GUIDE UTILISATEUR

PM AuditSécurité

Installer le logiciel, lancer un audit distant ou local autorisé, produire un PDF de restitution et comprendre les limites (exposition ≠ faille).

1. À quoi sert ce logiciel ?

PM AuditSécurité est un outil d'audit de sécurité défensif pour Windows. Il mesure l'exposition d'une cible autorisée (site / IP) et peut auditer ce PC (durcissement, LAN optionnel, modules avancés).

- Mode Simple / Expert : même moteur, présentation différente.
- Contrôles non destructifs : pas d'exploitation, brute force, furtivité ni DoS.
- Rapports PDF (charte PM Software) + JSON générés localement, sans télémétrie imposée.
- Un port ouvert = exposition. Une CVE par bannière = potentielle jusqu'à preuve.

N'utilisez le logiciel que sur des systèmes dont vous êtes propriétaire ou pour lesquels vous disposez d'une autorisation écrite.

2. Installation (Windows)

1. Décompressez le ZIP (standalone) ou placez PMAuditSecurite.exe dans un dossier dédié.
2. Conservez le fichier « Aide_PM_AuditSecurite.pdf » dans le même dossier que l'exécutable.
3. Double-cliquez sur PMAuditSecurite.exe.
4. Ouvrez Aide (F1) ou Paramètres → À propos pour relire ce guide.

Mode développeur : Tester_avec_Python.bat (Python 3.12+ / .venv). La compilation Nuitka se fait via Compiler_le_logiciel.bat / scripts de build.

3. Premiers pas — audit distant

1. Paramètres : renseignez l'engagement (client, référence, auditeur).
2. Nouvel audit : saisissez un FQDN ou une IPv4 explicitement autorisée.
3. Choisissez le profil Professionnel pour une restitution commerciale.

4. Lancez l'audit, puis exportez PDF Synthèse (décideur) et/ou Expert (IT).
5. Archivez aussi l'export JSON dans le dossier affaire.

4. Premiers pas — audit de ce PC

1. Obtenez l'accord utilisateur / RSSI.
2. Dans Paramètres, laissez activée la conformité MS / ANSSI / alignement CIS (gratuit, hors ligne).
3. Activez uniquement les autres modules nécessaires (LAN, WinRM, AD...).
4. Lancez Audit de ce PC et lisez la confirmation de périmètre.
5. Exportez un PDF Détaillé ou Expert ; discutez le plan 30 / 60 / 90 jours.

La conformité affichée est une estimation technique multi-référentiels. Ce n'est pas une certification CIS officielle.

5. Lire l'écran principal

Tableau de bord	Vue d'ensemble et raccourcis
Nouvel audit	Cible, profil, progression, constats
Historique	Audits sauvegardés, comparaison, PDF différentiel
Rapports	PDF Synthèse / Détaillé / Expert + JSON
Paramètres	Engagement, CVE, LAN, modules, aide
Simple / Expert	Ne relance pas l'audit — change l'affichage

6. Paramètres utiles

- Engagement : repris sur les PDF/JSON.
- Référentiels : MS Baselines + ANSSI + alignement CIS non officiel (catalogue local gratuit).
- CVE NVD : optionnelle (opt-in) ; catalogue local hors ligne toujours disponible.
- LAN : découverte bornée (/24), backend Auto ou Natif recommandé depuis l'EXE.
- WinRM / AD / SNMP / Wi-Fi / Cloud : modules optionnels, lecture seule.
- Actualiser les capacités réseau ; Page Npcap = site officiel uniquement.

7. Rapports PDF et JSON

Les PDF d'audit utilisent la même charte que l'aide (bandeau orange, pied gris, titres rouges, table Destinataire / Auditeur / Cible). Classification : document d'audit défensif.

Synthèse	Direction — score, matrice, priorités, plan 30/60/90
Détaillé	IT / RSSI — constats par domaine + ports
Expert	Admin — preuves et notes d'exécution
JSON	Archive technique du dossier
Différentiel	Depuis Historique (nouveaux / disparus / modifiés)

Le thème sombre de l'application n'altère pas les PDF d'audit (fond blanc imprimable).

8. Découverte LAN, Scapy et EXE

Depuis l'exécutable compilé, Scapy n'est pas embarqué (licence). Utilisez le backend Auto ou Natif Windows (SendARP).

- EXE : SendARP + cache ARP (+ TCP si besoin) — mode supporté.
- Scapy : uniquement en mode développeur (extra requirements-advanced.txt).
- Npcap : installation séparée sur npcap.com — jamais redistribué par l'app.
- Sans Scapy/Npcap : le logiciel reste pleinement utilisable.

