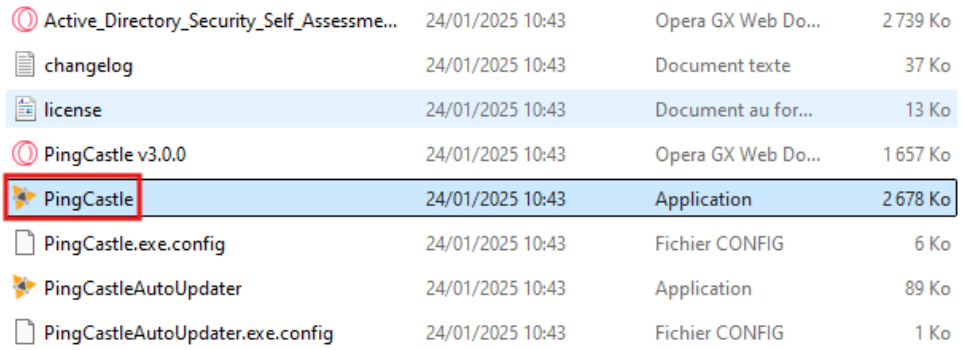
PingCastle

Qu’est ce que Pingcastle ?

Pingcastle est un outil de sécurité (comme lynis pour linux) qui évalue le niveau de sécurité d’un environnement Windows Server.

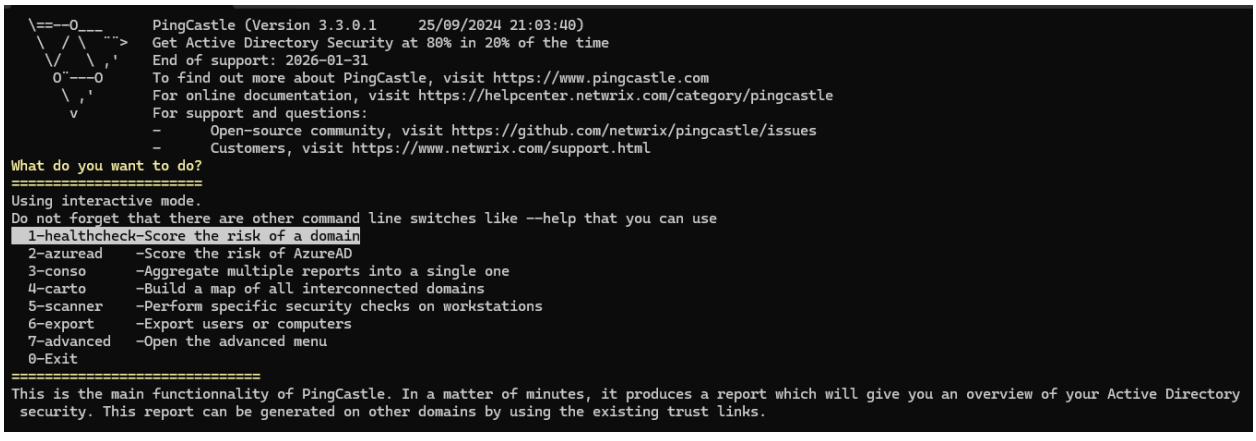
Pratique

Tout d’abord, il faut installer PingCastle sur le Windows Server, extraire le dossier télécharger. Ensuite on peut procéder de 2 façons, soit on décide de directement lancer le “PingCastle.exe” depuis le dossier PingCastle

