Date version document : 14/06/2025

Programme de Formation

RS6092 – Réaliser des tests d'intrusion (Sécurité Pentesting)

Objectifs finaux

Objectifs professionnels :

À l'issue de la formation, le stagiaire sera capable de :

- ✓ Cadrer un test d'intrusion et cibler son périmètre
- ✓ Réaliser un test d'intrusion selon les standards
- ✓ Identifier et catégoriser des vulnérabilités selon leur niveau de criticité

Catégorie

La catégorie prévue à l'article L.6313-1 est : Action de formation

Public

Personnes souhaitant développer leurs compétences professionnelles dans les tests d'intrusion (pentests) :
- Techniciens systèmes et réseaux
- Administrateurs systèmes et réseaux
- Développeurs ayant une bonne connaissance des systèmes et réseaux,
- Analystes SOC
- Professionnels de l'informatique souhaitant évoluer vers le pentest

Prérequis

Les conditions d'accès sont :
- Avoir des connaissances de base en réseaux : protocoles, adressage IP, routage.
- Avoir une compréhension du fonctionnement des systèmes Linux et/ou Windows : commandes de base, systèmes de fichiers.
- Être familier avec les systèmes de virtualisation comme VMWare, Hyper-V ou VirtualBox
- Avoir une appétence pour les grands domaines de la cybersécurité : sécurité des systèmes, des réseaux, des applications

Durée

Cette formation se déroule en 100 heures sur un durée de 90 jours (aménageable).
Horaires : flexibles – cette formation se déroule en 100% distanciel

Lieu

Cette formation est accessible en ligne sur la plateforme cyberini.com – des identifiants individuels seront fournis pour le suivi d'exécution de l'action

Cyberini

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France

Programme de Formation

Tarif

Cette formation est dispensée pour un coût de 1800 euros HT soit 1800 TTC (taux de tva 0% au titre de l'Art. 261.4.4 a du CGI).

Modalités et délais d'accès

L'inscription est réputée acquise lorsque : le candidat a validé son inscription et reçu l'e-mail de bienvenue.
Les délais d'accès à l'action sont : entre 11 et 30 jours ouvrés.

Moyens pédagogiques, techniques et d'encadrement

Méthodes et outils pédagogiques

Méthodes pédagogiques : Pédagogie active basée sur des séances vidéo, des supports de cours, des travaux pratiques et des QCM organisés à distance de façon asynchrone que le stagiaire devra réaliser et remettre lorsqu'il termine chaque module.
Outils pédagogiques : La plateforme pédagogique est proposée sous forme de Learning Management System (LMS) accessible au moyen d'une connexion internet
Supports pédagogiques : livret d'accueil et supports accessibles en ligne via la plateforme e-learning 24/7
Prise en compte du handicap : nous proposons des compensations et un accompagnement individualisé pour les PSH – la durée de la formation est adaptable. Tous nos supports de cours peuvent être modifiés pour répondre aux besoins et contraintes. Merci de nous contacter à l'adresse e-mail : support [arrobase] cyberini[point]com - pour la certification, des modalités d'évaluation adaptées peuvent être proposées – notre référent handicap M. Michel KARTNER vous accompagne dans les démarches.

Éléments matériels de la formation

Supports techniques : plateforme e-learning - Un compte Cyberini dédié permettra au stagiaire de suivre la formation dans son intégralité et d'effectuer le suivi individualisé. Accessibilité 24/7 à la plateforme en ligne (système LMS LearnDash). Le bénéficiaire doit être muni du matériel informatique répondant aux exigences de cette action : connexion Internet, micro et webcam (pour l'examen).
Documentation : supports de cours consultables 24/7 sur la plateforme.

Compétences des formateurs

La formation est réalisée par M. Michel KARTNER. L'assistance pédagogique et l'assistance technique sont assurées par M. MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années.

Formation ouverte à distance FOAD

Nature des travaux et durée estimée : QCM et travaux pratiques à rendre à la fin de chaque module. Temps de travail personnel total estimé : 50h dont 6h pour les travaux à rendre.
Modalités de suivi de l'action de formation : temps de connexion sur la plateforme, QCM, travaux réalisés, accompagnement pédagogique et technique.

Description des modalités de vérification des prérequis des candidats
Les prérequis sont vérifiés par le biais d'une série de questions d'analyse de besoins communiquée aux participants en amont de l'action de formation ou complétée lors d'un entretien individuel avec les candidats. Lors de l'entretien, il est demandé au candidat de lister les responsabilités qu'il exerce ou a exercées dans son poste actuel et/ou ses qualifications, en particulier celles liées au systèmes d'exploitation, cybersécurité, systèmes, réseaux et infrastructure globale.

