# Techniques de hacking & pentest – perfectionnement

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Domaine :** Cybersécurité - sécurité informatique

**Filière :** Sécurité offensive

**Rubrique :** Ethical Hacking - pentest

**Éligible au CPF :** Non

**Action collective :** Non

## PRÉSENTATION

### Objectifs & compétences

Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes - Comprendre et expérimenter des techniques de hacking avancées Appréhender des méthodes offensives par la pratique.

### Public visé

### Pré-requis

Connaissances générales en système, réseau, développement, test d'intrusion, Active Directory, Powershell, scripting ou avoir déjà suivi une formation de type Techniques de hacking - fondamentaux. Ref HS1

## PROGRAMME

**Programme détaillé**

**Jour 1 Matin**

**Section 1**

2019 : Menaces sur les SI
Les Modèles SI (Questions, Cloud Privé, C2 : Command & Control)
Statistiques (Blocage des malwares par type de contenu, Domaines les plus difficiles à défendre,
Vulnérabilités / Attaques, Motivations) Failles Connues et 0day (exploit.in)
Étude des séquences d'exploitation

**Section 2 partie 1**

Préparation et initialisation des phases à l'exploitation Terminologie Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)

**Jour 1 après-midi**

**Section 2 partie 2**

Création de différents types de charges pour l'exploitation Intégrer de nouveaux Exploits dans Metasploit
Différents types de connexions (Bind, Reverse) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)
TP 1 / Prise en main des outils
Création et intégration d'un payload

**Jour 2 Matin**

**Section 3 partie 1**

**Code de formation :** HS2

### € 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

### 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.

Positionnement
Attaquant Externe Introduction sur les attaques externes
Social Engineering (Techniques de "Phishing", Clone de page d'authentification, SPF)
Fichier malicieux (Macros Office, PDF, HTML, APK, HTA,PS1, PY, Exe)
TP 2 / Clone d'une page d'authentification

**Jour 2 après-midi**

**Section 3 partie 2**

Recherche d'identifiants sur les bases de "Leak" Les attaques Cloud (Office 365, Azure, AWS)
Étude et exploitation réseaux Wi-Fi environnant
TD / Compréhension de menaces et attaques physique (Rubber Ducky, Bash Bunny, Packet Squirrel, Lan Turtle LAN/3G)

**Section 4 partie 1**

Positionnement
Attaquant Interne Introduction sur les attaques internes Analyse et compréhension des vulnérabilités protocolaires (DHCP, DNS, NTP etc…)

**Jour 3 matin**

**Section 4 partie 2**

Identification de vulnérabilités,
Tentative d'utilisation d'exploits communs
Zoom sur la vulnérabilité MS17-010 LLMNR & NBT-NS Poisoning (Étude et crack des hashes, Attaque par "Relais" SMB, Attaques de type "Man In The Middle")
TP 4 / Attaque de type relais LLMNR & NBT-NS

**Jour 3 après-midi**

**Section 5 partie 1**

Phases de Post-Exploitation
Enumération Post-Exploitation (Extraction des profils Wi-Fi, Récupération de certificats, Identification de fichiers intéressants par classification inversée)
Étude des différents processus d'authentification Microsoft (Kerberos, LAN Manager, Smart card) Gestion des identifiants en mémoire (NTLM, Kerberos, Digest SSP, TSPKG, LiveSSP)
Credential Guard & Device Guard Présentation des outils "Mimikatz et Kekeo"
Extraction des identifiants en mémoire,
Extraction des hashes de la base SAM, Extraction des identifiants stockés dans les applications)
TP 5 / Lister différentes techniques d'utilisation de l'outil Mimikatz sans que celui-ci ne soit détecté. Sélectionner la technique qui semble la plus efficace, expliquer pourquoi, et la mettre en pratique

**Jour 4 Matin**

**Section 5 partie 1**

Présentation d'un outil de base de données relationnelle (BloodHound) Pivoting (Accès aux ressources internes,
Accès aux réseaux restreints type "ICS" via le montage d'un proxy socks4a),
Zoom sur la sécurité des systèmes industriels
TP 5 / Cas d'étude : Collecter des données pour Bloodhound et identifier le plus court chemin vers un compte à hauts privilèges vs attaque ICS

**Jour 4 après-midi**

**Section 6**

Escalade des privilèges Verticale (Modification de démarrage, Exploits,GPP, Mauvaise configuration)
Escalade des privilèges Horizontale (Identification des accès locaux distants, Listing des permissions ACLs / AD,
Recherche des délégations de droits, Pass-the-hash, Pass-the-ticket, Psexec/PsSession)
TP 6 / Cas d'étude : Atteindre le compte précédemment identifié via les différentes techniques enseignées (cf. TP 5)

**Section 7**

Persistance  Golden Ticket / Silver Ticket Skeleton Key Délégation Kerberos contrainte / Non-contrainte DCSync DCShadow AdminSDHolder WMI/COM DSRM

**Jour 5 matin**

**Section 8**

Autres techniques  Évasion des systèmes de défense (Sécurité Powershell et techniques de contournement,
Évasion des systèmes antivirus,
Obfuscation de code avec Powershell, AMSI Bypass, Applocker Bypass)

**Jour 5 après-midi**

TP 7 / Cas pratique :
Trouver un moyen d'exécuter un script powershell dans un environnement sécurisé
Bonus : Pentester Tips  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 ESD Academy de Techniques de hacking avancées.  Support :  Livret stagiaire : livret_stagiaire_techniquesdehackingavancees.pdf Cahier d'exercice : cahier_exercice_techniquesdehackingavancees.pdf Machines virtuelles : VM_techniquesdehackingavancees.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, 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.