UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Connaître les techniques de hacking et les contre-mesures

Sommaire

Introduction au Hacking Éthique

- Concepts de base
- Cadre juridique et éthique

Techniques de Hacking

- Reconnaissance (Reconnaissance)
- Scanning et énumération
- Exploitation des vulnérabilités
- Maintien de l'accès
- Escalade de privilèges
- Couverture des traces

Sommaire

Contre-mesures

- Reconnaissance et détection
- Renforcement des systèmes et des réseaux
- Protection contre les exploits
- Contrôle d'accès et gestion des privilèges
- Cryptographie et sécurisation des communications
- Plan de réponse aux incidents
- Formation et sensibilisation des utilisateurs

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Introduction au Hacking Éthique

Introduction au Hacking Éthique

Concepts de base

- Le **hacking éthique**, également appelé piratage éthique ou test d'intrusion, désigne la pratique consistant à pénétrer des systèmes informatiques, des réseaux ou des applications avec l'autorisation des propriétaires dans le but de découvrir des vulnérabilités que des hackers malveillants pourraient exploiter.
- Cette pratique est effectuée par des professionnels qualifiés appelés hackers éthiques ou pentesteurs, qui utilisent les mêmes techniques et outils que les cybercriminels, mais de manière légale et constructive pour améliorer la sécurité des systèmes.

Introduction au Hacking Éthique

Concepts de base

Le hacking éthique est crucial pour renforcer la sécurité informatique. Il aide les organisations à :

1. **Identifier et corriger les failles de sécurité** avant qu'elles ne soient exploitées.
2. **Évaluer l'efficacité des mesures de sécurité** en place, y compris les politiques de sécurité, l'accès aux points de contrôle, et les mécanismes de défense.
3. **Respecter les réglementations et normes de sécurité** qui requièrent des audits de sécurité réguliers, comme le GDPR, HIPAA, et PCI DSS.
4. **Sensibiliser et former** les équipes de sécurité et de développement sur les meilleures pratiques de sécurité et les dernières techniques de piratage.

Introduction au Hacking Éthique

Concepts de base

La différence fondamentale entre le hacking éthique et le hacking malveillant réside dans l'intention, la permission et l'impact de l'activité sur les systèmes ciblés.

1. **Intention**:
   - **Hacking éthique** : L'intention est de renforcer la sécurité. Les hackers éthiques cherchent à identifier et à réparer les vulnérabilités pour prévenir des attaques malveillantes. Leur but est bénéfique et vise à améliorer la situation.
   - **Hacking malveillant** : L'intention est de causer du tort, d'exploiter les failles à des fins personnelles ou criminelles, comme le vol de données, la perturbation des services, ou le gain financier.

Introduction au Hacking Éthique

Concepts de base

2. **Permission**:
   - **Hacking éthique** : Il est toujours réalisé avec la permission explicite des propriétaires des systèmes informatiques. Cette permission est souvent formalisée par un contrat ou un accord légal définissant le cadre de l'action.
   - **Hacking malveillant** : Il est effectué sans consentement, violant ainsi les lois et les politiques de confidentialité. Cela constitue une intrusion illégale dans les systèmes d'autrui.

Introduction au Hacking Éthique

Concepts de base

3. **Méthodologie**:
   - **Hacking éthique** : Les méthodes utilisées sont structurées et documentées. Les hackers éthiques suivent des lignes directrices éthiques strictes et s'assurent que leur travail est transparent et réversible. Ils rapportent toutes les vulnérabilités trouvées aux propriétaires et conseillent souvent sur les moyens de les réparer.
   -
   - **Hacking malveillant** : Les techniques peuvent être destructrices et visent souvent à masquer les traces de l'intrusion. Les hackers malveillants utilisent leurs compétences pour exploiter les failles sans en informer les victimes, et souvent en laissant des backdoors pour faciliter l'accès futur.

Introduction au Hacking Éthique

Concepts de base

4. **Impact**:
   - **Hacking éthique** : L'impact est positif, car il conduit à une meilleure sécurité et à une plus grande sensibilisation aux vulnérabilités et aux risques de sécurité.
   -
   - **Hacking malveillant** : L'impact est négatif, entraînant des pertes financières, des dommages à la réputation, la perte de données sensibles, et d'autres conséquences dommageables pour les victimes.

