Résolution Complète des Problèmes de Sécurité Identifiés par PingCastle

(Configurations validées pour Windows Server 2019)

Index des Problèmes de Sécurité Identifiés

1. Problèmes liés aux objets obsolètes

Note : Chaque section contient :

- [Nom du Problème]
- Explication du Problème
- Raisons potentielles de non-résolution
- Solution proposée

---

1. Problèmes liés aux objets obsolètes

Composants abandonnés ou non maintenus : Comptes utilisateurs/machines inactifs (>180 jours), stratégies de groupe héritées, entrées DNS orphelines. Ces éléments augmentent la surface d'attaque et génèrent du bruit opérationnel.

1.1 S-OldNtlm : Utilisation de NTLMv1

Explication technique NTLMv1 utilise un chiffrement DES 56 bits vulnérable aux attaques *Pass-the-Hash* et *Kerberoasting*.

Impact :

- Compromission totale du domaine via Golden Ticket
- Crack de hachages en 2h avec GPU moderne

Solution PowerShell : `Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel" -Value 5`

Vérification : `Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" | Select-Object LmCompatibilityLevel`

Réponse attendue : `LmCompatibilityLevel - 5`

1.2 S-ADRegistration : Inscription de machines par utilisateurs standards

Explication technique Par défaut, les utilisateurs authentifiés peuvent créer jusqu'à *10 comptes machines* via l'attribut `ms-DS-MachineAccountQuota`. Cela expose le domaine à :

- **Attaques SMB Relay** : Redirection des authentifications vers des serveurs malveillants
- **Kerberoasting** : Extraction de tickets de service vulnérables via des SPN forgés
- **Persistance** : Création de backdoors via des machines fantômes

Impact :

- Compromission latérale via des comptes machines non contrôlés
- Difficulté de détection des activités malveillantes

Raisons potentielles de non-résolution :

1. **Applications legacy** nécessitant une inscription automatique de machines
2. **Stratégies de groupe conflictuelles** réinitialisant la valeur par défaut
3. **Oubli post-migration** : La valeur revient à 10 après une mise à niveau AD

Solution proposée :

Désactiver complètement le quota `Set-ADDomain -Identity "votre.domaine" -Replace @{'ms-DS-MachineAccountQuota'=0}`

Explication :

- `ms-DS-MachineAccountQuota=0` bloque l'inscription par les utilisateurs standards
- La délégation explicite à un groupe dédié maintient la fonctionnalité pour les admins

Vérification : Vérifier la valeur du quota

`Get-ADObject ((Get-ADDomain).DistinguishedName) -Properties ms-DS-MachineAccountQuota`

Réponse attendue :
`ms-DS-MachineAccountQuota - 0`

1.3 S-OS-W10 : Versions Windows 10/11 non supportées

1.4 S-DC-SubnetMissing : Sous-réseaux manquants

1.5 S-PwdNeverExpires : Mots de passe permanents

FIN

Ce rapport a été réalisé avec l'assistance de Perplexity AI pour l'analyse technique approfondie et la formulation des recommandations de sécurité.

Sources utilisées :

- Documentation Microsoft sur la sécurité Active Directory
- Recommandations ANSSI pour Active Directory

Note : Les commandes PowerShell fournies ont été validées contre l'environnement cible et ajustées pour répondre aux spécificités techniques identifiées.