Retour d'expérience sur PingCastle

Steven Bolzer, Ingénieur plateformes IT
Etienne Chevillard, RSSI

Cbp Group

Forum ADN'Ouest – 18 mars 2019

Cbp Group
Leader européen de l'assurance emprunteur

Depuis 1990, Cbp est l'un des premiers cabinets de courtage français, spécialiste de l'assurance des emprunteurs. Cbp opère **en Europe Continentale**, par sa présence en France mais aussi en Allemagne, Italie, Espagne, Pologne et Portugal.

N°1 en France avec près d'un quart du marché en « contrats groupes » et plus de 950 000 contrats individuels.

Expert en matière **de conseil et de gestion** auprès des grands comptes du monde financier

Leader européen de l'assurance emprunteur avec 12 % des primes intermédiées et n°1 en Italie de la CQS

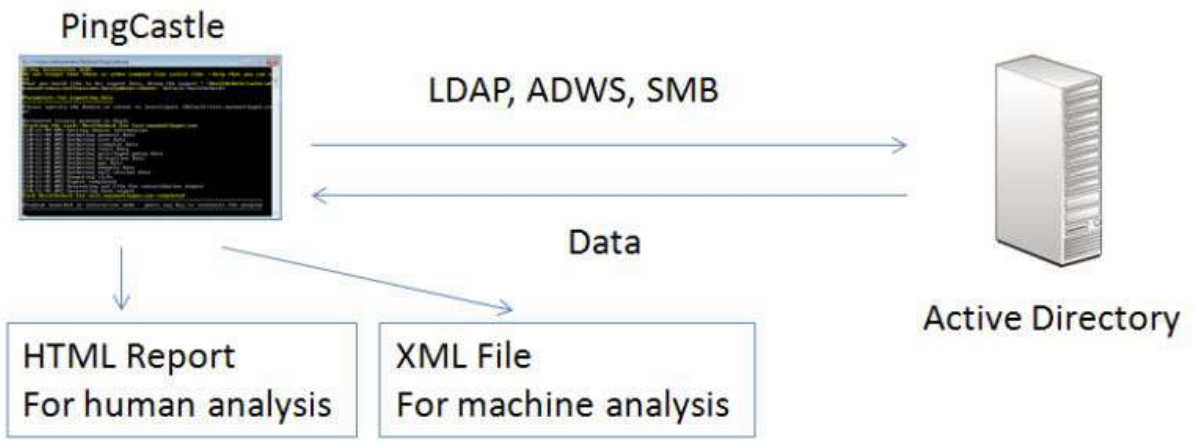
Exclusivement en **B to B**

Cbp Group
Indicateurs Europe

PingCastle

Présentation de l'outil

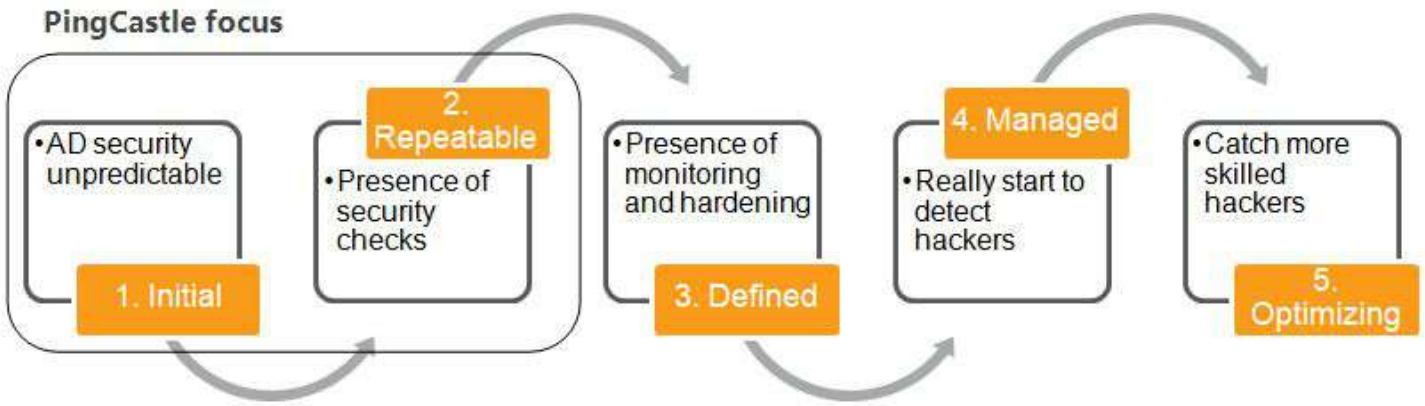
- Outil français développé dans le cadre d'un projet pour ENGIE
  - Version gratuite sous licence Open Source (OSL 3.0)
  - Version commerciale avec fonctionnalités avancées et support
- Recueil rapide des informations les plus pertinentes sur la sécurité d'un annuaire Active Directory
- A partir d'un modèle et de règles, évaluation du niveau de sécurité et génération d'un rapport
- Génération de rapports détaillés
- Web : https://www.pingcastle.com/



