Intrusions Réseau

1. **Quelle est la principale différence entre un ver et un virus ?**
   a) Un ver se propage seul, tandis qu'un virus a besoin d'un fichier hôte
   b) Un virus se propage seul, tandis qu'un ver a besoin d'un fichier hôte
   c) Un ver est toujours détectable par un antivirus, mais pas un virus
   d) Un virus est un type de ver

2. **Quel type de malware est souvent caché dans des logiciels légitimes pour donner un accès non autorisé au système ?**
   a) Un ver
   b) Un cheval de Troie
   c) Un rootkit
   d) Une bombe logique

3. **Quelle menace est conçue pour se déclencher à une date ou un événement précis ?**
   a) Un rootkit
   b) Un cheval de Troie
   c) Une bombe logique
   d) Un ver

4. **Quel malware est spécialement conçu pour cacher l'existence d'autres malwares ou activités malveillantes sur un système ?**
   a) Un virus
   b) Un rootkit
   c) Un cheval de Troie
   d) Un ver

5. **Quel terme désigne une méthode secrète permettant d'accéder à un système informatique en contournant les mécanismes de sécurité ?**
   a) Un rootkit
   b) Une porte dérobée
   c) Un virus
   d) Un cheval de Troie

6. **Un employé mécontent laisse intentionnellement un code malveillant dans un logiciel interne de son entreprise, qui supprime des fichiers après son départ. De quel type de menace s'agit-il ?**
   a) Un rootkit
   b) Une porte dérobée
   c) Une bombe logique
   d) Un virus

7. **Quel est l'objectif principal d'un rootkit ?**
   a) Supprimer les fichiers système
   b) Voler des informations bancaires
   c) Se cacher et permettre un accès secret à un attaquant
   d) Propager un ransomware

8. **Pourquoi un rootkit est-il particulièrement dangereux ?**
   a) Il crypte tous les fichiers de l'utilisateur
   b) Il modifie les paramètres réseau pour rediriger le trafic
   c) Il peut fonctionner en profondeur dans le système et échapper à la détection
   d) Il se propage automatiquement via les emails

9. **Quel type de malware modifie les fichiers exécutables pour s'attacher à eux et accéder à un système informatique ?**
   a) Un ver
   b) Un rootkit
   c) Un virus
   d) Un cheval de Troie

10. **Comment un ver informatique se propage-t-il généralement ?**
    a) Par un email contenant une pièce jointe infectée
    b) En exploitant des vulnérabilités réseau
    c) En remplaçant des fichiers système
    d) En attachant son code à d'autres exécutables

11. **Quel est l'objectif principal d'un spyware ?**
    a) Intercepter et manipuler la communication entre deux parties
    b) Détruire un serveur cible
    c) Installer un ransomware
    d) Lancer une attaque par force brute

12. **Quel type de logiciel malveillant peut enregistrer les frappes clavier d'un utilisateur pour voler des informations ?**
    a) Un cheval de Troie
    b) Un keylogger
    c) Un spyware
    d) Un adware

13. **Quelle est la meilleure pratique pour se protéger contre les intrusions réseau ?**
    a) Désactiver le pare-feu
    b) Utiliser des mots de passe simples pour éviter d'être oublié
    c) Mettre à jour régulièrement les systèmes et utiliser un pare-feu
    d) Se fier uniquement aux logiciels antivirus gratuits

14. **Qu'est-ce qu'une attaque de type DDoS ?**
    a) Une attaque où un hacker vole des données personnelles
    b) Une attaque qui vise à submerger un serveur avec un grand nombre de requêtes
    c) Une technique pour récupérer un mot de passe par force brute
    d) Une méthode pour injecter un virus via une clé USB

15. **Quelle est la méthode la plus courante utilisée pour tromper les utilisateurs et leur faire télécharger un logiciel malveillant ?**
    a) L'ingénierie sociale
    b) La force brute
    c) Le scan de ports
    d) Le cryptojacking

16. **Quel est le but principal d'une attaque par déni de service (DoS) ?**
    a) Voler des données sensibles sur un réseau.
    b) Surcharger un système ou un réseau, le rendant inaccessible aux utilisateurs.
    c) Diffuser des logiciels malveillants sur plusieurs appareils.
    d) Chiffrer des fichiers et exiger une rançon.

17. **Laquelle des caractéristiques suivantes caractérise un ver ?**
    a) Il s'attache à des programmes légitimes.
    b) Il se propage sans nécessiter d'interaction de l'utilisateur.
    c) Il affecte uniquement les fichiers d'un seul ordinateur.
    d) Il nécessite un support physique pour se propager.

18. **Laquelle des méthodes suivantes est couramment utilisée pour se protéger contre les virus et les vers ?**
    a) Désactiver les pares-feux.
    b) Mettre à jour régulièrement le logiciel antivirus.
    c) Partager et enregistrer les mots de passe sur le système.
    d) Utiliser les paramètres par défaut sur tous les appareils.

19. **À quoi sert généralement un « botnet » dans les attaques réseau ?**
    a) Pour crypter des fichiers et demander une rançon.
    b) Pour lancer des attaques par déni de service distribué (DDoS).
    c) Pour créer des canaux de communication sécurisés.
    d) Pour rechercher les vulnérabilités d'un réseau.

20. **Laquelle des pratiques suivantes est la meilleure pour prévenir les infections par des logiciels malveillants ?**
    a) Eviter de cliquer sur des liens dans des e-mails non sollicités.
    b) Utiliser des mots de passe robustes et activer l'authentification multifacteur.
    c) Désactiver les mises à jour logicielles pour éviter les interruptions.
    d) Partager des documents avec des clés USB.