LE PENTEST : LA RECHERCHE DES VULNÉRABILITÉS

Un outil fondamental pour traiter les vulnérabilités d'un système d'information avant qu'elles ne soient découvertes et exploitées à des fins malveillantes

high-jack.fr

DES PENTESTS ADAPTÉS À VOS BESOINS

Le Pentest est une **évaluation** ciblée des **vulnérabilités** d'un système d'information.

L'objectif principal est d'identifier les failles **avant** qu'elles ne soient découvertes et exploitées à des fins malveillantes.

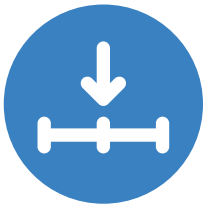
Les pentests sont réalisés par des auditeurs certifiés (*) d'High Jack. Ils ont la particularité d'être effectués selon des méthodologies éprouvées par les institutionnels puis complétées par **celles utilisées par les cyberattaquants** avec des tests approfondis sur les applications et les infrastructures.

À l'issue des tests, High Jack remet un rapport à l'entreprise qui dispose donc d'un outil lui permettant de prendre les mesures nécessaires pour :

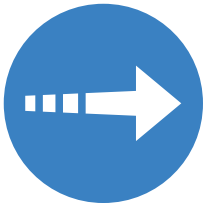
- renforcer sa continuité opérationnelle,
- conserver son avantage concurrentiel,
- rester en conformité avec la réglementation en vigueur.

High Jack propose 3 niveaux de pentests adaptés aux différents types d'organisations allant des TPE jusqu'aux grands groupes en passant par les ETI et les collectivités.

Pentest **Flash©**
Adapté pour les petites organisations qui souhaitent établir un premier niveau d'analyse de risque de leurs systèmes exposés sur internet.



Pentest **Intermédiaire**
Permet d'obtenir une vision claire et concise du niveau de risque des systèmes exposés sur internet.



Pentest **Avancé**
Destiné aux entreprises et groupes de toutes tailles qui cherchent à approfondir les techniques que pourraient utiliser les cybercriminels sur leurs systèmes internes et les systèmes exposés sur internet.

Pentest **Sur mesure**
Destiné aux organisations ayant des besoins spécifiques de recherches de vulnérabilités.

(*) Certifications détenues par les auditeurs d'High Jack : CRTO II, RTO, OSCP, eCPTX, eWPTXv2, CRTP, eCXD, eMAPT, OSWE, eCPPTv2, eWPT, eJPT, SANS Institute, Pentester Academy, Offensive Security, EC-Council, , AWS Certified Cloud Practitioner, Social Engineering Expert, Drone Security Operations Certificate (DSOC), CyberArk Trustee, ISO27001.

TROIS TYPES DE MÉTHODOLOGIE

Black Box - Test en boîte noire

- Connaissances du système : aucune ou très limitée.
- Approche : le pentester, sans accès au code source ni aux informations internes, simule une attaque externe en découvrant l'infrastructure cible de manière indépendante.
- Objectif : tester la résilience du système face à une attaque externe sans connaissances préalables.
- Avantages : réalisme dans la simulation d'une menace externe, permettant de détecter des vulnérabilités que des attaquants externes pourraient exploiter.

Grey Box - Test en boîte grise

- Connaissances du système : partiellement informé.
- Approche : le pentester connaît certaines informations sur le système (structure, flux de données, accès utilisateurs) mais pas l'ensemble des mécanismes internes.
- Objectif : simuler une attaque par un utilisateur légitime avec privilèges limités ou une personne ayant obtenu des infos internes.
- Avantages : plus ciblé que le Black box, grâce aux informations dont dispose le pentester.

White Box - Test en boîte blanche

- Approche : le pentester a un accès complet au système (code source, documentation, schémas d'architecture).
- Objectif : tester toutes les vulnérabilités possibles grâce à une compréhension complète des mécanismes internes.
- Avantages : approche exhaustive et efficace pour identifier les failles internes ou logiques.

Les différentes approches sont complémentaires et peuvent faire l'objet d'adaptations spécifiques à vos besoins.

UN DÉROULEMENT UNIQUE

Un pentest se déroule en 5 phases :

- Validation du devis commercial,
- Signature du mandat d'autorisation permettant de rester en conformité avec la réglementation,
- Phase technique de reconnaissance,
- Recherche et tentative d'exploitation des vulnérabilités,
- Production et restitution du rapport.

Le rapport présente l'ensemble des vulnérabilités identifiées au sein du système audité. Chaque vulnérabilité est classée selon son niveau de criticité (Critique, Majeure, Haute, Faible), accompagnée d'une description technique détaillée et de recommandations de remédiation permettant de réduire la surface d'exposition au risque.

