Plan d’action

Auteur : Mickaël Faivre

Client : Clinique de Frontignan

Date du rapport : 15/04/2025

Table des matières

1. Plan d'action à court terme

1.1 Criticité élevée

Vulnérabilité 01 – User-as-pass

- **Résumé :** Plusieurs comptes utilisent comme de passe leur identifiant (exemple : test/test).
- **Priorité :** 1/7
- **Solution :** Réinitialiser les mots de passe.
- **Ressource :** Recommandation pour maîtriser sa sécurité (CNIL)

Vulnérabilité 03 – Mot de passe dans un script

- **Résumé :** Un mot de passe administrateur a été trouvé, en clair, dans un script PowerShell.
- **Priorité :** 2/7
- **Solution :** Supprimer tous les scripts contenant des mots de passe.
- **Ressource :** Gérer ses credentials en PowerShell avec le module secret management (IT-Connect)

Vulnérabilité 04 – Mot de passe en clair dans une description AD

- **Résumé :** Un mot de passe est visible dans le champ « description » d'un utilisateur Active Directory.
- **Priorité :** 3/7
- **Solution :** Auditer les attributs de l'ensemble des utilisateurs avec PowerShell pour y supprimer les données sensibles.
- **Ressource :** Récupérer des informations Active Directory avec PowerShell (IT-Connect)

Vulnérabilité 02 – Partage de fichiers mal protégé

- **Résumé :** Des partages sont accessibles sans restriction appropriée.
- **Priorité :** 4/7
- **Solution :** Revoir les permissions NTFS et de partage. Implémenter le principe du moindre privilège.
- **Ressource :** Serveur de fichiers : permission NTFS et de partage (IT-Connect)

1.2 Criticité moyenne

Vulnérabilité 07 – Kerberoasting

- **Résumé :** Des comptes utilisateurs standards font tourner des services ce qui les rend vulnérables à des extractions de données.
- **Priorité :** 5/7
- **Solutions :**
  - Identifier tous les comptes avec un SPN en utilisant PowerShell : *Get-AdUser -Filter {ServicePrincipalName -like « * »}*
  - Remplacer ces comptes par des comptes de services dédiés. (gMSA)
  - Désactiver la délégation Kerberos non-nécessaire sur les comptes ayant un SPN.
- **Ressources :**
  - Kerberos Delegation (hackndo)
  - Comment se défendre contre l'analyse SPN dans Active Directory (Semperis)
  - Active Directory : utilisation des gMSA (group Managed Service Account) (IT-Connect)

Vulnérabilité 08 – Secrets stockés localement via DPAPI

- **Résumé :** DonPAPI permet d'extraire des mots de passes stockés dans les tâches planifiés ou dans les profils locaux.
- **Priorité :** 6/7
- **Solution :** Supprimer les tâches contenant des credentials et désactiver le stockage des mots de passe en local.
- **Ressource :** DonPAPI - Ou l'art d'aller plus loin que le Domain Admin (Login-securite)

Vulnérabilité 10 – lsass – Pass-the-ticket

- **Résumé :** Des identifiants sont récupérables depuis le processus lsass
- **Priorité :** 7/7
- **Solution :** Activer Windows Credentials Guard et restreindre l'accès RDP aux comptes nécessaires.
- **Ressources :**
  - Fonctionnement de Credential Guard (learn microsoft)
  - Configurer Credential Guard (learn microsoft)

2. Plan d'action à long terme

2.1 Criticité élevée

Vulnérabilité 05 – Réutilisation des mots de passe

- **Résumé :** Un même mot de passe est utilisé par plusieurs utilisateurs.
- **Priorité :** 1/6
- **Solutions :**
  - Utiliser les PSO (Password Setting Object) pour appliquer des exigences de mots de passe renforcées.
  - Interdire la réutilisation des mots de passe en configurant Password History.
  - Forcer la complexité et une longueur minimale (supérieure à 12 caractères).
  - Mener des audits sur les mots de passe avec un outil comme DSInterals.
  - Former les équipes à la nécessité d'utiliser des mots de passe robustes.
- **Ressources :**
  - Stratégie de mot de passe affinée (IT-Connect)
  - Recommandations relatives à l'authentification multifacteur et aux mots de passe (ANSSI)
  - DSInternals - Directiry Servuces Internals PowerShell Module and Framework (Github)

