Plan d’action

Client : Clinique de Frontignan - Nicolas Turing (DSI)

Auditeur : Jonathan Youssef

I. Plan d'action à court terme

Proposez l'ensemble de vos recommandations réalisables à court terme par le client pour améliorer son niveau de sécurité sur l'environnement Active Directory. Suivez le modèle proposé dans la première case.

- Recommandation R01 : *Réinitialiser immédiatement les mots de passe compromis*
- Vulnérabilité corrigée : *V02, V03, V07, V09, V11*
- Ordre de priorité : *1/20 (URGENT - À faire aujourd'hui)*

Actions à réaliser :

1. Sur le contrôleur de domaine DC01, exécuter les commandes PowerShell suivantes :

powershell

- *# Comptes avec mots de passe faibles (V02)*
- Set-ADAccountPassword -Identity backup -Reset
- Set-ADAccountPassword -Identity svcweb -Reset
- Set-ADAccountPassword -Identity test -Reset
-
- *# Credentials dans description LDAP (V03)*
- Set-ADAccountPassword -Identity amaillot -Reset
-
- *# Credentials dans script PowerShell (V07)*
- Set-ADAccountPassword -Identity scolin -Reset
-
- *# Credentials dans LSA Secrets (V09)*
- Set-ADAccountPassword -Identity anoel -Reset
-
- # Credentials extraits via Kerberoasting
- Set-ADAccountPassword -Identity dmorin -Reset
  Set-ADAccountPassword -Identity web_svc -Reset
-

- *# 🆕 Credentials en mémoire via Mimikatz (V11) - DOMAIN ADMIN COMPROMIS*
- *Set-ADAccountPassword -Identity pclerc -Reset*
-
- *# Forcer le changement au prochain logon*
- Set-ADUser -Identity backup -ChangePasswordAtLogon $true
- Set-ADUser -Identity svcweb -ChangePasswordAtLogon $true
- Set-ADUser -Identity test -ChangePasswordAtLogon $true
- Set-ADUser -Identity amaillot -ChangePasswordAtLogon $true
- Set-ADUser -Identity scolin -ChangePasswordAtLogon $true
- Set-ADUser -Identity anoel -ChangePasswordAtLogon $true
- Set-ADUser -Identity dmorin -ChangePasswordAtLogon $true
- Set-ADUser -Identity web_svc -ChangePasswordAtLogon $true
- Set-ADUser -Identity pclerc -ChangePasswordAtLogon $true

⚠️ PRIORITÉ ABSOLUE : pclerc dispose de privilèges Domain Admin et a permis le dump complet de la base AD (NTDS.DIT) via DCSync. Sa réinitialisation est CRITIQUE.

2. Générer des mots de passe temporaires complexes (minimum 20 caractères aléatoires)
3. Notifier les utilisateurs concernés par email ou téléphone
4. Documenter les comptes réinitialisés et la date de réinitialisation
5. ⚠️ ATTENTION PARTICULIÈRE pour pclerc :

   - Notifier immédiatement le DSI - Vérifier tous les accès récents avec cet utilisateur - Auditer les Event ID 4662 (accès NTDS.DIT) et 4673 (tentatives DCSync) - Considérer une rotation complète du hash krbtgt (voir R06bis)

Ressources :

- https://learn.microsoft.com/fr-fr/powershell/module/activedirectory/set-adaccountpassword

Recommandation R02 : Supprimer le script admin.ps1 et auditer tous

les partages

Vulnérabilité corrigée : V07, V05

Ordre de priorité : 2/20 (URGENT - À faire aujourd'hui)

Actions à réaliser :

1. *Supprimer immédiatement le fichier compromis :*

```
powershell
  Remove-Item
"\\10.10.10.112\Configuration\Windows\Safety\Shell\Remote\Scripts\admin.ps1" -Force
```

2. *Vérifier la suppression :*

```
powershell
  Test-Path
"\\10.10.10.112\Configuration\Windows\Safety\Shell\Remote\Scripts\admin.ps1"
  # Doit retourner : False
```

3. *Scanner tous les partages réseau pour identifier d'autres scripts sensibles :*

```
powershell
  Get-ChildItem -Path "\\10.10.10.112\Configuration" -Recurse -Include
*.ps1,*.bat,*.vbs,*.cmd,*.xml,*.txt |
      Select-String -Pattern
"password|passwd|pwd|credential|secret|apikey" |
      Out-File C:\Audit\scripts_sensibles.txt
```

