AYI NEDJIMI Consultants

Pentest Externe 2026 : Black-Box ou Gray-Box, Guide

16 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3611 mots • 17 vues •

> À retenir — Pentest externe 2026 Un pentest externe simule un attaquant Internet ciblant l'exposition externe (sites web, VPN, ZTNA, mail, services exposés) — première ligne de.

À RETENIR

À retenir — Pentest externe 2026

Un pentest externe simule un attaquant Internet ciblant l'exposition externe (sites web, VPN, ZTNA, mail, services exposés) — première ligne de défense.

Mode **black-box** : aucune info pré-fournie, OSINT poussé, durée 8-15 jours. Mode **gray-box** : périmètre IP/domaine fourni, durée 5-10 jours.

Top 5 findings 2024-2026 : interfaces admin exposées (cPanel, vCenter, ESXi, RDP), credentials par défaut, services obsolètes (Exchange 2013, RDP non-NLA), VPN avec CVE non patchées.

Outils incontournables : **Amass**, **Subfinder**, **Nuclei**, **Nmap**, **Burp Suite Pro**, **Gobuster**, **ffuf**, **SQLmap**.

Budget marché 2026 PME française : **5 000 à 14 000 € HT** pour 1-5 sous-domaines + IP ; ETI : 12 000 à 35 000 € HT pour 10-50 sous-domaines + ASN.

Un **pentest externe** évalue la résilience de l'*attack surface* exposée sur Internet : sites web, APIs publiques, VPN (SSL VPN, IPsec), services exposés (SMTP, IMAP, RDP, DNS, FTP), portails de prestataires, plateformes SaaS auto-hébergées. C'est la première ligne de défense — et celle la plus régulièrement testée car la moins risquée pour la production. Cette méthodologie 2026 détaille les phases d'un pentest externe black-box ou gray-box, les outils d'OSINT et de scan, les vulnérabilités les plus rencontrées sur le périmètre français (interfaces admin exposées, CVE non patchées sur VPN, secrets dans GitHub public), et le scoring CVSS adapté. Issue de 60+ missions PME et ETI françaises menées en 2024-2026.

Réponse sous 24h

Devis gratuit →