# Série de TD n° 1

## Exercice N°1 :

1) Quelles sont les ressources à protéger dans un système d'information ?
2) Pourquoi les systèmes sont vulnérables ?
3) Pourquoi la sécurité informatique ne doit être en aucun cas considérée comme une question conjoncturelle ?
4) Y a-t-il de solution "clef en main" dans le domaine de la sécurité ?
5) Y a-t-il de sécurité absolue ? Pourquoi ?
6) "La plus grande vulnérabilité d'un système d'information est l'être humain" expliquer pourquoi ?
7) Quelles sont les caractéristiques de la sécurité informatique ?
8) Quels sont les facteurs qui influencent sur le niveau de sécurité qu'on veut atteindre ?
9) Quelle est la différence entre une menace et un risque ?
10) Comment apprécier un risque ?
11) Expliquer la méthode PDCA.
12) La sécurisation d'un système est souvent un processus très couteux pour l'entreprise, y a-t-il de solutions alternatives ?

## Exercice N°2 :

1) Lors de la création d'une boite mail, on est souvent appelé à taper un code affiché sous forme d'image dans la même page d'inscription « Captcha », pourquoi ?
2) Même question concernant la question secrète ? peut-elle être source d'intrusion ?
3) Lors d'un changement d'un mot de passe, on est toujours appelé à retaper celui-ci une deuxième fois, pourquoi ?
4) Pourquoi on écrit le login (identifiant) en clair et le mot de passe en masqué ?
5) Quelle est la différence entre "Identification" et "Authentification" ?
6) Quels sont les objectifs possibles des attaques informatiques ?

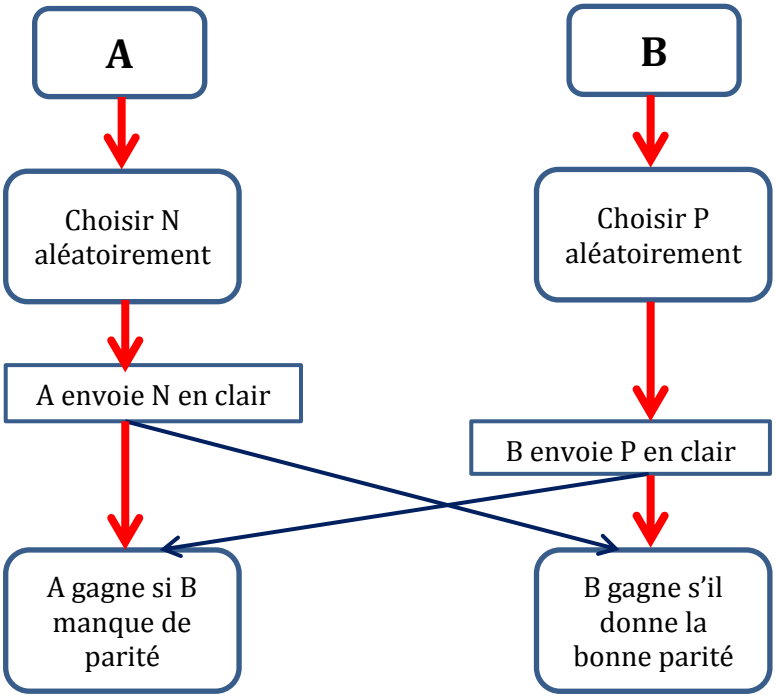
## Exercice N°3 :

1) Quels sont les objectifs de la SI démolis pour les cas suivants :
   a. Un pirate qui a pu s'introduire dans un serveur mail et lui causer un ralentissement énorme dans son fonctionnement.
   b. Un employé qui a utilisé le login/mot de passe de son responsable pour accéder aux données secrètes de ces collègues du même service, puis il a détruit quelques informations.
   c. Un intrus qui s'est introduit entre deux personnes et détourner leurs messages à son profit.
   d. X qui a pu prendre l'identité de B pour entrer dans sa boîte mail et :
      - Lire quelques mails et ensuite les marquer comme étant non lus.
      - Effacer quelques autres et ensuite vider la corbeille.
      - Ecrire et envoyer un message.
   e. Un pirate qui a pu voler les informations personnelles d'une autre personne (nom, prénom et n° de la carte de crédit) et ainsi faire des achats sur internet.
   f. Un tremblement de terre causant la destruction totale d'un système.

2) Pour chaque type de menaces (informatique ou non informatique, accidentelle ou intentionnelle, interne ou externe) donner 2 exemples.

## Exercice N°4 :

Deux étudiants A et B géographiquement distants veulent concevoir un protocole de communication asynchrone (par envoi de messages asynchrones) implémentant le principe du jeu de pile ou face, en utilisant les nombres et leur parité. Ainsi ils se mettent d'accord sur les étapes suivantes :




- **Etape 1 :** le premier joueur choisit aléatoirement un nombre N non nul, et l'autre choisit aléatoirement aussi la parité P (pair ou impair).
- **Etape 2 :** les deux joueurs s'échangent mutuellement les deux nombres en clair.
- **Etape 3 :** Décision : le deuxième joueur gagne s'il donne la bonne parité, sinon c'est l'autre qui gagne.