Modalités d'évaluation : test de positionnement**,** évaluations pendant le parcours de formation, évaluation de fin de formation.
Évaluation finale : certification Réaliser des tests d'intrusion (Sécurité Pentesting) RS6092

Accompagnement / assistance pédagogique : accompagnement réalisé par MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années. L'assistance pédagogique se fait par mail, par téléphone ou bien directement sur la plateforme pédagogique e-learning. Les réponses sont apportées soit en instantané dès que possible ou dans un délai de 48h les jours ouvrés.

Accompagnement / assistance technique : accompagnement réalisé par MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années. L'assistance pédagogique se fait par mail, par téléphone ou bien directement sur la plateforme pédagogique e-learning. Les réponses sont apportées soit en instantané dès que possible ou dans un délai de 48h les jours ouvrés.

Contenu de la formation

MODULE 1 : SE PRÉPARER AU DOMAINE DU HACKING ÉTHIQUE (16h))

- Reconnaître les grands domaines et métiers de la cybersécurité
- Définir des objectifs SMART pour réussir sa carrière
- Préparer son portfolio et sa présence en ligne pour améliorer son employabilité
- Découvrir l'écosystème des tests d'intrusion
- Comprendre l'architecture client/serveur avec les ports et protocoles populaires
- Distinguer les différents types de vulnérabilités et d'impacts
- Différencier les règlementations, normes et standards autour des pentests

MODULE 2 : METTRE AU POINT LES FONDAMENTAUX EN SYSTÈMES ET RÉSEAUX POUR LE HACKING (20h)

- Comprendre l'architecture et le système de fichier Linux
- Maîtriser les commandes de bases sous Linux
- Maîtriser les commandes de bases sur les chemins et les fichiers
- Comprendre les opérateurs sous Linux
- Administrer Linux : Variables d'environnement et gestion de paquets
- Administrer Linux : Processus et fichiers logs
- Comprendre les Permissions Linux
- Trouver des fichiers et remplacer du contenu
- Créer des shells scripts
- Comprendre les modèles OSI Et TCP/IP

- Mettre en pratique le modèle OSI de la couche 1 à 3
- Mettre en pratique le modèle OSI de la couche 4 à 7
- Analyser des Protocoles et du Trafic réseau avec Wireshark
- Projet Linux : Scanner de Port pour votre Portfolio
- Projet Linux : Créer un casseur de mot de passe ZIP
- TP : administrer un système Linux (temps estimé 45min)

MODULE 3 : PRÉPARER L'ENVIRONNEMENT ET LE PERIMÈTRE DU TEST D'INTRUSION (20h)

- Comprendre les besoins du marché autour des tests d'intrusion
- Comprendre les rôles et les responsabilités d'un pentester
- Maîtriser les standards de gestion des vulnérabilités (CVE, NVD et CWE)
- Maîtriser les standards de gestion des vulnérabilités (CVSS)
- Exercice : Définir un score CVSS
- Projet : Créer votre propre calculateur CVSS en Français
- Utiliser OTX Alien Vault pour le Threat Intelligence
- Utiliser MITRE ATT&CK pour le Threat Intelligence
- Trouver des techniques d'attaques avec Atomic Red Team
- Maîtriser la Cyber Kill Chain
- Cadrer le pentest et définir son périmètre
- Créer un devis et un contrat sur mesure pour le client
- TP : Cadrer un test d'intrusion (temps estimé 45min)

MODULE 4 : RÉALISER UN TEST D'INTRUSION EN ENVIRONNEMENT PROFESSIONNEL (24h)

- Réaliser un test d'intrusion en suivant les standards
- Faire l'étape de reconnaissance avec le Google Hacking, les sitemaps et fichiers robots
- Faire l'étape de reconnaissance avec des outils et moteurs de recherches spécialisés
- Faire l'étape de reconnaissance avec l'étude des certificats, technologies et sources
- Pratiquer avec l'OSINT
- Utiliser 5 outils de reconnaissance populaires (TheHarvester, Sublist3r, BlackBird...)
- Organiser et hiérarchiser les données avec Maltego CE
- Faire l'étape du Scanning sur l'environnement vulnérable de façon manuelle
- Faire l'étape du Scanning de façon automatisée avec Nmap
- Scanner le site vulnérable avec Nikto
- Trouver du contenu caché sur un site web avec Dirb
- Faire l'étape de l'Exploitation et obtenir les droits Administrateur (OWASP Juice Shop)
- Installer et utiliser Burp Suite pour intercepter des requêtes
- Gagner l'accès à travers la vulnérabilité CSRF
- Exploiter des données sensibles mal protégées dans l'environnement vulnérable
- Exploiter les vulnérabilités SQL et XSS
- Faire une exploitation SQL avancée
- Exploiter d'autres failles du Top 10 OWASP
- Réaliser la Post Exploitation
- Créer et Délivrer le rapport de pentest
- Projet : Faire un scanner de vulnérabilités web en Python
- TP : Faire un pentest avec rapport (temps estimé 1h30min)

