Sécurisation et audit de l'Active Directory (AD) avec PINGCASTLE

L'état de l'art et recommandations

- effectuer des points de contrôle avec des outils d'audit (PINGCASTLE, ORADAD, BLOODHOUND,...) ou des scripts

- avoir en tête quelques guides et référentiels avec les recommandations de l'ANSSI sur:
  -- la liste des points de contrôle AD
  --> https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
  -- la journalisation suffisante
  --> https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation
  --> https://cyber.gouv.fr/publications/recommandations-de-securite-pour-la-journalisation-des-systemes-microsoft-windows-en
  --- administration sécurisée des SI reposant sur l'AD
  --> https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad

- se référer également à des guides plus techniques sur internet
  -- adsecurity.org

- La difficulté est parfois de mettre en oeuvre toutes les recommandations à travers ces outils.

Recommandations sur la sécurité de l'AD

- tiering: séparation en couches étanches sur l'AD (découpage pyramidal en tiers 0, 1 et 2) afin d'obtenir une résilience
  -- administration de l'AD
  -- administration classique
  -- administration des machines classiques
- désactivation du NTLM
- forçage des contrôles d'intégrité

Quelques points de contrôles par rapport à des méthodes d'attaque parfois combinées:

- cpassword: recherche et récupération d'un mot de passe admin dans les GPO (CERTFR-2015-ACT-046)
- kerberoasting: comptes privilégiés avec l'attribut SPN (ServicePrincipalName) demandant 1 ticket kerberos pour se connecter au service TGS (un epartie du ticket signée avec le hash du mot de passe du compte; essayer les hash et attaque de type pass-the-hash).

> définition selon Microsoft " SPN est un identificateur unique pour l’instance de service du contrôleur de réseau, qui est utilisé par l’authentification Kerberos pour associer une instance de service à un compte de connexion de service ".

- PrintSpooler: la réception de notifications permet de forcer une authentification du serveur de domaine sur une machine d'un attaquant
- golden ticket: extraction de mot de passe du compte krbtgt
- une attaque de type relai NTLM comme avec service PKI/ADCS (PetitPotam, bulletin du CERTFR-2021-ACT-032)
- analyse de partages réseaux

L'audit en continu avec des outils comme PINGCASTLE

A la 1ere utilisation de PINGCASTLE

PINGCASTLE est un outil français créé en 2015 qui a émergé lors d'un projet de sécurisation d'une entreprise multinationale. L'idée était de construire une base de points de contrôle mais reproductibles afin de mener une mailleure sécurité. Il permet de générer un rapport avec un score sur les risques.

Objectif et principe:

- Il s'agit de réduire le score et donc le risques.
- Pour cela, choisir le scénario d'audit qu'on souhaite faire avec les bonnes options figurant dans les sous-menus
- Il se lance en ligne de commande depuis une fenêtre terminal ou Powershell et est scriptable.
- Peut lister les objets du domaine où chaque utilisateur a un SID propre (SID du domaine-RID) et utiliser des SID virtuels (compte virtuel pour chaque service installé)

exemple: S-1-5-21-1990400566-1867844161-3796721076-500

1- télécharger le fichier ZIP sur le Github https://github.com/vletoux/pingcastle ou depuis le site officiel https://www.pingcastle.com/download/
2- décompresser l'archive ZIP et lancer l'exécutable pingcastle.exe (double clic)
3- sélectionner le scénario ou mode HEALTHCHECK-Score the risk of a domain
-- par défaut il va remonter le domaine Active Directory correspondant au compte utilisé
-- valider avec la touche Entrée pour lancer l'audit sinon indiquer/saisir le nom du domaine (exemple: raisin-dc1.raisin.lab)
-- appuyer sur Entrée pour terminer
-- un rapport est généré sous la forme de 2 fichiers (HTML et XML)

Si c'est en ligne de commande il faut être dans un terminal et dans le répertoire où se trouve l'exécutable:

- saisir .\pingcastle.exe --log --interactive
- choisir les scénaraios et options souhaités.

Contenu du rapport et image

- Le principe:
  -- outil calculant 1 indice de risque souvent par défaut à 100 (le moins sécurisé).
  -- se base sur l'indicateur avec le plus mauvais score pour déduire le niveau de risque global (cadran avec l'aiguille et couleurs).
  -- utilise l'indicateur de maturité basé sur le système de notation de l'ANSSI.
  -- les principaux modules et scénarios

1. Healthcheck : Une vérification de "santé" établissant un scoring avec les vulnérabilités découvertes (le plus utilisée).
2. Conso : Avoir un rapport condensé sans explications détaillées des vulnérabilités trouvées.
3. Carto : Avoir une cartographie des domaines de confiance avec les liens directs (peut aller jusqu'à 5 niveaux de profondeur).
4. Scanner : Scan des différents éléments indépendants comme le listing des anti-virus présent sur le domaine, les partages,...

- cartographie et découverte des domaines approuvés
  -- dans le cas d'un AD sur le réseau interne et d'un AD en DMZ (relation d'approbation unidirectionnelle)
- plusieurs sections découvertes et problématiques liées:
  -- à la création et à la suppression de comptes utilisateurs et ordinateurs
  -- à la gestion des comptes privilégiés ou groupes spécifiques (Administrateurs, Tout le monde, Utilisateurs du domaine, Utilisateurs authentifiés)
  -- aux relations d'approbation entre des AD
  -- à des points de contrôle relevant de politique de sécurité (GPO).

Mise en place d'une correction progressive des anomalies

Quelques pistes:

- considérer le nombe de points pour chaque règle et à prioriser (règles critiques avec un nombre de points élevé)
  -- comme un mot de passe inchangé depuis plusieurs années
- considérer les règles propres aux comptes privilégiés
  -- le nombre de comptes pour l'administration
  -- les mécainismes de protection non actifs
- considérer les règles relevant des anomalies
  -- pas de LAPS
  -- politique d'audit
- considérer la rotation des mots de passe (krbtgt)

C'est à considérer en fonction du niveau de maturité de l'ANSSI et la liste des points de contrôle.

L'avantage avec PINGCASTLE est d'avoir un outil reproductible contrôlant de manière répétée avec des rapports comparables affichant les changements et les amélioration. Il est conseillé de recouper avec d'autres outils comme ORADAD ou le projet HardenAD.

Pour aller plus loin et atteindre un score de 0/100
https://www.it-connect.fr/securite-active-directory-comment-atteindre-un-score-de-0-100-dans-pingcastle/