

ÉVALUER VOTRE NIVEAU DE SÉCURITÉ : TESTS D'INTRUSIONS ET AUDIT TECHNIQUE

IRE32

3 jours (21h) 1 785,00 €^{HT}

Objectifs

Connaître l'approche et la méthodologie utilisés pour les tests d'intrusion • Appréhender la démarche d'un audit technique dans un environnement Windows et Linux • Se familiariser avec les outils et framework d'attaque et d'audit • Apprendre à rédiger le livrable associé et préparer la réunion de restitution

Profil Stagiaire(s)

ingénieurs réseaux-télécoms, personnes impliquées dans la vérification de la sécurité d'un site web ou d'un réseau informatique souhaitant connaître les fondamentaux du test d'intrusion

Pré-requis

fortes compétences réseaux et systèmes Windows et Linux

Profil Animateur(s)

consultant et expert en sécurité, nos animateurs, interne au sein d'un grand groupe ou consultant d'un cabinet SSI, exercent depuis plus de 15 ans dans la sécurité des Systèmes d'Information



PROGRAMME

Introduction

Introduction à la méthodologie sur les Tests d'Intrusion (TI)
Présentation / Installation du Labo du Hacker éthique

Pénétrer les réseaux Wifi et réaliser des écoutes et rejeux réseaux

LAB-1 : Attaques des réseaux sans-fil (Wifi, ...)

LAB-2 : Attaques et intrusion sur des réseaux filaires (écoute, modification et rejeu)

Étudier les différentes techniques d'attaques en déni de service (D)DoS

LAB-3 : Attaques en déni de services (flood, slow attack, reflexion, amplification, ...)

Techniques d'attaque d'un système industriel

LAB-4 : Attaques d'un système industriel (automates, Scada, ..)

LAB-5 : Attaques utilisant différentes techniques d'ingénierie sociale

Attaques distantes sur les couches systèmes et applicatives

LAB-6 : Recherche de vulnérabilités et intrusion au niveau du système

LAB-7 : Recherche de vulnérabilités et intrusion au niveau applicatif (Web)

Attaques locale et élévation de privilège

LAB-8 : Boot via un media externe

LAB-9 : Recherche de vulnérabilités Windows

LAB-10 : Déverrouillage de session Windows

Audit technique boîte blanche des systèmes Windows et Linux

LAB-11 : Audit Technique (Windows + Linux)

Comment formaliser les résultats d'audit dans un rapport et préparer la restitution au Client

Présentation de rapports de Tests d'Intrusion

Présentation du contenu de la réunion de restitution « client »

Conclusion

Contactez-nous

Conseiller formation
09 88 66 10 00
inscriptions@demoss.fr

ÉVALUER VOTRE NIVEAU DE SÉCURITÉ : TESTS D'INTRUSIONS ET AUDIT TECHNIQUE

IRE32

3 jours (21h) 1 785,00 €^{HT}

Méthode pédagogique

Cette formation Sécurité SI est rythmée par une alternance d'exposés et de travaux pratiques et utilise entre autres les outils fournis dans les distributions Backtrack / Kali et notamment le framework Metasploit

Supports visuels et documentaires en français.

Documents remis à chaque participant :

Supports de cours

Rapport de test d'intrusion type

Cette formation Sécurité SI est susceptible d'être modifiée en cours d'année, les dates et les prix pourront évoluer

Les sessions "A distance" sont réalisées avec l'outil de visioconférence Teams, permettant au formateur d'adapter sa pédagogie.

Moyens pédagogiques et techniques de mise en œuvre

Nos formateurs DEMOS sont recrutés conformément aux spécifications mentionnées pour chaque formation. Ce sont des professionnels en activité et/ou des experts dans leur domaine.

Ils utilisent des méthodes et outils appropriés aux formations qu'ils dispensent et adaptent leur pédagogie au public accueilli.

Par ailleurs, nos centres de formation DEMOS sont tous équipés :

- Salles de formation lumineuses, spacieuses, design, ergonomiques, mobiles et équipées d'écrans plasma, de PC portables/fixes si nécessaire à la formation suivie.
- Accès au wifi haut débit sur l'ensemble des lieux
- Espace de co-learning et webcorners
- Cafés, collations et rafraîchissement sont offerts

Et tous sont accessibles aux personnes à mobilité réduite

Le dispositif de suivi et d'évaluation

Pour assurer un suivi individuel, Demos a mis en place 2 types d'évaluation :

- Des évaluations des acquis en cours et en fin de formation

Elles peuvent être faites de différente manière selon le contenu de la formation suivie :

Quiz, exercice pratique, étude de cas, jeu de rôles, mise en situation, soutenance devant un jury pour les formations à finalité certifiante.

- Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

En complément

Avant cette formation vous pouvez suivre :

-