CHECKLIST AUDIT TERRAIN — CIS + COMMANDES

🔴 1. AUTHENTIFICATION & COMPTES

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 1.1.5	Password ≥ 14	net accounts	Minimum password length ≥ 14
CIS 1.1.1	Historique ≥ 24	net accounts	Password history length ≥ 24
CIS 1.2.1	Lockout ≤ 5	net accounts	Lockout threshold ≤ 5
CIS 1.2.2	Lockout ≥ 15 min	net accounts	Lockout duration ≥ 15
CIS 2.3.1.2	Guest OFF	net user guest	Account active = No
CIS 2.3.1.1	Admin renommé	net user	Pas de compte “Administrator”

🔴 2. PRIVILÈGES & ADMIN LOCAL

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 2.2.1	Accès réseau restreint	secpol.msc → User Rights	Liste limitée
CIS 2.2.4	Logon local limité	secpol.msc→ User Rights	Pas de “Everyone”
CIS 2.2.6	Guest refus réseau	secpol.msc→ User Rights	Guest dans “Deny”
CIS 18.9.85.1	UAC ON	reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA	= 1

Commandes terrain :

whoami /groups

net localgroup administrators

✔ Vérifier :

- Qui est admin local
- Présence de comptes anormaux

🔴 3. SERVICES & SURFACE D'ATTAQUE

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 18.3.2	SMBv1 OFF	Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol	Disabled
CIS 18.3.1	LLMNR OFF	gpedit.msc -> MA -> Reseau -> client DNS	Disabled
CIS 5.x	Services inutiles OFF	sc query / services.msc	Disabled

Commandes utiles :

Get-Service | Where-Object {$_.Status -eq "Running"}

✔ Vérifier :

- Telnet
- RemoteRegistry
- FTP

🔴 4. FIREWALL & RÉSEAU

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 9.x	Firewall ON	netsh advfirewall show allprofiles	ON
CIS 9.1.2	Inbound bloqué	même commande	Block inbound

🔴 5. RDP & ACCÈS DISTANT

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 18.9.84.2	RDP restreint	SystemPropertiesRemote.exe	Limité
CIS 18.9.84.3	Secure RPC	gpedit.msc -> MA-> System -> Appel procedure distante	Enabled

Tests terrain :

netstat -an | find "3389"

Scan externe/interne :

nmap -p 3389 <IP>

🟠 6. ANTIVIRUS / DEFENDER

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 18.9.45.4	Real-time ON	Get-MpComputerStatus	True
CIS 18.9.45.5	Cloud ON	même commande	True

🟠 7. POWERSHELL & EXÉCUTION

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 18.9.70.2	Script logging	reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell	Enabled
CIS 18.9.70.3	Transcription	Même clé registry	Enabled

🟡 8. USB / SUPPORT AMOVIBLE

Réf CIS	Check	Commande / Procédure	Résultat attendu
CIS 18.9.47.1	USB restreint	gpedit.msc -> Administrative Templates > System > Removable Storage Acces	Restricted

COLLECTER LES APPS INSTALLEES

```
# Création dossier si nécessaire
$outputDir = "C:\AUDIT"
New-Item -ItemType Directory -Path $outputDir -Force | Out-Null

# Fichier horodaté
$date = Get-Date -Format "yyyyMMdd_HHmmss"
$outputFile = "$outputDir\audit_local_$date.txt"

# Comptes par défaut à exclure
$defaultAccounts = @(
    "Administrator",
    "DefaultAccount",
    "Guest",
    "WDAGUtilityAccount"
)

# Fonction helper pour ajouter une section
function Add-Section {
    param (
        [string]$Title,
        [string[]]$Content
    )

@"
================================================
$Title
================================================
```

```
$($Content -join "`n")

"@ | Out-File -Append $outputFile
}

# ========================
# SECTION 1 - Commandes globales
# ========================

Add-Section "NET ACCOUNTS" (net accounts)
Add-Section "NET USER (tous)" (net user)
Add-Section "NET USER INVITÉ" (net user invité 2>&1)
Add-Section "LOCALGROUP ADMINISTRATEURS" (net localgroup administrateurs 2>&1)
Add-Section "SMB1 STATUS" (Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol | Out-String)
Add-Section "FIREWALL PROFILES" (netsh advfirewall show allprofiles)
Add-Section "DEFENDER STATUS" (Get-MpComputerStatus | Out-String)

# ========================
# SECTION 2 - Utilisateurs locaux détaillés
# ========================

$localUsers = Get-LocalUser

foreach ($user in $localUsers) {
    if ($defaultAccounts -notcontains $user.Name) {

        Add-Section "DETAIL UTILISATEUR : $($user.Name)" (net user $user.Name)
    }
}

Write-Host "Audit terminé : $outputFile" -ForegroundColor Green
```

