compatible group contains "Authenticated Users"	Informative rule
DsHeuristics has not been set to enable the mitigation for CVE-2021-42291	Informative rule
Authenticated Users can create DNS records	Informative rule
Anonymous Binding to the rootDse is enabled	Informative rule
The PowerShell audit configuration is not fully enabled.	Informative rule

Last AD backup has been performed 8 day(s) ago — + 15 Point(s)

Check for the last backup date according to Microsoft standard

Rule ID:
A-BackupMetadata

Description:
The purpose is to check if the backups are actually up to date in case they are needed. The alert can be triggered when a domain is backed up using non-recommended methods

Technical explanation:
A verification is done on the backups, ensuring that the backup is performed according to Microsoft standards. Indeed, at each backup the DIT Database Partition Backup Signature is updated. If for any reasons, backups are needed to perform a rollback (rebuild a domain) or to track past changes, the backups will actually be up to date. This check is equivalent to a *REPADMIN /showbackup* *.

Advised solution:
Plan AD backups based on Microsoft standards. These standards depend on the Operating System. For example with the wbadmin utility: *wbadmin start systemstatebackup -backuptarget:d:*

Points:
15 points if the occurence is greater than or equals than 7

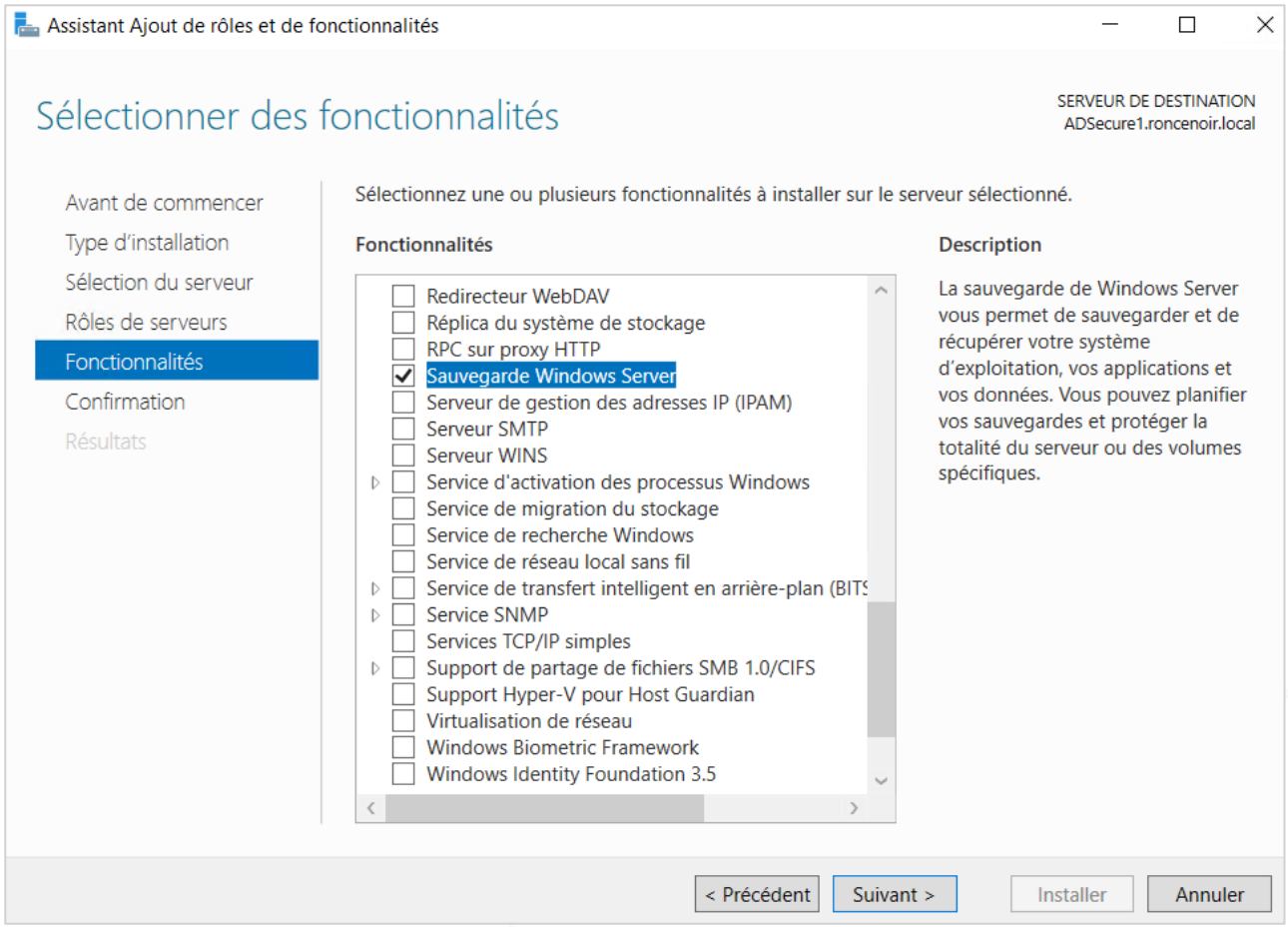
Documentation:
https://technet.microsoft.com/en-us/library/(j)130668(v=ws.10).aspx
[US]STIG V-25385 - Active Directory data must be backed up daily for systems with a Risk Management Framework categorization for Availability of moderate or high. Systems with a categorization of low must be backed up weekly.
[MITRE]Mitre Att&ck - Mitigation - Data Backup

