

## Formation Ethical Hacking - Les fondamentaux de la sécurité informatique

<b>Durée :</b>	2.0 jour(s)
<b>Objectifs :</b>	<ul style="list-style-type: none"> <li>• Découvrir la cybersécurité.</li> <li>• Identifier les attaques sur un SI.</li> <li>• Définir l'impact et la portée d'une vulnérabilité.</li> <li>• Savoir intégrer les outils de sécurité de base.</li> </ul>
<b>Public :</b>	<ul style="list-style-type: none"> <li>• RSSI - Ingénieurs / Techniciens - Administrateurs systèmes / réseaux.</li> <li>• Toute personne s'intéressant à la sécurité informatique.</li> </ul>
<b>Prérequis :</b>	<ul style="list-style-type: none"> <li>• Aucun.</li> </ul>
<b>Modalités et moyens pédagogiques</b>	<p>Démonstrations visuelles et pratiques à travers des exercices d'application et/ou des cas concrets des stagiaires.</p> <p>Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran.</p> <p>Portail web: <a href="http://maformation.vaelia.fr">maformation.vaelia.fr</a></p>
<b>Modalités d'évaluation</b>	Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
<b>Moyens d'encadrement</b>	Un formateur expert spécialisé en Systèmes et Réseaux dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
<b>Satisfaction globale :</b>	<p>4.25/5</p> <p><i>Calculée à partir des évaluations stagiaires sur les 12 derniers mois.</i></p>

## Jour 1

### Ethical Hacking : Introduction

- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

### Prise d'information

- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

### Réseau

- Rappels modèles OSI et TCP/IP
- Vocabulaire
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing
- ARP Cache Poisoning
- DoS / DDoS

### Attaques locales

- Cassage de mots de passe
- Elévation de privilèges
- Attaque du GRUB

## Jour 2

### Ingénierie sociale

- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing
- Outils de contrôle à distance

### Attaques à distance

- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaques d'un poste client
- Attaque d'un serveur
- Introduction aux vulnérabilités Web

### Les mises à jour

- Configurations par défaut et bonnes pratiques en cybersécurité
- Introduction à la cryptographie
- Présentation de la stéganographie
- Anonymat (TOR)