**Guide Pratique de Pentest**

## **1. Introduction au Pentest**

Le **Pentest** (test d’intrusion) est une méthode proactive visant à identifier et exploiter les vulnérabilités des systèmes informatiques, applications web, réseaux et infrastructures. Il constitue une partie essentielle de la **cybersécurité**, permettant aux organisations de sécuriser leurs données et systèmes contre les menaces externes et internes.

### **Objectifs principaux du Pentest**

* **Identifier les failles de sécurité** dans les systèmes et applications.
* **Évaluer la résistance réelle** face à des attaques potentielles.
* **Proposer des recommandations concrètes** pour corriger ou réduire les vulnérabilités.
* **Sensibiliser les utilisateurs et administrateurs** aux bonnes pratiques de sécurité.

## **2. Types de Pentest**

### **a) Pentest Réseau**

Évalue la sécurité des infrastructures réseau (LAN, WAN, VPN). **Techniques et outils :** - Scan des ports et services (**Nmap**, **Netcat**) - Analyse des configurations réseau - Test des firewalls et IDS/IPS

### **b) Pentest Web**

Évalue les applications web et API. **Techniques et outils :** - Injection SQL (**SQLMap**) - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF) - Tests d’authentification et de session (**Burp Suite**)

### **c) Pentest d’Applications Mobiles**

Analyse la sécurité des applications mobiles Android/iOS.

**Techniques et outils :** - Analyse du code source - Injection et manipulation de données - Test des API et communications sécurisées

### **d) Pentest Physique et Social Engineering**

Évalue la sécurité physique et humaine. **Techniques et outils :**

- Test d’accès aux locaux et équipements - Ingénierie sociale (**phishing, appels frauduleux**)

- Test des systèmes de contrôle d’accès

## **3. Méthodologie complète du Pentest**

| Étape | Description | Outils & Ressources |
| --- | --- | --- |
| **1. Planification** | Définir objectifs, périmètre et obtenir autorisation écrite | Documentation, checklist, accord légal |
| **2. Collecte d’informations** | Recueillir des informations publiques et technologiques | WHOIS, DNS, Shodan, Recon-ng |
| **3. Analyse des vulnérabilités** | Identifier les failles connues et configurations faibles | Nmap, OpenVAS, Nessus, Nikto |
| **4. Exploitation** | Tester les vulnérabilités identifiées et vérifier l’impact | Metasploit, SQLMap, Burp Suite |
| **5. Post-exploitation & Rapport** | Évaluer les risques, rédiger un rapport détaillé avec recommandations | Word, Excel, outils de reporting |

## **4. Outils indispensables pour les Pentesters**

* **Nmap** : scan réseau et découverte des hôtes
* **Metasploit** : exploitation de vulnérabilités
* **Burp Suite** : tests d’injection web
* **Wireshark** : capture et analyse du trafic réseau
* **SQLMap** : tests d’injection SQL automatisés
* **Kali Linux** : distribution complète pour le pentest

## **5. Bonnes pratiques et règles éthiques**

1. Toujours obtenir une **autorisation écrite**.
2. Ne jamais divulguer les informations collectées.
3. Limiter les tests aux systèmes autorisés.
4. Respecter la confidentialité et les lois en vigueur.
5. Documenter chaque étape pour un audit complet.

## **6. Référentiels et standards pour le Pentest**

| Standard | Description | Objectif / Utilité |
| --- | --- | --- |
| **OWASP Top 10** | Liste annuelle des 10 vulnérabilités web critiques | Sensibiliser aux risques majeurs et guider les tests de sécurité applicative |
| **PTES** | Penetration Testing Execution Standard | Fournir un cadre complet pour la réalisation de tests d’intrusion (pré-engagement, collecte d’infos, exploitation, post-exploitation, rapport) |
| **NIST SP 800‑115** | Guide du NIST pour les tests techniques de sécurité | Norme reconnue internationalement, méthodologie et documentation des tests, utile pour environnement régulé |

## **7. Plateformes de pratique et laboratoires virtuels**

| Plateforme | Niveau | Description | Exemple d’exercice | Capture d’écran |
| --- | --- | --- | --- | --- |
| **TryHackMe** | Débutant → Intermédiaire | Cours guidés interactifs, machines vulnérables en ligne | Scanning réseau, exploitation web, analyse de malware | [Insérer capture d’écran ici] |
| **HackTheBox** | Intermédiaire → Avancé | Machines réelles à compromettre, défis CTF | Escalade de privilèges sur serveur Linux, exploitation de services vulnérables | [Insérer capture d’écran ici] |
| **VulnHub** | Tous niveaux | Machines virtuelles vulnérables à télécharger | Exercice offline, pratique pour tests locaux et entraînement | [Insérer capture d’écran ici] |

