Révision

Sécurité des SI

ISIL

QCM /QCS

1) Un programme illicite qui s'insère dans des programmes légitimes appelés hôtes.
   - ☐ Virus
   - ☐ Cheval de Troie
   - ☐ Rootkit
   - ☐ Backdoor
2) Type d'attaque qui vise à rendre une application informatique incapable de répondre aux requêtes des utilisateurs :
   - ☐ Backdoor
   - ☐ **Dos**
   - ☐ Malware
   - ☐ Robot
3) 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 ;
   - ☐ Sniffing
   - ☐ Cracking
   - ☐ Spoofing
   - ☐ Spamming
4) Une attaque qui affecte les requêtes en cours d'exécution sur des bases de données:
   - ☐ Cross Site Scripting (XSS)
   - ☐ Revoke
   - ☐ SQL Injection
   - ☐ Déni de Service
5) Un protocole de communication sécurisé permettant à des utilisateurs (ou bien à des services TCP/IP) d'accéder à une machine distante à travers une communication chiffrée.
   - ☐ Le protocole https
   - ☐ Le protocole PGP
   - ☐ Le protocole SSH
   - ☐ Le protocole SSL
6) L'estimation de la possibilité qu'un événement redouté, un scénario de menace ou un risque, se produise est connue par :
   - ☐ Vulnérabilité
   - ☐ **Vraisemblance**
   - ☐ Impact
   - ☐ Menace
7) Comment appelle t'on l'attaque qui utilise les rayonnements électromagnétiques pour rendre le SI inopérant ?
   - ☐ Pouriel
   - ☐ Brouillage
   - ☐ Phreaking
   - ☐ Smurfing
8) Programme ou ensemble de programmes permettant de maintenir dans le temps un accès frauduleux à un SI
   - ☐ Dos
   - ☐ Robot
   - ☐ Backdoor
   - ☐ **Rootkit**
9) Un programme malveillant qui exploite les capacités des applications de logiciels de bureautique

- Virus email
- Virus d'amorçage
- Virus macro
- Virus programme

10) L'insertion par l'attaquant du code HTML ou java script dans une page web fourni par un serveur s'appelle :
- Cross Site Scripting (XSS)
- SQL Injection
- Déni de Service
- Man in the Middle

11) Un système qui place une ou plusieurs cartes d'interface réseau du système dédié en mode promiscuité afin qu'elles n'aient pas d'adresse IP:
- N-IDS
- H-IDS
- IPS
- IDS

12) Une attaque qui cible un réseau à tunnel chiffré consiste à se placer entre le client et le serveur afin d'intercepter les clés de l'encryptage.
- Sniffing
- Physhing
- Man In The Middle
- Spoofing

13) Un protocol de communication qui sécurise les échanges au niveau de la couche application
- SSL
- PGP
- Ipsec
- TLS

14) L'ensemble des procédés d'attaque d'un système cryptographique
- Cryptologie
- Cryptanalyse
- Cryptosysteme
- Cryptographie

15) Dans un système de chiffrement symétrique les communicants utilisent une clé
- Secrète
- Privée
- Publique
- Publique et privée

16) Quel protocole sécurisé permettant de protéger à la fois les données et les en-têtes IP
- Ipsec en mode transport
- Ipsec en mode tunnel
- Ipv4
- Ipv6

17) Comment peut-on éviter une attaque Deni de service dos :
- Contrôle et limitation des taux de connexion au serveur
- Contrôle du temps de réponse
- Contrôle d'accès des requêtes pour détecter toutes celles qui sont non autorisées
- Toutes les réponses précédentes

18) Bob veut envoyer le message m= 6 à Alice, il le chiffre avec sa clé RSA et il obtient c=62. Quel est la paire de clé utilisée
- (n=133, e=5) et (n=133, d=65)

- (n=133, e=3) et (n=133, d=75)
- (n=133, e=7) et (n=133, d=17)
- (n=133, e=17) et (n=133, d=65)

19) La caractéristique d'une entité constituant une faiblesse ou une faille au regard de la sécurité est connue par :
- **Vulnérabilité**
- Vraisemblance
- Impact

20) Un processus parasite qui consomme, détruit et se propage sur le réseau s'appelle :
- Virus
- **Vers**
- Cheval de troie

21) Un type d'attaque technique qui peut être déposée sur la cible par spam, vers, virus, cheval de troie.
- Dos
- **Robot**
- Rootkit

22) Un programme malveillant qui exploite les capacités des applications de logiciels de bureautique
- Virus email
- **Virus macro**
- Virus programme

23) Tout programme qui exploite les vulnérabilités d'un SI s'appelle :
- Spyware
- Backdoor
- **Malware**

