GUIDE DU PENTEST

Méthodologie • référentiels • kill chain • outils libres

1. Cadre légal, normes et référentiels

France : le socle juridique

Un test d'intrusion sur un système tiers sans autorisation peut relever des infractions relatives à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données.

- Toujours formaliser : commanditaire, périmètre, objectifs, dates/heures, adresses et domaines, exclusions, techniques interdites, gestion des preuves, contacts d'urgence et conditions d'arrêt.
- Données personnelles : appliquer minimisation, protection des preuves, accès restreint et durée de conservation adaptée. Ne collecter que ce qui est nécessaire à la mission.

Contractualisation, RGPD et responsabilité

Au-delà de l'autorisation de principe, plusieurs points doivent être verrouillés avant le premier scan.

- Autorisation écrite (lettre de mission / ROE) signée par une personne habilitée : c'est elle qui écarte la qualification d'accès ou de maintien frauduleux (Code pénal, art. 323-1 à 323-3-1) pour les actions strictement comprises dans le périmètre.
- RGPD : base légale de la mission, minimisation des données collectées, protection et chiffrement des preuves, durée de conservation limitée et suppression en fin de mission ; désigner un contact côté client en cas de découverte de données personnelles exposées.
- Assurance responsabilité civile professionnelle du prestataire et clause de confidentialité (NDA) réciproque.
- Procédure d'urgence : signalement immédiat, hors rapport final, de toute vulnérabilité critique ou donnée sensible découverte pendant le test.
- Toute action hors périmètre initial (ingénierie sociale, déni de service, tests visant un tiers hébergeur) nécessite un accord écrit distinct.

Les référentiels à connaître

Référentiel	À quoi sert-il ?	À retenir
ANSSI PASSI v2.2	Cadre français des prestations d'audit qualifiées	Architecture, configuration, code, intrusion, organisationnel/physique.
PTES	Structure d'un pentest de bout en bout	7 grandes sections : pré-engagement à reporting.
OWASP WSTG v4.2	Méthode de test des applications web	Recon, configuration, identité, auth, sessions, autorisation, entrées, logique métier, client.
OWASP ASVS 5.0.0	Exigences de vérification de sécurité applicative	Référentiel de contrôles vérifiables, utile pour cadrer la couverture.
NIST SP 800-115	Guide de planification et conduite des tests techniques	Planifier, exécuter, analyser et traiter les résultats.
OSSTMM	Méthodologie d'audit de sécurité	Approche structurée et métrique
ISO/IEC 27001 / 27002	SMSI et contrôles de sécurité	Cadre de gouvernance et de contrôles.

2. Types de pentest et périmètres

Selon la connaissance donnée au testeur

Type	Connaissance initiale	Cas d'usage typique
Boîte noire (black box)	Aucune information fournie, comme un attaquant externe.	Évaluer l'exposition réelle depuis l'extérieur ; réaliste mais plus long et moins exhaustif.
Boîte grise (grey box)	Informations partielles (compte utilisateur, accès réseau, documentation limitée).	Bon compromis coût/couverture ; simule un utilisateur ou un attaquant ayant déjà un pied dans le système.
Boîte blanche (white box)	Accès complet : code source, architecture, identifiants, documentation.	Couverture maximale dans un temps donné ; adapté à l'audit de code et aux revues de conception.

Selon le périmètre testé

- Externe / interne : depuis Internet, ou depuis le réseau local comme un attaquant déjà présent.
- Applicatif : web, mobile (iOS/Android), API, client lourd.
- Infrastructure : réseau, systèmes, Active Directory, cloud (IaaS/PaaS/SaaS), Wi-Fi.
- Humain et physique : ingénierie sociale (phishing, vishing), intrusion physique dans les locaux.

Pentest, Vulnerability Assessment, Red Team, Bug Bounty

- Vulnerability Assessment : détection et classement des failles, sans exploitation ; large mais peu profond.
- Pentest : exploitation contrôlée pour prouver l'impact réel, sur un périmètre et une durée définis.
- Red Team : exercice furtif et multi-vecteurs visant à tester la détection et la réponse des équipes (Blue Team), pas seulement les failles techniques.
- Bug Bounty : programme continu ouvert à des chercheurs externes sur un périmètre public, rémunéré à la découverte.

