Ref. formation 202312209733

Cybersécurité | Pentesting – Détection d'intrusion

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 :

• Etre sensibilisé à la Cybersécurité • Savoir naviguer sous Windows • Savoir installer un logiciel

Contrat de professionnalisation possible ?

Non

Objectif de la formation

• Acquérir une compréhension approfondie des concepts de pentesting. • Étudier les principes de base de la détection d'intrusion. • Élaborer une stratégie de pentesting en fonction des besoins. • Préparer l'environnement pour une détection d'intrusion efficace. • Utiliser des outils de scan pour identifier les vulnérabilités. • Interpréter les résultats des scans et prioriser les failles. • Mettre en œuvre des attaques pour évaluer la résistance du système. • Documenter les résultats des attaques pour une analyse approfondie. • Explorer des méthodes avancées de détection d'intrusion. • Appliquer des outils et des technologies pour surveiller les activités suspectes.

Contenu et modalités d'organisation

Module 1: Comprendre les Fondements du Pentesting et de la Détection d'Intrusion Acquérir une compréhension approfondie des concepts de pentesting. Étudier les principes de base de la détection d'intrusion. Module 2: Planifier et Préparer une Séance de Pentesting Élaborer une stratégie de pentesting en fonction des besoins. Préparer l'environnement pour une détection d'intrusion efficace. Module 3: Conduire des Scans de Vulnérabilité Utiliser des outils de scan pour identifier les vulnérabilités. Interpréter les résultats des scans et prioriser les failles. Module 4: Réaliser des Attaques Simulées de Pentesting Mettre en œuvre des attaques pour évaluer la résistance du système. Documenter les résultats des attaques pour une analyse approfondie. Module 5: Utiliser des Techniques de Détection d'Intrusion Avancées Explorer des méthodes avancées de détection d'intrusion. Appliquer des outils et des technologies pour surveiller les activités suspectes. Module 6: Analyser les Logfiles et les Alertes de Sécurité Examiner les logs générés par les systèmes pour détecter des anomalies. Répondre aux alertes de sécurité de manière proactive. Module 7: Développer des Scénarios de Simulation d'Attaque Créer des scénarios réalistes pour simuler des attaques. Évaluer la capacité de détection du système face à différentes menaces. Module 8: Utiliser des Outils Automatisés de Pentesting Intégrer des outils automatisés pour accroître l'efficacité du pentesting. Adapter les résultats des outils à une analyse approfondie. Module 9: Mettre en Place une Stratégie de Détection d'Intrusion Proactive Élaborer une stratégie proactive pour anticiper les intrusions. Intégrer des mécanismes de détection en temps réel. Module 10: Réaliser une Analyse Post-Intrusion Mener une analyse approfondie après une intrusion simulée. Documenter les leçons apprises et recommandations pour renforcer la sécurité. Nous pouvons adapter et personnaliser le programme en fonction de vos besoins par des compléments. N'hésitez pas à nous contacter pour ajuster le programme de votre formation !

Durées de la formation ***30h en FOAD**
Parcours de formation personnalisable ? **Oui** Type de parcours ***Non renseigné***

Validation(s) Visée(s)

> Attestation de fin de formation

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	(33)	EVOLUTION5		Non éligible	FPC
00532275	du 01/01/2025 au 31/12/2025	(33)	EVOLUTION5		Non éligible	FPC