FORMATION
CYBERSECURITE OPERATIONNELLE

PRINCIPES DE LA CYBERSECURITÉ OFFENSIVE APPLIQUÉS AUX INFRASTRUCTURES INTERNES

DURÉE DE LA FORMATION : 3 jours (21 heures)

LIEU DE LA FORMATION : Sur site apprenant ou à distance

OBJECTIFS DE LA FORMATION

- Découvrir les méthodologies d'attaque pratiquée par un attaquant externe à l'entreprise
- Découvrir les bases de la sécurité informatique appliquées aux réseaux et services réseaux
- Appliquer la méthodologie d'un audit de sécurité
- Reproduire les principales attaques pouvant être réalisée sur une infrastructure interne

PREREQUIS : Connaissances en infrastructures informatique et réseaux

PRIX DE LA FORMATION : 800.00 EUR / Stagiaires

Ziwit SAS
SIRET 525202917 00049 | RCS B 525 202 917
40 Avenue Théroigne de Méricourt
34000 Montpellier, France

Site | www.ziwit.com
Mail | contact@ziwit.com
Téléphone | + 33 (0) 4 11 93 45 03
Fax | + 33 (0) 4 11 93 45 04

PROGRAMME DE FORMATION

1) Introduction à la cybersécurité offensive (4h)

I- Introduction à la cybersécurité et rappel des bases de connaissances (vocabulaire, outils, bonnes pratiques connues) – 1h
II- Atelier de formation : La vision de l'attaquant : pourquoi TPE ; PME et grands groupes sont victimes de cyberattaques – 1h
III- Principes de la cybersécurité offensive : Objectifs, étapes, méthodologie organisationnelle et aspects légaux d'un audit sécurité - 2h

2) Approfondir l'approche générale de la cybersécurité appliquée aux réseaux, systèmes et applicatifs internes (7h)

I- Définition d'un périmètre auditable
II- Sécurité des systèmes : standard, évaluation et bonnes pratiques
III- Sécurité des applications : Détection, exploitabilité et contre-mesures des failles

3) Cas pratique : Réalisation d'une simulation d'audit de sécurité sur périmètre infrastructure interne (10 heures)

I- Définition d'un périmètre d'audit
II- Présentation et simulation de différentes attaques (type ARP Spoofing, exploitation de service, failles applicatives...)
III- Réalisation d'un test d'intrusion sur une infrastructure exemple (Labs), et suivi d'une méthodologie pragmatique, parmi les éléments suivants (liste non exhaustive) :

a) - Scan de port (TCP et UDP) sur l'ensemble des adresses IP composants le périmètre
b) - Identification du type et de la version des services actifs

c) - Identification des noms de domaines associés aux services et équipements exposés

d) - Scan de vulnérabilités afin d'identifier les défauts de configuration et les vulnérabilités publiques liées aux versions des services ou composants logiciels identifiés

e) - Analyse des protocoles et des moyens d'authentification proposés par chaque service

f) - Énumération ou découverte (par brute force) des identifiants et mots de passe communs (ou par défaut) des services proposant une authentification (ex : SSH, VPN IPSec/SSL, Telnet, RDP, FTP, SNMP, Bases de données, Annuaires, . . .),

g) - Énumération découverte (par brute force) des répertoires et des interfaces d'administration des services web exposés,

h) - Analyse de la sécurité de la couche transport (Signature, protocoles, algorithmes de chiffrement autorisés, taille de clés, révocation ou expiration des certificats) des services web ou d'administration exposés ex : HTTPS, VPN IPSec ou SSL, SSH, . . .).

ORGANISATION DE LA FORMATION

Délais et modalité d'accès

1. Prendre contact avec nos experts et consultants par téléphone ou par mail : montpellier@ziwit.com / 01 85 09 15 09
2. Compléter le formulaire « Contactez-nous » (https://www.ziwit.com/fr/ziwit-academy)
3. Le délai d'accès est régi par l'agenda de l'organisme de formation (entre 2 et 8 semaines à réception du devis validé).

Localisation de la formation :

- En visio via les plateformes Teams, Zoom ou autres outils de partage d'écran
- En présentiel dans votre organisation, sur vos ordinateurs ou sur votre réseau via une machine virtuelle configurée à cet effet

Equipe pédagogique

L'équipe pédagogique est composée de hackers éthiques et formateurs ayant à minima 10 années d'expérience professionnelle en audit de sécurité et sécurité opérationnelles.

Les formateurs mobilisés pour cette formation sont :

- CV – Auditeur sécurité et pentester – Senior
- PC – Consultant en Sécurité des Systèmes d'Information spécialisé réseau – Senior
- MT – Consultant en Sécurité des Systèmes d'Information spécialisé architecture réseau - Senior

Moyens pédagogiques et techniques

- Accueil des stagiaires dans une salle dédiée à la formation et/ou à distance via visioconférence
- Présentation projetée au format PowerPoint dynamique (x 2 présentations powerpoint)

- Documentation pédagogique reprenant les concepts cités lors de la formation (x2 PDF)
- Présentation des concepts avant mise en pratique par des exercices en autonomie guidée par le formateur collectivement
- Alternance d'apports théoriques et nombreux exercices de mise en pratique
- Etude de cas concrets
- Echanges avec le formateur
- Mise à disposition en ligne de documents supports à la suite de la formation.

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

- Feuilles de présence.
- Questions orales et écrites (QCM).
- Mises en situation et réalisation d'un cas concret
- Formulaires d'évaluation de la formation (à chaud et à froid)
- Certificat de réalisation de l'action de formation (Attestation de formation professionnelle)

Nos formations sont ouvertes à tous. Si vous avez des besoins spécifiques, notamment liés à une situation de handicap, n'hésitez pas à nous contacter. Notre équipe vous accueillera et se tient prête à répondre à vos besoins