Vulnérabilité 12 – Pass-the-ticket (Rubeus)

- **Résumé :** Les TGT peuvent être injectés pour usurper l'identité d'un utilisateur AD.
- **Priorité :** 2/6
- **Solutions :**
  - Activer la journalisation avancée des événements de sécurité
  - Restreindre l'accès aux outils d'administration (Rubeus, mimikatz, etc.).
  - Implémenter une détection du comportement (SOC).
- **Ressources :**
  - Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory (ANSSI)
  - Définition d'un SOC (Oracle)

Vulnérabilité 11 – Mot de passe dans le planificateur de tâche

- **Résumé :** Un mot de passe AD a été récupéré, via DonPAPI, depuis une tâche planifiée.
- **Priorité :** 3/6
- **Solutions :**
  - Activer LSA Protection et Credential Guard pour limiter la possibilité de récupérer les clés de déchiffrement DPAPI.
  - Remplacer les tâches contenant des credentials par des scripts sans mot de passe (clé API, MSA, gMSA).
- **Ressources :**
  - Windows secrets extraction : a summary (Synacktiv)
  - Comment manipuler une API en PowerShell (It-Connect)

2.2.1 Mesures complémentaires pour les comptes à privilèges

Intégrer les comptes sensibles au groupe Protected Users

- **Objectif :** limiter les risques de compromission post-authentification (pass-the-hash, délégation, etc.)
- **Application :** les comptes d'administration, de backup et d'audit doivent être placés dans ce groupe.
- **Ressource :** Protected Users Security Group (Learn Microsoft)

Déployer LAPS (Local Administrator Password Solution)

- **Objectif :** empêcher la réutilisation de mots de passe locaux sur les machines du domaine.
- **Application :** doit être activé sur l'ensemble des postes clients et serveurs du domaine.
- **Ressource :** What is Windows LAPS ? (Learn Microsoft)

Déployer des PAW (Privileged Access Workstations)

- **Objectif :** fournir des postes d'administrations isolés.
- **Application :** les comptes à privilèges doivent disposer de machines spécifiques (administration système, audit, supervision, etc.)
- **Ressource :** Sécurisation des appareils dans le contexte de l'accès privilégié (Learn Microsoft)

2.3 Criticité moyenne

Mise en place d'un SOC (Security Operations Center)

- **Résumé :** le système n'a aucune surveillance active et ne dispose d'aucune détection des anomalies
- **Priorité :** 4/6
- **Solutions :**
  - Déployer un SIEM pour corréler les événements AD.
  - Mettre en place une supervision SOC : journalisation, alertes, détections de brute-force, etc.
- **Ressources :**
  - The Open Source Security Plateform (Wazuh)
  - Security Operations Center (SOC) : fonction, avantages et mise en oeuvre (Insyncom)

Formation des équipes techniques

- **Résumé :** Des erreurs de sécurité récurrentes et facilement évitables existent (stockage de mot de passe en clair, droits mal appliqués, etc.)
- **Priorité :** 5/6
- **Solutions :**
  - Planifier des formations internes régulières sur les bonnes pratiques de sécurité.
  - Mettre en place une politique de cybersécurité interne.
- **Ressources :**
  - Meilleures pratiques pour la sécurisation d'Active Directory (Learn Microsoft)
  - Guides essentiels et bonnes pratiques de cybersécurité : par où commencer ? (ANSSI)
  - Comment former vos équipes à la sécurité informatique en toute simplicité ? (Efficience IT)

Audit et durcissement de l'environnement Active Directory

- **Résumé :** Aucune politique d'audit périodique ou de durcissement de l'environnement n'existe.
- **Priorité :** 6/6
- **Solutions :**
  - Appliquer les recommandations de CIS Benchmark pour Active Directory.
  - Mener des audits périodiques avec des outils comme PingCastle.
- **Ressources :**
  - Auditer l'Active Directory avec PingCastle (IT-Connect)
  - Center for Internet Security (CIS) Benchmarks (Learn Microsoft)
  - Microsoft Windows Server (CIS Security)
  - Active Directory and Group Policy Management Best Practices (CIS Security)