PingCastle

Approche de Cbp

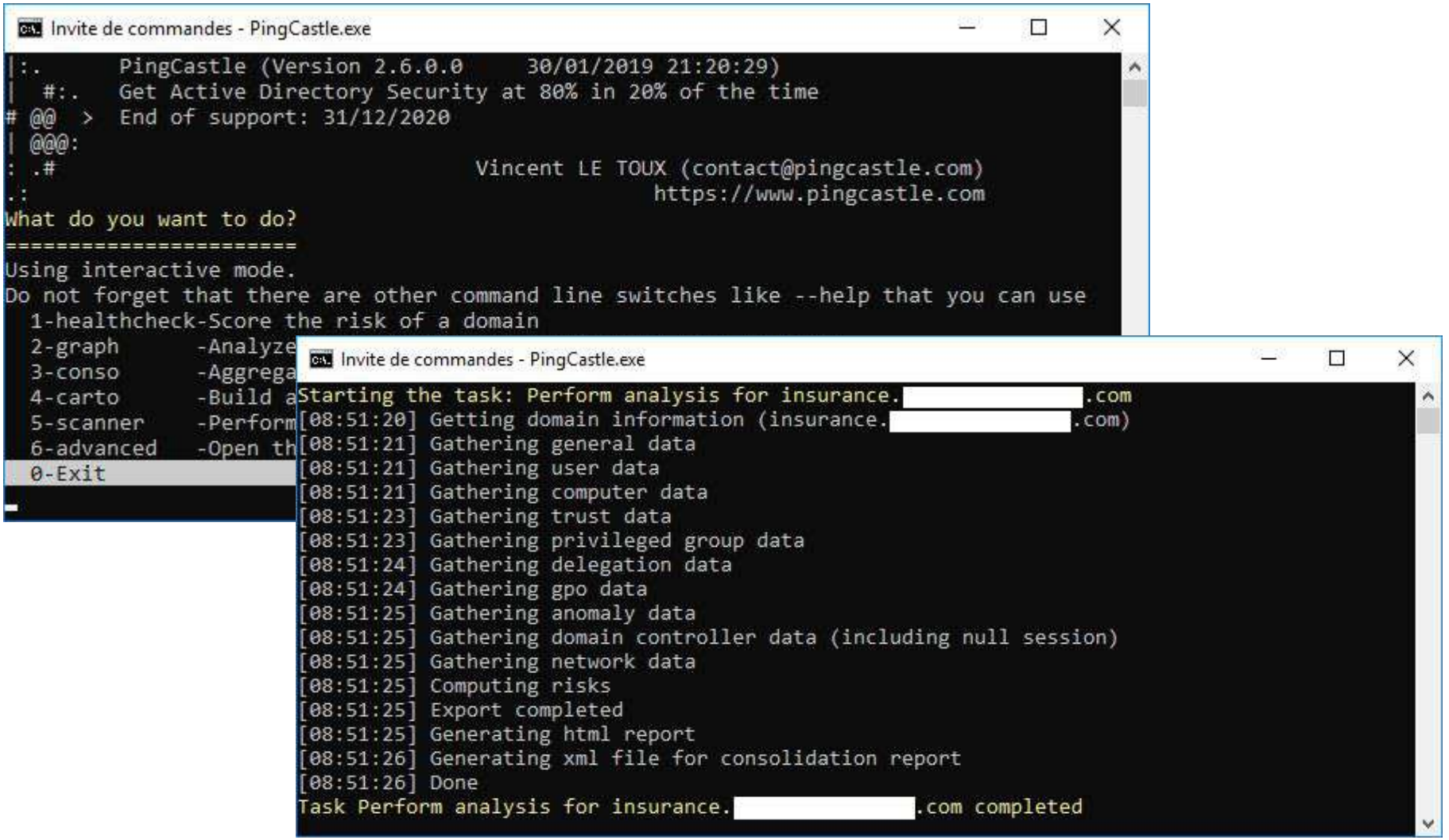
- PingCastle se positionne sur les étapes 1 et 2 du modèle de maturité CMMI :



