Guide pédagogique : Les étapes d’un Pentest Web

Un test d’intrusion web (ou pentest web) est une simulation d’attaque contrôlée sur une application web. Il permet d’identifier les failles de sécurité avant qu’un attaquant ne les exploite. Ce guide présente les étapes d’un pentest web, avec explications simples et outils couramment utilisés.

1. Définition du périmètre et préparation

On définit les objectifs (quelles applications tester) et les règles (heures, méthodes). Exemple : test en Black Box (aucune information), Grey Box (quelques infos), White Box (accès complet).

2. Collecte d’informations (Reconnaissance)

But : découvrir des infos utiles (technologies, domaines, versions). Outils : nmap (scan de ports), whois (infos domaine), sublist3r (sous-domaines). Exemple de commande : nmap -sV site.com

3. Cartographie de l’application

But : comprendre le fonctionnement du site (pages, formulaires, API, cookies). Outils : Burp Suite, OWASP ZAP. Exemple : analyser un formulaire de connexion et les requêtes envoyées.

4. Analyse des vulnérabilités

But : rechercher les failles. Outils : Nikto (scan web), OWASP ZAP (scanner), Nessus. Exemple : tester une injection SQL sur un champ de recherche.

5. Exploitation

But : prouver qu’une vulnérabilité est exploitable. Exemples : injection SQL avec sqlmap, XSS avec Burp Suite, upload d’un fichier malveillant.

6. Escalade de privilèges

But : vérifier si on peut devenir administrateur ou accéder à plus de données. Exemple : exploiter une API interne pour obtenir des informations sensibles.

7. Post-Exploitation

But : évaluer l’impact réel (exfiltration de données, accès persistant). Exemple : montrer que l’on peut lire les emails des utilisateurs.

8. Rapport

But : présenter les résultats. Contenu : résumé pour la direction, détails techniques pour les développeurs, recommandations.

9. Correctifs et re-test

Après correction, on vérifie que les vulnérabilités ne sont plus exploitables.

Conclusion

Un pentest web est essentiel pour renforcer la sécurité d’une application. Il suit une méthode rigoureuse : de la collecte d’informations à la rédaction du rapport. L’objectif n’est pas seulement de trouver des failles, mais aussi d’aider les équipes à les corriger efficacement.