TEST D'INTRUSION : MISE EN SITUATION D'AUDIT

Le PenTest par la pratique

Code : PNT

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur votre S.I.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise. En effet, le PenTest 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 y étudierez notamment l'organisation et les procédures propres à ce type d'audit ; ainsi qu'à utiliser vos compétences techniques (des compétences équivalentes au cours HSA sont recommandées) et les meilleurs outils d'analyse et d'automatisation des attaques (outils publics ou privés développés par nos équipes) 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 en fin de module par le formateur.

JOUR 1

Méthodologie de l'audit

La première journée sera utilisée pour poser 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 PenTest

- Qu'est-ce qu'un PenTest?
- Le cycle du PenTest
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du PenTest
- Limites du PenTest
- 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
- Evaluation de risque
- Exemples d'impacts
- Se mettre à la place du mandataire

Une revue des principales techniques d'attaques et 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, un réseau d'entreprise.

Le système d'information audité comportera diverses vulnérabilités (Web, Applicatives, 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 pour qui 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 de terrain
- mettre en pratique la partie théorique de la première journée
- élaborer un planning
- aider les stagiaires à trouver et exploiter les vulnérabilités présentes
- formater les découvertes faites en vue d'en faire un rapport pour le client

Suite...

PROGRAMME

JOUR 5

Le dernier jour sera consacré au rapport. La rédaction de ce dernier et les méthodes de transmission seront abordées.

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
- Description des vulnérabilités trouvées

Transmission du rapport
- Précautions nécessaires
- Méthodologie de transmission de rapport
- Que faire une fois le rapport transmis ?

PROCHAINES DATES

4 avr. 2022,
17 oct. 2022

OBJECTIFS

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

INFORMATIONS GÉNÉRALES

Code : PNT
Durée : 5 jours
Prix : 3 350 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux

PRÉ-REQUIS

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP et HTTP(S)
- Connaissances des systèmes Windows et Linux et des bases de données
- Notions de développement Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement virtualisé Windows de démonstration (Windows 2003...) et Linux
- Chaque participant a accès à une infrastructure virtualisée permettant l'émulation de systèmes d'exploitation modernes
- Le test d'intrusion s'effectue sur un SI simulé et mis à disposition des participants