Mecmeche Fayssal Christopher Mbarapa
SIO2-SLAM-B3-TESTS-DE-SÉCURITÉ-TD1 -D 1 à 5

DIAPO 2

Q1 : Pentest représente quel type de piratage ?

Cela représente un piratage éthique

Q2 : De quel moyen dispose-t-on pour effectuer des tests de sécurité de type intrusion ?

Les différentes étapes de cette stratégie reposent sur l'identification des points de vulnérabilité et sur une tentative d'intrusion au cœur du système.

Q3 : Quelle est la finalité des test d'intrusion ?

La finalité est d'obtenir des informations clés pour améliorer la cybersécurité.

Q4 : Un test de sécurité peut-il est assimiler à un audit ?

Non, l'audit de sécurité doit être différencié du pentest. Il ne s'agit pas pour le testeur de se mettre dans la peau d'un hacker professionnel mais de réaliser une étude approfondie du système d'information de son client, sur la base d'échanges avec l'équipe informatique et l'analyse de sa documentation technique.

Q5 : De combien de personnes se composent une équipe Red Team et quel est le rôle de chacun ?

Elle est composé de 4 personnes :

- un rôle de Vulnerability Assessments
- un rôle de Pénétration tess
- un rôle de Social Engineering
- un rôle de Security researchers

Q6 : Quel type de scénarios développe cette équipe ? Donnez des exemples.

Elle permet de confronter l'entreprise à des scénarios crédibles en laissant les équipes internes réagir et se défendre.

Par exemple :

- l'intrusion physique de personnes tierces susceptibles d'accéder aux outils informatiques, telles que des prestataires ou des fournisseurs,
- les tentatives de manipulation des salariés (ingénierie sociale) comprenant la récupération d'informations par des e-mails frauduleux ou des appels téléphoniques ciblés,
- la vulnérabilité des infrastructures physiques (accessibilité des serveurs et des postes informatiques, logiciels de sécurité installés, etc.).

DIAPO 3

Q7 : Quels types de risques peuvent concerner une organisation ? Donnez des exemples.

Q8 : Quelle est la finalité d'un test de sécurité ?

La finalité du test de sécurité permet de formaliser un plan d'action pragmatique, comprenant des préconisations techniques, organisationnelles, opérationnelles et humaines.

Q9 : Qu'est-ce qu'un test de sécurité n'est PAS ?

Un test de sécurité ne consiste pas à établir la liste des vulnérabilités d'un système.

Q10 : Quelles sont les actions possibles d'une entreprise pour intégrer un risque ?

Les actions possibles sont :

- L'acceptation des risques
- La réduction des risques
- La surveillance des risques
- souscrire à une police d'assurance couvant les risques cybersécurité

Q11 : Que contient un bon rapport d'audit ?

Un bon rapport d'audit doit contenir trois éléments :

- Un inventaire des vulnérabilités détectées
- Un plan d'action doté d'un prisme opérationnel.
- synthèse managériale.

DIAPO 4

Q12 : Pour chaque méthodologie de test White, Grey et Black Box, donnez un exemple d'utilisation ?

Pentest Black Box : l'auditeur simule une attaque en se mettant dans la peau d'un hacker, dans les conditions d'un piratage réel.

Pentest White Box : l'auditeur travaille en étroite collaboration avec la DSI de son client

Pentest Grey Box : intégrer l'entreprise en tant que salarié d'un service sensible et posséder son propre compte utilisateur

Q13 : Pourquoi dans le cas de la BlackBox, l'organisation possède du temps pour réagir ?

Q14 : Pourquoi la méthodologie GreyBox possède les avantages des deux autres méthodes ?

DIAPO 5

Q15 : Quel est l’objectif de la première phase de préparation du test de sécurité ? Préciser par quoi
cela se traduit ?

Q16 : Quel document définit les conditions légales d’intervention de l’auditeur ?

Q17 : Quel est la dernière étape assurant les bonnes conditions de réalisation des test de sécurité ?

Q18 : Que doit on préciser dans cette dernière étape ? Donnez des exemples.

Q19 : Que doit proposer l’auditeur dans cette dernière étape ?

Q20 : Que doit demander l’organisation à l’auditeur pour le dissuader d’une éventuelle divulgation
d’information ?