- Objectif de Cbp : automatiser un contrôle périodique de la sécurité de nos 2 forêts Active Directory
  - **Aujourd'hui : contrôle périodique** (mensuel) avec correction des anomalies
  - **Mi-2019 : monitoring** via un rapport hebdomadaire avec alerte automatique en cas de dégradation ou nouvelle anomalie.

PingCastle

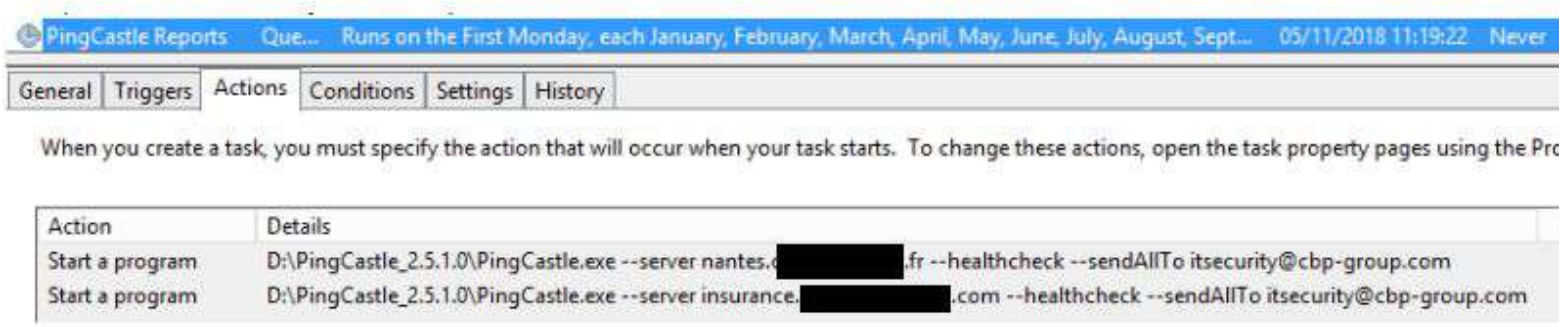
Mise en oeuvre : test en ligne de commande



