

# Techniques de hacking & pentest – initiation

## 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 :** HS1

## PRÉSENTATION

### Objectifs & compétences

L'objectif de cette formation est de détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage, appliquer des mesures et des règles basiques pour lutter contre le hacking ainsi que de comprendre le mécanisme des principales attaques Cybers.

### Public visé

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

### € Tarifs

**Prix public :** 4049 €

### 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

## PRÉREQUIS

Posséder des bases dans la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

## 📍 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

### Jour 1 matin

Histoire et chiffres

Qu'est ce que la cybersécurité ?

Histoire de la cybersécurité Impacts suite à une cyber-attaque

Les types d'attaquants (White hat, ...)

Qu'est ce que le hacking ?

Les types d'attaques (Malware, MITM, SE, ...)

Les différentes phases d'une attaque (Cyber Kill-Chain)

Les métiers de la Cybersécurité

### 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

### Jour 1 après-midi

Les différentes lois & référentiels (PTES, OWASP, Article 323, Les normes ISO 27000, MITRE : ATT&CK, Scoring CVSS)

TD / Technique d'intrusion hardware (Bypass de sessions Windows et Linux)

### Jour 2 Matin

Reconnaissance passive & active Utilisation d'outils publics pour obtenir des informations sur une cible (Google Dorks, OSINT Framework, Social Engineering, Maltego..)

TP 1 / Reconnaissance passive d'une entreprise.

TD / Création de dictionnaire (Crunch, cupp.py, Top probable)

TP 2 / Technique d'attaque par dictionnaire

### Jour 2 après-midi

Présentation des outils de reconnaissance active (Nmap, Hping3) et leur signature (Wireshark)

Banner grabbing : Description des services d'une cible Présentation des outils d'analyse (NmapSE, Metasploit)

Analyse de vulnérabilités (Nessus, OpenVas, ExploitDB, CVE, CWE, CAPEC, NVD, ...) TP 3 / Récupération d'informations sur une infrastructure virtualisée

**Jour 3 Matin**

Attaques réseau Liste des protocoles les plus vulnérables  
Compréhension et utilisation des techniques de "l'homme du milieu" (MITM)  
Attaques sur les protocoles réseaux (IDLE Scan, LLMNR, WPAD, DoS, ARP, usurpation d'IP & MAC, DHCP, DNS)  
TP 4 / Mise en pratique des techniques MITM

**Jour 3 après-midi**

Description des Protocoles 802.11 et attaques associées TD / Evil-Twin, brute-force WPA2

Attaques web Présentation du TOP 10 OWASP  
Apprentissage et compréhension des injections  
Exploitation de failles Cross-Site Scripting (XSS)  
Exploitation des mauvaises configurations de sécurité  
Reconnaissance et utilisation des références directes non sécurisées à un objet

**Jour 4 Matin**

TD / Démonstration Injection et XSS Cross-Site Request Forgery (CSRF)

**Jour 4 après-midi**

Exploitation de vulnérabilités connues  
TP 5 / Challenge WEB client et serveur  
Exploitation Présentation et prise en main des frameworks offensifs (Metasploit, Empire)  
Recherche et obtention d'accès via une vulnérabilité identifiée  
TD / Utilisation de la faille "Eternalblue"

**Jour 5 Matin**

Création d'une charge (Payload)  
TP 6 / Création d'une charge malveillante  
Post-Exploitation TD / Démonstration du module Meterpreter

**Jour 5 après-midi**

Identification des modules de post-exploitation Pour aller plus loin...  
TP 7 / Création d'une persistance ou d'une porte dérobée sur une machine compromise  
Modalité d'évaluation des acquis : Examen pour l'obtention d'un Badge ESD Academy de Techniques de hacking Fondamentaux

**Documents :**

Supports Livret stagiaire : livret\_stagiaire\_techniquesdehackingfondamentaux.pdf Cahier d'exercice : cahier\_exercice\_techniquesdehackingfondamentaux.pdf Machines virtuelles : VM\_techniquesdehackingfondamentaux.ova

**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, autodiagnostic, 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.