Fiche : Méthodologies de Pentest

Les tests d'intrusion (pentests) reposent sur différentes méthodologies normalisées. Elles fournissent des guides, étapes et standards pour assurer des audits fiables, reproductibles et complets.

1. MITRE ATT&CK

- Description :
  - Base de données publique et mise à jour regroupant toutes les tactiques et techniques utilisées par des attaquants réels (APT, ransomware, groupes criminels).
  - Chaque technique est documentée avec : méthode d'attaque, exemples réels, outils utilisés, détection, contre-mesures.
- Utilisation pratique :
  - Lors d'un pentest Red Team, le pentester mappe ses actions sur le framework pour simuler un attaquant crédible.
  - Utile aussi pour un SOC qui veut tester sa capacité à détecter des attaques connues.
- ✓ Avantage : Réaliste (basé sur attaques réelles).
- ✗ Limite : Ce n'est pas une méthodologie de pentest complète (plutôt un référentiel d'attaques).

Référentiel : MITRE ATT&CK®

2. OWASP WSTG (Web Security Testing Guide)

- Description :
  - Guide publié par l'OWASP (Open Web Application Security Project).
  - Focalisé uniquement sur les applications web.
  - Décrit des tests pratiques pour chaque type de vulnérabilité (SQLi, XSS, CSRF, mauvaise config…).
- Utilisation pratique :
  - Suivi comme checklist lors d'un audit web.
  - Permet de ne rien oublier (exemple : tester la gestion des cookies, vérifier les headers HTTP, etc.).
- ✓ Avantage : Pratique, très utilisé, mis à jour régulièrement.
- ✗ Limite : Ne couvre que les applications web, pas le réseau ou la sécurité physique.

Référentiel : OWASP Web Security Testing Guide | OWASP Foundation

3. NIST SP 800-115

- Description :
  - Publié par le NIST (USA), référence officielle.
  - Conçu comme un guide de planification et d'exécution de pentests.
- Phases détaillées :

1. Planification : objectifs, périmètre, autorisations légales.
2. Discovery : scan réseau, scan de vulnérabilités, fingerprinting.
3. Attack : exploitation des vulnérabilités.
4. Reporting : rapport technique + exécutif.

- Utilisation pratique :

Très utilisé dans les administrations, banques et industries réglementées.

- ✓ Avantage : Normatif, reconnu, clair.
- ✗ Limite : Assez générique (manque parfois de profondeur technique).

Référentiel : SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC

4. OSSTMM (Open Source Security Testing Methodology Manual)

- Description :
  - Méthodologie extrêmement complète couvrant : réseaux, systèmes, humains, physique, télécoms.
  - Chaque aspect est mesuré avec des indicateurs de sécurité mesurables (RAV, TRUST, CONTROL, etc.).
- Utilisation pratique :
  - Sert pour des audits globaux : test réseau, social engineering, sécurité physique d'un site.
  - Rarement suivi intégralement, mais beaucoup de pentesters en reprennent des morceaux.
- ✓ Avantage : Très complet, couvre tout.
- ✗ Limite : Très dense et complexe → difficile à appliquer entièrement dans un pentest classique.

OSSTMM. 3 : Free Download, Borrow, and Streaming : Internet Archive

5. PTES (Penetration Testing Execution Standard)

- Description :
  - Créé par la communauté sécurité pour standardiser les pentests en entreprise.
- Étapes détaillées :

1. Pré-engagement : définir périmètre, règles, attentes du client.
2. Renseignement : collecte d'infos (OSINT, scans).
3. Modélisation des menaces : identifier ce qui est critique pour l'entreprise.
4. Exploitation : attaques réseau, applicatives, sociales.
5. Post-exploitation : escalade de privilèges, persistance, exfiltration simulée.
6. Reporting : rapport détaillé + recommandations.

- Utilisation pratique :
  - La plus adaptée aux entreprises qui veulent un pentest structuré, clair et exploitable.
- ✅ Avantage : Structurée, pragmatique, largement adoptée.
- ❌ Limite : Ne couvre pas la sécurité physique comme OSSTMM.

[Standard PTES : Méthodologie Complète pour un Pentest Efficace]

6. ISSAF (Information Systems Security Assessment Framework)

- Description :
  - Proposé par l'ISSAF (Information Systems Security Assessment Framework).
  - Similaire au PTES, mais plus académique.
- Phases :
  - Planification → Collecte d'infos → Évaluation → Exploitation → Post-exploitation → Rapport.
- ⚙ Utilisation pratique :
  - Peu utilisé aujourd'hui, mais sert comme base théorique et documentation.
- ✅ Avantage : Bon cadre académique.
- ❌ Limite : Plus vraiment maintenu, peu d'outils concrets.

Résumé :

- Si tu fais un pentest web → OWASP WSTG
- Si c'est un pentest global en entreprise → PTES
- Si c'est pour un audit complet et profond (réseau + humain + physique) → OSSTMM
- Si c'est un cadre institutionnel ou légal → NIST SP 800-115
- Si tu veux mapper ton pentest aux techniques réelles des attaquants → MITRE ATT&CK
- Si en académique/formation → ISSAF