

# Piratage éthique et contre-mesures – niveau perfectionnement

## 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

**Code de formation :** PECM2

## € Tarifs

**Prix public :** 3500 €

### 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](mailto:contact@aston-institut.com)

## PRÉSENTATION

### Objectifs & compétences

Utiliser le piratage éthique pour souligner les faiblesses du SI Identifier les contre-mesures à adopter Engager des actions préventives et correctives

### Public visé

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

### Pré-requis

Avoir des compétences en systèmes et réseaux Avoir suivi le cours Ref PECM1

## 📍 Lieux & Horaires

**Durée :** 35 heures

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

## PROGRAMME

### Programme détaillé

#### Jour 1

##### Section 1

Sécurité Wi-Fi Introduction Les normes et protocoles 802.11  
TD 1 / Analyse de flux avec wireshark Contexte de la sécurité Wi-Fi  
TD 2/ Présentation de la suite Aircrack-ng  
TD 3/ SSID Caché Etude des protocoles (WEP, WPA, WPS; ...)  
TD 4 / Attaque sur le protocole WPA2 Méthodes et attaques des réseaux sans fil

#### Jour 2

Contre-mesures et sécurisation (WIDS/802.1x)  
TD5 / Chellam

#### Jour 3

##### Section 2

Introduction aux applications Web  
Composants du web (Client/serveur, AJAX, DOM)  
Protocole HTTP(S)  
Présentation de l'outil Burpsuite  
TD 6 / Présentation de Burp suite

##### Section 3

Top 10 OWASP 2017 Injections (SQL, LDAP, code, etc)  
TD7 / Injection SQL manuelle et automatisée TP1/ Injection SQL

#### Jour 4

## 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

**Faiblesse d'authentification**

TD8/ Bruteforce avec burp suite Exposition de données sensibles  
TD9/ Exposition de donnée sensible  
TD10/ Recherche de fichier sensibles XML External Entities (XXE) Faiblesse des contrôles d'accès  
TD11/ IDOR / LFI / RFI / CSRF / VERB Mauvaise configuration de sécurité Cross-Site Scripting-XSS (Stored/Reflected/DOM Based)  
TD12 / Vol de cookie avec XSS TP4/ Exploitation XSS Désérialisation non sécurisée  
Composants vulnérables  
TD13 / Exploitation de composant vulnérable Logging et monitoring laxiste

**Jour 5****Section 4**

Fuzzing et Post-Exploitation Post-exploitation web (weeveily, webshell, ...)  
Fuzzing web (Payload, ZED, ...)  
TD11 / Présentation des outils de fuzzing

**Section 5**

Analyse et rapport Étude et analyse des résultats Mise en perspective des résultats  
Rédaction de rapport Restitution de livrables exploitable par un CODIR Recommandations, plan d'actions et suivi TP6 / Réalisation d'un test d'intrusion web Exemple de travaux pratiques  
TD 12/ Analyse de flux avec wireshark  
TD 13/ Présentation de la suite Aircrack-ng  
TD 14/ SSID Caché (voir le contenu du programme)  
Modalité d'évaluation des acquis Questions réponses, QCM ou Examen pour l'obtention d'un badge 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, 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.