Question 1 : Citez 3 outils utiles pour tester les failles d’un site WEB dans le cadre d’un audit de sécurité ?

Question 2 : Décrivez brièvement ce qu’est ‘Metasploit’ et donnez un exemple d’utilisation concret

Question 3 : Peut-on utiliser Metasploit sur un site comme <https://www.swisscom.ch> (développez votre réponse) ?

Question 4 : Qu’est-ce que le ‘black box testing’ et quels sont ses avantages et inconvénients comparé à d’autres techniques ? (Style VEGA et Wapiti)

Réponse 1 : Vega, wapiti, Snyk.

Réponse 2 : C’est un outil de sécurité des systèmes informatiques. Son but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion. On va l’utiliser dans le cadre d’un rapport d’audit qui va nous indiquer les failles de notre site. Il est plus précis(ciblé) que Vega et autres.

Réponse 3 : Non. C’est illégal d’audit un site qui ne nous appartiens pas ou qu’on ne nous a rien demander. De plus, il s’agit d’un site en production et non en débug, il faudrait être mandater pour pouvoir auditer le site SEULEMENT en débug. (Risque de plantage du site de production)

Réponse 4 : Il s’agit d’une manière de tester le site seulement aux éléments ouverts aux clients (input). Il va tester toutes les entrées et analyser les sorties pour détecter des patterns indiquant des vulnérabilités. Il ne possède pas le code source, il va donc essayer tous ce qu’il peux faire à l’aveugle.