

# 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

- 1.1 **S-OldNtlm** - Utilisation du protocole NTLMv1 vulnérable
- 1.2 **S-ADRegistration** - Inscription de machines par utilisateurs standards
- 1.3 **S-OS-W10** - Versions Windows 10/11 non supportées
- 1.4 **S-DC-SubnetMissing** - Sous-réseaux manquants dans la topologie AD
- 1.5 **S-PwdNeverExpires** - Mots de passe permanents sur des comptes critiques

---

**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

#### 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.*