secpol.msc

gpedit.msc

SystemPropertiesRemote.exe

services

panneau de configuration

```
<#
.SYNOPSIS
Vérifie la présence ou absence de Microsoft LAPS (Local Administrator Password Solution)
Scope : Local + GPO (pas Azure / Intune)

.OUTPUTS
- Fichier texte exporté : registre LAPS
- Vérification logs LAPS
- Vérification paramètres GPO LAPS

.AUTOR
Audit / Pentest
#>

# --- Paramètres ---
$OutputDir = "C:\Temp\Audit_LAPS"
```

```
if (-not (Test-Path $OutputDir)) { New-Item -Path $OutputDir -ItemType Directory }

$MachineName = $env:COMPUTERNAME
$ReportFile = "$OutputDir\LAPS_Check_$MachineName.txt"

# --- 1. Vérification du registre ---
$RegPath = "HKLM\Software\Microsoft\Policies\LAPS"
$RegCheck = Test-Path $RegPath

Add-Content $ReportFile "=== Vérification du registre LAPS ==="
Add-Content $ReportFile "Chemin : $RegPath"
if ($RegCheck) {
    Add-Content $ReportFile "Résultat : clés LAPS trouvées"
    $RegValues = Get-ItemProperty -Path $RegPath
    $RegValues | Format-List | Out-String | Add-Content $ReportFile
} else {
    Add-Content $ReportFile "Résultat : clés LAPS ABSENTES"
}

# --- 2. Vérification des logs LAPS ---
Add-Content $ReportFile "`n=== Vérification des logs LAPS ==="
try {
    $LAPSLogs = Get-WinEvent -LogName "Microsoft-Windows-LAPS/Operational"
-ErrorAction Stop
    if ($LAPSLogs) {
        Add-Content $ReportFile "Logs LAPS TROUVES :"
        $LAPSLogs | Select-Object -First 5 | Format-Table | Out-String | Add-Content
$ReportFile
    } else {
        Add-Content $ReportFile "Aucun log LAPS détecté"
    }
} catch {
```

```
    Add-Content $ReportFile "Aucun log LAPS détecté (log non existant)"
}

# --- 3. Vérification GPO Administrative Templates ---
Add-Content $ReportFile "`n=== Vérification GPO Administrative Templates ==="
$GPOPath = "Computer Configuration\Policies\Administrative Templates\LAPS"
try {
    $GPOCheck = Get-GPRegistryValue -Name "LAPS" -Key $RegPath -ErrorAction Stop
    if ($GPOCheck) {
        Add-Content $ReportFile "GPO LAPS détectée :"
        $GPOCheck | Format-List | Out-String | Add-Content $ReportFile
    } else {
        Add-Content $ReportFile "Aucune GPO LAPS détectée"
    }
} catch {
    Add-Content $ReportFile "Aucune GPO LAPS détectée ou module RSAT non installé"
}

# --- 4. Résumé final ---
Add-Content $ReportFile "`n=== RÉSUMÉ ==="
if (-not $RegCheck -and (!$LAPSLogs) -and ($GPOCheck -eq $null)) {
    Add-Content $ReportFile "Conclusion : LAPS ABSENT sur cette machine"
} else {
    Add-Content $ReportFile "Conclusion : LAPS POTENTIELLEMENT actif ou configuré (vérifier détails)"
}

Add-Content $ReportFile "`nRapport complet exporté dans : $ReportFile"
Write-Output "Audit LAPS terminé. Rapport disponible : $ReportFile"
```