4. *Scanner également SYSVOL et NETLOGON :*

```
powershell
  Get-ChildItem -Path "\\10.10.10.101\SYSVOL" -Recurse -Include
*.ps1,*.bat,*.vbs,*.xml |
      Select-String -Pattern "password|passwd|pwd|cpassword" |
      Out-File C:\Audit\sysvol_audit.txt
```

5. *Supprimer ou chiffrer tous les fichiers contenant des credentials*
6. *Restreindre les permissions du partage Configuration aux seuls*

administrateurs

Ressources :

- *https://www.varonis.com/blog/powershell-file-search*

Recommandation R03 : Supprimer la description LDAP contenant le mot de passe

Vulnérabilité corrigée : V03

Ordre de priorité : 3/20 (URGENT - À faire aujourd'hui)

Actions à réaliser :

1. Supprimer la description problématique du compte amaillot :

powershell

```
Set-ADUser -Identity amaillot -Description "Compte support IT"
```

2. Auditer tous les comptes pour identifier d'autres descriptions sensibles :

powershell

```
Get-ADUser -Filter * -Properties Description |
    Where-Object {$_.Description -match
"password|passwd|mdp|pwd|mot de passe"} |
    Select SamAccountName, Description |
    Export-Csv C:\Audit\descriptions_sensibles.csv -NoTypeInformation
```

3. Établir une politique de description standardisée :
    - Format : "[Fonction] - [Service]"
    - Exemple : "Administrateur systèmes - Service IT"
    - **INTERDICTION FORMELLE** d'inclure des hints de mots de passe
4. Former les administrateurs IT à ne jamais inclure d'informations sensibles dans les attributs LDAP

Ressources :

- https://learn.microsoft.com/fr-fr/powershell/module/activedirectory/set-aduser

Recommandation R04 : Mettre en place une politique de mot de passe forte ET blocage de compte

Vulnérabilité corrigée : V02, V03, V07, V10

Ordre de priorité : 4/20 (URGENT - À faire cette semaine)

Actions à réaliser :

1. Configurer la politique de domaine sur DC01 :

```
powershell
 Set-ADDefaultDomainPasswordPolicy -Identity travers.ic `
    -MinPasswordLength 14 `
    -ComplexityEnabled $true `
    -PasswordHistoryCount 24 `
    -MaxPasswordAge "90.00:00:00" `
    -MinPasswordAge "1.00:00:00" `
    -LockoutThreshold 5 `
    -LockoutDuration "00:30:00" `
    -LockoutObservationWindow "00:30:00"
```

⚠️ **IMPORTANT - Protection contre le password spraying :**

- **`-LockoutThreshold 5`** : Blocage automatique du compte après 5 tentatives échouées
- **`-LockoutDuration "00:30:00"`** : Compte bloqué pendant 30 minutes
- **`-LockoutObservationWindow "00:30:00"`** : Fenêtre de surveillance de 30 minutes

Cette mesure bloque les attaques par password spraying comme celle qui a permis de compromettre les comptes backup, svcweb, test et scolin.

2. Vérifier que la politique est bien appliquée :

```
powershell
 Get-ADDefaultDomainPasswordPolicy
```

3. Créer une Fine-Grained Password Policy pour les administrateurs (politique encore plus stricte) :

```
powershell
 New-ADFineGrainedPasswordPolicy -Name "AdminPasswordPolicy" `
    -MinPasswordLength 16 `
```

```
    -ComplexityEnabled $true `
    -PasswordHistoryCount 24 `
    -MaxPasswordAge "60.00:00:00" `
    -MinPasswordAge "1.00:00:00" `
    -LockoutThreshold 3 `
    -LockoutDuration "01:00:00" `
    -Precedence 10

 Add-ADFineGrainedPasswordPolicySubject -Identity
"AdminPasswordPolicy" `
    -Subjects "Domain Admins","wksadmins","srvadmins"
```

Pour les administrateurs, politique encore plus stricte :

- **`-LockoutThreshold 3`** : Blocage après seulement 3 tentatives
- **`-LockoutDuration "01:00:00"`** : Blocage pendant 1 heure
- **`-MinPasswordLength 16`** : Mots de passe de 16 caractères minimum

4. Mettre en place une procédure de déblocage :
    - Identifier qui peut débloquer les comptes (HelpDesk, Domain Admins)
    - Documenter la procédure de déblocage :

```
powershell
 # Débloquer un compte
 Unlock-ADAccount -Identity username

 # Vérifier l'état du compte
 Get-ADUser -Identity username -Properties LockedOut | Select Name,
LockedOut
```