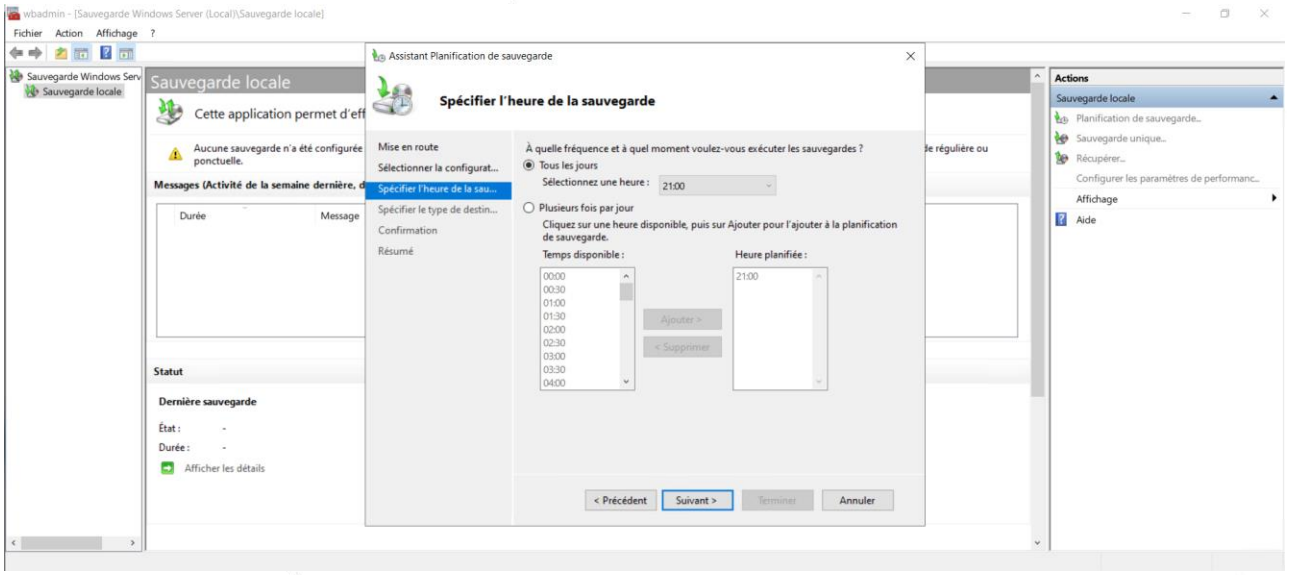
Details:
The detail can be found in Backup

Améliorer ces points est important pour avoir un environnement active directory mieux protégé.

Si je déroule l'un des points mentionnés, tout m'est expliqué. Son danger, sa cause possible, sa méthode de résolution.