9. Score et vocabulaire

Exposition	Surface observée (port, service) — pas forcément une faille
CVE potentielle	Corrélation version/bannière non confirmée
Score	Indicateur 0–100, pas une certification
Sévérités	Info / Faible / Moyen / Élevé / Critique

10. Problèmes fréquents

Cible non résolue	DNS, VPN, orthographe, périmètre
Peu de ports ouverts	Pare-feu / hébergeur ; essayer profil Professionnel
Manuel introuvable	Placer Aide_PM_AuditSecurite.pdf à côté de PMAuditSecurite.exe
Scapy absent (EXE)	Normal — utiliser backend Auto/Natif
Npcap non détecté	Installer depuis npcap.com puis Actualiser
Antivirus bloque l'EXE	Faux positif possible ; signature si disponible
NVD lent	Désactiver NVD ; catalogue local suffit

11. Mentions

Produit	PM AuditSécurité V2.0a
Auteur	Pascal Mouneyrat
Éditeur	PM Software — (c) PM Software
Fichier d'aide	Aide_PM_AuditSecurite.pdf — V2.0a
Tagline	Logiciels indépendants & outils spécialisés

Interdits produit : exploitation, brute force, furtivité, DoS, scan Internet massif, dumping NTDS, attaques Wi-Fi.

Annexe A (pages suivantes) : audit technique complet des capacités (équivalent à Audit_Technique_Capacites_PM_AuditSecurite.pdf), intégré dans ce même fichier.

ANNEXE A

Audit technique des capacités

Contenu intégré (équivalent au fichier Audit_Technique_Capacites_PM_AuditSecurite.pdf). Inventaire factuel dérivé du code — produit 100 % gratuit.

Cette annexe fait partie du guide utilisateur : un seul fichier PDF pour l'aide (F1) et la référence technique.

AUDIT TECHNIQUE — CAPACITÉS (COMPLET)

PM AuditSécurité V2.0a

Inventaire factuel des capacités réellement implémentées dans le code, y compris conformité multi-référentiels MS / ANSSI / alignement CIS. Aucune fonctionnalité inventée. Document régénéré depuis le dépôt source.

Éditeur : PM Software — Auteur : Pascal Mouneyrat — Date : 2026-08-27 — EXE : PMAuditSecurite.exe — (c) PM Software — Logiciel 100 % gratuit, hors ligne pour le cœur.

Périmètre : usage défensif uniquement, systèmes possédés ou explicitement autorisés. Observation et mesure — pas d'exploitation.

1. Identité produit et stack

Élément	Valeur constatée	Source
Nom affiché	PM AuditSécurité	`app/branding.py`
Version produit	2.0a	`app/__init__.py`
Version fichier Windows	2.0.0.1	`WINDOWS_FILE_VERSION`
Éditeur	PM Software	Produit gratuit
Organisation Qt	PMSoftware / PMAuditSecurite	QSettings
Runtime	Windows 10/11 x64, Python ≥ 3.12, PySide6	README
Packaging	Nuitka standalone / onefile	`main.py`
Données embarquées	CVE catalog + baselines JSON (`app.data`)	`--include-package-data=app.data`

2. Architecture d'exécution

UI PySide6 → `AuditWorker` → `AuditEngine` (`scanner.py`) → `AuditPlan` / `AuditCheck` → Findings → Risk → PDF / JSON / Historique.

Un seul moteur pour Mode Simple et Mode Expert. `AuditOrchestrator` = socle événements V2 ; l'exécution métier passe par `AuditEngine`.

3. Modes d'utilisation

Aspect	Simple	Expert
Détail finding	Titre + explication	+ preuve technique
Filtres	Masqués	Sévérité / catégorie (libellés FR)
Profils TCP	Rapide / Standard / Professionnel	+ TCP 1–1024
PDF défaut	Synthèse	Expert
Conformité baselines	Bandeau % MS / ANSSI / CIS-aligné	+ constats `BL-WKS-*` filtrables

Profil `full-tcp` (1–65535) : présent dans le code, **non exposé** dans le combo UI.

