

Date : 14/12/2021 Session : 2021-2022

Diplôme / filière / niveau : Master II

UE : SSI

Épreuve :

Note : (de 0 à 20)

Appréciation du correcteur :

Signature du/des correcteur(s) :

Partie EBIOS :

Question 2 :

Les 7 composantes d'un risque sont :

- la source de menace
- le mode opératoire, la menace
- la vulnérabilité
- le bien support
- le bien essentiel
- les leviers de sécurité
 - confidentialité
 - intégrité
 - disponibilité
- l'impact, conséquence

Si votre composition
comporte plusieurs
feuilles

numérotez les/.....

Question 4:

~~Cette décision~~

Cette décision s'appelle les objectifs de sécurité.

Les objectifs de sécurité sont divisés en 4 options :

- réduire le risque : agir sur les vulnérabilités du bien support
- transférer le risque : déléguer le risque à une tierce
- éviter le risque : enlever le bien support auquel est lié le risque
- prendre le risque : ne rien faire et estimer que le risque est minime

Question 5:

L'acceptation du risque est la deuxième grande décision de la gestion du risque. Cette décision est prise avec la direction de l'entreprise qui décide si oui ou non elle accepte les risques ~~résiduels~~ résiduels.

En cas de non-acceptation, une nouvelle itération du boucle de la gestion du risque doit être refaite.

Question n°1 (4 points)

Pour la liste des libellés ci-dessous :

- Veuillez dire s'il s'agit d'une menace ou d'une vulnérabilité
- Veuillez donner des vulnérabilités associées s'il s'agit d'une menace.
- Veuillez donner des menaces associées s'il s'agit d'une vulnérabilité.

Vulnérabilité ou Menace ?	V ou M	Catégorie de bien support concerné	Indiquez une liste de vulnérabilités exploitables par la menace ou des menaces capables d'exploiter la vulnérabilité
Données non effacées des serveurs du prestataire et rendues accessibles	V	SYSRES	Pirater le serveur Voler les données
Espionnage	M	LOC	Absence d'authentification Salle ouverte
Transfert du mot de passe en clair	M	SYSLOG	Absence de surveillance Cliquer par erreur sur l'option "en clair"
Politique de mot de passe faible	V	SYSLOG	Hacking mains exhaustives du mot de passe
Faible loyauté	V	ORGPAP	Dénoncer les actions d'un directeur Rapporter des informations
Action d'un aimant sur un disque dur	M	SYSMAT	Disque dur non isolé non protégé
Datacenter mal protégé contre les catastrophes naturelles	V	LOC	Séisme - tremblement de terre - inondation
Sujet à la dissipation	V	ORGPAP	accident incendiaire brûler

Question n°2 (2 points)

Veillez rappeler quelles sont les sept composantes d'un risque et retrouvez ces sept composantes dans le risque rédigé suivant :

Risque

Les administrateurs du site de vente en ligne de l'entreprise commettent une erreur de configuration due à un manque de formation. Ceci entraîne une indisponibilité du site qui est aggravée par un manque d'organisation dans le processus de sauvegarde / restauration. L'impact est une perte financière de 10 000 € à chaque heure d'indisponibilité.

Vous pouvez présenter les résultats sous la forme d'un tableau de ce type :

Composante 1 Source de menace	Les administrateurs
Composante 2 menace	commettre une erreur de configuration
Composante 3 vulnérabilité	manque de form peu formés
Composante 4 lien support	ordinateur
Composante 5 lien essentiel	site de vente en ligne de l'entreprise
Composante 6 besoin de sécurité	disponibilité - traçabilité
Composante 7 impact	perte 10 000 € à chaque heure d'indisponibilité.

Question n°3 – 8 points

Dans cette question, les libellés des objets manipulés ne sont pas utiles à la réalisation de l'exercice. Votre travail consiste ici, à l'aide des tableaux fournis, à identifier et estimer les risques.

Voici quatre scénarios de menace identifiés avec leur vraisemblance :

En utilisant les tableaux précédents, veuillez identifier et estimer les risques.

- Si les vulnérabilités V1 et V3 sont présentes, alors la source de risque SR1 pourra utiliser M9 (vraisemblance 1)

Risque 1 : Les liens supports S2 et S4 sont concernés, Les liens essentiels en danger sont E5 et E2. E5 a des besoins de sécurité faibles (0-0-1) mais E2 a des besoins plutôt élevés (3-4-3). Mais les liens supports S2 et S4 sont pas faciles à exploiter.

- Si les vulnérabilités V2 et V5 sont présentes, alors la source de risque SR2 pourra utiliser M20 (vraisemblance 3)

Risque 2 : Les liens support S1 et S2 sont concernés. Les liens essentiels E2 et E5 seraient en danger, nous avons définis la grande hauteur des besoins au dessus. De plus, les liens support concernés sont facilement vulnérables à cette menace, surtout la V5 de la S2 qui est facilement exploitable.

- Si les vulnérabilités V4 ou V5 sont présentes, alors la source de risque SR3 pourra utiliser la menace M14 (vraisemblance 2)

Risque 3 : Les liens supports concernés sont S3 ou S2. Si la S3 est attaquée 2 liens essentiels seraient en danger ~~on~~ comparé à S2 qui n'a qu'un lien essentiel. Les besoins de sécurité de ces liens sont assez importantes. La vulnérabilité de la S2 est facilement exploitable contrairement à celle de la S3.

- Si les vulnérabilités (V1 et V6) ou (V2 et V5) sont présentes, alors la source de risque SR4 pourra utiliser la menace M13 (vraisemblance 2)

Risque 4 : Dans le cas où les vulnérabilités (V1 et V6) sont présentes. Le lien support serait en grand danger car facilement exploitable.

Dans l'autre cas où les vulnérabilités (V2 et V5), ce risque serait similaire au risque 2.

Question n°4 (3 points)

Nous passons à la phase de traitement du risque.

Les 4 risques identifiés et estimés à la question 3 sont présentés au maître d'ouvrage par le maître d'œuvre de l'étude de sécurité. Notre maître d'ouvrage doit décider de la façon dont va être engagé le traitement de ce risque.

Comment s'appelle cette décision ?

Ce type de décision peut appartenir à quatre grandes catégories. Veuillez lister ces catégories et expliquer en quoi consiste chacune d'entre-elles.

Question n°5 (3 points)

Pour les 4 risques, on décide de mettre en place 10 mesures de sécurité. Le tableau suivant donne la couverture des risques par les mesures. Chaque case du tableau représente une estimation de l'abaissement du risque si la mesure est mise en place. Les risques de valeur inférieur ou égal à 2 sont considérés comme acceptables.

Calculez le risque résiduel.

	Risque initial	Risque résiduel	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
R1				0,5	0.5				0.5			
R2			1	0.5	0.5		0.5					0,5
R3			1	0.5	0.5			1		1	1	
R4			0.5			0.5	0.5					

L'acceptation des risques est-elle possible en l'état ? Sinon que peut-on faire ? Avec qui validez-vous cette décision ?

— FIN —