PingCastle

Mise en oeuvre : automatisation

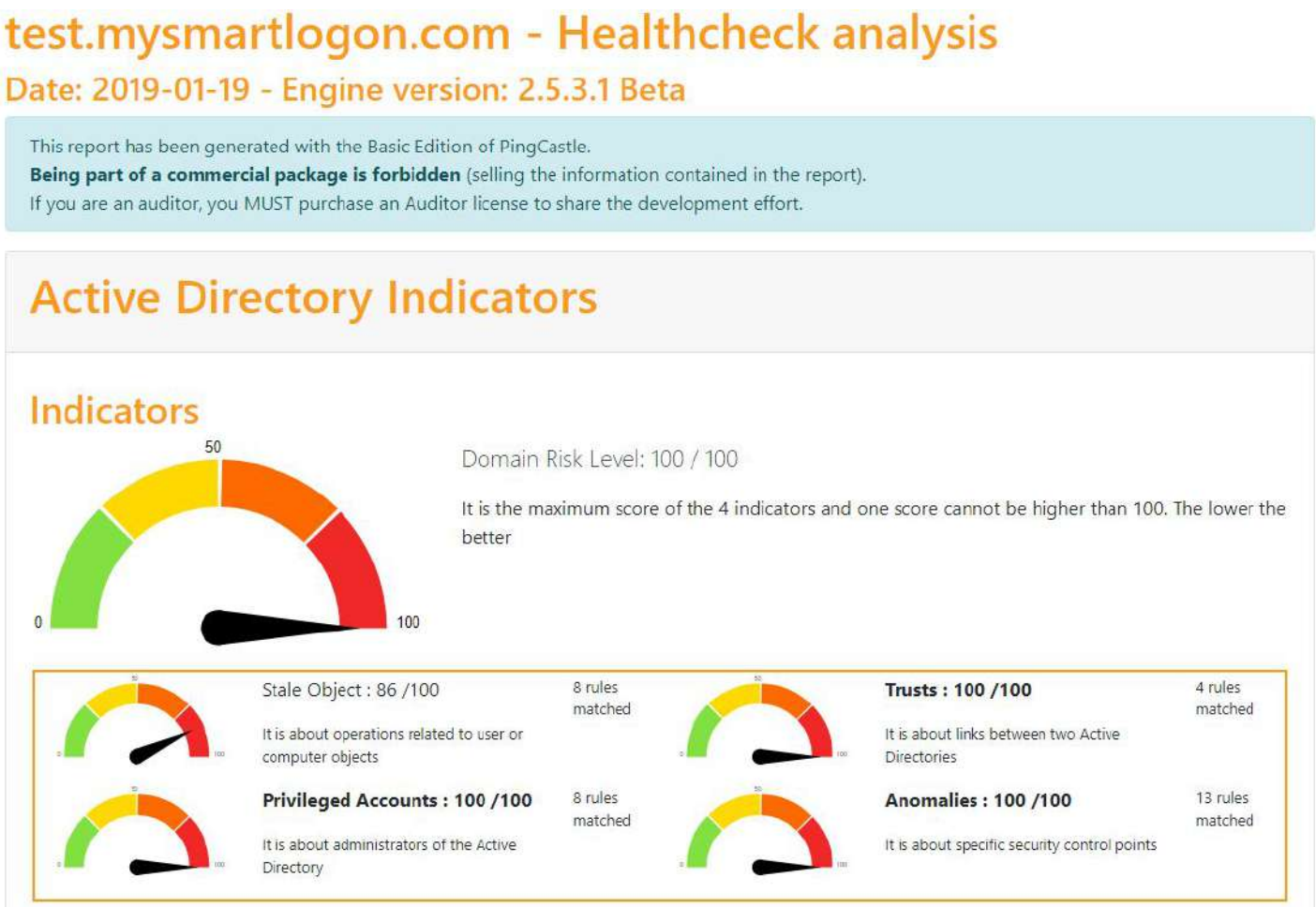
- Déploiement :
  - Copier l'exécutable sur le serveur cible (serveur d'administration)
  - Configurer l'outil via le fichier de configuration (serveur SMTP, email expéditeur)
  - Planifier l'exécution via une tâche planifiée (ou ordonnanceur)
  - Paramètres de l'outil :
    - nom du domaine AD à auditer
    - type de contrôle
    - email destinataire



PingCastle

Exemple de rapport

Partie 1 : scoring (indicateurs)



PingCastle

Exemple de rapport

Partie 2 : détails du niveau de risque par domaine

4 domaines :

- Comptes à privilèges
- Liens entre AD
- Objets de l'AD (délégation, …)
- Anomalies de sécurité

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			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

PingCastle

Exemple de rapport

Partie 3 : résultats par domaine et par règle/contrôle

Anomalies rule details [13 rules matched]

Number of passwords found in GPO: 3	+ 60 Point(s)
Last change of the Kerberos password: 2512 day(s) ago	+ 50 Point(s)
Number of account using a smart card whose password is not changed: 3	+ 30 Point(s)
Last AD backup has been performed 2512 day(s) ago	+ 15 Point(s)
LAPS doesn't seem to be installed	+ 15 Point(s)
Suspicious admin activities detected on 1 user(s)	+ 15 Point(s)
Number of DC with NULL SESSION enabled: 1	+ 10 Point(s)
Policy where the password complexity is less than 8 characters: 4	+ 10 Point(s)

PingCastle

Exemple de rapport

Partie 3 : résultats par domaine et par règle/contrôle

Last change of the Kerberos password: 2512 day(s) ago

+ 50 Point(s)

Mitigate golden ticket attack via a regular change of the krbtgt password

Description:
The purpose is to alert when the password for the krbtgt account can be used to compromise the whole domain. This password can be used to sign every kerberos ticket, and monitoring it closely often mitigates the risk of golden ticket attacks greatly.