DIFFÉRENTES CARACTÉRISTIQUES

		Pentest Flash©	Pentest Intermédiaire	Pentest Avancé
Dimensionnement	Nombre maximum de noms de domaines à cibler	1	2	5
	Nombre maximal d'adresses IP publiques à cibler	2	5	10
Méthodologie	Blackbox	✅	✅	✅
	Grey box	❌	✅	✅
	White box	❌	❌	✅
	Stress test	❌	❌	✅ Inclus 3 cibles
	Evaluation du niveau de robustesse de la configuration AD	❌	❌	✅ Inclus 1 forêt
	Remise de rapport avec description détaillées de remédiations	❌ Descriptions synthétiques uniquement	✅	✅
	Recherche des vulnérabilités sur les systèmes internes	❌	✅ Forfait 2 jours	✅ Forfait 4 jours
	Réunion de restitution en visio sécurisée ou sur site en France métropolitaine	✅ Forfait visio 30 minutes	✅ Forfait : 1/2 journée	✅ Forfait : 1 journée
Suivi	Suivi de la mise en œuvre du plan de remédiation avec Test de vulnérabilités de contrôle	❌	En option sur devis	✅ Contre audit Flash à + de 6 mois sur 5 vulnérabilités

(*) Les éléments budgétaires mentionnés dans ce document sont donnés à titre indicatifs et ne constituent pas un engagement contractuel. Chaque prestation fait l'objet d'un devis personnalisé et adapté en fonction des besoins exprimés par le client.

EN SAVOIR PLUS

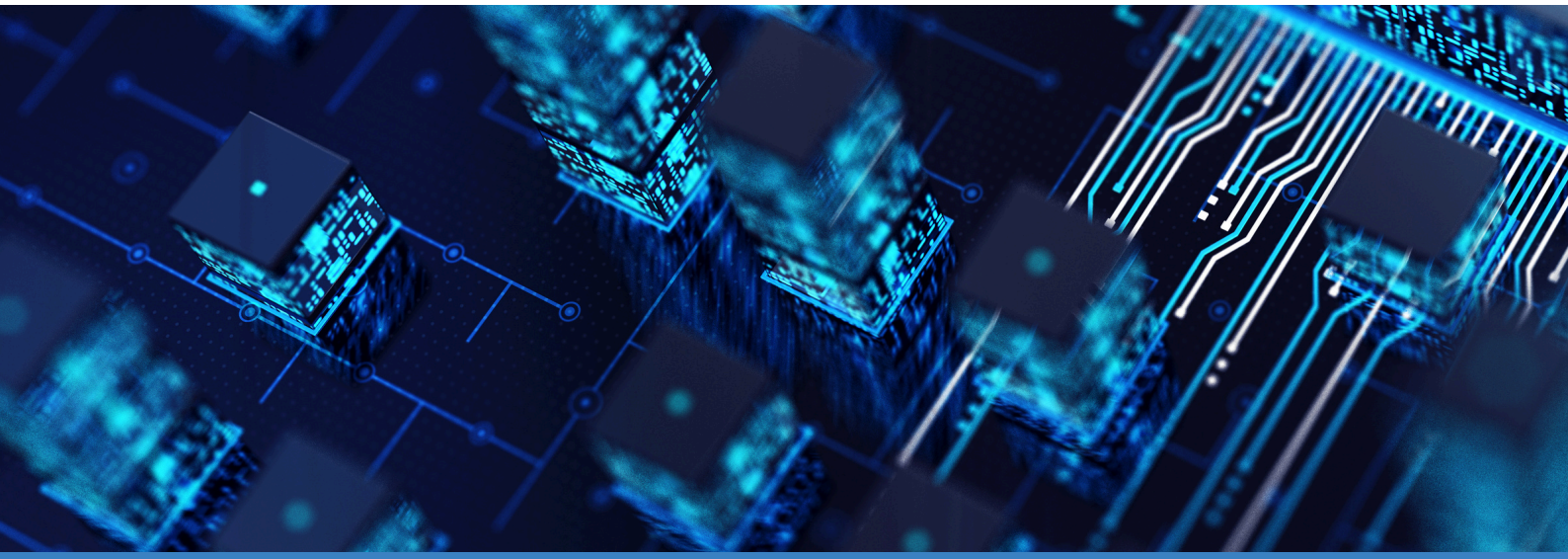
En effectuant des pentests de manière régulière, vous maintenez un niveau de connaissance précis et actualisé sur l'exposition réelle de vos systèmes aux menaces, vous permettant ainsi d'ajuster vos mesures de sécurité de manière proactive.

Nous sommes à votre disposition pour élaborer l'approche la plus adaptée à vos besoins afin de vous permettre de garder le contrôle sur la sécurité de votre système d'information.

Contactez-nous pour un accompagnement complet dans vos démarches de sécurisation informatique.

HIGH JACK

REIMS, NANCY, LIMOGES



HIGHJACK
CYBER-SÉCURITÉ

Siège social : 74 rue du Docteur Lemoine, 51100 Reims

contact@high-jack.fr

03 10 45 40 01

IAS ACCREDITED Management Systems Certification Body MSCB 154 TNV
An ISO 27001 : 2022 certified

2025

DOCUMENT NON CONTRACTUEL