LOGIN
SÉCURITÉ

LE PENTEST DE A À Z : MÉTHODOLOGIE & BONNES PRATIQUES

Dans un contexte où les hackers ne cessent d'améliorer leurs techniques et que les nouveaux usages facilitent l'accès aux données sensibles, le pentesting permet d'adapter et d'optimiser la sécurité informatique, tout en anticipant et en facilitant la prise de décision.

Des **entreprises** plus que jamais **vulnérables**

60 %

des **cyberattaques** exploitent des données **d'identification volées, soit** des vulnérabilités logicielles connues.

200 %

c'est l'**augmentation** entre 2018 et 2019 des **données exposées signalées**.

Le **pentest** : késako ?

Le pentest, également appelé test d'intrusion en français, est une **technique de piratage éthique** consistant à tester la vulnérabilité d'un système informatique, d'une application ou d'un site web en **détectant les failles susceptibles d'être exploitées par un hacker ou un logiciel malveillant**.

La finalité du test d'intrusion ne consiste pas à établir la liste des vulnérabilités d'un système mais de **formaliser un plan d'action pragmatique**, comprenant des préconisations techniques, organisationnelles, opérationnelles et humaines. Celles-ci doivent pouvoir être implémentées par les équipes IT et adaptées au budget qui leur est alloué.

Le **pentest** : en mode Red Team ou Purple Team ?

RedTeam

Mettre à l'épreuve le système de sécurité informatique d'une organisation. **Orchestrée à la manière d'une véritable attaque**, cette prestation permet de réaliser tous types de scénarios réalistes sans qu'aucune limite préalable ne soit posée. Elle permet de tester tous les aspects relatifs à la sécurité informatique.

PurpleTeam

Créer une seule et même équipe (d'assaillants et d'opposants), afin de **fédérer et renforcer la collaboration** entre les auditeurs et tous les acteurs internes de la sécurité informatique. Le PurpleTeam s'appuie sur différents leviers permettant de jauger la réactivité du service informatique et des salariés.

Chaque méthode possède ses avantages, mais certaines nécessitent un travail de fond et une implication rigoureuse des entreprises. En règle générale, **il est recommandé de commencer par un pentest ou un audit de sécurité**, avant d'envisager des méthodologies qui reposent sur des mises en situation réelles, comme le RedTeam.

Greybox : le nouveau standard.

BlackBox

Aucune information

L'auditeur simule une attaque en se mettant dans la peau d'un hacker, dans les conditions d'un piratage réel.

GreyBox

Quelques informations

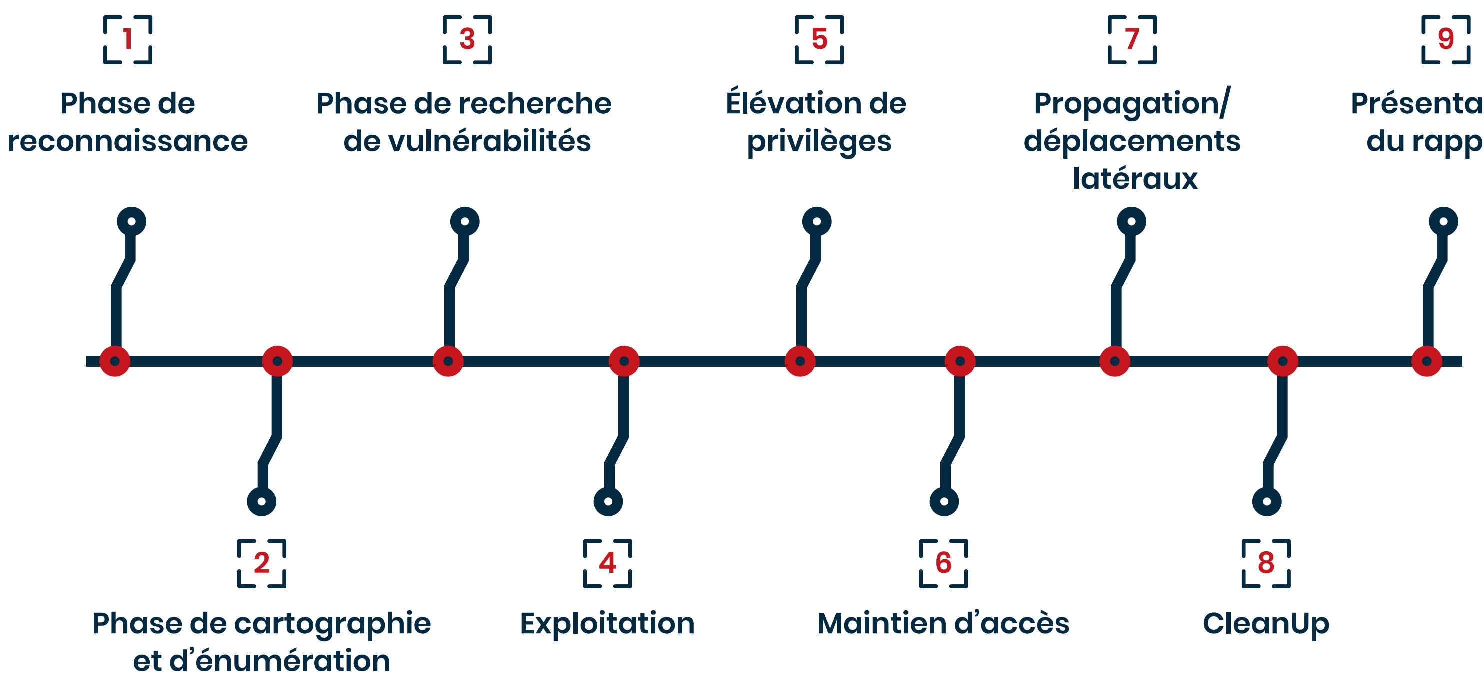
Méthodologie intermédiaire, qui permet de bénéficier des avantages du BlackBox et du WhiteBox.

