QCM 2 – Exploitation, Livraison, Maintien, IA

1. Quelle est la différence entre vulnérabilité et exploit ?
   a) Aucune
   b) Une vulnérabilité est un programme
   c) L'exploit est le moyen de tirer parti de la vulnérabilité
   d) La vulnérabilité est une attaque active

2. Que signifie SQLi ?
   a) SQL Insertion
   b) Structured Query Injection
   c) SQL Injection
   d) Secure Query Language

3. Quelle requête SQL illustre une injection ?
   a) SELECT * FROM users
   b) SELECT '1' FROM DUAL
   c) SELECT * FROM users WHERE username='' or 1=1 --
   d) SELECT * FROM users WHERE id=5

4. Que permet une attaque XSS ?
   a) Accéder à la base de données
   b) Exécuter du JavaScript dans le navigateur de la victime
   c) Lancer un ransomware
   d) Injecter du HTML dans une image

5. Quel outil est utilisé pour automatiser des exploits connus ?
   a) Metasploit
   b) GDB
   c) GCC
   d) Burp Proxy

6. Quelle attaque consiste à injecter du code serveur dans une page web ?
   a) XSS
   b) SSI
   c) LFI
   d) CSRF

7. Dans quelle attaque utilise-t-on `<!--#exec cmd="ls" -->` ?
   a) XSS
   b) LFI
   c) SSI
   d) Phishing

8. Une page de phishing contient :
   a) Un lien vers Google
   b) Un formulaire redirigé vers un serveur attaquant
   c) Un PDF légitime
   d) Du code HTML chiffré

9. Le tunneling SSH permet :
   a) De forcer une mise à jour système
   b) D'exécuter des commandes sur la victime à travers SSH
   c) De bloquer le pare-feu
   d) D'envoyer des cookies

10. La stéganographie LSB consiste à :
    a) Chiffrer les images en AES
    b) Remplacer les bits de poids fort dans une image
    c) Cacher des données dans les bits de poids faible
    d) Supprimer les métadonnées

11. Que fait le fichier `stealer.php` dans un phishing ?
    a) Exécute des requêtes SQL
    b) Récupère les identifiants et les stocke
    c) Bloque les cookies
    d) Chiffre la page HTML

12. Quelle est la différence entre LFI et RFI ?
    a) LFI utilise Internet
    b) RFI permet d'inclure un fichier distant
    c) LFI est une attaque passive
    d) Aucune

13. Quel type de scan est souvent détecté par un IDS ?
    a) SYN scan
    b) XMAS scan
    c) UDP stealth
    d) Full scan

14. Que signifie obfuscation ?
    a) Rendre le code plus lisible
    b) Cacher les données dans des images ou formats
    c) Ajouter un firewall
    d) Supprimer les logs

15. Quel module Python permet le SSH tunneling ?
    a) scapy
    b) openssh
    c) paramiko
    d) twisted

16. Quelle IA est utilisée pour détecter du texte généré automatiquement ?
    a) pandas
    b) transformers
    c) selenium
    d) keras

17. Que permet une prompt injection ?
    a) Exécuter du code sans authentification
    b) Exécuter un code malicieux en trompant un LLM
    c) Injecter du code dans un shell
    d) Exploiter une faille réseau

18. L'exploit du PHP-CGI (CVE-2012-1823) permet :
    a) De modifier un mot de passe root
    b) D'exécuter du code PHP arbitraire
    c) D'injecter des cookies
    d) D'empêcher les logs

19. Pourquoi l'IA est-elle efficace pour le phishing ?
    a) Elle crypte les mails
    b) Elle détecte les antivirus
    c) Elle génère du contenu crédible et personnalisé
    d) Elle contourne les firewalls

20. Un deepfake vocal permet :
    a) De forcer une réauthentification
    b) D'imiter la voix d'un humain pour tromper la cible
    c) De modifier des images
    d) De voler des certificats SSL

Correction QCM 2 – Exploitation, Livraison, Maintien, IA

1. ✅ **c) L’exploit est le moyen de tirer parti de la vulnérabilité**
   Une vulnérabilité est une faiblesse ; un exploit est le code ou le procédé qui l'utilise.
   Ex : SQLi est une vulnérabilité, une requête forgée est l’exploit.