5. Communiquer la nouvelle politique aux utilisateurs via email
6. Prévoir un support renforcé pendant 48h pour aider les utilisateurs
7. Surveiller les blocages de comptes :

```
powershell
 # Script de monitoring des comptes bloqués
 Get-ADUser -Filter {LockedOut -eq $true} -Properties LockedOut,
LastBadPasswordAttempt |
    Select Name, SamAccountName, LockedOut,
LastBadPasswordAttempt |
    Export-Csv C:\Logs\comptes_bloques_$(Get-Date -Format
'yyyyMMdd').csv
```

Impact :

- ✅ Bloque efficacement les attaques par password spraying
- ✅ Force l'utilisation de mots de passe robustes
- ⚠️ Risque temporaire : augmentation des appels au HelpDesk

Ressources :

- https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-#fine_grained_pswd_policy_mgmt

Recommandation R05 : Supprimer les outils de pentest du contrôleur de domaine

Vulnérabilité corrigée : V04

Ordre de priorité : 5/20 (URGENT - À faire cette semaine)

Actions à réaliser :

1. Supprimer immédiatement le partage Tools ou restreindre l'accès :

```
powershell
  # Option 1 : Supprimer complètement le partage
   Remove-SmbShare -Name "Tools" -Force

   # Option 2 : Restreindre aux Domain Admins uniquement
   Grant-SmbShareAccess -Name "Tools" -AccountName
"TRAVERS\Domain Admins" -AccessRight Full
   Revoke-SmbShareAccess -Name "Tools" -AccountName "Everyone"
-Force
```

2. Supprimer tous les outils offensifs du serveur :

```
powershell
  Remove-Item "C:\Tools\Mimikatz" -Recurse -Force
   Remove-Item "C:\Tools\Rubeus.exe" -Force
   Remove-Item "C:\Tools\SharpHound.exe" -Force
   Remove-Item "C:\Tools\Snaffler.exe" -Force
```

3. Si ces outils sont nécessaires pour l'équipe IT, les stocker sur un serveur dédié (pas le DC !)

4. Établir une procédure stricte pour l'utilisation d'outils de sécurité :
    - Stockage sur machine dédiée et isolée
    - Accès limité aux administrateurs sécurité
    - Logging de tous les accès

Ressources :

- https://learn.microsoft.com/fr-fr/powershell/module/smbshare/

Recommandation R06 : Déployer Credential Guard et protéger les comptes à privilèges

Vulnérabilité corrigée : V11

Ordre de priorité : 6/20 (URGENT - À faire sous 7 jours)

Actions à réaliser :

1. Vérifier les prérequis matériels pour Credential Guard :

- TPM 2.0

- UEFI avec Secure Boot

- Virtualisation activée (VT-x/AMD-V)

powershell

 # Vérifier la compatibilité

Get-ComputerInfo | Select-Object -Property DeviceGuardSmartStatus

2. Activer Credential Guard via GPO :

- Computer Configuration > Policies > Administrative Templates > System > Device Guard

- Turn On Virtualization Based Security : Enabled

- Select Platform Security Level : Secure Boot and DMA Protection

- Credential Guard Configuration : Enabled with UEFI lock

3. Lier la GPO à toutes les OU contenant des serveurs et PAW

4. Ajouter les comptes Domain Admins au groupe "Protected Users" :

powershell

 # Ajouter tous les Domain Admins au groupe Protected Users

Add-ADGroupMember -Identity "Protected Users" -Members pclerc,rbertin,tnicolas

⚠️ Impact du groupe "Protected Users" :

• Empêche le stockage des credentials en mémoire en clair

• Force Kerberos uniquement (pas de NTLM, Digest, CredSSP)

• Pas de cache de credentials (DCC2)

• Durée de vie TGT limitée à 4 heures (pas 10 heures)

5. Configurer une GPO pour surveiller les sessions NewCredentials (Event ID 4648) :

- Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy

- Logon/Logoff > Audit Logon : Success, Failure

6. Créer un script de monitoring PowerShell pour détecter l'utilisation suspecte de RunAs :

```
powershell

# Script à exécuter quotidiennement

Get-WinEvent -FilterHashtable @{

    LogName='Security'

    ID=4648

    StartTime=(Get-Date).AddHours(-24)

} | Where-Object {

    $_.Properties[5].Value -match 'Domain
Admins|pclerc|rbertin|tnicolas'

} | Select TimeCreated,

    @{N='Account';E={$_.Properties[1].Value}},

    @{N='TargetAccount';E={$_.Properties[5].Value}},

    @{N='TargetServer';E={$_.Properties[8].Value}} |

Export-Csv "C:\Logs\NewCredentials_$(Get-Date -Format
'yyyyMMdd').csv"
```

