

Formation Ethical Hacking V13

Présentation

Cette formation en Ethical Hacking V13 couvre l'introduction au piratage éthique, l'empreinte numérique, l'analyse des réseaux, l'énumération, l'analyse des vulnérabilités, et le piratage de systèmes. Elle inclut également des modules sur les menaces liées aux logiciels malveillants, l'écoute réseau, l'ingénierie sociale, et bien plus encore pour une compréhension complète et appliquée.

Durée : 35,00 heures (5 jours)

Tarif INTRA : [Nous consulter](#)

Objectifs de la formation

- Comprendre les fondamentaux du piratage éthique et les concepts de cybersécurité.
- Acquérir des compétences pratiques pour identifier, analyser et exploiter les vulnérabilités des systèmes.
- Maîtriser les techniques de reconnaissance, de scanning et d'énumération pour évaluer la sécurité des réseaux.
- Apprendre à détecter et à prévenir les attaques courantes telles que l'injection SQL, le déni de service et l'ingénierie sociale.
- Explorer les menaces liées aux logiciels malveillants, aux réseaux sans fil, aux plateformes mobiles et aux objets connectés (IoT).
- Découvrir les méthodes pour sécuriser les serveurs web, les applications et les environnements cloud.
- Comprendre les principes de la cryptographie et son rôle dans la protection des données.

Prérequis

- Connaissances de base en informatique et en réseaux (protocoles TCP/IP, architecture des systèmes).
- Familiarité avec les systèmes d'exploitation (Windows, Linux).
- Notions de programmation (Python, Bash, etc.) pour automatiser des tâches et comprendre les scripts.



- Aucune expérience préalable en piratage éthique n'est nécessaire, mais une curiosité pour la cybersécurité est un atout.

Public

- Professionnels de l'informatique souhaitant se spécialiser en cybersécurité.
- Administrateurs systèmes et réseaux désireux de renforcer la sécurité de leurs infrastructures.
- Développeurs web et applicatifs cherchant à comprendre les vulnérabilités courantes.
- Étudiants en informatique ou en cybersécurité voulant acquérir des compétences pratiques.
- Toute personne intéressée par le piratage éthique et la protection des systèmes d'information.

Programme de la formation

- 1/ Introduction au piratage éthique**
- 2/ Empreinte numérique et reconnaissance**
- 3/ Analyse des réseaux**
- 4/ Énumération**
- 5/ Analyse des vulnérabilités**
- 6/ Piratage de systèmes**
- 7/ Menaces liées aux logiciels malveillants**
- 8/ Écoute réseau (sniffing)**
- 9/ Ingénierie sociale**
- 10/ Attaques par déni de service**
- 11/ Détournement de session**
- 12/ Contournement des IDS, pare-feux et honeypots**
- 13/ Piratage de serveurs web**
- 14/ Piratage d'applications web**
- 15/ Injection SQL**
- 16/ Piratage des réseaux sans fil**
- 17/ Piratage des plateformes mobiles**
- 18/ Piratage des objets connectés (IoT) et systèmes opérationnels (OT)**
- 19/ Cloud computing**
- 20/ Cryptographie**

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.