## **8. Certifications Pentest**

| Certification | Niveau | Contenu | Avantages | Capture d’écran |
| --- | --- | --- | --- | --- |
| **eJPT** | Débutant | Réseaux, systèmes, vulnérabilités web basiques | Valide les compétences initiales en pentest | [Insérer capture d’écran ici] |
| **OSCP** | Avancé | Exploitation avancée, pivoting, escalade de privilèges, rapport complet | Très reconnue, test pratique de 24h avec plusieurs machines | [Insérer capture d’écran ici] |

## 

## **9. Exercices pratiques**

| Exercice | Objectif | Outils suggérés |
| --- | --- | --- |
| Scan de réseau interne | Découvrir les hôtes et services actifs | Nmap, Netcat |
| Injection SQL sur site de test DVWA | Identifier et exploiter une vulnérabilité simple | DVWA, SQLMap |
| Test de mot de passe faible | Comprendre l’importance de mots de passe robustes | Hydra, John the Ripper |
| Analyse de trafic | Capturer et analyser des paquets pour identifier informations sensibles | Wireshark |
| Pentest web complet | Simulation d’attaque web avec rapport final | Burp Suite, OWASP WebGoat |

**Astuce pédagogique :** Chaque exercice doit être réalisé dans un **environnement sécurisé et légal**, comme des machines virtuelles ou laboratoires de test.

## **10. Développement pratique avancé**

Il est conseillé de réaliser un **projet de Pentest complet** incluant :

1. **Choix d’un environnement de test** : machine virtuelle ou réseau de test.

2. **Application de la méthodologie complète** : de la planification au rapport final.

3. **Exploitation sécurisée** : tester les failles sans compromettre les systèmes réels.

4. **Rédaction d’un rapport détaillé** : inclure captures d’écran, résultats des scans et recommandations.

## **11. Nmap - Scan de réseau**

**Objectif :** Découvrir les hôtes actifs et les ports ouverts.

**Commande typique :**

nmap -sS -Pn 192.168.1.0/24

**Exemple de sortie :** Capture Nmap

**Encadre pédagogique :** Observez les IP et les ports ouverts. Les ports courants sont 22 (SSH), 80 (HTTP), 443 (HTTPS). Cela vous aidera à identifier les services en ligne et potentiellement vulnérables.

**Exercice pratique :** - Scanne ton réseau local avec Nmap. - Note les hôtes actifs et les ports ouverts.

## **12. Burp Suite - Interception et Analyse HTTP**

**Objectif :** Intercepter et analyser le trafic entre le navigateur et le serveur.

**Fonctionnalités principales :** Proxy, Repeater, Scanner.

**Exemple de capture :** Capture Burp Suite

**Encadré pédagogique :** Utilisez Burp Suite pour comprendre comment les données sont envoyées et reçues. Vous pouvez tester la modification des paramètres pour analyser la sécurité d’une application web.

**Exercice pratique :** - Intercepte une requête HTTP. - Modifie un paramètre et observe la réponse du serveur.

## **13. SQLMap - Test d’injection SQL**

**Objectif :** Identifier et exploiter des vulnérabilités SQL.

**Commande typique :**

sqlmap -u "http://site-vulnerable.com/page?id=1" --dbs

**Exemple de sortie :** Capture SQLMap

**Encadré pédagogique :** SQLMap automatise la recherche de vulnérabilités SQL. Analysez attentivement les résultats et notez les bases de données trouvées, mais n’exécutez jamais ces tests sur un site non autorisé.

**Exercice pratique :** - Tester une injection SQL sur un site de test. - Lister les bases de données disponibles.

## **14. Conclusion**

Ces outils permettent de réaliser un test d’intrusion complet et d’identifier les faiblesses de sécurité d’un système.

**Encadre pédagogique :** Respectez toujours les règles éthiques et légales en cybersécurité. Le Pentest est un moyen d’améliorer la sécurité, pas de causer des dommages.

Le Pentest est un outil essentiel de la cybersécurité, permettant de prévenir les attaques et de renforcer la sécurité des systèmes informatiques. La pratique régulière, combinée à la maîtrise des outils et des méthodologies, permet aux étudiants de développer des compétences avancées et de contribuer efficacement à la protection des données et des infrastructures numériques.