1) Sachant que les deux étudiants se méfient mutuellement et n'ont pas de mémoire partagée, étudier la sécurité et la fiabilité de ce protocole.
2) Quelles sont les fraudes possibles de la part de chaque joueur ?

Supposons que ces deux étudiants utilisent ce protocole uniquement pour déterminer qui doit jouer le premier aux échecs.

3) Comment peut-on évaluer le risque d'être cibles à une attaque MITM ?
4) Même question si le protocole est utilisé pour choisir celui qui va dans une excursion organisée par l'université ?

## Exercice N°5 :

Choisir la bonne réponse :

**1)** Dans la sécurité informatique, _____ signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées.

A. *La confidentialité*
B. *L'intégrité*
C. *La disponibilité*
D. *L'authenticité*

**2)** Dans la sécurité informatique, _____ signifie que les informations contenues dans un système informatique ne sont accessibles en lecture que par les personnes autorisées.

A. *La confidentialité*
B. *L'intégrité*
C. *La disponibilité*
D. *L'authenticité*

**3)** Le _____ est un code incorporé dans un programme légitime configuré pour «exploser» lorsque certaines conditions sont remplies.

A. *Porte dérobée*
B. *Cheval de Troie*
C. *Bombe logique*
D. *Virus*

**4)** Lequel des programmes malveillants suivants ne se répliquent pas automatiquement ?

A. *Cheval de Troie*
B. *Virus*
C. *Ver*

**5)** _____ est une forme de virus explicitement conçue pour éviter la détection par des logiciels antivirus.

A. *Virus furtif*
B. *Virus polymorphe*
C. *Virus parasite*
D. *Virus de macro*

**6)** _____ est utilisé pour valider l'identité de l'expéditeur du message auprès du destinataire.

A. *Cryptage*
B. *Décryptage*
C. *Signature numérique*
D. *Aucune de* ces réponses n'est vraie.

**7)** L'art de cacher l'information est appelé :

A. *Cryptographie*
B. *Cryptanalyse*
C. *Stéganographie*
D. *Watermarking*

**8)** Le chiffrement symétrique permet de garantir :

A. *La confidentialité*
B. *L'intégrité*
C. *L'authentification*
D. *La disponibilité*
E. *La nonrépudiation*

**9)** Le chiffrement symétrique permet de garantir :

A. *La confidentialité*
B. *L'intégrité*
C. *L'authentification*
D. *La disponibilité*
E. *La nonrepudiation*

**10)** Les fonctions de hachage jouent un rôle très important pour garantir :

A. *La confidentialité*
B. *L'intégrité*
C. *L'authentification*
D. *La disponibilité*
E. *La nonrepudiation*

## Exercice N°6 :

Attribués sous forme d'exposés :

1. Termes : hacking, cracking (cassage de logiciel), rétro-ingénierie, keylogger, spyware, sniffer, spam,
2. Termes : virus (worm, wabbit,..), cheval de Troie (Trojan horse), bombe logique, porte dérobée (backdoor), machine zombie, bot informatique (robot), rootkit.
3. Commandes ping et traceroute : définition, exemple d'utilisation, informations obtenues, objectifs, leur utilisation par les hackers.
4. Ingénierie sociale : définition, mécanismes, exemples d'utilisation en informatique, contre-mesure.
5. Ports scanning (scan de ports) : définition, outils utilisés, résultat, types de scan (simple furtif, ..),
6. Attaques informatiques : définition, objectifs, types, mécanisme, attaque active vs attaque passive, anatomie (étapes) d'une attaque.
7. Attaque « man in the middle » : définition, principe, objectif, contre-mesures.
8. Usurpation d'identité : définition, objectif, mécanismes (IP-Spoofing, ARP-Spoofing, DNS spoofing ..), contre-mesures.
9. Fraude SALAMI : définition, principe, utilisation en informatique, gravité, contre-mesure.
10. Phishing (hameçonnage) : définition, principe, types (bas niveau et haut niveau), gravité, contre-mesures.
11. DoS (Denial of Service) : définition, principe, types (SYN flooding, DDoS, smurfing, ..) gravité, contre-mesures.
12. Attaque sur les mots de passe : principe (espionnage, force brute, dictionnaires, ..),
13. Attaque sur la signature numérique : fonction de hachage, principe (attaque des anniversaires),
14. Manipulation d'url et Crosse-site scripting (XXS) : principe, exemples, gravité, contre-mesures.
15. IDS & NIDS : définition, objectif, principe de fonctionnement, types, avantage/inconvénients.
16. Firewall (pare-feu) : définition, objectif, principe de fonctionnement, types, points forts et points faibles.
17. Proxy : définition, objectif, principe de fonctionnement, types, points forts et points faibles.
18. Antivirus : définition, objectif, principe de fonctionnement, types, points forts et points faibles.
19. Stéganographie : définition, objectif, application en informatique, avantages/inconvénients.
20. Le ChatGPT : définition, utilisation, avantages et risques.