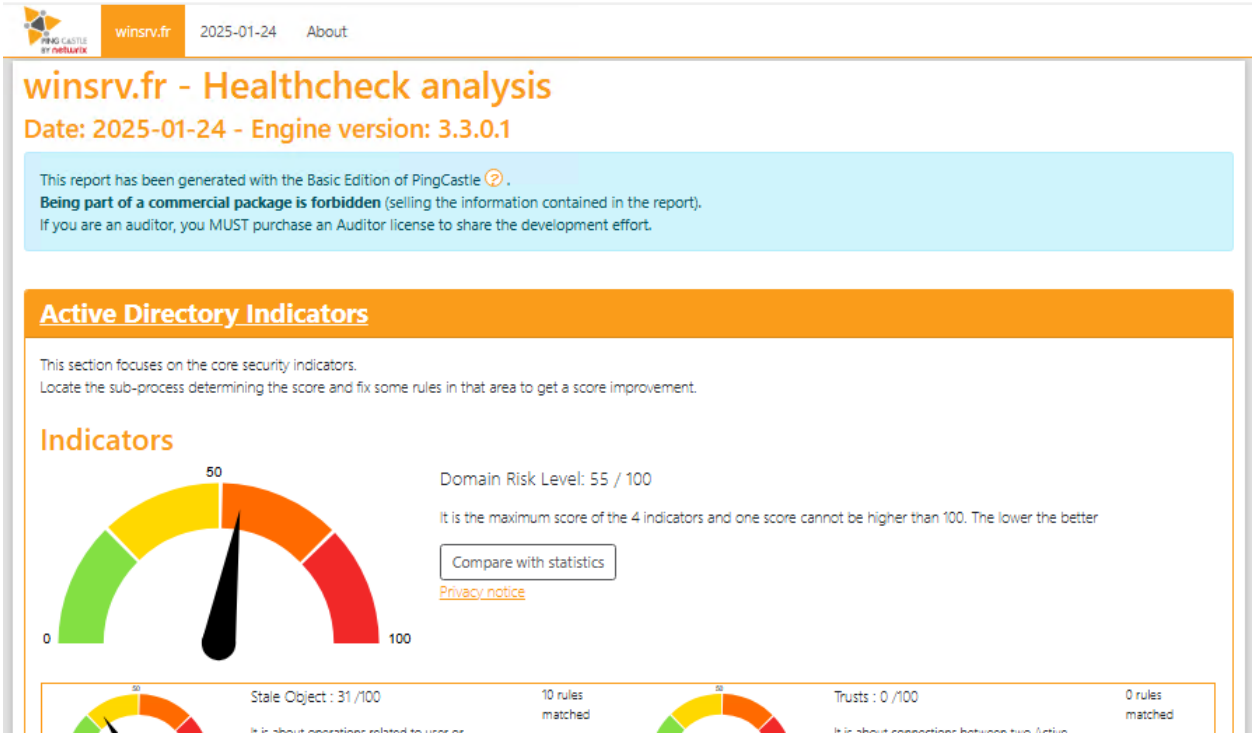


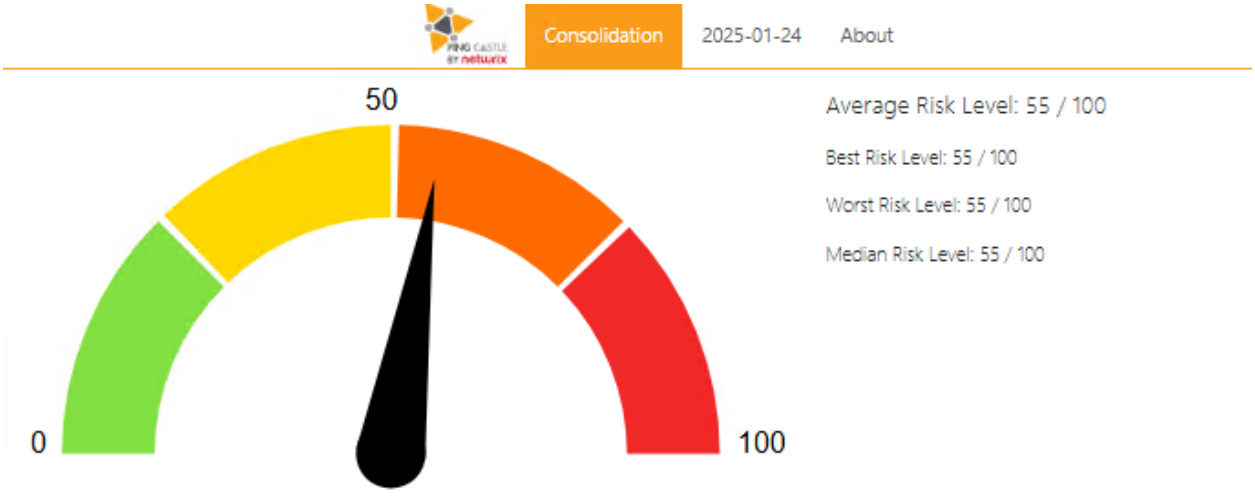
Soit on se rend sur l’invite de commande du PC (CMD), on rentre le chemin d’accès du dossier et on tape la commande “PingCastle.exe”.

Dans les 2 cas, cela lancera PingCastle. On peut ensuite choisir ce qu’on veut faire, vérifier, etc....



A la fin des analyses, PingCastle fera un rapport sous forme de fichier à ouvrir sur un navigateur de recherche. Ce rapport, affiche une jauge correspondant au niveau de sécurité de l'infrastructure et se trouve dans le dossier PingCastle. Ce rapport donne aussi des astuces/conseilles pour améliorer la sécurité du Windows Server.





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