Partie I : QCM

Consignes :

Sélectionner la ou les bonne(s) réponse(s)
(2 points par bonne réponse, -0,5 point par mauvaise réponse).

1. **Laquelle (lesquelles) des assertions suivantes n'est (sont) pas vraie(s) ?**
   a) La cybersécurité et la sécurité informatique ont les mêmes enjeux
   b) Un rootkit permet à des cybercriminels de contrôler un appareil à distance
   c) Un ver se propage toujours en utilisant un virus existant
   d) Il est impossible de pouvoir éradiquer un rootkit
   e) Un adware est logiciel indésirable et espion

2. **Le _____ est un code qui reconnaît une séquence d'entrée spéciale ou qui est déclenché par une séquence d'événements improbable.**
   a) Porte à piège (Trap doors)
   b) Cheval de Troie
   c) Bombe logique
   d) Virus

3. **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

4. **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

5. **Sélectionner les attaques qui sont généralement de type « ciblée » :**
   a) Phishing ou hameçonnage ;
   b) Ransomware ou rançongiciel ;
   c) Social engineering ou ingénierie sociale ;
   d) Spear phishing ou « l'arnaque au président ».

6. **Pour un système informatique, en quoi consiste la procédure d'authentification d'un utilisateur ?**
   a) Vérifier l'identité de l'utilisateur avant de lui donner accès à des ressources (systèmes, réseaux, applications ...)
   b) Demander à l'utilisateur d'entrer son mot de passe à intervalles réguliers au cours de sa session.
   c) Établir une correspondance entre le pseudo entré par l'utilisateur et son véritable nom
   d) Demander d'entrer une seconde fois son mot de passe à l'utilisateur qui souhaite en changer
   e) Garder la trace de la visite de l'utilisateur sur le système (identifiant, dates et heures de connexion et de déconnexion, ...)

7. **Vérifier l'identité de l'utilisateur avant de lui donner accès à des ressources (systèmes, réseaux, applications ...) consiste à :**
    a) Demander à l'utilisateur d'entrer son mot de passe à intervalles réguliers au cours de sa session.
    b) Établir une correspondance entre le pseudo entré par l'utilisateur et son véritable nom
    c) Demander d'entrer une seconde fois son mot de passe à l'utilisateur qui souhaite en changer
    d) Garder la trace de la visite de l'utilisateur sur le système (identifiant, dates et heures de connexion et de déconnexion, ...)

8. **En quoi consiste l'hameçonnage (phishing) ?**
    a) À envoyer un courriel à plusieurs personnes
    b) À établir un lien entre deux correspondants
    c) À obtenir des renseignements personnels dans un but frauduleux
    d) À attirer des clients

9. **En matière de sécurité informatique, Que désigne-t-on par cheval de Troie ?**
    a) Un logiciel malveillant qui se propage par courrier électronique en exploitant les failles des logiciels de messagerie
    b) Un logiciel malveillant ayant l'apparence d'un logiciel inoffensif mais qui comporte des instructions nuisibles qui s'exécutent une fois le logiciel installé
    c) Un courrier électronique malveillant qui s'envoie lui-même aux adresses contenues dans tout le carnet d'adresses de l'ordinateur sur lequel il se trouve
    d) Un logiciel malveillant qui s'installe discrètement sur l'ordinateur et collecte et envoie des informations personnelles à des organismes tiers.

10. **Lequel des programmes malveillants suivants ne se réplique pas automatiquement ?**
    a) Cheval de Troie
    b) Virus
    c) Ver
    d) Zombie

11. **Que permet de faire un serveur proxy récent ?**
    a) Joue le rôle de passerelle entre l'utilisateur et le réseau Internet.
    b) Permet de filtrer le trafic entrant et sortant
    c) Assure le rôle d'un cache pour un accès rapide aux pages web déjà visités
    d) Protège les utilisateurs et le réseau interne des menaces externes.
    e) Aucune des réponses précédentes n'est valide.

