**Cadrer le Pentest et Définir son Périmètre**

Ce document liste les questions à poser à une entreprise dans le but d’établir tous les éléments permettant de bien définir le préambule du pentest. Il permet de mettre à l’écrit le contexte, les besoins, les autorisations reçues et les systèmes concernés.

# 1) Ciblage des besoins et de l’approche à tenir :

# Dans quel secteur d’activité évolue l’entreprise ?

# Quels sont les principaux risques identifiés vis-à-vis du système ou de l’application concerné(e) ?

# Quel est l’objectif de réalisation du test d’intrusion ? (Obligation réglementaire, vérification avant mise en production, test de renouvellement, autre…) ?

# Quelle est l’approche souhaitée pour les tests d’intrusion (boîte noire, grise ou blanche) ?

* + Si boite blanche : prévoir de fournir les plages d’adresses IP, les informations sur les utilisateurs et les systèmes et éventuellement les codes sources concernés
  + Si boite grise : prévoir de fournir un compte utilisateur valide pour le pentester
  + Si boite noire : prévoir de fournir le nom de domaine ou l’adresse IP ciblée

Est-ce qu’il est possible de réaliser le test d’intrusion à distance ?

Quelles sont les modalités de communication des livrables et le budget ?

Quelles sont les limitations (plage horaire, connexions d’appareils au réseau…) ?

Y a-t-il un PAS, PAQ ou une PSI lié(e) à l’hébergement ?

# 2) Cartographie technique du système visé :

# Quelle est l’URL ou l’adresse IP du ou des service(s) ciblé(s) ?

# Quels services, URL, IP, application ou systèmes sont à exclure du test d’intrusion ?

# Est-ce un environnement en production ou en développement ?

# Combien y a-t-il d’utilisateurs ? d’applications ?

# Quelles sont les technologies impliquées ? ou tout élément d’infrastructure utile pour le pentester (selon pertinence vis-à-vis de l’approche souhaitée)

Qui héberge le site (si pertinent) ? cloud privé ? hébergeur tiers ?

Quelles sont les coordonnées d’un responsable technique à contacter en cas d’incident ?

Disposez vous d’une lettre de consentement officielle de l’entreprise à auditer et quelles sont les exigences de confidentialité ?

Y a-t-il des informations additionnelles à nous communiquer ?