2. ✅ **c) SQL Injection**
   SQLi est l’abréviation standard de SQL Injection : technique consistant à injecter du code SQL malicieux dans des champs non filtrés.

3. ✅ **c) SELECT * FROM users WHERE username='' or 1=1 --**
   Cette requête contourne l'authentification en forçant la clause WHERE à toujours être vraie (`1=1`).

4. ✅ **b) Exécuter du JavaScript dans le navigateur de la victime**
   L'attaque XSS consiste à injecter du JS qui s’exécute côté client (navigateur) et peut voler des cookies ou rediriger vers un faux site.

5. ✅ **a) Metasploit**
   Metasploit est un framework d'exploitation utilisé pour automatiser l’envoi d’exploits. Il inclut une base d’exploits (exploit-db).

6. ✅ **b) SSI**
   Server Side Includes (SSI) permet d'injecter des commandes à exécuter côté serveur via des balises comme `<!--#exec cmd="ls" -->`.

7. ✅ **c) SSI**
   L’exécution de `ls` dans une balise SSI est un cas typique d’exploitation de cette vulnérabilité si le serveur accepte ces inclusions.

8. ✅ **b) Un formulaire redirigé vers un serveur attaquant**
   Une page de phishing est une copie visuelle d’un site légitime, mais dont le formulaire envoie les données à l’attaquant.

9. ✅ **b) D'exécuter des commandes sur la victime à travers SSH**
   Le SSH tunneling permet à une cible compromise de se connecter à un serveur distant pour exécuter ou recevoir des commandes.

10. ✅ **c) Cacher des données dans les bits de poids faible**
    La stéganographie LSB insère des données dans les derniers bits de chaque pixel. Cela rend la modification invisible à l'œil nu.

11. ✅ **b) Récupère les identifiants et les stocke**
    `stealer.php` est un script côté serveur qui récupère les identifiants d’un formulaire (phishing) et les stocke en local ou en base.

12. ✅ **b) RFI permet d'inclure un fichier distant**
    LFI = inclusion locale (sur le serveur), RFI = inclusion distante (via URL). Le danger du RFI est d'exécuter du code hébergé ailleurs.

13. ✅ **d) Full scan**
    Un full TCP scan (connect scan) est bruyant car il établit une connexion complète (3-way handshake) et est facilement détectable par un IDS.

14. ✅ **b) Cacher les données dans des images ou formats**
    L'obfuscation consiste à dissimuler des données dans des fichiers ou à les encoder de manière difficile à lire pour les antivirus.

15. ✅ **c) paramiko**
    `paramiko` est une bibliothèque Python permettant de gérer des connexions SSH. Elle est utilisée pour les reverse shells, tunnels chiffrés, etc.

16. ✅ **b) transformers**
    `transformers` de Hugging Face permet d'analyser le style d'un texte pour détecter s'il a été généré par une IA (ex. GPT, LLaMA...).

17. ✅ **b) Exécuter un code malicieux en trompant un LLM**
    Une injection de prompt modifie les consignes internes d'un LLM pour l'amener à fournir des réponses malveillantes.

18. ✅ **b) D'exécuter du code PHP arbitraire**
    La faille PHP-CGI (CVE-2012-1823) permet, via une mauvaise gestion des requêtes, d'injecter et exécuter des commandes PHP.

19. ✅ **c) Elle génère du contenu crédible et personnalisé**
    Les LLMs permettent de créer des messages de phishing ultra-réalistes, sans fautes, adaptés à la langue ou au contexte de la victime.

20. ✅ **b) D'imiter la voix d'un humain pour tromper la cible**
    Un deepfake vocal utilise l'IA pour cloner la voix d'une personne réelle, typiquement pour arnaquer une entreprise via ingénierie sociale.