FORMATION: **Hacking et protection**

Date de mise à jour 30/01/2024 Version 1.3

REFERENCE: **LMSISecHack1**

TARIF INTER: **1800€/ht/session/participant soit 2160€/ttc**

TARIF INTRA: **3500€/ht soit 4200€/ttc (jusqu'à 6 personnes)**

Indicateur annuel de satisfaction 90% **Nombre de stagiaires ayant participés en 2023** 2

ACQUISITION DES COMPETENCES

OBJECTIFS DE LA FORMATION

-Acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques

-Déduire des solutions de sécurité avancées

A QUI S'ADRESSE CETTE FORMATION

PROFIL

Administrateurs de systèmes ainsi que les techniciens chargés du support mais également toute personne impliquée dans la sécurité du système d'information.

PRE-REQUIS

AUCUN

LES PLUS DE CETTE FORMATION

Cette formation permet de comprendre les risques informatiques pouvant impacter les entreprises, l'objectif est de mettre des actions devant des mots que l'on entend régulièrement, et qui habituellement reste abstrait.

MODALITES PEDAGOGIQUES

Présentation des concepts, apport du formateur, échange entre les participants, exercices.

La FOAD chez LMSI ne se contente pas de «dispenser» des cours.
Un réel suivi pédagogique est effectué grâce aux outils d'échange, ce qui permet un ajustement permanent des contenus à la nécessité des auditeurs.
«Chat», mail, forums privés avec le formateur, plages horaires de contacts téléphoniques, visio-conférence: tous les moyens nécessaires peuvent être mis en oeuvre pour que l'auditeur soit accompagné.
Avant le début de la formation le stagiaire n'a pas d'exercice à réaliser dans sa démarche d'apprentissage.
C'est un élément fondamental de réussite qui n'est jamais négligé.
La formation sera jalonnée de tp sur des machines qui sont mises à disposition et que le stagiaire pour prendre en main à distance via l'outil de visio conférence. Ces tp seront suivis par le formateur.
Les situations de handicap seront étudiés au cas par cas.

MOYENS DE FORMATION

Formateur expert du domaine, un ordinateur par personne

MODALITES DE REALISATION

Classe à distance (prévoir une connexion adsl 8Mb/s minimum) ou présentiel, la formation se déroule sur site chez le client.

MODALITES D'EVALUATION

Au cours de la formation, suivi du responsable de projet.
Evaluation écrite à l'issue de la formation où le participant donnera ses impressions par écrit et à l'oral.

NOTRE ENGAGEMENT QUALITE

ORGANISATION

DUREE

Cinq jours soit 35 heures

EFFECTIF

Minimum : 1 personne **Maximum : 6 personnes**

La session peut être annulée 48h avant la date de réalisation s'il n'y a qu'un seul participant, car pour nous la formation sécurité est aussi un moment de partage des bonnes pratiques entre les différents stagiaires.

SUIVI

Feuille d'émargement signée par ½ journée, évaluation de satisfaction et d'auto-évaluation stagiaire. Attestation de stage

INTERVENANT

Damien Lamy, intervient régulièrement dans diverses entreprises depuis plus de 10 ans, membre de la réserve citroyenne de cyberdéfense et l'auteur de la video Kali Linux aux éditions ENI, réalise des audits réseaux depuis 20 ans.

RESPONSABLE PEDAGOGIQUE ET ADMIN.

Damien LAMY 04 58 17 28 58 dlamy@lmsi.eu

Contact HANDICAP

Damien LAMY 04 58 17 28 58 dlamy@lmsi.eu

DATES DE FORMATION

Pour toute demande de calendrier adressez un mail formation@lmsi.eu en précisant le nom du stage.

CONTACT ET MODALITES D'INSCRIPTION

Pour s'inscrire à la formation ou recevoir des informations envoyer un mail à l'adresse formation@lmsi.eu en précisant le code de la formation.
Contact Lamy Damien 04 58 17 28 58

COORDONNES DE L'ORGANISME DE FORMATION

Lmsi sasu Capital 1000€ http://www.lmsi.eu
4502 route de hautecombe 73370 La Chapelle du Mont du Chat
Organisme de formation enregistré 84260258126
Siret: 817 999 709 00022 Code APE 6202A

FORMATION: **Hacking et protection**

Date de mise à jour 30/01/2024 Version 1.3

REFERENCE: **LMSISecHack1**

TARIF INTER: **1800€/ht/session/participant soit 2160€/ttc**

TARIF INTRA: **3500€/ht soit 4200€/ttc (jusqu'à 6 per-**

LES MODULES DE FORMATION

MODULE 1 - LA SSI (Jour 1 matin)

- Les menaces d'aujourd'hui
- Paysage de la sécurité
- Les normes
- La sécurité dans les entreprises françaises
- Le cycle d'une attaque

MODULE 2 - LA RECONNAISSANCE PASSIVE (Jour 1 apm)

- Découverte et recherche d'informations sensibles
- Le social engineering
- Google Dorks
- Maltengo

MODULE 3 - LA RECONNAISSANCE ACTIVE (Jour 2)

- Découverte des réseaux
- Découverte des port
- Découverte des OS
- Découverte des vulnérabilités

MODULE 4 - LES ATTAQUES WEB (Jour 3)

- Découvrir une vulnérabilité sur un serveur Web
- Le top 10 de l'OWASP
- Injection de commande et injections SQL
- Cross-site scripting et cross-site request forgery
- File inclusion et file upload

MODULE 5 - LES ATTAQUES RESEAU (Jour 4)

- L'écoute passive
- Attaques « Man in the middle »
- Les protocoles vulnérables
- L'ARP poisoning
- Outillage : Ettercap et MITMF

MODULE 6 - POST EXPLOITATION (Jour 5)

- Rechercher une vulnérabilité
- Exploiter une vulnérabilité
- Outils Metasploit