	Audit distant	Audit local
Cible	FQDN / IP	Cet ordinateur
Plan	`AuditPlan.remote`	`AuditPlan.local`
Options	Campagne WAN ≤ 25	Baselines (défaut ON), LAN, WinRM, AD, netdev, Wi-Fi, Cloud

4. Capacités — audit distant

Check ID	Module	Capacité	Contraintes
`dns-resolve`	targets	Résolution DNS	Max 4 IPs analysées
`dns-records`	dns_audit	SPF/DMARC/DKIM/DNSSEC/MTA-STS…	Catégorie dns
`tcp-connect`	tcp_scan	Connect TCP + bannière	Timeouts 0,7–1,2 s ; workers ≤ 128
`udp-probe`	udp_probe	Sondes UDP limitées	Max 3 ports ; 1,2 s
`http-headers`	http_audit	En-têtes / cookies	Si ports HTTP

tls-certificate	tls_audit	Certificat / cipher / TLS	Si ports TLS
service-hardening	service_audit	SSH/SMB/RDP/SMTP/FTP…	Non destructif
cve-correlation	cve_audit	CVE **potentielles**	Catalogue local ; NVD opt-in

4.1 Profils TCP

Profil	Ports	UI
quick	28	Oui
standard	59	Oui
professional	79	Oui
full-1024	1024	Expert
full-tcp	65535	Code seul

4.2 Campagne WAN

`engines/wan/campaign.py` : ≤ **25** cibles ; parallèle 1–4 ; ScopeGuard sur la liste déclarée.

5. Capacités — audit local (PC)

Check ID	Module	Capacité
local-interfaces	local_audit	Interfaces réseau
local-listeners	local_audit	Ports en écoute
local-firewall	local_windows	Pare-feu
local-services	local_windows	Services
local-hardening	windows_hardening P1–P4	Durcissement RO (SMB, Defender, BitLocker, RDP/NLA, UAC, Secure Boot, Credential Guard, ASR, SmartScreen, WDigest, LSA, LLMNR, AlwaysInstallElevated, firewall, LAPS, WDAC…)
baseline-compliance	app/core/baselines	Conformité MS + ANSSI + alignement CIS (voir §6)

6. Conformité multi-référentiels (nouveau — produit gratuit)

Catalogue `win_workstation_v1.json` version **1.0.0** — **40** règles (MS : 40, ANSSI : 40, CIS-aligné : 40). Profil : `windows_workstation`. OS cibles : windows_10_22h2, windows_11_23h2, windows_11_24h2.

Conformité estimée aux recommandations Microsoft Security Baselines et ANSSI, avec alignement technique sur des pratiques de type CIS Level 1. Ce logiciel n'est pas un produit CIS officiel et ne remplace pas un audit CIS SecureSuite.

Composant	Rôle	Chemin
Modèles	Rule / Status / ConformitySummary	`baselines/models.py`
Catalogue	Chargement JSON ouvert	`baselines/catalog.py`
Évaluateur	Pass prioritaire puis fail / snapshot	`evaluator.py`
Moteur	Findings BL-* + scores	`baselines/engine.py`
Check	Après local-hardening	`baseline-compliance`
UI	Case Paramètres (défaut ON) + bandeau %	pages / main_window
PDF audit	Section conformité	`pdf_report._baseline_block`

6.1 Fonctionnement

- Réutilise les findings `LOCAL-HARDEN-*` (pass prioritaire si conflit).
- Émet scores INFO (`BASELINE-SCORE-MICROSOFT|ANSSI|CIS_ALIGNED`) + écarts `BL-WKS-*`.
- Métadonnée `result.metadata['baseline_compliance']` pour PDF/UI.
- Désactivable : Paramètres → case conformité, ou `baselines_enabled=false`.

6.2 Échantillon d'IDs

`BL-WKS-001, BL-WKS-002, BL-WKS-003, BL-WKS-004, BL-WKS-005, BL-WKS-006, BL-WKS-007, BL-WKS-008…` (voir `docs/BASELINES_INVENTAIRE_H0.md`).

6.3 Licences (gratuit)

Source	Usage	Interdit
Microsoft Security Baselines	Réglages techniques + citation	Se dire produit MS
ANSSI (docs publics)	Règles + références	Logo / certification ANSSI
CIS Benchmarks PDF	**Non embarqué**	Copie texte propriétaire
Alignement CIS	Tags thématiques non officiels	Certification CIS

7. Modules optionnels

Module	Engine	Dépendance	Limites
LAN	LanDiscoveryEngine	Natif ; Scapy/Npcap opt.	/24 max ; ≤ 256 hôtes
WinRM	WindowsAuditEngine	winrm/pypsrp	Workers ≤ 8 ; allowlist collecteurs
AD LDAP	ActiveDirectoryAuditEngine	ldap3	RO ; timeout ~20 s
Netdev	NetworkDeviceAuditEngine	pysnmp/netmiko	SNMP 3 s ; SSH show allowlist
Wi-Fi	WifiAuditEngine	netsh	Pas de clés ; pas d'attaque
Cloud Graph	CloudGraphAuditEngine	msal	RO ; jetons non persistés