7. Interdire les sessions interactives pour les Domain Admins sur les serveurs non-DC :

- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

- Deny log on locally : Ajouter "Domain Admins"

- Deny log on through Remote Desktop Services : Ajouter "Domain Admins"

⚠️ Exception : Autoriser uniquement sur DC01

Impact :

✅ Credential Guard empêche l'extraction de credentials en mémoire via Mimikatz

✅ Protected Users empêche le stockage en clair (sessions NewCredentials)

✅ Monitoring Event ID 4648 permet de détecter les usages suspects de RunAs

✅ Bloque la vulnérabilité V11 qui a permis la compromission Domain Admin

Ressources :

- **https://learn.microsoft.com/fr-fr/windows/security/identity-protection/credential-guard/credential-guard-manage**
- **https://learn.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/protected-users-security-group**

Recommandation R07 : Rotation du hash krbtgt et monitoring DCSync

Vulnérabilité corrigée : V11 (conséquence critique)

Ordre de priorité : 7/20 (URGENT - À faire sous 14 jours)

Contexte :

La compromission du compte pclerc (Domain Admin) a permis l'attaque DCSync pour dumper l'intégralité de la base Active Directory, incluant :

• Hash Administrator du domaine

• Hash krbtgt (permettant la création de Golden Tickets)

• Tous les hashes NTLM du domaine (78 utilisateurs + 3 machines)

Actions à réaliser :

1. Rotation du mot de passe krbtgt (PROCÉDURE CRITIQUE) :

⚠️ ATTENTION : La rotation du hash krbtgt doit être faite 2 FOIS à 10 heures d'intervalle minimum.

powershell

```
# Première rotation (T+0)

Set-ADAccountPassword -Identity krbtgt -Reset


# Attendre 10 heures minimum


# Deuxième rotation (T+10h)

Set-ADAccountPassword -Identity krbtgt -Reset
```

📋 **Pourquoi 2 fois ?**

Active Directory maintient l'historique des 2 derniers mots de passe krbtgt. Un Golden Ticket créé avec l'ancien hash reste valide jusqu'à ce que les deux rotations soient effectuées.

2. Planifier les rotations pour minimiser l'impact :

- Première rotation : Vendredi 18h00 (début de weekend)

- Deuxième rotation : Samedi 04h00 (10 heures après)

3. Activer le monitoring DCSync (Event ID 4662 et 4673) :

powershell

```
# Activer l'audit des accès à l'objet domaine
Get-ADObject -Identity "DC=travers,DC=ic" | Set-Acl -AuditRules @(
  New-Object System.DirectoryServices.ActiveDirectoryAuditRule(
    [System.Security.Principal.SecurityIdentifier]"S-1-1-0",
    [System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,
    [System.Security.AccessControl.AuditFlags]::Success,
    [Guid]"1131f6aa-9c07-11d1-f79f-00c04fc2dcd2"  # DS-Replication-Get-Changes
  )
)
```

4. Configurer des alertes SIEM pour les Event ID suivants :

- Event ID 4662 : Opération sur un objet AD (filtrer sur

DS-Replication-Get-Changes)

- Event ID 4673 : Service sensible appelé (filtrer sur DCSync)

- Event ID 5136 : Objet AD modifié (filtrer sur krbtgt)

5. Script de détection DCSync à exécuter quotidiennement :

```
powershell

# Détecter les tentatives DCSync dans les dernières 24h

Get-WinEvent -FilterHashtable @{

    LogName='Security'

    ID=4662

    StartTime=(Get-Date).AddHours(-24)

} | Where-Object {

    $_.Message -match 'DS-Replication-Get-Changes' -and

    $_.Properties[0].Value -notmatch 'DC01\$'  # Exclure le DC légitime

} | Select TimeCreated,

    @{N='Account';E={$_.Properties[1].Value}},

    @{N='Object';E={$_.Properties[6].Value}} |

Export-Csv "C:\Logs\DCSync_Detection_$(Get-Date -Format
'yyyyMMdd').csv"
```

6. Vérifier qu'aucun Golden Ticket n'est actif :

```
bash
```

 # Depuis la machine d'audit

impacket-GetUserSPNs travers.ic/backup:backup -dc-ip 10.10.10.101

 # Vérifier l'absence de tickets Kerberos anormaux

Impact :

✅ Rotation krbtgt invalide tous les Golden Tickets potentiels

✅ Monitoring DCSync détecte les futures tentatives d'extraction NTDS.DIT

✅ Empêche la persistance post-compromission

⚠️ Risques de la rotation krbtgt :

