20 outils incontournables

Pour les pros et ceux qui débutent ...

1. Kali Linux - Système d’exploitation avec des milliers d’outils préinstallés
2. Wireshark - Capture et analyse de protocoles réseau
3. Nmap - Scanner de ports (à utiliser avec précaution)
4. Burp Suite - Sécurité web
5. Gophish - Kit d’outils de phishing open source
6. Aircrack-NG - Sécurité Wi-Fi
7. Have I Been Pwned - Pour vérifier si vos emails ont été retrouvés dans un leak
8. Metasploit Framework - Outil de pentest polyvalent (à utiliser avec précaution)
9. Nikto - Scanner de vulnérabilités
10. HackTheBox - Entraînement à la cybersécurité
11. pfSense - Pare-feu/Routeur
12. Cyber Chef - Boîte à outils polyvalente, disponible en ligne et installable localement
13. Suricata - Système de détection d’intrusions (IDS)
14. Ghidra - Reverse engineering, développé par la NSA
15. Dehashed - Pour savoir si vous avez été compromis
16. OpenVAS - Scanner de vulnérabilités interne et externe (version open source de Nessus maintenue par l’armée allemande)
17. OSSEC - Détection et prévention des intrusions
18. SQLMap - Détection et exploitation d’injections SQL (à utiliser avec précaution)
19. REMnux - Reverse engineering et analyse, notamment pour la décompilation de malwares
20. Zed Attack Proxy (OWASP ZAP) - Scanner de sécurité des applications web

---

Revision #1
Created 2024-10-31 07:46:17 UTC by Admin
Updated 2024-10-31 07:46:45 UTC by Admin