3. PTES : les 7 étapes d'un pentest

PTES organise le test en sept grandes sections, du pré-engagement au rapport. Il s'agit d'une structure méthodologique, à compléter par les référentiels techniques adaptés au contexte.

Étape	Question	Livrable / résultat
1. Pré-engagement	Qu'avons-nous le droit de tester ?	Périmètre, objectifs, exclusions, contacts, fenêtres.
2. Renseignement	Que savons-nous de la cible ?	Actifs, domaines, technologies, comptes/infos publiques.
3. Modélisation des menaces	Quels scénarios sont crédibles ?	Cibles prioritaires, chemins d'attaque, valeur métier.
4. Analyse des vulnérabilités	Qu'est-ce qui peut être exploité ?	Findings validés, faux positifs écartés, hypothèses.
5. Exploitation	Quel est l'impact réel ?	Preuve contrôlée de compromission, sans destruction.
6. Post-exploitation	Jusqu'où peut aller l'attaquant ?	Privilèges, découverte, mouvement latéral, accès aux données — selon ROE.
7. Reporting	Que doit faire le client ?	Constats, preuves, criticité, impact, recommandations, roadmap, retest.

La règle d'or : passer de la vulnérabilité au scénario

Le pentester cherche à établir une chaîne : actif → faiblesse → exploitabilité → privilège/accès → impact métier.

- Scanner = signal.
- Validation manuelle = confiance.
- Exploitation contrôlée = preuve.
- Contexte métier = priorité.

4. Kill Chain, ATT&CK et raisonnement offensif

Cyber Kill Chain

La Cyber Kill Chain de Lockheed Martin décrit sept étapes classiques d'une intrusion ciblée.

Étape	Lecture pentest
Reconnaissance	Identifier l'exposition et les informations utiles.
Weaponization	Préparer ou sélectionner le mécanisme d'exploitation adapté.
Delivery	Déterminer comment l'attaque atteint la cible.
Exploitation	Déclencher la faiblesse.
Installation	Établir la persistance si elle est explicitement autorisée.
Command & Control	Évaluer le maintien et le contrôle d'un accès, sans nuire.
Actions on Objectives	Démontrer l'impact : données, privilèges, interruption, etc.

MITRE ATT&CK : plus précis pour décrire les techniques

ATT&CK ne remplace pas PTES : il décrit les tactiques et techniques utilisées par les adversaires. La matrice Enterprise comprend notamment Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Discovery, Lateral Movement, Collection, C2, Exfiltration et Impact.

À ne pas confondre

- PTES = organisation d'une mission de pentest.
- WSTG = profondeur et couverture des tests web.
- ATT&CK = langage de description des comportements adverses.
- Kill Chain = modèle séquentiel d'une intrusion ciblée.
- PASSI = cadre français professionnel/qualification des prestataires.

5. Pentest web : couverture minimale

OWASP WSTG organise les tests web autour de la collecte d'information, configuration/déploiement, gestion des identités, authentification, autorisation, sessions, validation des entrées, gestion des erreurs, cryptographie faible, logique métier et côté client.

Domaine	Questions essentielles
Recon / exposition	Quels hôtes, sous-domaines, endpoints, technologies et fichiers sont exposés ?
Configuration	TLS, headers, CORS, méthodes HTTP, fichiers de sauvegarde, composants obsolètes ?
Authentification	MFA, bruteforce/rate limiting, récupération de compte, mots de passe, erreurs ?
Sessions	Cookies, Secure/HttpOnly/SameSite, expiration, fixation, invalidation ?
Autorisation	Peut-on accéder aux ressources d'un autre utilisateur ou rôle ? IDOR ?
Entrées	Injection SQL, XSS, upload, désérialisation, traversée de chemin ?
API	Endpoints non documentés, méthodes, auth, contrôle d'accès objet, fuite de données ?
Logique métier	Peut-on contourner une étape, une limite, un prix, une quantité ou un workflow ?
Client	DOM XSS, JavaScript, stockage local, secrets côté client ?
Erreurs / crypto	Messages trop bavards, secrets, algorithmes/protocoles faibles ?

