RAPPORT AUDIT SECURITE ANSSI COMPLET

Audit Windows conforme aux recommandations ANSSI, CIS et Microsoft Security Baseline

Genere: 06/01/2026 23:06:29 | Machine: === INFORMATIONS SYSTEME ===

SCORE DE SECURITE GLOBAL

42%

75 / 179 points

Niveau: FAIBLE

0	11	6
Findings CRITIQUES	Findings MAJEURS	Findings MINEURS

17

Total Findings

Findings Securite et Remediations ANSSI

[Authentification] LSASS Protection desactivee

MAJEUR CVSS 8.5

Description: RunAsPPL non active. Risque d'extraction de credentials via mimikatz.

Remediation:

```
reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Lsa' /v RunAsPPL /t REG_DWORD /d 1 /f
REDEMARRAGE REQUIS
```

[Securite] Ports sensibles exposes

MAJEUR CVSS 8.5

Description: SMB, WinRM exposes. Risque de pivots lateraux et attaques.

Remediation:

```
New-NetFirewallRule -DisplayName 'Block Dangerous Ports' -Direction Inbound -Protocol TCP -
LocalPort 139,445,5985,5986 -Action Block -Profile Public
```

[Securite] BitLocker non active

MAJEUR CVSS 8

Description: Disque non chiffre. Donnees sensibles accessibles sans protection.

Remediation:

```
Enable-BitLocker -MountPoint C: -EncryptionMethod Aes256 -UsedSpaceOnly
```

[Securite] Secure Boot desactive ou non supporte

MAJEUR CVSS 7.5

Description: Risque de rootkit au demarrage sans Secure Boot.

Remediation:

```
# ACTION MANUELLE: Redemarrer sur UEFI/BIOS et activer Secure Boot
```

[Comptes] LAPS non configure

MAJEUR CVSS 7.5

Description: Local Admin Password Solution absent. Mots de passe admin non geres.

Remediation:

```
# Installer LAPS depuis Microsoft
# Configurer via GPO ou registre
Set-ItemProperty 'HKLM:\Software\Policies\Microsoft Services\AdmPwd' -Name AdmPwdEnabled -
Value 1
```

[Authentification] WDigest stocke les mots de passe en clair

MAJEUR CVSS 7

Description: WDigest peut extraire les mots de passe en memoire.

Remediation:

```
Set-ItemProperty 'HKLM:\System\CurrentControlSet\Control\SecurityProviders\WDigest' -Name
UseLogonCredential -Value 0
```

[Reseau] USB Autorun actif

MAJEUR CVSS 6.5

Description: Risque d'infection par cles USB compromises.

Remediation:

```
Set-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer' -Name
NoDriveTypeAutoRun -Value 255
```

[Reseau] Signature SMB non requise

MAJEUR CVSS 6.5

Description: Communications SMB non signees. Risque d'interception et modification.

Remediation:

```
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
```

[Comptes] RestrictAnonymous non configure

MAJEUR CVSS 6.5

Description: Acces anonyme trop permissif au registre et partages.

Remediation:

```
Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name RestrictAnonymous -
Value 1
```

[Reseau] LLMNR actif (spoofing DNS possible)

MAJEUR CVSS 6

Description: LLMNR non desactif. Risque de spoofing et MITM.

Remediation:

```
Set-ItemProperty 'HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient' -Name
EnableMulticast -Value 0
```

[Comptes] UAC ConsentPromptBehaviorAdmin faible

MAJEUR CVSS 6

Description: Niveau de notification UAC insuffisant pour les administrateurs.

Remediation:

```
Set-ItemProperty 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System' -Name
ConsentPromptBehaviorAdmin -Value 1
```

[Authentification] **Credential Guard non active** MINEUR CVSS 4.5

Description: Protection avancee des credentials non activee.

Remediation:

```
# Hypervisor-Protected Code Integrity requis
Reg add
'HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrit
y' /v Enabled /t REG_DWORD /d 1 /f
```

[Reseau] **RDP Restricted Admin desactive** MINEUR CVSS 4

Description: Mode Restricted Admin non active. Risque de Pass-The-Hash via RDP.

