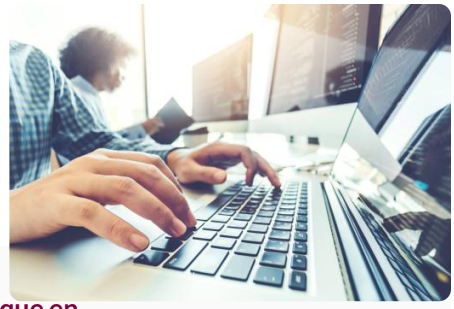
Cybersécurité - Pentester (H/F/X)



Informatique - Numérique | Professionnel qualifié

Durée	Tranche d'âge	Finalité	Pratique en entreprise / Alternance	Métier en pénurie / Fonction critique
2 ans	18 à 25 ans 25 ans et +	Diplôme	Oui	Oui

Vous adorez le challenge, l'IT et la cybersécurité ? Vous ne lâchez jamais l'affaire et arrivez toujours à vos fins, peu importe les moyens ? Vous savez dresser la frontière entre le "bien" et le "mal" ? Alors devenez Pentester grâce à cette formation garantie sans intrusion !

Le Pentester et la Pentesteuse, aussi appelés Testeurs d'intrusion, sont des **experts en cybersécurité dont le rôle est de simuler des attaques informatiques**. Ils tentent de hacker des systèmes, des réseaux, des applications, des sites web... afin de **détecter les vulnérabilités et les failles de sécurité** avant que des hackers "non éthiques" ne les exploitent. Une fois les tests d'intrusion terminés, ils proposent des solutions pour améliorer la sécurité. Les Pentesters sont des membres de la "Red Team" et pratique une "cybersécurité offensive".

Au cours de cette formation en Professionnel Qualifié, vous développerez toutes les compétences et apprendrez toutes les techniques nécessaires au métier de Cybersécurité - Pentester :

- **Tester et attaquer les systèmes** : vous apprenez à maîtriser les différents types de cyberattaques. Vous apprenez à évaluer les systèmes informatiques et assimilez les notions liées au Red Teaming. Vous apprenez à mettre en œuvre et à réaliser des attaques en vous basant sur les étapes et techniques du Red Teaming. Vous appréhendez le contexte du Web Pentesting ainsi que les normes et référentiels associés. Vous vous appropriez des méthodes complexes pour mener des attaques avancées. Vous apprenez à conduire un test d'intrusion sur un environnement Active Directory et en analysez le niveau de sécurité.
- **Réaliser le reporting des tests effectués** : vous apprenez à effectuer les différentes tâches de reporting suite aux tests de pénétrations effectués. Vous apprenez à rédiger un rapport professionnel à transmettre à votre équipe ou votre client.
- **Collecter, analyser et corréler des informations issues de sources multiples** : vous apprenez à examiner un système d'exploitation (Windows / Linux) afin de détecter des anomalies, des traces d'intrusion, des logiciels malveillants, des configurations sensibles ou des actions malveillantes. Vous apprenez à observer et monitorer le trafic et à repérer les comportements anormaux.

- **Maîtriser les connaissances générales en lien avec les applications en matière de cybersécurité** : vous apprenez l'anglais de manière adaptée au contexte professionnel de la cybersécurité. Vous apprenez le vocabulaire spécifique et les termes techniques. Vous apprenez à comprendre et à mettre en application le cadre légal et réglementaire propre au domaine de la cybersécurité. Vous apprenez à effectuer une veille documentaire et technologique sur le secteur afin de toujours être à jour. Vous assimilez les concepts fondamentaux liés à l'IA ainsi que leurs usages en cybersécurité. Vous appliquez les principes de gouvernance propres au secteur et faites preuve d'éthique dans votre pratique professionnelle.
- **Maîtriser les aspects techniques de base de l'IT** : vous appréhendez et exploitez les réseaux informatiques, leurs interactions ainsi que le fonctionnement élémentaire des systèmes d'exploitation, des applications et des bases de données. Vous apprenez à comprendre le fonctionnement et les failles potentielles des applications web.

Alors si vous souhaitez un avenir professionnel sans failles, venez tester cette formation dans l'un des Centres IFAPME qui la proposent !

Pratique en entreprise ?

En 2ème année, la pratique en entreprise est obligatoire dans cette formation :

- de préférence via le modèle de formation en alternance *(https://www.ifapme.be/decouvrir-lalternance)* : ± 8h de cours en horaire décalé et ± 30h de pratique en entreprise par semaine ; rémunérées.
- sinon via un ou des **stages de pratique professionnelle** : pour un total de 180h en 2ème année (au second semestre) ; non-rémunérées.

Métier en pénurie ?

Cette formation mène à un métier répertorié comme « Métier en pénurie ou sous tension » : la demande de main d'œuvre est supérieure au nombre de candidats ou de candidats qualifiés, vous aurez donc de nombreuses possibilités d'emploi à la suite de votre formation.

Les chercheurs d'emploi peuvent notamment profiter d'une prolongation de la durée des allocations et d'un assouplissement de certaines obligations *(https://www.ifapme.be/liens-utiles/question/faq#droit-assouplissement-allocation-insertion)* liées au statut de chercheur d'emploi/chômeur.

Cette mention est uniquement valable pour l'année académique 2026-2027.