12. **Que permet de faire un pare-feu ?**
    a) Gérer les licences d'utilisation des logiciels
    b) Protéger l'ordinateur contre les surtensions
    c) Filtrer les flux de données émanant des serveurs distants conformément à une politique de sécurité
    d) Analyser le contenu des sites web visités en vue de fournir un accès indexé de type "moteur de recherche"
    e) Filtrer le contenu des messages électroniques selon leur expéditeur

13. **Parmi les catégories de cyberattaques définies par le gouvernement, citer celles qui figurent dans cette classification :**
    a) Sabotage
    b) Détournement de session
    c) Atteinte à l'image
    d) Usurpation d'identité

14. **Qu'est-ce qui peut récupérer un mot de passe à l'insu de son propriétaire ?**
    a) Un anti-virus
    b) Un spam
    c) Un hameçonnage (phishing)
    d) Un logiciel espion
    e) Un canular électronique

15. **Qu'appelle-t-on logiciel espion ou espiogiciel ou spyware ?**
    a) Un logiciel de cryptage des données.
    b) Un programme permettant d'envoyer à des "pirates" des informations pouvant être confidentielles telles que des mots de passe.
    c) Un système de transmission des données sans fil concurrent du wifi.
    d) Une erreur dans un programme. L'équivalent d'un "bug".
    e) Un logiciel antivirus.

16. **Qu'est-ce qu'un hoax ?**
    a) Une rumeur circulant par courrier électronique
    b) Un virus
    c) Un anti-virus
    d) Une blague diffusée sur la toile
    e) Un logiciel espion

17. **Quelle affirmation sur la mise à jour d'un anti-virus est FAUSSE ?**
    a) La mise à jour de l'anti-virus doit être faite régulièrement afin de bénéficier des dernières définitions de virus
    b) La mise à jour de l'anti-virus peut être lancée automatiquement
    c) La mise à jour de l'anti-virus peut se faire par Internet
    d) La mise à jour de l'anti-virus peut être lancée manuellement
    e) La mise à jour de l'anti-virus peut se faire sans connexion à Internet, à partir du CD d'installation

18. **_____ 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

19. **Depuis Internet, lorsqu'un attaquant réussit à contourner les mécanismes d'authentification et interroger directement la base de données par écriture de commandes spécifiques, on parle de :**
    a) Hacking
    b) XSS (Cross Site Scripting)
    c) Injection SQL
    d) Malware
    e) Administration d'une base de données

20. **Sélectionner les fausses assertions ?**
    a) Un antivirus peut détruire un fichier infecté
    b) Un antivirus peut interdire l'accès à des sites infectés
    c) Un antivirus peut détecter et ne pas réparer un fichier infecté
    d) Un antivirus peut détecter, isoler, réparer un fichier Infecté
    e) Un antivirus peut mettre en quarantaine un fichier suspect

21. **Parmi les types de fichiers suivants, quels sont ceux qui sont susceptibles de contenir des virus ?**

a) Zip
b) Exe
c) Jpg
d) Xls
e) txt

22. **Le social engineering est une technique utilisée par les cybercriminels afin d'obtenir des informations confidentielles ou un accès aux sources de données :**
    a) Grâce aux réseaux sociaux
    b) A cause d'une erreur humaine
    c) Par le biais de l'ingénierie humaine
    d) En exploitant une inclination naturelle et à faire confiance en se servant des utilisateurs peu méfiants

23. **Parmi les fichiers suivants reçus par courriel, lesquels sont sans risque pour un ordinateur ?**
    a) Un fichier texte seul : Travail.txt
    b) Un fichier image : Travail.jpg
    c) Un fichier de traitement de texte : Travail.doc
    d) Un fichier compressé : Travail.zip

24. **Parmi les assertions suivantes, dire celle(s) qui est(sont) vraie(s) ?**
    a) Une attaque active provoque des dangers superficiels alors que l'attaque passive inflige énormément de dégâts aux ressources du système
    b) Les attaques passives empêchent les ports ouverts qui ne sont pas protégés par des pare-feu
    c) Une attaque active peut être détectée par un antivirus mis à jour
    d) Dans une attaque par social engineering, il est possible d'utiliser la technique du phishing.

25. **Un antivirus intelligent est un antivirus qui : ?**
    a) S'appuie sur un système apprenant
    b) Se met à jour automatiquement
    c) Il se transforme par changement de signature
    d) Aucune des réponses précédents n'est vraie

Partie II : Question à développer

En quelques lignes, donner les règles fondamentales à respecter pour prévenir des attaques par des malwares.