• Invalidation temporaire de certains tickets Kerberos légitimes

• Possible impact sur les services utilisant des SPNs

• Nécessite de planifier en dehors des heures ouvrées

Ressources :

• https://github.com/microsoft/New-KrbtgtKeys.ps1

• https://adsecurity.org/?p=483

• https://www.microsoft.com/en-us/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

Recommandation R08 : Déployer LAPS (Local Administrator Password Solution)

Vulnérabilité corrigée : V08

Ordre de priorité : 6/20 (IMPORTANT - À faire sous 30 jours)

Actions à réaliser :

1. Télécharger et installer LAPS sur DC01 :
    - Télécharger depuis : https://www.microsoft.com/en-us/download/details.aspx?id=46899
    - Installer LAPS.x64.msi sur le contrôleur de domaine
2. Étendre le schéma Active Directory :

powershell

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
```

3. Définir les permissions LAPS :

powershell

```
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Computers,DC=travers,DC=ic"
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Servers,DC=travers,DC=ic"
```

4. Créer et configurer une GPO LAPS :
    - Computer Configuration > Policies > Administrative Templates > LAPS
    - **Enable local admin password management** : Enabled
    - **Password Settings** :
        - Password Length : 20 caractères
        - Password Age (Days) : 30 jours
        - Password Complexity : Large letters + small letters + numbers + special
    - Lier la GPO à toutes les OU contenant des ordinateurs
5. Déployer le client LAPS via GPO sur toutes les machines
6. Tester sur 2-3 machines pilotes (DESKTOP01, FILER01)
7. Vérifier que les mots de passe sont bien gérés :

powershell

```
Get-AdmPwdPassword -ComputerName DESKTOP01
```

```
Get-AdmPwdPassword -ComputerName FILER01
```

8. Déploiement complet sur toutes les machines

Impact : Élimine complètement la vulnérabilité V08 (Pass-the-Hash avec le même hash local)

Ressources :

- https://www.microsoft.com/en-us/download/details.aspx?id=46899
- https://learn.microsoft.com/fr-fr/windows-server/identity/laps/laps-overview

---

Recommandation R09 : Activer SMB Signing obligatoire

Vulnérabilité corrigée : V01

Ordre de priorité : 7/20 (IMPORTANT - À faire sous 30 jours)

Actions à réaliser :

1. Créer une GPO pour forcer SMB Signing sur tous les serveurs et clients :
   - Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
2. Configurer les paramètres suivants :
   - **Microsoft network client: Digitally sign communications (always)** : Enabled
   - **Microsoft network server: Digitally sign communications (always)** : Enabled
3. Lier la GPO à toutes les OU contenant des ordinateurs
4. Forcer la mise à jour des GPO :

powershell

```
Invoke-Command -ComputerName DC01,FILER01,DESKTOP01
-ScriptBlock {gpupdate /force}
```

5. Vérifier l'application sur les machines :

bash

```
crackmapexec smb 10.10.10.0/24
```

```
# Vérifier que "signing:True" apparaît sur toutes les machines
```

6. Tester la connectivité des applications après activation

Impact : Élimine les attaques SMB Relay

Ressources :

- https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/networking/overview-server-message-block-signing

Recommandation R10 : Désactiver ou supprimer le compte de test

Vulnérabilité corrigée : V10

Ordre de priorité : 8/20 (IMPORTANT - À faire sous 30 jours)

Actions à réaliser :

1. Vérifier si le compte est encore utilisé :

powershell

```
Get-ADUser -Identity test -Properties LastLogonDate, whenCreated
```

2. Si le compte n'est plus utilisé, le désactiver (pour possibilité de rollback) :

powershell

```
Disable-ADAccount -Identity test
```

3. Après validation (48-72h), supprimer définitivement :

powershell

```
Remove-ADUser -Identity test -Confirm:$false
```

4. Établir une procédure de revue trimestrielle des comptes :

powershell

```
# Script à exécuter tous les trimestres
```

```
Get-ADUser -Filter * -Properties LastLogonDate |
    Where-Object {$_.LastLogonDate -lt (Get-Date).AddDays(-90)} |
    Select SamAccountName, LastLogonDate, Enabled |
    Export-Csv C:\Audit\comptes_inactifs.csv
```

5. Désactiver automatiquement les comptes inactifs > 90 jours (après validation manuelle)

Ressources :

- https://learn.microsoft.com/fr-fr/powershell/module/activedirectory/disable-adaccount

---

Recommandation R11 : Désactiver la connexion SMB anonyme

Vulnérabilité corrigée : V06

Ordre de priorité : 9/20 (MOYEN - À faire sous 60 jours)

Actions à réaliser :

1. Créer une GPO pour désactiver l'accès anonyme SMB :
   - Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
2. Configurer :
   - **Network access: Do not allow anonymous enumeration of SAM accounts** : Enabled
   - **Network access: Do not allow anonymous enumeration of SAM accounts and shares** : Enabled
   - **Network access: Let Everyone permissions apply to anonymous users** : Disabled
   - **Network access: Restrict anonymous access to Named Pipes and Shares** : Enabled
3. Lier la GPO au DC01
4. Forcer la mise à jour :