24) L'insertion par l'attaquant du code HTML ou java script dans une page web fourni par un serveur s'appelle :
- **Cross Site Scripting (XSS)**
- SQL Injection
- Déni de Service

25) Afin de surmonter le problème d'abus de privilèges d'accès à une BDD (DB) l'administrateur A_1 a décidé de supprimer tout les privilèges de tout les autres utilisateurs de la base en exécutant une requête SQL, laquelle ?
- REVOKE from all
- REVOKE all To all
- **REVOKE all from all**

26) Un programme illicite qui s'insère dans des programmes légitimes appelés hôtes.
- **Virus**
- Vers
- Rootkit

27) Un type d'attaque qui consiste à piéger l'utilisateur en lui faisant croire qu'il s'adresse à un tiers de confiance pour lui soutirer des informations confidentielles :
- **Hameçonnage**
- Craquage
- Renifflage

28) Type d'attaque qui vise à rendre une application informatique incapable de répondre aux requêtes des utilisateurs :

- Backdoor
- **Dos**
- Malware

29) En analyse des risques l'agent responsable du risque s'appelle :
- Source
- Actif
- **Menace**

30) 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 ;
- **Technique de renifflage (sniffing)**
- Technique de craquage (cracking)
- Techniques de mascarade (spoofing)

31) Une attaque qui affecte les requêtes en cours d'exécution sur des bases de données:
- Cross Site Scripting (XSS)
- **SQL Injection**
- Déni de Service

32) Un protocole de communication sécurisé permettant à des utilisateurs (ou bien à des services TCP/IP) d'accéder à une machine distante à travers une communication chiffrée.
   a) Le protocole Secure HTTP
   b) Le protocole SSH (Secure Shell)
   c) Le protocole SSL (Secure Sockets Layers)

33) L'estimation de la possibilité qu'un événement redouté, un scénario de menace ou un risque, se produise est connue par :
   a) Vulnérabilité
   b) Vraisemblance
   c) Impact

34) Un programme ayant une fonction annoncée et en réalisant une autre (illicite) :
   a) Virus
   b) Vers
   c) Cheval de troie

35) Programme ou ensemble de programmes permettant de maintenir dans le temps un accès frauduleux à un SI
   a) Dos
   b) Robot
   c) Rootkit

Questions de cours

1) Un système d'information est composé du (1) matériel informatique, (2) des logiciels, (3) des données ainsi que (4) des ressources humaines qui les mettent en œuvre.

-Proposer pour chacun de ces composants un mécanisme de protection adéquat

Réponse.

Sécurité du matériel

- Contrôles d'accès adéquats au matériel ;
- Qualité de l'alimentation électrique ;

- Certification adéquate du câblage du réseau local et des accès aux réseaux extérieurs ; la capacité des infrastructures de communication est très sensible à la qualité physique du câblage et des connexions ;
- Pour l'utilisation de réseaux sans fil, placement méticuleux des bornes d'accès, réglage de leur puissance d'émission et contrôle des signaux en provenance et à destination de l'extérieur.

Sécurité des logiciels

- Droit d'accès en consultation (lecture) en modification (écriture, destruction, création), de blocage et en exécution ;
- Antivirus, antispyware

Sécurité des données

- Sauvegarde régulière des données sur des supports physiques adéquats distincts des supports utilisés en production ;
- Transport régulier de copies de sauvegarde en dehors du site d'exploitation ;
- Aménagement d'un site de secours pour les applications vitales.
- Cryptographie

Sécurité des ressources humaines

- Qualification et sensibilisation du personnel à propos des règles de sécurité sur les lieux de travail
- L'aménagement ou le réaménagement des lieux de travail ou des installations

2) Définir le spoofing, le spamming et le phishing.

Réponse :

- Spoofing : Usurpation d'identité on se fait passer pour une autre machine.
- Spamming : Envoie de courriers non sollicités à but commercial
- Phishing : Envoie de courriers permettant le détournement d'information

3) Soit les scenarios d'attaque ci-dessous, identifier le type d'attaque:

- L'utilisateur installe sur sa machine un CD de jeu, puis le responsable de l'attaque lui fournit une adresse IP, un nom d'utilisateur et un mot de passe pour accéder au pc de sa victime.
- Une menace détectée sur la machine client après la lecture d'un document bureautique.
- L'utilisateur clique sur le lien en croyant qu'il se connecte sur un site de vente en ligne, puis il saisit des informations confidentielles. Mais en réalité, il se connecte sur un faux site et un pirate récupère ses informations

Réponse :

- 1/➔cheval de Troie
- 2/➔ virus macro
- 3/➔ Hameçonnage (Phishing)
-

4) Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données, lesquels ?

Réponse :

- Limiter et contrôler l'accès aux données
- Les rendre inintelligibles en les chiffrant