

Date : Session : 1

Diplôme / filière / niveau : M2 TI

UE : SSI - PARTIE BIOS

Épreuve : SSI - PARTIE BIOS

Note : (de 0 à 20)

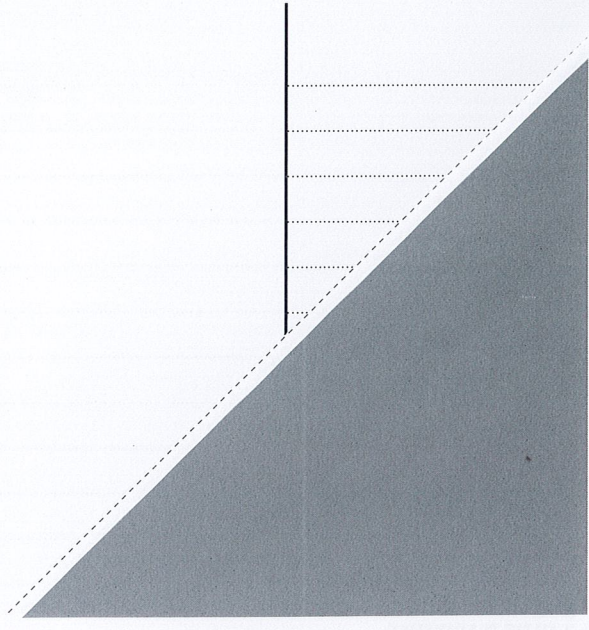
Appréciation du correcteur :

Signature du/des correcteur(s) :

- 4) Cette décision s'appelle l'objectif de sécurité. les 4 catégories sont :
- Éviter le risque : enlever le bien support au quelle le risque est lié
 - Réduire le risque : agir sur les vulnérabilités du bien support
 - Prendre le risque : ne rien faire et estimer que le risque est minime
 - Transférer le risque : le donner à une tierce

Si votre composition
comporte plusieurs
feuilles

numérotez les/.....



8/ - Source de risque

- Menace, Mode opératoire

- Vulnérabilité

- Bien support

- Bien essentiel

- Besoins de sécurité

- Impact conséquences

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	M	SysLOG	les données peuvent être accessibles à tous et peut faire l'objet de chantage
Espionnage	M	ORG: SP ORG PER	le pirate cherche à s'attaquer aux données personnelles
Transfert du mot de passe en clair	M	SysRES	le mot de passe peut être intercepté par un pirate car il n'a pas été crypté
Politique de mot de passe faible	V	SysLOG	le mot de passe peut être facilement exploité
Faible loyauté	V	ORG-0 ORG PER	Peut divulguer des informations confidentielles
Action d'un aimant sur un disque dur	M	SysMAT	Peut endommager la Carte du disque dur
Datacenter mal protégé contre les catastrophes naturelles	V	LOC	Peut être balayé par une tempête.
Sujet à la dissipation	M	SysLOG	Peut se retrouver sur les Réseaux sociaux

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 du risque	les administrateurs du site de vente en ligne
Composante 2 Menace, Mode d'attaque	Mauvaise configuration,
Composante 3 Vulnérabilité	Manque de formation, ou sensibilisation
Composante 4 Brienssupport	Réseau d'hébergement
Composante 5 Bien essentiel	Indisponibilité du site
Composante 6 Besoins de sécurité	Processus de sauvegarde et restauration
Composante 7 Impact, Conséquence	Perte financière de 10.000€ Chaque heures.

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 : Dépassement des limites d'un logiciel

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

Risque 2 : Espionnage d'une personne à distance

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

Risque 3 : Écoute passive d'un canal informatique ou de téléphonie

- 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 : Attaque du milieu sur un canal informatique ou de téléphonie

On donne le tableau de *croisement des biens essentiels (E1, ..., E5) et biens supports (S1, ..., S5)*.

	E1	E2	E3	E4	E5
S1		x			
S2					x
S3	x		x		
S4		x			
S5				x	

Voici le tableau de *synthèse des besoins de sécurité*.

	Disponibilité	Intégrité	Confidentialité
E1	1	1	4
E2	3	4	3
E3	2	2	0
E4	1	1	0
E5	0	0	1

Les menaces génériques suivantes ont été sélectionnées dans la base de connaissance de la méthode.

Support	Type	Code	Libellé	D	I	C
LOG	DEP	M9	Dépassement des limites d'un logiciel	x		
RSX	USG	M13	Attaque du milieu sur un canal informatique ou de téléphonie	x	x	
RSX	ESP	M14	Écoute passive d'un canal informatique ou de téléphonie			x
PER	ESP	M20	Espionnage d'une personne à distance			x

Voici le tableau des vulnérabilités et les biens supports concernés. Les niveaux de vulnérabilités sont indiqués avec l'échelle suivante représentant la complexité d'utilisation :

3 : Facile à exploiter

2 : Moyen

1 : Complexe

	V1	V2	V3	V4	V5	V6
S1		2				
S2	1				3	
S3				1		
S4			2			
S5						3

Vous utiliserez ce tableau pour calculer la valeur du risque.

Vraisemblance de la menace		Improbable : 1			Probable : 2			Certain : 3		
Facilité d'exploitation		C	M	F	C	M	F	C	M	F
Valeur des biens	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7

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 —