Collecteurs WinRM : `defender, firewall, hotfixes, listeners, local_admins, os_info, rdp, services_sample, smb`

Contrôles AD défaut : RootDSE; Transport LDAP; Politique mot de passe; Groupes privilégiés; Comptes utilisateurs inactifs; PasswordNeverExpires; Inventaire SPN; Inventaire GPO; machineAccountQuota; Délégations Kerberos.

8. Scapy / Npcap

Contexte	Comportement
EXE Nuitka	Scapy **non embarqué**
Python/venv	Scapy si installé (extra)
Npcap	Détection seule — jamais redistribué
Usage Scapy	ARP /24 uniquement si prêt

Sans Scapy	SendARP + cache ARP + TCP fallback

9. ScopeGuard et limites réseau

- Fail-closed ; refuse `0.0.0.0/0` et `::/0`.
- LAN opérationnel : /24 max.
- WAN : cibles exactes ≤ 25.
- Annulation : Event / CancellationToken.

10. Résultats et risque

Finding : titres simple/expert, sévérité, confiance, catégorie, observation, recommandation, preuve, metadata.

Score V1 : 100 − Σ (INFO0 / LOW2 / MED6 / HIGH14 / CRITICAL28).

Priorité métier V2 : sévérité × confiance × criticité × exposition → LOW/MEDIUM/HIGH/URGENT + horizons 30/60/90. Catégorie `baseline-compliance` traitée comme locale.

Exposition ≠ CVE potentielle ≠ vulnérabilité confirmée. Les % baselines ne sont pas une certification.

11. Reporting et persistance

Sortie	Implémentation	Notes
PDF Synthèse/Détaillé/Expert	PdfReportGenerator	Style transmission + section baselines
PDF Diff	compare.py	Retest
JSON historique	~/.miniaudit/history/	V1 + sidecar V2
Préférences	QSettings	Dont baselines/enabled
Credentials	keyring / mémoire	Jamais dans JSON/PDF
Aide utilisateur	Aide_PM_AuditSecurite.pdf	Charte PM Software
Télémétrie	Aucune imposée	Cœur hors ligne

12. Non-capacités

- Pas d'exploitation, brute force, stuffing, contournement d'auth.
- Pas de fuzzing, DoS, furtivité, persistance, exfiltration, évasion EDR.
- Pas d'attaque Wi-Fi ; pas de PowerShell arbitraire ; SSH show uniquement.
- Pas de texte CIS Benchmarks embarqué ; pas de certification CIS/ANSSI/MS.
- Pas de remédiation automatique (pas d'écriture GPO/registre).
- Pas de Scapy/Npcap dans l'EXE standard.

13. Dépendances et modes dégradés

Cœur : PySide6, httpx, dnspython, cryptography, psutil.

Optionnels : scapy, pywinrm/pypsrp, ldap3, pysnmp, netmiko, msal, keyring. Absent → skip / message.

Baselines : **aucune dépendance externe** (JSON local).

14. Matrice de synthèse

Domaine	Dispo.	Condition
Audit distant mono-cible	Oui	ScopeGuard
Campagne WAN ≤ 25	Oui	Liste déclarée
Profils TCP UI	Oui	quick/std/pro/1024
DNS/HTTP/TLS/UDP/services/CVE	Oui	Selon ports
Hardening local P1–P4	Oui	Windows
Baselines (40 règles MS/ANSSI/CIS-aligné)	Oui	Défaut ON ; désactivable
LAN /24	Oui	Flag ; Scapy seulement en Python
WinRM / AD / SNMP-SSH / Wi-Fi / Graph	Oui	Flags + extras
PDF + section conformité	Oui	Local
Exploitation / CIS officiel	Non	Interdit / hors licence

15. Chemins de référence

app/branding.py, scanner.py, plan.py, checks.py, windows_hardening*.py, app/core/baselines/*, app/data/baselines/win_workstation_v1.json, app/engines/*, app/providers/*, reporting/pdf_report.py, gui/pages.py, docs/PLAN_BASELINES_CIS_MS_ANSSI.md.

Régénérer : .venv\Scripts\python.exe scripts\generate_technical_audit_pdf.py — PM AuditSécurité V2.0a — 2026-08-27.