```
powershell
gpupdate /force
```

5. Vérifier avec enum4linux que l'énumération anonyme ne

fonctionne plus :

bash

```
enum4linux 10.10.10.101 -A
# Doit retourner "Access Denied"
```

Ressources :

- https://learn.microsoft.com/fr-fr/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts

Recommandation R12 : Restreindre l'accès au partage Configuration

Vulnérabilité corrigée : V05

Ordre de priorité : 10/20 (MOYEN - À faire sous 60 jours)

Actions à réaliser :

1. Auditer le contenu actuel du partage Configuration :

powershell

```
Get-ChildItem "\\10.10.10.112\Configuration" -Recurse |
    Select FullName, Length, LastWriteTime |
    Export-Csv C:\Audit\configuration_content.csv
```

2. Identifier les fichiers réellement nécessaires
3. Restreindre les permissions du partage aux seuls administrateurs :

powershell

```
# Sur FILER01
Revoke-SmbShareAccess -Name "Configuration" -AccountName "Everyone" -Force
Revoke-SmbShareAccess -Name "Configuration" -AccountName "Domain Users" -Force
```

```
Grant-SmbShareAccess -Name "Configuration" -AccountName "Domain Admins" -AccessRight Full
Grant-SmbShareAccess -Name "Configuration" -AccountName "srvadmins" -AccessRight Change
```

4. Configurer également les permissions NTFS :

powershell

```
$acl = Get-Acl "C:\Configuration"
$acl.SetAccessRuleProtection($true, $false)
$acl.Access | ForEach-Object { $acl.RemoveAccessRule($_) }

$rule1 = New-Object System.Security.AccessControl.FileSystemAccessRule("Domain Admins","FullControl","ContainerInherit,ObjectInherit","None","Allow")
$rule2 = New-Object System.Security.AccessControl.FileSystemAccessRule("srvadmins","Modify","ContainerInherit,ObjectInherit","None","Allow")
$acl.AddAccessRule($rule1)
$acl.AddAccessRule($rule2)
Set-Acl "C:\Configuration" $acl
```

5. Documenter le contenu légitime du partage

Ressources :

- https://learn.microsoft.com/fr-fr/powershell/module/smbshare/grant-smbshareaccess

À noter : Vos recommandations devront être hiérarchisées par ordre de priorité. Un lien vers une ou plusieurs ressources est un plus lors de la remontée des recommandations, mais ce n'est pas obligatoire.

Au moins 5 recommandations à court terme sont attendues.

II. Plan d'action à long terme

Proposez des recommandations génériques pour améliorer la sécurité de l'environnement sur le long terme. Suivez le même format que dans l'exemple fourni.

Recommandation R13 : Activer l'authentification multi-facteurs (MFA) pour tous les administrateurs

Vulnérabilité corrigée : Protection générale contre V02, V07, V09

Ordre de priorité : 11/20 (IMPORTANT - À faire sous 90 jours)

Actions à réaliser :

1. Choisir une solution MFA adaptée :
    - **Option 1** : Azure MFA (si Microsoft 365 / Azure AD)
    - **Option 2** : Duo Security (solution tierce populaire)
    - **Option 3** : Windows Hello for Business
2. Déploiement pilote sur 3-5 administrateurs pendant 2 semaines
3. Former tous les administrateurs à l'utilisation du MFA
4. Activer le MFA obligatoire pour tous les membres des groupes :
    - Domain Admins
    - wksadmins (Admins Workstations)
    - srvadmins (Admins Serveurs)
5. Configurer les politiques d'accès conditionnel :
    - MFA obligatoire pour tout accès RDP
    - MFA obligatoire pour tout accès WinRM
6. Générer et distribuer des codes de secours (backup codes)

Impact : Même si un mot de passe est compromis, l'attaquant ne peut pas se connecter sans le 2ème facteur

Ressources :

- https://learn.microsoft.com/fr-fr/azure/active-directory/authentication/concept-mfa-howitworks
- https://duo.com/docs/rdp

Recommandation R14 : Migrer les comptes de service vers des gMSA

Vulnérabilité corrigée : V02, V09

Ordre de priorité : 12/20 (IMPORTANT - À faire sous 120 jours)

Actions à réaliser :

1. Créer la KDS Root Key :

powershell
```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

