Cybersécurité: Les fondamentaux techniques

Durée 2 jour(s) (SECU-FONDAMENTAUX)

Comprendre les principes fondamentaux de la cybersécurité

Description

La formation est mise au point et animée par l'équipe de pentesters de Zenika. Le contenu du cours comprend différentes thématiques fondamentales à la compréhension de l'univers cybersécurité. Cette formation est un moyen de se mettre dans la peau d'un attaquant et de comprendre comment des personnes malveillantes attaquent des réseaux internes. Notre objectif est de donner les clés à un public technique pour qu'ils puissent être à l'aise et comprendre au mieux les enjeux et menaces qui pèsent sur les systèmes d'informations. Plusieurs ateliers sont proposés sur les différentes thématiques permettant la mise en pratique des concepts abordés.

Objectifs

- Connaissance de la terminologie et des concepts cybersécurité
- Cartographie des services et des vulnérabilités associées
- Des connaissances générales sur la sécurité de l'information d'aujourd'hui et des menaces actuelles

Public

Tous profils technique

Prérequis

Pas de pré-requis.

Répartition

30% Théorie, 70% Pratique

Evaluations des acquis

L'évaluation des acquis de la formation se fera en séance au travers d'ateliers, d'exercices et/ou de travaux pratiques. Dans le cas d'une formation officielle éditeur, veuillez nous consulter afin que nous vous fassions part des modalités d'évaluation.

A l'issue de la formation, vous sera transmis une évaluation à chaud de l'action de formation qui vous permettra de nous faire part de vos retours quant à votre expérience apprenant avec Zenika.

Ressources pédagogiques

Les ressources pédagogiques proviennent de productions des équipes Zenika et/ou de la documentation éditeur dans le cas d'une formation "Officielle". Les documents sont en français ou en anglais.

RQTH et ma formation Zenika

Si vous êtes sujet à un handicap, prenez contact avec nos équipes pour que nous puissions définir ensemble comment nous pourrons aménager la session afin que vous puissiez vivre une expérience en formation inchangée.

Programme

Concept et terminologie

Réseau

- Rappel des modèles OSI et TCP/IP
- Étude de différents protocoles
- Attaque réseau (MITM, Déni de service)

Cartographie et scan de vulnérabilité

- Cartographie d'un réseau
- Découverte de vulnérabilités

Cryptographie

- Fondamentaux
- Chiffrement symétrique et asymétrique
- Certificat et PKI
- Gestion des secrets
- Attaque et sécurisation de services SSH

Pour aller plus loin

- DevSecOps
- Test D'intrusion
- Bonne pratiques de développement

Parcours

Développement sécurisé

Cybersécurité: Le DevSecOps par la pratique

Cybersécurité: Test d’intrusion