

Hacking et Sécurité – Les fondamentaux

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Outils

Rubrique : Fortinet - Shibboleth

Code de formation : SO001

€ Tarifs

Prix public : 2990 €

Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.

Le dispositif FNE-Formation.

L'OPCO (opérateurs de compétences) de votre entreprise.

France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

CPF -MonCompteFormation

Contactez nous pour plus d'information : contact@aston-institut.com

PRÉSENTATION

Objectifs & compétences

Comprendre comment il est possible de s'introduire frauduleusement sur un système distant

Savoir quels sont les mécanismes en jeu dans le cas d'attaques système

Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes

Public visé

Consultants en sécurité

Ingénieurs / Techniciens

Administrateurs systèmes / réseaux

Toute personne intéressée par la pratique de la sécurité

Pré-requis

Connaissances de Windows ou Linux

📍 Lieux & Horaires

Campus : Ensemble des sites

Durée : 28 heures

Délai d'accès : Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

Distanciel possible : Oui

PROGRAMME

Le programme

1 - Introduction sur les réseaux

Prise d'informations (Prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants)

Informations publiques

Localiser le système cible

Énumération des services actifs

2 - Attaques à distance

Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants, et prise de contrôle des postes utilisateurs par troyen

Authentification par brute force

Recherche et exploitation de vulnérabilités

Prise de contrôle à distance

3 - Attaques systèmes

Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion

Attaque du Bios

Attaque en local

Cracking de mot de passe

Espionnage du système

4 - Sécuriser le système

Outils de base permettant d'assurer le minimum de sécurité à son S.I.

Cryptographie

Chiffrement des données

Détection d'activité anormale

Initiation à la base de registre

Firewalling

Anonymat

📅 Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

■ 19 / 05 / 2025

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 28 heures

📅 : 4 jours

■ 28 / 07 / 2025

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 28 heures

📅 : 4 jours

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

Pendant la formation : mises en situation, autodiagnosics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.

Assiduité : certificat de réalisation.

Validations des acquis : grille d'évaluation des acquis établie par le formateur en fin de formation.