Techniques de hacking & pentest avancées

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Sécurité offensive

Rubrique : Ethical Hacking - pentest

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 œuvre 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

Consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur, pentester.

Pré-requis

Avoir suivi le cours Techniques de hacking avancées Ref HS2 ou disposer des compétences équivalentes

PROGRAMME

Programme détaillé

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

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)

LES PILIERS DE LA SÉCURITÉ

Confidentialité Intégrité Disponibilité Traçabilité

LES GRANDS PRINCIPES DE LA SÉCURITÉ IAAA

Authentification Need to know Least Privilege Non répudiation
Défense en profondeur

LA SÉCURITÉ PHYSIQUE

Notion de sécurité physique Mise en correspondance des notions avec les principes précédents

Code de formation : HS3

€ Tarifs

Prix public : 4299 €

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

Durée : 35 heures

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

Prochaines sessions

Consultez-nous pour les prochaines sessions.

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

SÉCURISER LE SYSTÈME

Hardenning sur Linux Hardenning sur Windows Mise en place d'HIDS SUPERVISION DE LA SÉCURITÉ
Présentation SOC Présentation SIEM
Présentation de ELK et Splunk
Mise en place de ELK ou Splunk pour analyser les Logs

RÉPONSE À INCIDENT

Rejouer les attaques Analyser les logs Utiliser WireShark
Exemple de travaux pratiques Cf dans le descriptif de chaque section, les exercices sont précédés de TD (Travaux dirigés) ou de TP (Travaux pratiques)

Modalité d'évaluation des acquis Examen pour l'obtention d'un badge Analyse de malware ESD Academy

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.