**Cadrer le Pentest et Définir son Périmètre – Exemple de réponses**

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 ?

Elle évolue dans le e-commerce (vente en ligne)

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

Le site est vieux et a été développé par une société non française. Nous pensons être attaqués par des concurrents car nous avons beaucoup de spam et de trafic inutile ces derniers jours… Il se peut donc que nous soyons aussi vulnérables à des cyberattaques.

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

D’une part il s’agirait donc de vérifier qu’il n’y ait pas de trous de sécurité, et dans l’idéal nous serions partant pour des conseils de mise en conformité RGPD.

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

Nous pouvons vous fournir un compte d’utilisateur ayant acquis un produit pour étudier l’interface permettant de gérer les commandes (boite grise).

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

Oui

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

Budget : 1000€ maximum, rapport à fournir sous 7 jours, date prévisionnelle : 01/04 9h00 au 07/04 17h00.

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

Audit à faire en matinée si possible, la plateforme doit être accessible au plus tard au 07/04 17h00

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

Non

# 2) Cartographie technique du système visé :

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

<http://example.net> 192.168.0.1, site Wordpress et plugin woocommerce

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

Environnement cloud pour la comptabilité, non concerné par le pentest, adresse IP 192.168.0.2

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

Production

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

1578 clients, 1 seul site avec 12 plugins dont woocommerce, un plugin anti spam, un plugin de sécurité et des plugins pour traiter les ventes

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

Langage php, js, html, css, connexion base de données SQL locale

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

Hébergeur OVH cloud

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

M. X Y, mail : [m\_x\_x@example.net](mailto:m_x_x@example.net)

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

Oui, jointe par email après signature du contrat

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

Non