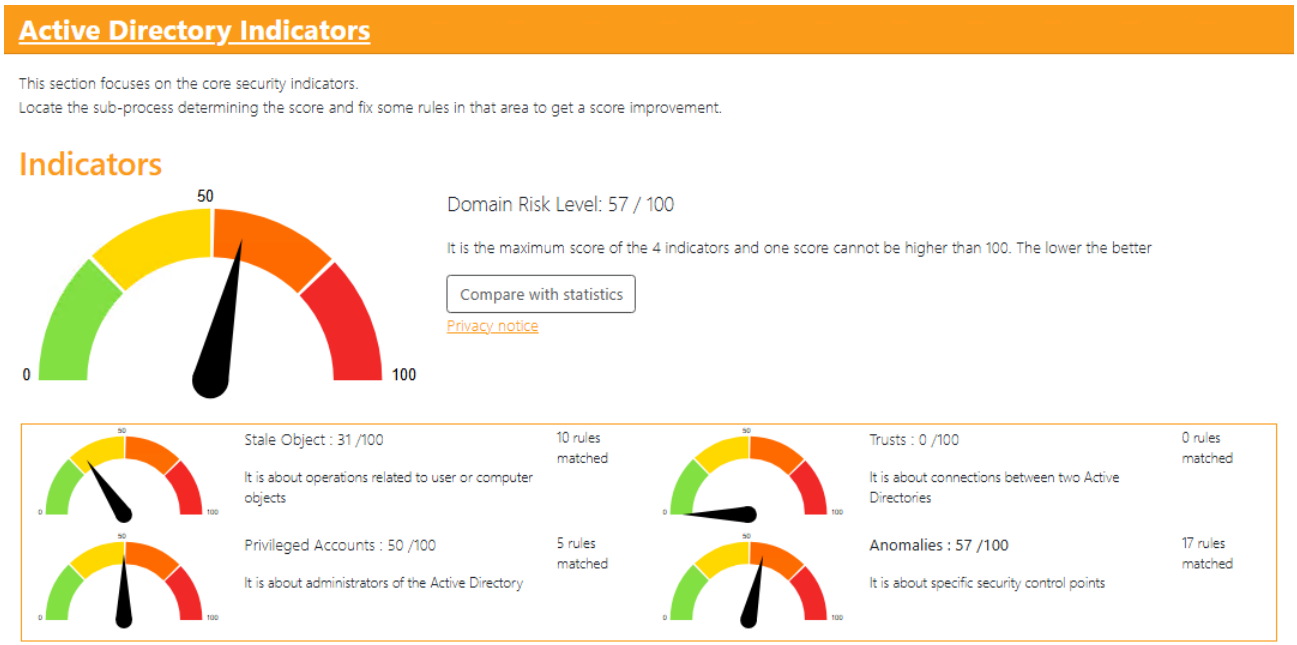
Pour exemple, je vais tenter de résoudre le problème de manque de Backup en installant la fonctionnalité « sauvergarde Windows Server » sur mon serveur active directory.





Grâce à cette fonctionnalité, je peux plannifier des sauvegardes régulières de mon serveur (j'ai créé un disque virtuel exprès avec un volume libre au format NTFS pour le faire).

Une fois terminé et ma première sauvegarde effectuée, je relance un audit pingcastle. En regardant le rapport issu de celui-ci, on peut constater que ma note a légèrement baissé. J'ai donc amélioré l'état de sécurité de mon active directory.



Pour auditer facilement un annuaire Active Directory, PingCastle est une très bonne solution ! Son utilisation repose sur un simple fichier "setup.exe" qui n'a pas besoin d'être réellement installé sur la machine, ce qui est avantageux. Nous venons de voir l'utilisation de la fonctionnalité principale de PingCastle, mais il est possible d'aller plus loin.

En effet, PingCastle intègre d'autres fonctionnalités que vous pouvez explorer à partir du menu de l'application (en naviguant avec le clavier) ou en regardant la documentation. Par exemple, vous pouvez réaliser un export des objets ordinateurs ou utilisateurs de votre Active Directory, mais aussi utiliser la fonction "Scanner" pour vérifier certains éléments de configuration sur les objets ordinateurs de votre Active Directory (exemple : rechercher la présence d'un partage ouvert).