

- *Comprendre comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables*
- *Identifier les « faiblesses » des éléments constitutifs du SI par des prises d'empreintes*
- *Disposer des compétences techniques nécessaires pour réaliser différentes attaques et ainsi en comprendre les subtilités*
- *Être en mesure de protéger le SI par un système de contre-mesures adaptées*

5**Prix : 3,475 €€ / HT****OUTILS PÉDAGOGIQUES****MODALITÉS D'ÉVALUATION****MODALITÉS DE FINANCEMENT****MODALITÉS ET DÉLAIS D'ACCÈS****OBJECTIFS PÉDAGOGIQUES****ACCESSIBILITÉ****LES POINTS FORTS DE LA FORMATION****PRÉ-REQUIS**

- Connaissances de l'administration de postes Windows ou Linux
- Connaissance de TCP/IP
- La maîtrise de Linux en ligne de commande est un plus

MODALITÉS ET DÉLAIS D'ACCÈS**ATTESTATION OBTENUE****EFFECTIF DE LA FORMATION****CERTIFICATION****MODALITÉ PÉDAGOGIQUE**

Cours dispensé en mode présentiel avec une alternance d'apports théoriques et méthodologiques, et de mises en situations pratiques

PROCHAINES SESSIONS

Le 14/02/2022

Le 25/05/2022

Le 14/02/2022

Le 25/05/2022

Le 14/02/2022

Le 25/05/2022

PROGRAMMES DE HACKING ET SÉCURITÉ – NIVEAU AVANCÉ**INTRODUCTION**

- Rappels sur TCP/IP

INTRODUCTION À LA VEILLE

- Vocabulaire
- Base de données de vulnérabilité et exploitation

- Informations générales

PRISE D'INFORMATIONS

- Informations publiques
- Moteur de recherches
- Prise d'information active

SCAN ET PRISE D'EMPREINTE

- Énumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

VULNÉRABILITÉS INFORMATIQUES

- Vulnérabilités réseau
- Vulnérabilités applicatives
- Vulnérabilités web
- Exploitation des vulnérabilités
- Maintien de l'accès à une machine

ATELIER PRATIQUE EN LABORATOIRE

- Mise en oeuvre d'une stratégie d'attaque sur un laboratoire créé spécialement pour la formation
- Lancement de l'attaque et tentative d'exploitation
- Capture de drapeau
- Étude des contre-mesures appropriées