ASVS : pour transformer la couverture en exigences

L'OWASP ASVS fournit une base de vérification des contrôles techniques d'une application web et sert aussi à formaliser des exigences dans les projets et contrats.

6. Boîte à outils libre : choisir selon l'étape

Étape / besoin	Outils libres / gratuits à connaître	Usage typique
Recon / réseau	Nmap, Masscan, RustScan	Ports, services.
DNS / OSINT	Amass, theHarvester	Domaines, sous-domaines, informations publiques.
Fingerprint web	WhatWeb, Nikto	Technologies, configuration et exposition.
Proxy / web	OWASP ZAP, Burp Suite Community	Interception, requêtes, tests manuels.
Fuzzing / contenu	ffuf, Gobuster	Répertoires, fichiers, endpoints, paramètres.
Injection	sqlmap	Validation assistée des injections SQL.
Vulnérabilités	Nuclei, OpenVAS/Greenbone Community	Détection automatisée à valider manuellement.
Exploitation	Metasploit, SearchSploit, Netcat	Validation contrôlée, recherche d'exploits, réseau.
Windows / AD	Impacket, NetExec, BloodHound CE, PowerView, Mimikatz, Responder	Énumération, relations AD, authentification et post-exploitation.
Credentials	Hashcat, John the Ripper, Hydra	Audit de mots de passe / secrets selon périmètre.
Post-exploitation	LinPEAS, WinPEAS, pspy	Énumération locale et recherche d'élévation.
Réseau	Wireshark, tcpdump, Scapy, socat	Capture, analyse et manipulation de trafic.
Wi-Fi	Aircrack-ng, Kismet, hcxdumptool/hcxtools	Audit Wi-Fi autorisé.
Système	Lynis	Audit de configuration Linux.

7. Workflow pratique

Avant le test

- Vérifier l'autorisation.
- Identifier la cible exacte et les exclusions.
- Préparer la journalisation des actions et des preuves.
- Définir les critères d'arrêt et le contact d'urgence.

Pendant le test

Phase	Actions	Question de contrôle
Recon	DNS, domaines, ports, services, web, OSINT.	Ai-je couvert la surface connue ?
Énumération	Versions, endpoints, rôles, technologies, chemins.	Qu'est-ce qui est réellement accessible ?
Analyse	Observations, vulnérabilités et logique métier.	Le finding est-il confirmé ?
Exploitation	PoC minimal et contrôlé.	Puis-je démontrer l'impact sans aller trop loin ?
Post-exploitation	Étendre seulement selon objectifs/ROE.	Quel est le chemin vers l'objectif métier ?
Preuves	Captures, requêtes/réponses, timestamps, hashes si utiles.	Un autre pentester peut-il reproduire ?

Après le test : le rapport

Le reporting PTES distingue notamment la restitution technique et exécutive. Le rapport doit permettre de comprendre le risque, reproduire les constats et prioriser les corrections. Les recommandations PTES insistent sur les preuves, la reproductibilité, la synthèse des résultats et la roadmap de remédiation.

- Résumé exécutif : 3 à 5 messages clés.
- Périmètre et méthodologie : ce qui a été testé et comment.
- Findings : description, preuve, impact, conditions, criticité (ex. score CVSS), recommandations.
- Scénarios : chaînes d'attaque utiles, pas une simple liste de CVE.
- Roadmap : corriger d'abord ce qui casse réellement un scénario à fort impact.
- Retest : vérifier la correction et fermer les constats avec preuve.

8. Références officielles

- ANSSI — PASSI v2.2 / référentiels de qualification
- ANSSI — mise à jour PASSI v2.2 / PRIS
- ANSSI — NIS2
- NIST — SP 800-115
- PTES — Technical Guidelines
- OWASP — WSTG v4.2
- OWASP — ASVS 5.0.0
- MITRE — ATT&CK Enterprise tactics
- MITRE — ATT&CK Enterprise techniques
- Lockheed Martin — Cyber Kill Chain
- ISO — ISO/IEC 27001:2022
- OSSTMM — référence fournie