AVANCÉ

FORMATION PENTEST

TEST D'INTRUSION : MISE EN SITUATION D'AUDIT

Le test d'intrusion (pentest) par la pratique

Code : TEST-INT

Vous effectuerez un test d'intrusion : des tests techniques jusqu'à la réalisation du rapport. Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type test d'intrusion (pentest) sur votre SI.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise. En effet, le test d'intrusion est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure à auditer, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations.
Vous étudierez notamment l'organisation et les procédures propres à ce type d'audit, vous utiliserez vos compétences techniques. Vous découvrirez les meilleurs outils d'analyse et d'automatisation des attaques pour la réalisation de cette intervention.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation grâce à 80% d'exercices pratiques et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Méthodologie de l'audit

La première journée posera les bases méthodologiques d'un audit de type test d'intrusion. L'objectif principal étant de fournir les outils méthodologiques afin de mener à bien un test d'intrusion. Les points abordés seront les suivants :

Objectifs et types de test d'intrusion

- Qu'est-ce qu'un test d'intrusion ?
- Le cycle du test d'intrusion
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du test d'intrusion
- Limites du test d'intrusion
- Cas particuliers
  - Dénis de service
  - Ingénierie sociale

Aspect réglementaire

- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

Exemples de méthodologies et d'outils

- Préparation de l'audit
  - Déroulement
  - Cas particuliers
  - Habilitations
  - Dénis de service
  - Ingénierie sociale
- Déroulement de l'audit
  - Reconnaissance
  - Analyse des vulnérabilités
  - Exploitation
  - Gain et maintien d'accès
  - Comptes rendus et fin des tests

Éléments de rédaction d'un rapport

- Importance du rapport
- Composition
  - Synthèse générale
  - Synthèse technique
- Évaluation du risque
- Exemples d'impacts
- Se mettre à la place du mandataire

Une revue des principales techniques d'attaques et des outils utilisés sera également faite afin de préparer au mieux les stagiaires à la suite de la formation.

JOURS 2, 3 & 4

Une mise en situation d'audit sera faite afin d'appliquer, sur un cas concret, les outils méthodologiques et techniques vus lors de la première journée.

L'objectif étant de mettre les stagiaires face à un scénario se rapprochant le plus possible d'un cas réel.

Le système d'information audité comportera diverses vulnérabilités (applicatives, systèmes, web, Active Directory, etc.) plus ou moins faciles à découvrir et à exploiter.
L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information.

Pour ce faire, le formateur se mettra à la place d'un client dont les stagiaires auront à auditer le système d'information. Ces derniers seront laissés en autonomie et des points méthodologiques et techniques seront régulièrement faits par le formateur afin de guider les stagiaires tout au long de la mise en situation.

Le formateur aura un rôle de guide afin de :

- faire profiter les stagiaires de son expérience terrain
- mettre en pratique la partie théorique de la première journée
- élaborer un planning
- aider les stagiaires à trouver et exploiter les vulnérabilités présentes
- formaliser les découvertes faites en vue d'en faire un rapport pour le client

PROGRAMME

JOUR 5

Le dernier jour sera consacré au rapport. La rédaction de ce dernier et les méthodes de transmission seront abordées via des exemples et des modèles de rapports.

Préparation du rapport
- Mise en forme des informations collectées lors de l'audit
- Préparation du document et application de la méthodologie vue lors du premier jour

Écriture du rapport
- Analyse globale de la sécurité du système
- Évaluation du risque lié au périmètre client
- Description des vulnérabilités trouvées
- Rédiger des recommandations pertinentes pour corriger les vulnérabilités.

Transmission du rapport
- Précautions nécessaires
- Méthodologie de transmission de rapport

PROCHAINES DATES

17 février 2025
30 juin 2025
25 août 2025
27 octobre 2025

OBJECTIFS

- Maîtriser les différentes vulnérabilités sur les applications Web
- Maîtriser les différentes méthodologies de pivot sur un réseau interne
- Exploiter un Buffer Overflow
- Exploiter des vulnérabilités sur un domaine Active Directory
- Rédiger et relire un rapport de test d'intrusion

INFORMATIONS GÉNÉRALES

Code : TEST-INT
Durée : 5 jours
Prix : 3 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Toute personne souhaitant apprendre le pentest (test d'intrusion)

PRÉ-REQUIS

- Avoir des notions techniques de sécurité informatique
- Avoir suivi une formation HSA (ou d'un niveau équivalent) ou avoir participé à des CTF
- Avoir des connaissances en systèmes Windows et Linux et des bases de données
- Avoir des notions de développement Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne
- Chaque participant a accès à sa propre instance d'un réseau d'entreprise virtualisée pour mener le test d'instrusion