AYI NEDJIMI Consultants

Pentest Interne 2026 : Méthodologie & Livrables PASSI

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3780 mots • 21 vues •

À retenir — Pentest interne 2026 Un pentest interne simule un attaquant ayant déjà obtenu un accès réseau (poste compromis, insider, phishing réussi) — couvre 70 % des.

À RETENIR

À retenir — Pentest interne 2026

Un pentest interne simule un attaquant ayant déjà obtenu un accès réseau (poste compromis, insider, phishing réussi) — couvre 70 % des scénarios ransomware réels.

Durée typique : **8 à 15 jours** selon taille (250-3 000 postes), Active Directory mature ou flat network, scope blackbox/graybox.

Top 5 chemins d'attaque trouvés en 2024-2026 : **kerberoasting**, LLMNR/NBT-NS poisoning, NTLM relay, ACL misconfig AD, secrets en clair dans GPP/Sysvol.

Livrables obligatoires : rapport exécutif (8-12 pages), rapport technique (40-120 pages), scoring CVSS 3.1, plan de remédiation priorisé, restitution orale 2h.

Budget moyen 2026 PME française : **9 000 à 18 000 € HT** pour 200-500 postes ; ETI : 18 000 à 45 000 € HT pour 1 000-5 000 postes.

Un **pentest interne** reproduit la posture d'un attaquant ayant franchi le périmètre — typiquement par phishing, vol de credentials VPN, insider, ou compromission d'un sous-traitant. C'est la simulation la plus pertinente face à la menace ransomware moderne, qui passe en moyenne **5 jours** entre intrusion initiale et chiffrement (rapport CrowdStrike Global Threat Report 2026). Cette méthodologie 2026 détaille les six phases d'un pentest interne aligné PTES / ANSSI PASSI, les outils utilisés (Impacket, BloodHound, NetExec, Mimikatz contrôlé, Responder, NTLMrelayx), les chemins d'attaque les plus fréquents sur AD français, la structure des livrables, le scoring CVSS, et le plan de remédiation priorisé attendu. Issue de 50+ missions menées sur PME, ETI et OIV/OSE entre 2024 et 2026.

Réponse sous 24h

Devis gratuit →