Hacking et sécurité : expert

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 : SO003

PRÉSENTATION

Objectifs & compétences

Savoir protéger son système d'information
Comprendre comment sécuriser tous les aspects d'un SI : réseau, applicatifs et Web
Acquérir les connaissances et compétences nécessaires pour détecter des failles et mettre en oeuvre des parades
Savoir correctement réagir en cas d'attaque soudaine
Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Public visé

Développeurs
Administrateurs systèmes / réseaux
Ingénieur sécurité
Consultant sécurité

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes

PROGRAMME

Le programme
1 - Introduction
Définition du hacking
Panorama 2018/2019
Référentiel de sécurité (ANSSI, ENISA, CLUSIF, Cybermalvaillance.gouv etc...)
Les différents types de hackers
Les différents types d'attaques
Les différents outils utilisés par le hacker
Le cycle de l'attaquant
2 - Le Hacking
Scan de réseau/ports/versions
Exploitation de CVE
Élévation de privilège
Mise en place d'une backdoor
Récupération d'informations, création d'un dictionnaire + Bruteforce
Payload msfvenom MITM
Saut de VLAN (yersinia et/ou table overflow)
3 - Les piliers de la sécurité
Confidentialité
Intégrité
Disponibilité
Traçabilité
4 - Les grands principes de la sécurité
IAAA
Authentification
Need to know
Least Privilege
Non répudiation
Défense en profondeur

€ Tarifs

Prix public : 3890 €

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

Lieux & Horaires

Campus : Ensemble des sites

Durée : 35 heures

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

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 12 / 05 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 35 heures
  : 5 jours
- 21 / 07 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 35 heures
  : 5 jours
- 29 / 09 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 35 heures
  : 5 jours
- 08 / 12 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 35 heures

Informations non contractuelles - PDF généré le 27/04/2025

5 - La sécurité physique
Notion de sécurité physique
Mise en correspondance des notions avec les principes précédents
6 - Sécuriser le réseau
La sécurité de la couche 2 : Port security, vLlan, Ssh, dhcp snooping, Defense contre arp MITM, Sécurité pour DTP,CDP,VTP,STP.
La sécurité de la couche 3 : IPSec, routeur filtrant
La sécurité de la couche 4 : Explication de la passerelle d'interconnexion de l'ANSSI, Travaux pratiques sur PFsense, explication des IDS/IPS , présentation de Snort, travaux pratiques sur Snort
La sécurité de la couche 5 : Le proxy
7 - Sécuriser le système
Hardenning sur Linux
Hardenning sur Windows
Mise en place d'HIDS
8 - Supervision de la sécurité
Présentation SOC
Présentation SIEM
Présentation de ELK et Splunk
Mise en place de ELK ou Splunk pour analyser les Logs
9 - Réponse à incident
Rejouer les attaques
Analyser les logs
Utiliser WireShark

: 5 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, autodiagnostics, 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'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 27/04/2025