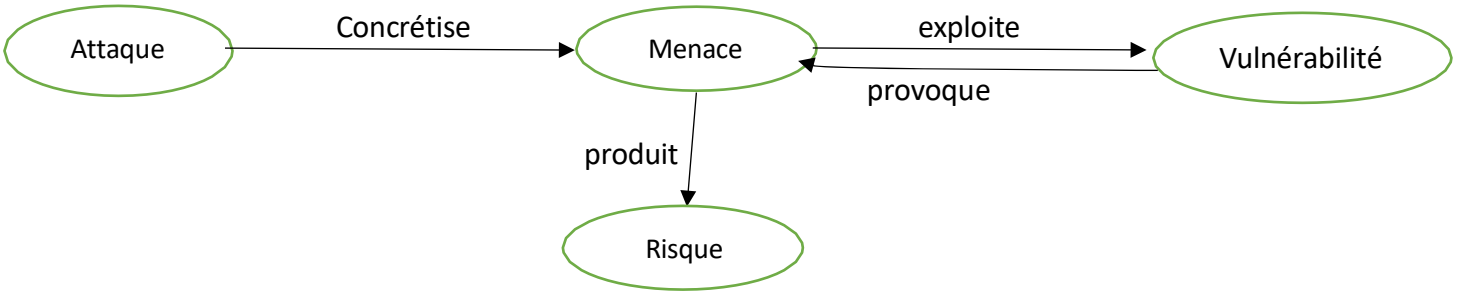
Solution td 01

Exercice 1 :

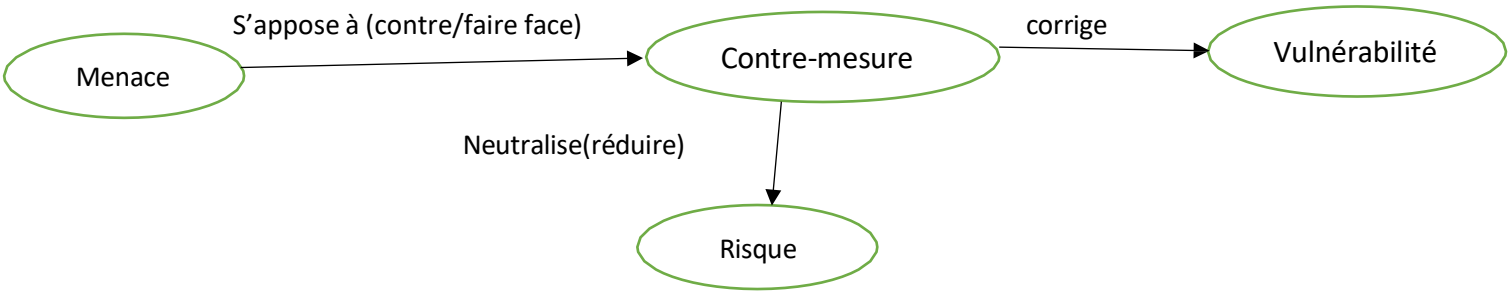
Définition concise des concepts :

- **a- Vulnérabilité** : Trou de sécurité dans un système (absence de protection).
- **b- Menace** : violation potentielle de la sécurité qui peut endommager un système.
- **c- Attaque** : action malveillante qui concrétise une menace.
- **d- Risque** : mesure de danger provoque par la présence d'une menace.
- **e- Intrusion** : attaque réussie (partiellement ou complétement).
- **f- Contre-mesure** : techniques et moyens employés pour réduire le risque.

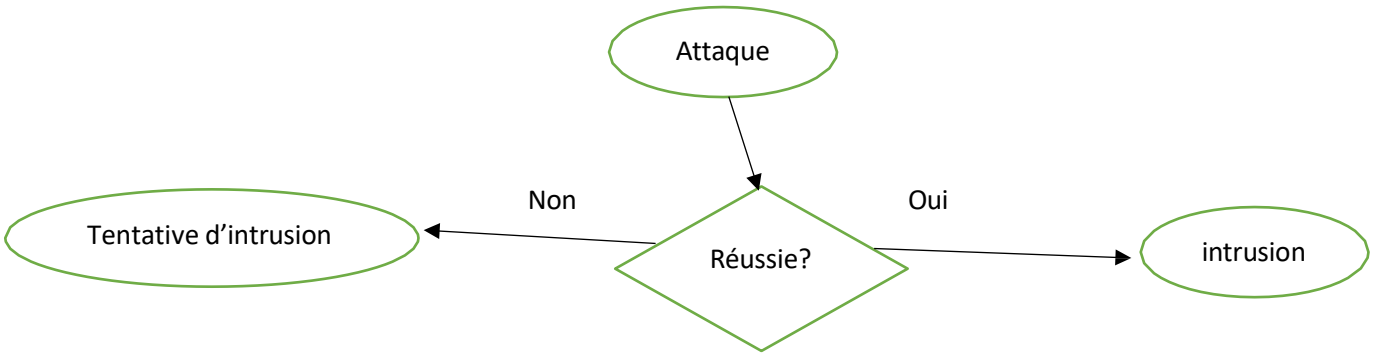
2) Les relations qui existent entre le concept menace et les concepts : attaques, vulnérabilité et risque.



3) Les relations qui existent entre le concept contre-mesure el les concepts : menace, vulnérabilité et risque.



4) Différence entre une attaque et une intrusion :



Une intrusion est une attaque réussie (complément ou partiellement).mais une attaque est une tentative (essai) d'intrusion.

Exercice 2 :

Vulnérabilités	Menaces
1- Système sans authentification 2- Absence de sauvegarde 3- La non duplication d'un serveur critique	1- Script malveillant attache a une page web 2- Prise de contrôle d'un serveur 3- Coupure d'électricité 4- Défaillance de logiciel 5- Explosion 6- Panne de disque 7- Espionnage

Exercice 3 :

1) **Définition de la sécurité informatique** : mécanismes et moyens employés pour protéger les systèmes contre les attaques .
2) **Les objectifs de la sécurité informatique** :
   - **a) Confidentialité** : l'information secrète n'est lue que par les personnes autorisées.
   - **b) Intégrité** : l'information secrète n'est modifiée que par les personne autorisées.
   - **c) Disponibilité** : l'accès a un services/système est toujours possible pour les personnes autorisées.
   - **d) Non répudiation** : les deux corresponds dans une transaction ne peuvent pas nier avoir participe a la transaction.
   - **e) Authentification** : mécanisme d'identification et de vérification de l'identité d'une entité.
3) **<u>Scénarios d'attaques et objectifs de sécurité compromis :</u>**

Scénario d'attaque	Objectifs compromis (atteints)	Mécanisme de sécurité adéquat
A	Confidentialité	Algorithmes de chiffrement
B	Confidentialité Intégrité	Algorithmes de chiffrement Fonction de hachage
C	Non répudiation	Signature numérique
D	Disponibilité	Garantir la continuité de service a travers la duplication du serveur (serveur miroir)
E	Non répudiation	Signature numérique
F	Disponibilité	Garantir la continuité de service a travers la duplication du serveur (serveur miroir)
g	Authentification Intégrité Confidentialité	Certificat numérique Contrôle d'accès Contrôle d'accès