2. Identifier tous les services utilisant actuellement svcweb ou d'autres comptes standards
3. Créer un gMSA pour chaque service :

powershell
```
New-ADServiceAccount -Name "gMSA-WebService" `
    -DNSHostName "filer01.travers.ic" `
    -PrincipalsAllowedToRetrieveManagedPassword "FILER01$"
```

4. Installer le gMSA sur la machine cible :

powershell
```
Install-ADServiceAccount -Identity "gMSA-WebService"
```
```

5. Reconfigurer les services pour utiliser le gMSA

6. Une fois validé, désactiver l'ancien compte svcweb

**Impact :** Rotation automatique tous les 30 jours, pas de mot de passe statique

**Ressources :**
- https://learn.microsoft.com/fr-fr/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

---

### **Recommandation R15** : Déployer des PAW (Privileged Access Workstations)**

**Ordre de priorité :** 13/20 (STRUCTUREL - À faire sous 180 jours)

**Actions à réaliser :**

1. Acquérir 5-10 postes dédiés pour l'administration

2. Installer Windows 10/11 Pro avec durcissement maximal :
```

- Credential Guard activé
- Device Guard activé
- AppLocker en mode whitelist strict
- Pas d'accès Internet
- Pas d'accès email

3. Créer des comptes administrateurs dédiés séparés des comptes standards :
- Format : adm-[username]

4. Configurer une GPO pour empêcher les connexions admin sur les postes non-PAW

5. Former les administrateurs à la séparation des tâches

Impact : Isole complètement les sessions administratives

Ressources :
-
https://learn.microsoft.com/fr-fr/security/privileged-access-workstations/privileged-access-devices

---

Recommandation R16 *: Désactiver NTLM et migrer vers Kerberos uniquement**

Ordre de priorité : 14/20 (STRUCTUREL - À faire sous 180 jours)

Actions à réaliser :

1. **Phase 1 - Audit (4 semaines)** :
- Activer l'audit NTLM
- Analyser les Event ID 8004 pendant 4 semaines
- Identifier toutes les applications utilisant NTLM

2. **Phase 2 - Remédiation (4 semaines)** :
- Reconfigurer les applications pour utiliser Kerberos
- Créer les SPNs nécessaires

3. **Phase 3 - Blocage progressif (4 semaines)** :
- Déployer le blocage NTLM par OU progressivement

4. **Phase 4 - Blocage complet**

Impact : Élimine les attaques Pass-the-Hash basées sur NTLM

Ressources :
-
https://learn.microsoft.com/fr-fr/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain

---

Recommandation R17 : Segmenter le réseau avec des VLANs**

Ordre de priorité : 15/20 (STRUCTUREL - À faire sous 240 jours)

Actions à réaliser :

1. Concevoir l'architecture réseau segmentée :
```
VLAN 10 : Serveurs (DC01, FILER01)       - 10.10.10.0/26
VLAN 20 : Workstations (DESKTOP01, etc.) - 10.10.20.0/24
VLAN 30 : Administration (PAW)           - 10.10.30.0/28
VLAN 40 : Imprimantes / IoT              - 10.10.40.0/24
```

2. Définir les règles de firewall inter-VLAN
3. Acquérir le matériel réseau nécessaire
4. Migrer progressivement

Impact : Limite drastiquement le mouvement latéral

Ressources :

- https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/10023-1.html

---

Recommandation R18 : Déployer un SIEM pour la détection des attaques

Ordre de priorité : 16/20 (GOUVERNANCE - À faire sous 240 jours)

Actions à réaliser :

1. Choisir une solution SIEM :
    - **Option 1** : Wazuh (Open Source - gratuit)
    - **Option 2** : Splunk (Commercial)
    - **Option 3** : Microsoft Sentinel
2. Déployer le SIEM
3. Installer les agents sur toutes les machines

4. Créer des règles de détection pour :
    - Password spraying (Event ID 4625 répétés)
    - Pass-the-Hash
    - Credential dumping
    - Modifications de groupes privilégiés
5. Configurer des alertes automatiques

Impact : Détection en temps réel des attaques

Ressources :

- https://wazuh.com/
- https://www.elastic.co/fr/elastic-stack

Recommandation R19 : Formation et sensibilisation des utilisateurs

Ordre de priorité : 17/20 (GOUVERNANCE - Programme continu)

Actions à réaliser :

