Formation « Hacking et Cybersécurité »

Format	Formation à distance - 12 heures
Dates	2 sessions possibles
	Jeudi 28 et vendredi 29 mai de 9h à 17h
	Lundi 1er au Jeudi 4 juin de 17h à 20h
Tarif	790 €

Objectifs pédagogiques

▶ La formation Hacking et Cybersécurité a pour objectif de vous aider à détecter des menaces dans la configuration informatique de votre organisation.

<u>Les compétences cibles :</u>
Vous serez capable :
- D'identifier les principales menaces
- D'appréhender l'aspect humain de la sécurité
- De mettre en œuvre un environnement de test
- De pratiquer des tests de pénétration

Programme détaillé

Module 1 : Menaces sur les organisations

Au travers de l'étude de trois cas réels de cyberattaques, le participant apprendra à déterminer les faiblesses et les éléments de prévention face aux risques.
Thèmes abordés :

- Risques, menaces, vulnérabilités et criticités
- Advanced persistent threat
- Arnaque au président
- Crypto-locker et autres vulnérabilités
- Matrice de chaleur

Module 2 : Social Engineering

Par la compréhension des mécanismes du cerveau, le participant apprendra quelles méthodes peuvent utiliser des hackers pour étudier une cible et prendre son contrôle (manipulation)

Thèmes abordés :

- Cerveau triunique selon MacLean
- Quatre secteurs de la connaissance selon Herrmann
- Triangle dramatique de Karpman
- Biais cognitifs
- Recueil d'informations avec Maltego
- Google hacking

Module 3 : Créer son environnement de « hacker éthique »

Le participant apprendra à créer une clef usb bootable, fonctionnant sur mac ou pc, permettant de démarrer un système d'exploitation dédié au hacking.

Thèmes abordés :

- Kali Linux et Parrot OS
- Créer une clef usb amorçable
- Créer un environnement de test sur son ordinateur
- Tester le Wifi

Module 4 : Tests de vulnérabilité

Dans le respect du cadre légal, le participant apprendra à créer une stratégie simple d'évaluation de la sécurité du système d'information de son organisation.

Thèmes abordés :

- Recueil passif et actif d'informations
- Détecter les IDS/IPS
- Vulnérabilités avec nmap
- Exploiter les failles avec metasploit

- Accès à des ressources complémentaires pour affiner ses nouvelles compétences

Formateur : Miguel LIOTTIER

Enseignant-chercheur en **Management et SI, Miguel LIOTTIER est titulaire d'un** Doctorat en Sciences de Gestion
Domaines d'enseignement :Systèmes décisionnels, Machine learning, Neurosciences et cyber-sécurité.
Domaines de recherche :Traduction des principes de la République française dans la communication des Start-up bénéficiant d'un financement d'Etat, Résilience d'une organisation face aux tentatives de déstabilisation : le cas de la France face aux attentats de 2015.
Publication : **Miguel LIOTTIER** est co-auteur de nombreux ouvrages de référence, comme « Management des systèmes d'information » (Dunod, 2020) et « Survivre à une cyberattaque » (VA Press, Versailles, 2018).

▶ **Pour plus d'information :**

Olivier Baudin, Responsable de la Formation continue :
Tèl. : O1 40 53 74 34
Mail : obaudin@iscparis.com