Ref. formation 202312209733

Cybersécurité et Pentesting : Intrusion, Hacking, et Protection Contre les Hackers et Virus

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

EVOLUTION5
Jean-Denis Coindre
06.29.78.66.25
contact@evolution5.fr

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Dossier

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Aucune

Prérequis pédagogiques :

Cette formation est accessible à tous, même sans expérience préalable en cybersécurité. À la fin, vous aurez acquis les compétences nécessaires en sécurité informatique, systèmes, réseaux et infrastructures pour atteindre les prérequis nécessaires pour passer les examens. Une connaissance de base en informatique, une aisance sous Windows, ainsi que la maîtrise des outils courants (bureautique, gestion de fichiers, navigation web) sont recommandées. La formation vous accompagnera pour acquérir ces compétences de manière progressive.

Contrat de professionnalisation possible ?

Non

Objectif de la formation

• Définir les enjeux du test d'intrusion. • Identifier les scénarios d'attaque probables. • Appliquer une méthodologie reproductible. • Concevoir et adapter les outils d'intrusion. • Réaliser les phases du test d'intrusion. • Analyser les failles de sécurité. • Exploiter les vulnérabilités détectées. • Proposer un plan d'action correctif. • Rédiger un rapport de Penteste. • Défendre les résultats à l'oral.

Contenu et modalités d'organisation

Module 1 : Introduire le Pentesting et la Sécurité Informatique • Contexte et objectifs du test d'intrusion. • Présentation des enjeux légaux et éthiques. • Introduction à la méthodologie générale du Pentesting. Module 2 : Définir les bases des tests d'intrusion • Identifier les objectifs du test d'intrusion (C.1.1 / E.1). • Identifier les contraintes du test d'intrusion (C.1.1 / E.1). • Définir les scénarios d'attaque probables. • Comprendre les contraintes légales et techniques. Module 3 : Comprendre les environnements informatiques • Analyser les réseaux et systèmes (C.1.1). • Vue d'ensemble des architectures réseau et des systèmes d'exploitation. • Identifier les surfaces d'attaque potentielles. Module 4 : Appliquer les méthodologies et standards des tests d'intrusion • Appliquer une méthodologie basée sur les étapes de la killchain (C.1.2 / E.2). • Utiliser les outils adaptés (C.1.2 / E.2). • Évaluer le niveau de sécurité d'un SI (C.1.2 / E.2). • Introduction à OWASP, NIST et autres standards de tests. Module 5 : Planifier un test d'intrusion • Préparer les outils et scénarios de test. • Étudier les vecteurs d'attaque : réseaux, applications, systèmes. • Planifier les phases du test d'intrusion. Module 6 : Utiliser les outils d'intrusion pour le scanning et l'énumération • Présentation des outils de scanning (Nmap, OpenVAS, etc.) (C.1.3 / E.3). • Déterminer des failles potentielles (C.1.3 / E.3). • Réajuster les outils d'intrusion selon les besoins (C.1.3 / E.3). • Classifier la criticité des failles (C.1.3 / E.3). Module 7 : Exploiter les failles identifiées • Exploiter les failles identifiées (C.1.4 / E.4). • Exploiter différents systèmes (C.1.4 / E.4). • Attaquer des systèmes critiques (C.1.4 / E.4). Module 8 : Analyser les vulnérabilités détectées • Identifier les vulnérabilités critiques (C.1.4). • Utiliser les résultats de l'exploration pour affiner les tests. • Introduction aux outils d'analyse de vulnérabilité (Metasploit). Module 9 : Exploiter les vulnérabilités de manière avancée • Réajuster les outils d'intrusion selon les besoins (C.1.3). • Utilisation d'exploits spécifiques pour différents systèmes. • Introduction aux attaques sur les réseaux sans fil. Module 10 : Effectuer la post-exploitation et maintenir l'accès • Techniques pour maintenir un accès persistant (C.1.4). •

…

Parcours de formation personnalisable ? **Oui** **Type de parcours** **Mixte**

Validation(s) Visée(s)

Réaliser des tests d'intrusion (Sécurité Pentesting) - *Sans niveau spécifique*

MON COMPTE FORMATION Éligible au CPF

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00425135	du 01/01/2024 au 31/12/2024	Mérignac (33)	EVOLUTION5		MON COMPTE FORMATION	FPC
00532275	du 01/01/2025 au 31/12/2025	Mérignac (33)	EVOLUTION5		MON COMPTE FORMATION	FPC