1. **Programme de formation initiale** :
    - Session 1 : Bonnes pratiques mots de passe (1h)
    - Session 2 : Identification du phishing (1h)
    - Session 3 : Sécurité des données patients (2h)
2. **Campagnes de phishing simulées (Mensuel)**
3. **Communications régulières (Mensuel)** :
    - Newsletter sécurité
4. **Formation spécifique administrateurs (Annuel)**

Impact : Réduction du risque humain

Ressources :

- https://www.knowbe4.com/
- https://www.cybermalveillance.gouv.fr/

Recommandation R20 : Établir une gouvernance de la sécurité avec audits réguliers

Ordre de priorité : 18/20 (GOUVERNANCE - Programme continu)

Actions à réaliser :

1. **Audits semestriels (Tous les 6 mois)**

2. **Revue trimestrielle des comptes**
3. **Tests d'intrusion annuels**
4. **Comité de pilotage sécurité (Mensuel)**
5. **Veille sécurité continue**
6. ⚙️ **GESTION DES MISES À JOUR ET PATCHING : Politique de mise à jour :**
    - **Patches critiques** : 7 jours maximum
    - **Patches importants** : 30 jours
    - **Patches modérés** : 60 jours
7. **Procédure :**
    - Phase 1 - Postes de test (J+0 à J+3)
    - Phase 2 - Serveurs non-critiques (J+3 à J+5)
    - Phase 3 - Workstations (J+5 à J+7)
    - Phase 4 - Serveurs critiques (J+7)
8. **Configuration WSUS recommandée**
9. **Documentation à jour**
10. **Indicateurs de suivi (KPI)** :
    - Nombre de comptes à mot de passe faible
    - Taux de couverture du MFA (objectif 100% admins)
    - Taux de déploiement LAPS (objectif 100%)
    - 🆕 **Taux de conformité des patches (objectif > 95%)**
    - 🆕 **Délai moyen d'application des patches critiques (objectif < 7 jours)**

Impact : Maintien d'un niveau de sécurité élevé dans le temps

Ressources :

- https://www.cert.ssi.gouv.fr/
- https://www.cert-sante.fr/
- https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- 🆕 **https://msrc.microsoft.com/update-guide/**

SYNTHÈSE DU PLAN D'ACTION

Priorisation par délai :

🔴 URGENT (À faire AUJOURD'HUI - J+0) :

- R01 : Réinitialiser les mots de passe compromis (9 comptes dont pclerc - Domain Admin)
- R02 : Supprimer le script admin.ps1
- R03 : Supprimer la description LDAP d'amaillot

🟠 TRÈS IMPORTANT (À faire CETTE SEMAINE - J+7) :

- R04 : Politique de mot de passe forte + blocage
- R05 : Supprimer les outils de pentest du DC
- R06 : Déployer Credential Guard + Protected Users (V11 - CRITIQUE)
- R07 : Rotation krbtgt + Monitoring DCSync (J+14 max)

🟡 MOYEN TERME (À faire sous 30-60 jours) :

- R08 : Déployer LAPS (J+30)
- R09 : Activer SMB Signing (J+30)
- R10 : Supprimer le compte de test (J+30)
- R11 : Désactiver SMB anonyme (J+60)
- R12 : Restreindre accès partage Configuration (J+60)

🟢 LONG TERME (À faire sous 90-240 jours) :

- R13 : MFA pour administrateurs (J+90)
- R14 : Migration vers gMSA (J+120)
- R15 : Déployer des PAW (J+180)
- R16 : Désactiver NTLM (J+180)
- R17 : Segmentation réseau (J+240)
- R18 : SIEM (J+240)
- R19 : Formation continue (Programme continu)
- R20 : Gouvernance et audits (Programme continu)

📊 STATISTIQUES DU PLAN D'ACTION :

Total de recommandations : 20

Vulnérabilités couvertes : 11/11 (100%)

Comptes compromis à réinitialiser : 9

Répartition par criticité :

- 🔴 URGENT (J+0) : 3 recommandations
- 🟠 TRÈS IMPORTANT (J+7-J+14) : 4 recommandations
- 🟡 MOYEN TERME (J+30-J+60) : 5 recommandations
- 🟢 LONG TERME (J+90-J+240) : 8 recommandations

⚠️ PRIORITÉ ABSOLUE :

La compromission du compte pclerc (Domain Admin via Mimikatz) a permis le dump complet de la base Active Directory (78 utilisateurs + krbtgt + Administrator). Les recommandations R01, R06bis et R06ter doivent être implémentées en urgence absolue pour sécuriser le domaine.