Remediation:

```
Set-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name DisableRestrictedAdmin
-Value 0
```

[Journalisation] **Sysmon non installe** MINEUR CVSS 3.5

Description: Journalisation avancee absente. Visibilite limitee.

Remediation:

```
# Telecharger Sysmon depuis Microsoft
Sysmon64.exe -i -n -l
```

[Reseau] **NetBIOS Name Release trop permissif** MINEUR CVSS 3

Description: Risque de spoofing NetBIOS.

Remediation:

```
Set-ItemProperty 'HKLM:\System\CurrentControlSet\Services\Netbt\Parameters' -Name
NoNameReleaseOnDemand -Value 1
```

[Reseau] **IPv6 actif (si non utilise)** MINEUR CVSS 2.5

Description: IPv6 peut creer des vecteurs d'attaque inutiles si non utilise.

Remediation:

```
Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters' -Name
DisabledComponents -Value 0xFF
```

[Authentification] **Windows Hello/Passport non configure** MINEUR

CVSS 2

Description: Authentification biometrique ou PIN non active.

Remediation:

```
# Windows Hello requiert une TPM 2.0 ou capteur biometrique
```

Systeme

Informations OS

```
=== INFORMATIONS SYSTEME ===
Nom: Microsoft Windows Server 2019 Standard
Version: 10.0.17763
Build: 17763
Architecture: 64-bit
Installation: 03/01/2025 10:09:33
Dernier boot: 01/06/2026 22:40:56
```

Uptime Systeme

```
Uptime: 0 jours, 0 heures
```

BitLocker Status

```
=== BITLOCKER STATUS ===
```

Derniers Hotfixes

HotFixID	Description	InstalledOn
KB5004335	Update	05/08/2021 00:00:00
KB5005112	Security Update	05/08/2021 00:00:00
KB5005030	Security Update	05/08/2021 00:00:00

Comptes et Identites

Comptes Privilegies

```
=== VERIFICATION COMPTES PRIVILEGIES ===
Administrateur actif: True
Guest actif: False
```

Utilisateurs Locaux

Name	Enabled	PasswordRequired	PasswordExpires	PasswordLastSet	LastLogon
Administrator	True	True		01/03/2025 10:09:31	06/01/2026 23:01:36
DefaultAccount	False	False			
Guest	False	False			
michel	True	True	12/04/2025 13:17:44	01/03/2025 12:17:44	
sshd	True	True		06/01/2026 22:35:36	
WDAGUtilityAccount	False	True	12/04/2025 11:03:07	01/03/2025 10:03:07	

Groupe Administrateurs

Name	ObjectClass
WIN-RNGUKIGIR06\Administrator	User
WIN-RNGUKIGIR06\michel	User

Configuration UAC

```
=== UAC CONFIGURATION ===
EnableLUA: 1
ConsentPromptBehaviorAdmin: 5
PromptOnSecureDesktop: 1
FilterAdministratorToken:
```

Politique de Mots de Passe

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.
```

Authentification

Configuration NTLM

```
=== NTLM CONFIGURATION ===
LMCompatibilityLevel:
NoLMHash: 1
```

Securite Base SAM

```
=== SECURITE BASE SAM ===
NoLMHash: 1
RestrictAnonymous: 0
EveryoneIncludesAnonymous: 0
ForceGuest: 0
```

Parametres LSA Avances

```
=== PARAMETRES LSA AVANCES ===
RunAsPPL:
DisableRestrictedAdmin:
NullSessionPipes:
```

WDigest Credentials

```
WDigest UseLogonCredential:
```

LAPS Configuration

```
LAPS: Non configure
```

Credential Guard

```
Credential Guard: 0
```

Authentification Biometrique

```
=== AUTHENTIFICATION BIOMETRIQUE ===
PassportForWork Enabled:
UsePassportForWork:
```

Reseau et Services

Profils Firewall

Name	Enabled	DefaultInboundAction
Domain	True	NotConfigured
Private	True	NotConfigured
Public	True	NotConfigured

Configuration SMB

```
=== SMB CONFIGURATION ===
EnableSMB1Protocol: False
EncryptData: False
RequireSecuritySignature: False
EnableSecuritySignature: False
```

Protocoles Multicast

```
=== PROTOCOLES MULTICAST ===
LLMNR Enabled:
NetBIOS NoNameReleaseOnDemand:
```

Statut IPv6

