

---

# 🛡️ Introduction à l’Ethical Hacking

---

## 1. Qu’est-ce que l’Ethical Hacking ?

### ✔ Définition :

L’**Ethical Hacking**, ou **piratage éthique**, est la pratique de tester et d’évaluer la sécurité des systèmes informatiques, réseaux et applications **de manière légale et autorisée**, dans le but de découvrir et corriger les vulnérabilités **avant qu’un hacker malveillant ne les exploite**.

Un ethical hacker est parfois appelé **white hat (chapeau blanc)**.

---

## 2. Objectifs du piratage éthique

- ✔ Identifier les failles de sécurité (logiciel, réseau, humain).
  - ✔ Simuler des attaques réelles pour tester la résistance du système.
  - ✔ Proposer des contre-mesures ou des correctifs.
  - ✔ Aider les entreprises à **se conformer aux normes de cybersécurité**.
  - ✔ Protéger les données sensibles (personnelles, financières, etc.).
- 

## 3. Types de Hackers

Type	Nom commun	Objectif principal
👤💰	White Hat Ethical Hacker	Sécuriser les systèmes
☐♂	Black Hat Malicious Hacker	Vol, sabotage, espionnage
👤👤	Grey Hat Mixte	Peut enfreindre la loi, mais informe la cible

---

## 4. Domaines couverts par l’Ethical Hacking

- 🔐 Test d'intrusion (Penetration Testing)
- 🌐 Hacking Web (SQLi, XSS, CSRF...)

- 🔍 Reconnaissance (Scanning, OSINT, footprinting)
  - 🦂 Sniffing et écoute réseau
  - 🔑 Brute force & cracking de mots de passe
  - 👤 Ingénierie sociale
  - ☐ Analyse de malware
- 

## 5. Étapes d'un test d'intrusion éthique (Pentest)

1. **Reconnaissance** (passive & active)
  2. **Scanning** (ports, vulnérabilités)
  3. **Gaining Access** (exploitation des failles)
  4. **Maintaining Access** (tests de persistance)
  5. **Effacement des traces** (facultatif en éthique, mais simulé)
  6. **Rapport** (avec solutions)
- 

## 6. Outils populaires utilisés

Catégorie	Exemples
OS Hacking	Kali Linux, Parrot OS
Scanning	Nmap, Nessus, OpenVAS
Exploitation	Metasploit Framework
Web Hacking	Burp Suite, OWASP ZAP
Cracking	John the Ripper, Hashcat
Sniffing Réseau	Wireshark, Tcpdump

---

## 7. Cadres et certifications en Ethical Hacking

- 🏢 CEH (Certified Ethical Hacker) – EC-Council
  - 🏢 OSCP (Offensive Security Certified Professional)
  - 🏢 CISSP, CompTIA Security+, GPEN, etc.
- 

## 8. Aspects légaux et éthiques

- ⚖️ L'ethical hacking doit toujours être **autorisé par contrat** ou mandat.

- ⚠ Agir sans autorisation = activité illégale (même si l'intention est bonne).
  - 📄 Signature d'un **NDA (Non-Disclosure Agreement)** souvent requise.
- 

## 9. Qualités d'un bon ethical hacker

- 🧠 Curiosité et logique
  - 🖥 Connaissance des systèmes, réseaux, OS, web, etc.
  - 🔒 Maîtrise des vulnérabilités courantes (OWASP Top 10)
  - 💬 Bonne communication (rédaction de rapports, échanges avec clients)
  - ⚖ Intégrité morale et respect des lois
- 

## 10. Ressources pour débiter

- 🔗 [TryHackMe](#)
  - 🔗 [Hack The Box](#)
  - 🔗 [Root-Me](#)
  - 📖 Livres :
    - *The Web Application Hacker's Handbook*
    - *Hacking: The Art of Exploitation*
    - *Metasploit: The Penetration Tester's Guide*
-