



Apprendre à entrer **pour savoir fermer.**

Vous aimeriez tester vous-même vos sites et vos serveurs, plutôt que d'attendre le prochain audit ? Cinq jours pour mener une intrusion du début à la fin, sur des machines prévues pour, et repartir avec la méthode et le rapport qui va avec.

DURÉE	TARIF INTER	INTRA	NIVEAU
5 jours	3 750 € HT	dès 1 500 € HT/jour	Avancé

À l'issue de la formation

- Maîtriser la méthodologie complète de test d'intrusion PTES
- Produire un rapport professionnel livrable au COMEX
- Réaliser une simulation d'attaque réaliste end-to-end
- Automatiser les phases de reconnaissance et d'exploitation

Pour qui

- Consultants souhaitant structurer leur méthodologie
- Techniciens sécurité voulant passer à l'offensif
- Candidats préparant l'OSCP
- Équipes red team en montée en compétences

Prérequis

Linux (navigation, bash basique), TCP/IP, notions HTTP. Kali Linux requis.

Déroulé

Jour 1 Reconnaissance & OSINT

- Méthodologie PTES et cadre légal (PASSI)
- Reconnaissance passive : OSINT, Shodan, Maltego
- Reconnaissance active : Nmap, Masscan, Nuclei
- Cartographie de la surface d'attaque

Jour 2 Exploitation web

- OWASP Top 10 en conditions réelles
- SQLi, XSS, IDOR, SSRF, File inclusion
- Exploitation avec Burp Suite Pro
- APIREST / GraphQL : vulnérabilités spécifiques

Jour 3 Exploitation réseau & systèmes

- Services exposés : SMB, RDP, WinRM, SSH
- Vulnérabilités de configuration et CVE
- Metasploit : automatisation et modules post-expl
- Privesc Linux et Windows

Jour 4 Post-exploitation & pivoting

- Persistence, exfiltration, C2 (Cobalt Strike concepts)
- Pivoting SSH, proxy SOCKS, chisel
- Mouvement latéral réseau
- Anti-forensic et discrétion

Jour 5 Red team avancé & rapport

- Simulation d'attaque APT complète
- Rédaction rapport technique + exécutif
- Restitution orale : angle technique + management
- Revue des IOCs et recommandations

Ce qui est compris

- Environnements de lab dédiés (VM fournies)
- Modèles de rapport professionnel (Word + PDF)
- Checklists PTES et OWASP annotées
- Accès aux scripts et outils commentés

Prochaines sessions inter-entreprises

DATES	LIEU ET FORMAT	PLACES
18 - 22 janvier 2027	Paris · Présentiel ou distanciel	6 places

DATES	LIEU ET FORMAT	PLACES
24 - 28 mai 2027	À distance · Distanciel	8 places
4 - 8 octobre 2027	Paris · Présentiel ou distanciel	8 places

Résistez aux hackers - organisme de formation certifié Qualiopi. Prise en charge OPCO possible, les pièces sont fournies.

Inscription et devis : <https://resistez-aux-hackers.com/contact.html> - formation@resistez-aux-hackers.com

Programme susceptible d'évoluer. Version du 08/10/2026. Accessibilité : nous contacter pour toute situation de handicap, nous étudions les adaptations possibles.