WhiteBox

Toutes les informations

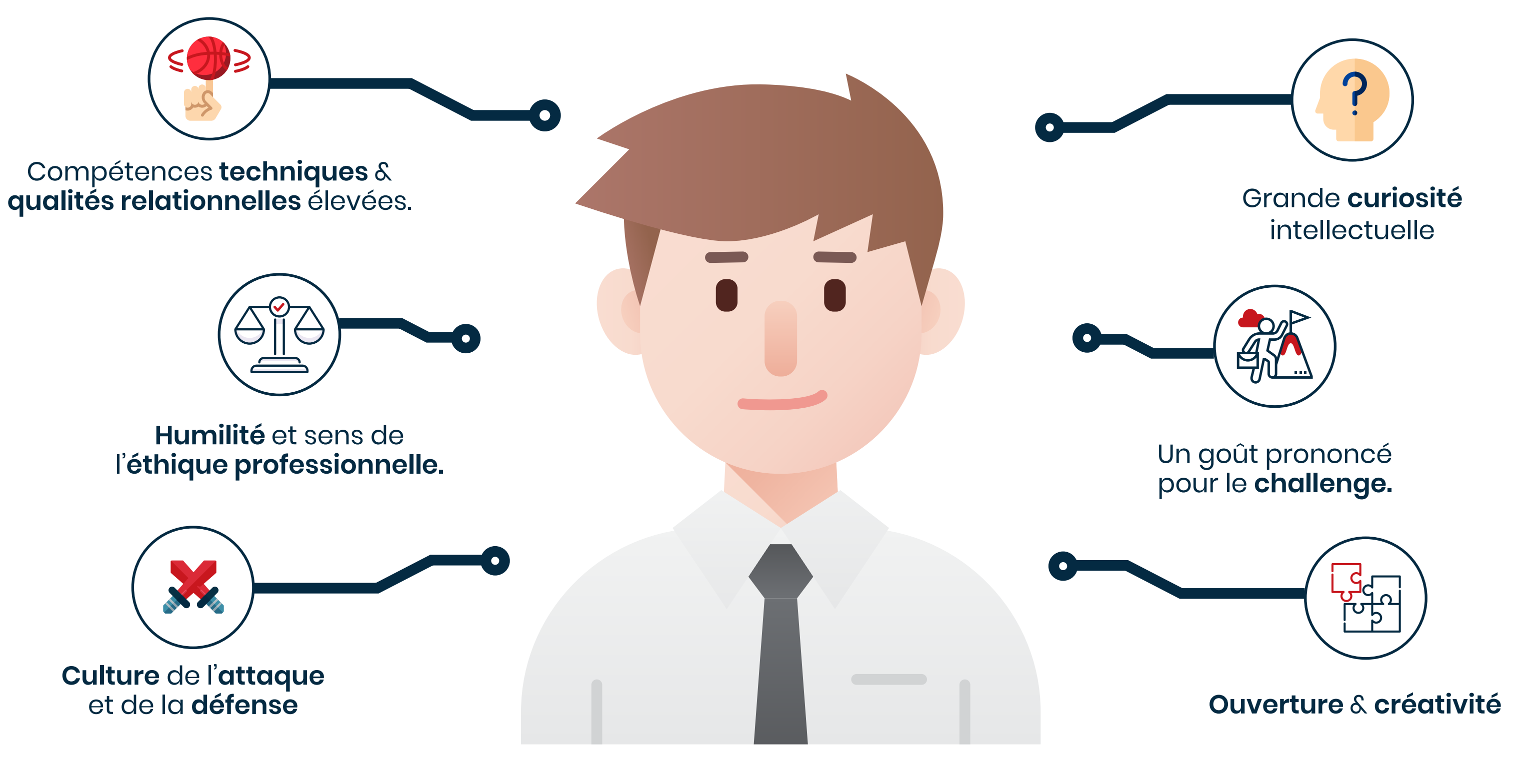
L'auditeur travaille en étroite collaboration avec la DSI de son client.

