Cours : Outils et Méthodes en Ethical Hacking

🔑 1. Introduction

L'**ethical hacking** suit une **démarche méthodologique** rigoureuse, appuyée par **des outils puissants et spécialisés**. Chaque étape (exploration, attaque, exploitation, etc.) utilise ses propres méthodes et outils, dans un cadre légal et éthique.

□ 2. Méthodologie d'un test d'intrusion (Pentest)

La démarche suit généralement ces 6 étapes :

Étape	Description courte	Objectif principal
1⃣ Reconnaissance	Collecter un maximum d'informations	Identifier la surface d'attaque
2⃣ Scanning	Scanner ports/services/OS	Détecter les points d'entrée techniques
3⃣ Gaining Access	Exploiter les vulnérabilités	Obtenir un accès au système cible
4⃣ Maintaining Access	Maintenir l'accès (optionnel)	Simuler une attaque persistante
5⃣ Covering Tracks	Nettoyage des traces (simulé ou observé)	Évaluer la détection et les logs
6⃣ Reporting	Rédiger un rapport clair et complet	Informer, corriger, sécuriser

Cette méthode est standardisée dans les cadres comme **OSSTMM**, **OWASP**, ou **PTES**.

🛠 3. Outils par catégorie

🔍 Reconnaissance (Passive & Active)

Objectif	Outils
WHOIS/DNS	`whois`, `nslookup`, `dig`

Objectif	Outils
Email/User info	`theHarvester`, `Maltego`
OSINT	`Recon-ng`, `SpiderFoot`

📡 Scan et Enumération

Objectif	Outils
Scan réseau	`Nmap`, `Masscan`, `Netcat`
Enumération	`enum4linux`, `SNMPwalk`
Scan Web	`Nikto`, `WhatWeb`, `Wappalyzer`

💣 Exploitation des failles

Objectif	Outils
Framework d'attaque	`Metasploit`, `ExploitDB`, `Searchsploit`
Exploitation Web	`Burp Suite`, `SQLmap`, `Commix`
Reverse shells	`Netcat`, `msfvenom`, `nc`

□ Analyse de vulnérabilités

Outils	Description
`Nessus`	Scanner de vulnérabilités commercial
`OpenVAS`	Scanner libre et open-source
`Nikto`	Scanner de serveurs Web

🔑 Cracking & Brute Force

Cible	Outils
Mots de passe	`John the Ripper`, `Hashcat`, `Hydra`
Fichiers hashés	`CrackStation`, `RainbowCrack`

📶 Sniffing & Spoofing

Objectif	Outils
Analyse réseau	`Wireshark`, `tcpdump`

Objectif	Outils
ARP/DNS Spoofing	`Ettercap`, `Bettercap`

🎁 Post Exploitation / Maintien d’accès

Objectif	Outils
Escalade de privilèges	`Linux Exploit Suggester`, `BeRoot`, `LinPEAS`
Persistence	`Metasploit`, `Empire`

□ Reporting et documentation

Objectif	Outils
Création de rapport	`CherryTree`, `Dradis`, `KeepNote`, `Faraday`
Screenshots	`Flameshot`, `Shutter`

□ 4. Méthodes d’approche

A. Boîte noire (Black Box)

- Le hacker n’a **aucune connaissance** du système cible.
- Situation proche d’un attaquant réel.

B. Boîte grise (Gray Box)

- Le hacker a **des accès partiels ou des infos limitées** (ex : accès utilisateur).

C. Boîte blanche (White Box)

- Le hacker a un **accès complet au code source et à l’infrastructure**.

⚖ 5. Cadres de test d’intrusion

Cadre	Description
OWASP	Sécurité des applications Web (Top 10)
OSSTMM	Open Source Security Testing Methodology Manual
PTES	Penetration Testing Execution Standard

Cadre	Description
NIST SP 800-115	Guide américain pour les tests techniques de sécurité

📚 6. Bonnes pratiques

- Obtenir **une autorisation écrite (engagement légal)**.
- Travailler en environnement de test ou sandboxé.
- **Documenter** chaque étape (screens, logs, résultats).
- Préserver la **confidentialité** des données analysées.
- Être transparent dans le **rapport final**.

🎓 7. Exercices pour débutants

- 🔲 Lancer un scan Nmap sur votre propre machine virtuelle :

```
nmap -sS -A 127.0.0.1
```

- 🔐 Brute force d'un service SSH sur une machine test avec `Hydra` :

```
hydra -l admin -P wordlist.txt ssh://192.168.1.10
```

- 🌐 Scanner un site Web local avec `Nikto` :

```
nikto -h http://localhost
```

🔗 8. Ressources utiles

- https://nmap.org
- https://exploit-db.com
- https://owasp.org
- https://tryhackme.com