MODULE 5 : PRÉPARER L'EXAMEN DE CERTIFICATION ET ALLER PLUS LOIN (20h)

- Comprendre et utiliser l'outil Samba
- Casser des mots de passe avec Hashcat
- Casser des mots de passe SSH avec Hydra
- Exploiter une vulnérabilité logicielle et élever ses privilèges
- Corriger les vulnérabilités et sécuriser les systèmes
- EXERCICE GUIDÉ : Exemple tout-en-un de pentest avec rapport
- Mettre toutes ses chances de son côté pour réussir l'examen
- Entraînement à l'examen + Examen blanc
- Exploiter une vulnérabilité (exemple tout-en-un avec Metasploit)
- Sélectionner votre propre environnement de pentest
- Télécharger et Installer Docker Desktop
- Installer et utiliser Exegol pour les tests d'intrusion
- Comprendre Docker et les Dockerfiles
- Installer des environnements vulnérables et s'entraîner
- Préparer la suite de votre apprentissage et conseils pour vos pentests
- Utiliser l'IA pour les tests d'intrusion
- Comprendre l'ingénierie sociale et lancer une campagne de Phishing ciblée

Suivi et évaluation

Exécution de l'action

Les moyens permettant de suivre l'exécution de l'action sont :

☑ *Relevés de connexion de la plateforme*
☑ *QCM et évaluations formatives*
☑ *Évaluation des acquis en fin de session*

Les résultats, les relevés de connexions et le suivi pédagogique et technique sont enregistrés nominativement.

Modalités d'évaluation des résultats (ou d'acquisition des compétences)

Les moyens mis en place pour déterminer si le stagiaire a acquis les connaissances ou les gestes professionnels précisés dans les objectifs sont :

☑ *Questions orales ou écrites (QCM)*
☑ *Travaux à rendre sur la plateforme*
☑ *Évaluation finale*

Programme de Formation

Évaluation finale et Sanction de la formation :

Certification Réaliser des tests d'intrusion (Sécurité Pentesting) enregistrée à France Compétences sous le numéro RS6092 le 29/09/2022. L'examen a lieu pendant les 15 derniers jours de la formation, en ligne et à distance sur la plateforme cyberini.com. Il s'agit d'une mise en situation professionnelle en temps limité et d'une durée de 4H à partir d'un besoin exprimé ou généré. Réalisation d'un mini projet dans le cadre d'une étude de cas.

Après l'étude de cas de 4 heures, le candidat présentera un rapport au jury qu'il défendra à l'oral durant un temps maximum de 1H30 en détaillant la méthode, les outils choisis ainsi que les contre-mesures adéquates vis-à-vis des menaces et vulnérabilités identifiées lors de son pentest. Une grille d'évaluation est complétée par le jury avec un score minimal de 70/100 pour la validation de l'ensemble des compétences de la certification.

Un jury organisé par le certificateur sous 3 mois décidera enfin de la délivrance de la certification. Équivalences, passerelles et suite de parcours : N/A.

Cette certification atteste l'acquisition de l'ensemble des compétences indispensables afin d'effectuer des tests d'intrusions, consistant à examiner l'ensemble du système d'information en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail. L'examen de certification est inclus dans la formation, il se déroule sur la plateforme de l'organisme de formation Cyberini. Le stagiaire s'engage à le réaliser en ligne lorsqu'il a terminé sa formation. La planification à l'examen s'effectue à partir du démarrage de la formation (délai examen prévisionnel : 1 à 15 jours après la formation). L'examen dure 4h suivi d'une soutenance orale de maximum 1h30 en visio devant un jury. L'examen est dispensé en français. La surveillance est faite par un logiciel et est enregistrée à des fins de contrôle de conformité. Un accès à Internet ainsi qu'un ordinateur compatible et équipé d'une webcam et d'un micro sont requis. Une fois l'examen réalisé, le candidat reçoit par e-mail une confirmation de passage.