Débouché(s) métier(s)

Pentester / Pentesteuse dans une entreprise spécialisée en cybersécurité
Employé / Employée dans une société spécialisée
Employé / Employée dans le service informatique / sécurité d'une entreprise

Débouché(s) future(s) formation(s)

Spécialisation : Cybersécurité - Incident response analyst *(https://www.ifapme.be/formations/professionnel-qualifie/ifapme/cybersecurite-incident-response-analyst-hfx) response-analyst-hfx)* (pour compléter ses compétences en Cybersécurité défensive)

Administrateur en infrastructure IT *(https://www.ifapme.be/formations/coordination-et-encadrement/administrateur-en-infrastructure-it)*

Administrateur réseaux et système *(https://www.ifapme.be/formations/coordination-et-encadrement/administrateur-reseaux-et-systemes)*

Point(s) fort(s)

Métier en pénurie (nombreux emplois + prolongation de la durée des allocations pour les chercheurs d'emploi)
Métier d'avenir Créativité Evolutions rapides dans le secteur Activités variées

Finalité

Diplôme de Professionnel qualifié homologué par la Communauté française

Conditions d'accès

- Ne plus être soumis à l'obligation scolaire ;
- Satisfaire à une de ces 3 exigences :
  - Soit **être titulaire d'un certificat IFAPME d'apprentissage** ou avoir terminé avec fruit les cours généraux et professionnels de fin d'apprentissage et réussir l'examen pratique au plus tard en fin de la seconde année de formation ;
  - Soit avoir suivi avec fruit le **2ème degré de l'enseignement secondaire général, technique ou artistique**, ou le 3ème degré de l'enseignement secondaire professionnel et dans ce cas avoir obtenu le certificat de qualification ;
  - Soit avoir satisfait à un **examen d'entrée**.
- S'inscrire dans les **3 mois après le début des cours** *(https://www.ifapme.be/actualites/dates-rentree)* . Il est possible de s'inscrire à certaines formations *(https://www.ifapme.be/rentree-janvier)* pendant le mois de **janvier**.
- De plus, le candidat assistera à une **séance d'information** organisée par le Centre IFAPME et complètera un **dossier de motivation** pour accéder à la formation.

Aptitudes

- Le métier s'exerce sous pression et nécessite de pouvoir être réactif dans des situations stressantes en gardant son sang-froid.
- Les technologies évoluent rapidement, le métier nécessite de réaliser une veille permanente tant sur les aspects techniques que juridiques.
- Capacités à suivre des procédures et respecter le cadre légal
- Etre doté d'un esprit analytique et de créativité
- Etre patient et persévérant

Programme

1ère année (cours en commun avec l'Incident response Analyst *(https://www.ifapme.be/formations/professionnel-qualifie/ifapme/cybersecurite-incident-response-analyst-hfx) incident-response-analyst-hfx)*) **:**

- X96/X97/31 Anglais technique (20h)
- X96/X97/31 Cadre légal, règlementaire et éthique (12h)
- X96/X97/31 IA appliquée à la cybersécurité (16h)
- X96/X97/31 Gouvernance (ISO 27001 & NIS2) (24h)
- X96/X97/31 Réseaux informatiques (40h)
- X96/X97/31 OS et logiciels (40h)
- X96/X97/31 Analyse système (40h)
- X96/X97/31 Analyse network (40h)
- X96/X97/31 Network pentesting (72h)

2ème année :

- X97/32 Anglais (20h)
- X97/32 Cadre légal, règlementaire et éthique (12h)
- X97/32 Gouvernance (ISO 27001 & NIS2) (16h)
- X97/32 Network pentesting (40h)
- X97/32 Red teaming (52h)
- X97/32 Web pentesting (72h)
- X97/32 Active Directory (44h)
- X97/32 Audit AD (16h)
- X97/32 Reporting (16h)
- X97/32 Coaching TFE (16h)

S'inscrire à une formation pour adultes

Délais et informations

- L'inscription aux cours est ouverte **jusqu'à 3 mois après le début des cours** *(https://www.ifapme.be/actualites/dates-rentree)*. Il est possible de s'inscrire à certaines formations *(https://www.ifapme.be/rentree-janvier)* pendant le mois de **janvier**.
- **Des droits d'inscription sont requis**. Le montant varie d'une formation à l'autre mais est compris généralement entre 350 et 450€ ou plus.
- Prenez contact avec le Centre IFAPME *(https://www.ifapme.be/centres)* qui organise la formation : consultez les modalités d'inscription pour l'année 2026-2027 *(https://www.ifapme.be/inscriptions2026)*.

S'inscrire

Pour l'inscription proprement dite, munissez-vous des documents suivants :

- votre **carte d'identité** ;
- une **copie du dernier diplôme** (ou bulletin) obtenu ;
- si vous êtes demandeur d'emploi et que vous vous inscrivez à une formation à un "métier en pénurie" *(https://www.ifapme.be/penurie)*, une **attestation d'inscription au FOREM** *(https://www.leforem.be/)* pour profiter d'une éventuelle dispense.

Trouver un stage

Après cette inscription, **si l'Alternance est possible pour cette formation**, vous pouvez trouver une entreprise avec laquelle signer une convention de stage.
Pour préparer votre convention de stage ou en cas de difficultés pour trouver une entreprise-formatrice, contactez un Service Alternance IFAPME près de chez vous. Pour ce rendez-vous, munissez-vous des documents suivants :

- votre carte d'identité
- la preuve de votre inscription à la formation.

Sites de formation

Dinant, Charleroi - Site E6K, Tournai.