Les différentes **phases d'un pentest**



1. **Phase de reconnaissance**
2. **Phase de cartographie et d'énumération**
3. **Phase de recherche de vulnérabilités**
4. **Exploitation**
5. **Élévation de privilèges**
6. **Maintien d'accès**
7. **Propagation/ déplacements latéraux**
8. **CleanUp**
9. **Présentation du rapport**

La **recette** d'un bon pentester



Compétences **techniques** & **qualités relationnelles** élevées.

Humilité et sens de l'**éthique professionnelle.**

Culture de l'**attaque** et de la **défense**

Grande **curiosité** intellectuelle

Un goût prononcé pour le **challenge.**

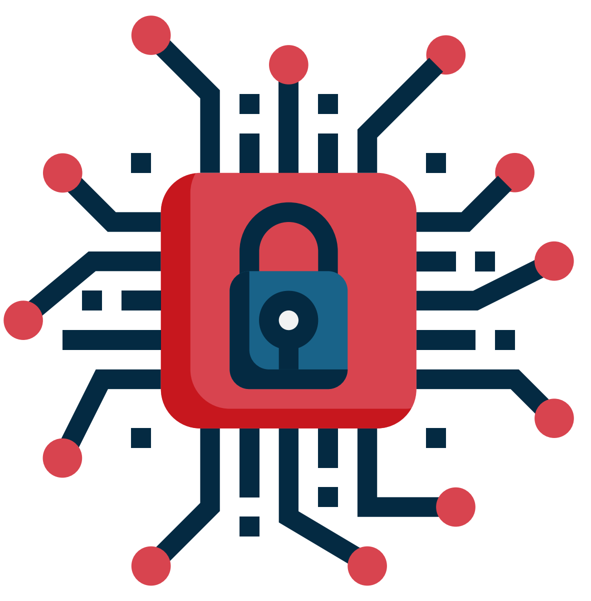
Ouverture & **créativité**

Formation	**Validation des acquis**	**Compétitions**
Généralement issu d'une **école d'ingénieur en technologie de l'information**	RootMe -Hacking platform- Newbie Contest Les seules limites sont les vôtres	CTF TIME **Evénements** DEFCON Chaos C.Club NUIT DU HACK

Le **pentest**, un élément indispensable dans une **démarche globale de sécurité** en constante évolution.

Si le pentest est l'un des leviers permettant d'optimiser la sécurité d'un système informatique, il n'est pas une fin en soi. Il s'agit d'un outil efficace qui prend corps dans une **démarche globale**, impliquant l'ensemble des acteurs du SI.

Le pentesting doit être considéré comme un **moment d'échange constructif** entre les audités et les auditeurs. Pour l'entreprise, le test d'intrusion s'affirme comme l'opportunité d'**obtenir un avis objectif**, émanant d'un expert extérieur. Il doit toujours superposer la découverte de vulnérabilités à un plan d'action effectif, prenant en compte la réalité opérationnelle et les risques métiers de l'entreprise.



LOGIN
SÉCURITÉ

www.login-securite.com

+33 1 58 75 79 00

pentest@login-securité.com