Plan d’action

Client : Clinique de Frontignan

Auditeur : Binder Benjamin

Failles de Sécurité Identifiées dans le Rapport

1. **Version d'OpenSSH obsolète et vulnérable** : Le service SSH sur les serveurs DC01 et FILER01 utilise une version 7.7 datée, permettant l'énumération d'utilisateurs.
2. **Énumération des utilisateurs via Kerberos** : Une mauvaise configuration du service Kerberos a permis de découvrir des noms d'utilisateurs valides (test, administrator) sans authentification.
3. **Mots de passe faibles et identiques aux noms d'utilisateurs** : L'attaque par dictionnaire a révélé que les comptes test et backup utilisaient leur propre nom comme mot de passe, permettant un accès initial facile.
4. **Mot de passe en clair dans la description d'un compte Active Directory** : Le mot de passe Support2021 du compte Alex Maillot était stocké en clair dans le champ "description" de son objet utilisateur AD.
5. **Mot de passe en clair dans un script de connexion** : Le mot de passe T3RmIn4l du compte administrateur de serveur lbrunet a été découvert en clair dans un fichier connect.bat.
6. **Mots de passe de comptes de service faibles (Kerberoasting)** : Les comptes de service dmorin (azertyuiop) et websvc (p4ssw0rd) utilisaient des mots de passe extrêmement faibles, qui ont été craqués en quelques secondes après l'extraction de leurs hashes Kerberos.
7. **Absence de protection du processus LSASS** : Il a été possible de créer un "dump" complet de la mémoire du processus LSASS sur le serveur FILER01, permettant d'extraire le mot de passe d'un administrateur de domaine (pclerc) avec Mimikatz.
8. **Droits d'accès excessifs** : Un utilisateur standard (test) avait la possibilité de se connecter via SSH et RDP sur des serveurs critiques (contrôleur de domaine, serveur de fichiers), ce qui viole le principe du moindre privilège.

1. Plan d’action à court terme

- **Recommandation R01 : Supprimer les mots de passe stockés en clair**
  - **Vulnérabilités corrigées :** Faille 4, Faille 5
  - **Ordre de priorité : Priorité Critique**
  - **Actions à réaliser :**
    - Réinitialiser immédiatement le mot de passe du compte ***Alex Maillot*** et supprimer l'ancien mot de passe de sa description.
    - Réinitialiser immédiatement le mot de passe du compte ***lbrunet***.
    - Supprimer les identifiants en clair du script ***connect.bat*** et privilégier l'utilisation d'un coffre-fort de mots de passe.
    - Lancer un audit sur l'ensemble des descriptions d'objets AD et des scripts sur les partages réseau pour rechercher d'autres identifiants.
  - **Ressources :** Guide des bonnes pratiques de sécurité de l'AD fourni par l'ANSSI.

- **Recommandation R02 : Renforcer la politique de mots de passe du domaine**
  - **Vulnérabilités corrigées :** Faille 3, Faille 6
  - **Ordre de priorité : Priorité Élevée**
  - **Actions à réaliser :** Modifier la politique de mot de passe (GPO) avec à minima :
    - Exiger des mots de passe d'au moins **14 caractères**.
    - Exiger des mots de passe complexes (majuscules, minuscules, chiffres, caractères spéciaux).
    - Configurer un **seuil de verrouillage de compte** (ex: 5 tentatives échouées) pour bloquer les attaques par force brute.
    - Forcer la réinitialisation des mots de passe des comptes de service dmorin et websvc avec des mots de passe longs, uniques et complexes.
  - **Ressources :** Recommandations de Microsoft sur les politiques de mot de passe.

- **Recommandation R03** : **Activer la protection du processus LSASS**
  - **Vulnérabilité corrigée :** Faille 7
  - **Ordre de priorité : Priorité Élevée**
  - **Actions à réaliser :**
    - Activer la fonctionnalité **Credential Guard** sur les systèmes compatibles (Windows Server 2016+).
    - Activer la protection LSA (RunAsPPL) via GPO pour empêcher les processus non autorisés d'accéder à la mémoire de LSASS.
    - Limiter les droits d'administrateur local et de domaine aux seuls comptes qui en ont un besoin absolu.
  - **Ressources :** Documentation Microsoft sur la configuration de la protection LSA.

- **Recommandation R04** : **Mettre à jour les services vulnérables**
  - **Vulnérabilité corrigée :** Faille 1
  - **Ordre de priorité :** Priorité Moyenne
  - **Actions à réaliser :**
    - Mettre à jour le service **OpenSSH version 7.7** sur DC01 et FILER01 vers la dernière version stable.
    - Mettre en place un processus de veille et de gestion des correctifs de sécurité pour tous les services exposés sur le réseau.
  - **Ressources :** Site officiel d'OpenSSH, Bulletins de sécurité du CERT-FR.

- **Recommandation R05** : **Appliquer le principe du moindre privilège**
  - **Vulnérabilités corrigées :** Faille 2, Faille 8
  - **Ordre de priorité :** Priorité Moyenne
  - **Actions à réaliser :**
    - Révoquer les droits de connexion à distance (SSH/RDP) pour les utilisateurs standards (comme test) sur les serveurs critiques.
    - Durcir la configuration de Kerberos pour empêcher l'énumération anonyme des utilisateurs.
    - Segmenter les droits d'administration : les administrateurs de postes ne doivent pas avoir de droits sur les serveurs, et inversement.
  - **Ressources :** Guide sur le principe du moindre privilège (CERT-FR).

2. Plan d’action à long terme

- **Recommandation R06** : **Mise en place d'une solution de supervision (SIEM)**
  - **Objectif :** Centraliser et analyser les journaux de sécurité pour détecter en temps réel les comportements anormaux (tentatives de connexion multiples, utilisation d'outils suspects, etc.).
  - **Actions à réaliser :** Définir les besoins, choisir une solution, et configurer la collecte des journaux depuis les contrôleurs de domaine, serveurs et postes de travail.

- **Recommandation R07** : **Sensibilisation et formation du personnel**
  - **Objectif :** Faire des utilisateurs et du personnel IT des acteurs de la sécurité.
  - **Actions à réaliser :** Organiser des formations régulières sur les bonnes pratiques de gestion des mots de passe, la détection du phishing, et la sécurisation des scripts.

- **Recommandation R08** : **Durcissement des configurations Active Directory et des accès**
  - **Objectif :** Réduire la surface d'attaque en appliquant les configurations de sécurité recommandées.
  - **Actions à réaliser :** Réaliser des audits de configuration réguliers et appliquer les guides de durcissement de l'ANSSI via des GPO.