Compétences attestées :

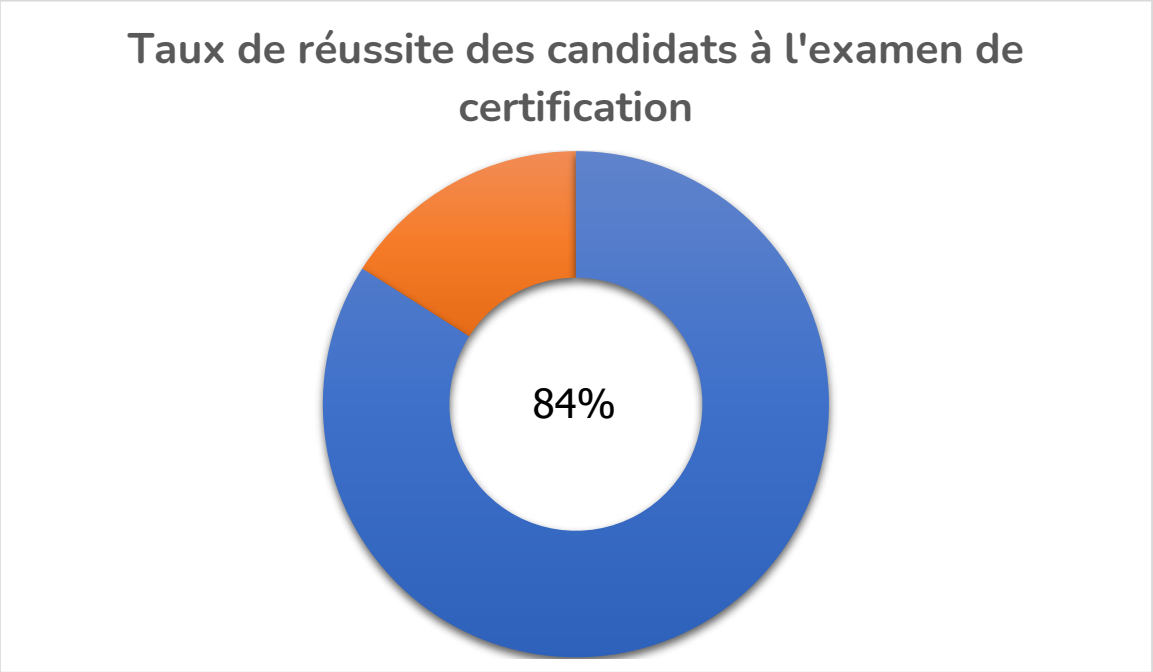
- Définir les enjeux et contraintes du test d'intrusion dans l'objectif de définir les scénarios les plus probables ainsi que l'obtention du consentement légal
- Appliquer une méthodologie de test d'intrusion clair et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches
- Concevoir et réaligner des outils d'intrusions dans l'objectif de répondre aux différents besoins d'un test d'intrusion
- Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d'intrusions évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l'organisation
- Remonter et restituer les différentes vulnérabilités identifiées ainsi qu'un plan d'action contenant les mesures de sécurité permettant à l'organisation de corriger ses failles

Le référentiel de compétences et d'évaluation est accessible sur la page France compétences : https://www.francecompetences.fr/recherche/rs/6092/

Date version document : 14/06/2025

Programme de Formation

UNE FORMATION ET DES RÉSULTATS



Taux de réussite entre octobre 2024 et juin 2025. Plus de 8 candidats sur 10 réussissent leur examen

- Les candidats obtiennent en moyenne **8/10** à l'oral (qui compose 30% du score final)
- Le plus haut score final est **100/100** et le plus bas est **44/100 pour un score moy. de 73/100**
- Les examens blanc et officiel sont **inclus sans frais supplémentaires avec la formation**
- **Un rattrapage est disponible pour les candidats qui échouent**
- Les candidats ont noté cette formation **4.84/5 sur le CPF entre octobre 2024 et juin 2025**

☑ **REJOINDRE CYBERINI C'EST OPTER POUR DES RÉSULTATS ET DES DÉBOUCHÉS**

▸ Cliquez ici pour rejoindre la formation

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France

Date version document : 14/06/2025

Programme de Formation

CRITÈRES QUALITÉ

Cyberini© dispose d'une charte qualité avec **4 engagements** :

1. L'adaptation de la formation au stagiaire
2. L'application des compétences dans le monde réel
3. La satisfaction du client
4. L'amélioration continue

Cyberini© est un centre de formation spécialisé en cybersécurité. Découvrez plus d'informations sur Cyberini dans la page « À propos »

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

ACTIVATEUR [N] FRANCE NUM

ACN Alliance pour la confiance numérique

FRANCE compétences CERTIFICATION enregistrée au Répertoire spécifique

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France