Technical explanation:
Kerberos is an authentication protocol. It is using to sign its tickets a secret stored as the password of the krbtgt account. If the hash of the password of the krbtgt account is retrieved, it can be use to generate authentication tickets at will.
To mitigate this attack, it is recommanded to change the krbtgt password every 40 days. If it not the case, every backups done until the last password change of the krbtgt account can be used to emit Goldent tickets, compromising the entiere domain.
Retrieval of this secret is one of the highest priority in an attack, as this password is rarely changed and offer a long term backdoor.
Also this attack can also be performed using the former password of the krbtgt account

Advised solution:
The password of the krbtgt account should be changed twice to invalidate the golden ticket attack.
Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers
There are several possibilities to change the krbtgt password. First, a Microsoft script can be run in order to guarantee the correct replication of these secrets. Unfortunately this script supports only English operating systems. Second, a more manual way is to essentialy reset the password manually once, then to wait 3 days, then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden ticket attack.

Points:
50 points if the occurence is greater or equals than 732
then 40 points if the occurence is greater or equals than 366
then 30 points if the occurence is greater or equals than 180
then 20 points if the occurence is greater or equals than 70

Documentation:
https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51
ANSSI CERTFR-2014-ACT-032

PingCastle

Exemple de rapport

Partie 4 : détail des résultats

Domain Information

Domain	Netbios Name	Domain Functional Level	Forest Functional Level	Creation date	DC count	Schema version
test.mysmartlogon.com	TEST	Windows Server 2008	Windows Server 2008	2012-03-03 18:12:40Z	2	Windows Server 2008 R2

Showing 1 to 1 of 1 entries

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 Passwo not Req
22	18	4	4	14	0	4	3	1	

PingCastle

Avantages : point de vue de l'administrateur système

Déploiement :

- Pas de setup, un simple binaire à exécuter sur un poste ou serveur connecté à l'AD
- Possibilité d'envoyer le rapport automatiquement par email
- L'outil ne se met pas à jour automatiquement (déploiement manuel).

Rapports :

- Rapports HTML : faciles à lire et explicites
- Solutions avec liens vers les recommandations et/ou procédures de remédiation.

cbp

PingCastle

Avantages : point de vue du RSSI

Déploiement :

- Peu intrusif : pas de logiciel à installer, aucun droit administrateur nécessaire pour exécuter l'outil (requêtes GET et interrogations d'API en consultation uniquement)

Rapports :

- Les contrôles de sécurité standard sont intégrés à l'outil (OS obsolètes, mots de passe qui n'expirent jamais, mots de passe < 8 caractères, SMB v1, sauvegarde de l'AD, etc.)
- Rapports XML : automatisation/consolidation des résultats
- Possibilité de chiffrer les rapports avant envoi par email (RSA)
- Possibilité de créer un rapport consolidé pour plusieurs AD
- Possibilité de générer un tableau de bord de synthèse au format PPTX (non testé).

cbp

Avertissement

Ce document a été établi par le groupe Cbp à partir d'informations publiques estimées fiables. Les informations contenues dans ce document ont été préparées dans le seul but de fournir des éléments de présentation .

Ce document ne peut être utilisé qu'à cette fin et ne peut être photocopié, reproduit ou transmis à d'autres personnes qu'avec l'accord préalable écrit du groupe Cbp.

Cette présentation est incomplète sans l'explication orale du groupe Cbp.

La responsabilité du groupe Cbp et de ses employés ne peut être engagée de quelque manière que ce soit quant à l'exactitude ou à l'exhaustivité de ce document.

Cbp Group filiale du
Groupe Financière CEP
11, rue Royale
75008 PARIS
Tel : + 33 1 80 52 35 00

Cbp Group
www.cbp-group.com
11, rue Royale
75008 PARIS
Tel : + 33 1 80 52 32 90

Steven BOLZER
Ingénieur plateformes IT

Etienne CHEVILLARD
Responsable Sécurité SI