Sécurité des SI

I.

1. Répondre aux questions suivantes :
   - Proposer deux solutions pour assurer la confidentialité des données.
   - Quelles est la différence entre l'identification et l'authentification ?
2. Remplir les vides :

1) est un programme illicite qui s'insère dans des programmes légitimes appelés hôtes.
2) est un type d'attaque qui vise à rendre une application informatique incapable de répondre aux requêtes des utilisateurs :
3) est une attaque qui consiste à placer des sondes sur le réseau pour écouter et récupérer des informations à la volée, puis on analyse le trafic pour récupérer des mots de passe et des informations confidentielles ;
4) est une attaque qui affecte les requêtes en cours d'exécution sur des bases de données:
5) est l'attaque qui utilise les rayonnements électromagnétiques pour rendre le SI inopérant
6) est un programme ou ensemble de programmes permettant de maintenir dans le temps un accès frauduleux à un SI
7) est un programme malveillant qui exploite les capacités des applications de logiciels de bureautique
8) L'insertion par l'attaquant du code HTML ou java script dans une page web fourni par un serveur s'appelle :
9) est une t*echnique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.*
10) Dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.
11) est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu.

II.

Donner le type de chacune de ces vulnérabilités

1. Mots de passe par défaut (commun) utilisé pour une longue durée
2. Sensibilité des équipements vis à vis le changement de voltage
3. Sensibilité des équipements vis à vis l'humidité et le changement de température
4. Sécurité de câblage non adéquate
5. Control d'accès physique et logique non adéquat
6. Mauvaise administration du réseau
7. Protection insuffisante des clés cryptographiques
8. Mauvais remplacement des anciens équipements
9. Supervision insuffisante des employés,
10. Disqualification des employés

Sécurité des SI

1. LE VIRUS est un programme illicite qui s'insère dans des programmes légitimes appelés hôtes.
2. DOS est un type d'attaque qui vise à rendre une application informatique incapable de répondre aux requêtes des utilisateurs :
3. LE SNIFFING est une attaque qui consiste à placer des sondes sur le réseau pour écouter et récupérer des informations à la volée, puis on analyse le trafic pour récupérer des mots de passe et des informations confidentielles ;
4. SQL INJECTION est une attaque qui affecte les requêtes en cours d'exécution sur des bases de données:
5. le BROUILLAGE est l'attaque qui utilise les rayonnements électromagnétiques pour rendre le SI inopérant
6. LE ROOTKIT est un programme ou ensemble de programmes permettant de maintenir dans le temps un accès frauduleux à un SI
7. LE VIRUS MACROS est un programme malveillant qui exploite les capacités des applications de logiciels de bureautique
8. L'insertion par l'attaquant du code HTML ou java script dans une page web fourni par un serveur s'appelle :XSS Cross Site Scripting (XSS)
9. Le phising est une t*echnique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.*
10. Keyloggers : Dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.
11. Non répudiation: est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu.

II-Donner le type de chacune de ces vulnérabilités

1. Mots de passe par défaut (commun) utilisé pour une longue durée/HUMAINE
2. Sensibilité des équipements vis à vis le changement de voltage/MISE EN OEUVRE
3. Sensibilité des équipements vis à vis l'humidité et le changement de température //
4. Sécurité de câblage non adéquate /MISE EN OEUVRE
5. Control d'accès physique et logique non adéquat / HUMAINE
6. Mauvaise administration du réseau /HUMAINE, TECHNOLOGIQUE
7. Protection insuffisante des clés cryptographiques /HUMAINE, TECHNOLOGIQUE
8. Mauvais remplacement des anciens équipements/MISE EN ŒUVRE
9. Supervision insuffisante des employés/ ORGANISATIONNELLE
10. Disqualification des employés /ORGANISATIONNELLE

I-1 CRYPTAGE DE DONNEES ET LE CONTROL D'ACCES

I-2 Authentification: permet de prouver l'identité des entités. L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.

Identification : consiste à établir l'identité de l'utilisateur. "Nom d'utilisateur" ou "Login" en anglais qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.