```
IPv6 DisabledComponents:
```

Configuration RDP

```
=== RDP CONFIGURATION ===
fDenyTSConnections: 1
SecurityLayer: 2
UserAuthentication: 1
MinEncryptionLevel: 2
```

RDP Restricted Admin

```
RDP DisableRestrictedAdmin:
```

Statut WinRM

```
WinRM: Running - Automatic
```

Autorun USB

```
USB AutoRun NoDriveTypeAutoRun:
```

Ports en Ecoute

LocalAddress	LocalPort	OwningProcess
::	49675	660
::	49669	652
::	49668	2552
::	49666	1620
::	49665	1164
::	49664	508
::	47001	4
::	5985	4
::	5357	4
::	445	4
::	135	928
::	22	2632
0.0.0.0	49675	660

0.0.0.0	49669	652
0.0.0.0	49668	2552
0.0.0.0	49666	1620
0.0.0.0	49665	1164
0.0.0.0	49664	508
10.0.2.15	139	4
0.0.0.0	135	928
0.0.0.0	22	2632

Securite OS

LSASS Protection

```
=== LSASS PROTECTION ===
RunAsPPL:
```

Windows Defender

```
=== WINDOWS DEFENDER ===
DisableRealtimeMonitoring: False
DisableBehaviorMonitoring: False
DisableIOAVProtection: False
```

Secure Boot

```
Secure Boot:
```

Journalisation et Audit

Audit Policy

```
System audit policy

Category/Subcategory                    Setting
```

```
System
  Security System Extension               No Auditing

  System Integrity                        Success and Failure

  IPsec Driver                            No Auditing

  Other System Events                     Success and Failure

  Security State Change                   Success

Logon/Logoff
  Logon                                   Success and Failure

  Logoff                                  Success

  Account Lockout                         Success

  IPsec Main Mode                         No Auditing

  IPsec Quick Mode                        No Auditing

  IPsec Extended Mode                     No Auditing

  Special Logon                           Success

  Other Logon/Logoff Events               No Auditing

  Network Policy Server                   Success and Failure

  User / Device Claims                    No Auditing

  Group Membership                        No Auditing

Object Access
  File System                             No Auditing

  Registry                                No Auditing

  Kernel Object                           No Auditing

  SAM                                     No Auditing

  Certification Services                  No Auditing

  Application Generated                   No Auditing

  Handle Manipulation                     No Auditing

  File Share                              No Auditing

  Filtering Platform Packet Drop          No Auditing

  Filtering Platform Connection           No Auditing

  Other Object Access Events              No Auditing

  Detailed File Share                     No Auditing

  Removable Storage                       No Auditing

  Central Policy Staging                  No Auditing

Privilege Use
  Non Sensitive Privilege Use             No Auditing

  Other Privilege Use Events              No Auditing

  Sensitive Privilege Use                 No Auditing
```

```
Detailed Tracking
  Process Creation                          No Auditing

  Process Termination                       No Auditing

  DPAPI Activity                            No Auditing

  RPC Events                                No Auditing

  Plug and Play Events                      No Auditing

  Token Right Adjusted Events               No Auditing

Policy Change
  Audit Policy Change                       Success

  Authentication Policy Change              Success

  Authorization Policy Change               No Auditing

  MPSSVC Rule-Level Policy Change           No Auditing

  Filtering Platform Policy Change          No Auditing

  Other Policy Change Events                No Auditing

Account Management
  Computer Account Management               Success

  Security Group Management                 Success

  Distribution Group Management             No Auditing

  Application Group Management              No Auditing

  Other Account Management Events           No Auditing

  User Account Management                   Success

DS Access
  Directory Service Access                  Success

  Directory Service Changes                 No Auditing

  Directory Service Replication             No Auditing

  Detailed Directory Service Replication    No Auditing

Account Logon
  Kerberos Service Ticket Operations        Success

  Other Account Logon Events                No Auditing

  Kerberos Authentication Service           Success

  Credential Validation                     Success
```

Configuration WSUS

```
=== CONFIGURATION WSUS ===
WUServer:
UseWUServer:
```

Sysmon

```
Sysmon: Non installe
```