Introduction au Hacking Éthique

Cadre juridique et éthique

La législation relative à la sécurité informatique varie considérablement d'un pays à l'autre, mais elle couvre généralement plusieurs aspects fondamentaux pour protéger les données et les systèmes informatiques contre les menaces de sécurité.

Introduction au Hacking Éthique

Cadre juridique et éthique

1. Union européenne (UE) - Règlement général sur la protection des données (RGPD)

- **Objectif** : Protéger les données personnelles des citoyens de l'UE.
- **Implications** : Impose des exigences strictes sur la collecte, le stockage et la gestion des données personnelles, y compris la nécessité d'obtenir un consentement explicite, le droit à l'oubli, et des notifications obligatoires en cas de violation de données.

Introduction au Hacking Éthique

Cadre juridique et éthique

2. États-Unis - Health Insurance Portability and Accountability Act (HIPAA)

- **Objectif** : Protéger les informations médicales privées.
- **Implications** : Définit comment les informations de santé personnelles doivent être protégées, y compris des exigences pour les mesures de sécurité physiques, administratives et techniques.

Introduction au Hacking Éthique

Cadre juridique et éthique

3. États-Unis et UE - Privacy Shield Framework

- **Objectif** : Faciliter le transfert transatlantique de données personnelles entre l'UE et les États-Unis dans le respect de la protection de la vie privée.
- **Implications** : Fournit un mécanisme pour les entreprises américaines pour se conformer aux exigences de protection des données de l'UE.

Introduction au Hacking Éthique

Cadre juridique et éthique

4. États-Unis - Children’s Online Privacy Protection Act (COPPA)

- **Objectif** : Protéger les enfants de moins de 13 ans lorsqu'ils utilisent des services en ligne.
- **Implications** : Exige que les sites web et services en ligne dirigés vers les enfants obtiennent le consentement parental avant de collecter des informations personnelles des enfants.

Introduction au Hacking Éthique

Cadre juridique et éthique

5. International - Payment Card Industry Data Security Standard (PCI DSS)

- **Objectif** : Protéger les données des titulaires de cartes de crédit.
- **Implications** : Établit des normes de sécurité opérationnelle pour tous les membres, marchands et prestataires de services qui stockent, traitent ou transmettent des informations de titulaire de carte.

Introduction au Hacking Éthique

Rôle et responsabilité des hackers éthiques

- Les hackers éthiques jouent un rôle crucial dans la protection des systèmes informatiques contre les attaques malveillantes.
- Leur travail consiste à tester de manière proactive la sécurité des systèmes pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées par des acteurs malveillants.

Introduction au Hacking Éthique

Rôles des hackers éthiques

1. **Évaluation de la sécurité** : Réaliser des tests d'intrusion et des audits de sécurité pour évaluer la robustesse des systèmes, des réseaux, des applications web et mobiles contre les tentatives d'intrusion.
2. **Identification des vulnérabilités** : Utiliser des méthodes et outils avancés pour découvrir les failles de sécurité dans les infrastructures informatiques, y compris les failles logicielles, les configurations erronées, et les pratiques inadéquates de gestion des données.
3. **Rapport détaillé** : Fournir des rapports détaillés sur les vulnérabilités détectées, leur niveau de risque, et les méthodes d'exploitation potentielles. Ceux-ci incluent également des recommandations pratiques pour sécuriser les systèmes.
4. **Validation des correctifs** : Après que les vulnérabilités identifiées ont été corrigées par les équipes de TI, réaliser une nouvelle série de tests pour s'assurer que les correctifs sont efficaces et ne créent pas de nouvelles failles.
5. **Formation et sensibilisation** : Éduquer les développeurs, le personnel TI et les utilisateurs finaux sur les meilleures pratiques de sécurité, les nouvelles menaces et comment se protéger contre les attaques.

Introduction au Hacking Éthique

Responsabilités des hackers éthique

1. **Confidentialité** : Maintenir la confidentialité des informations découvertes lors des tests. Les hackers éthiques ne doivent pas divulguer ou utiliser ces informations à des fins personnelles ou non autorisées.
2. **Intégrité** : Agir avec intégrité en évitant d'endommager les systèmes cibles ou de perturber leurs opérations normales lors des tests.
3. **Légalité** : Opérer toujours dans les limites de la loi, avec la permission explicite des propriétaires des systèmes. Ils doivent suivre un cadre légal strict pour éviter les implications juridiques pour eux-mêmes et pour les organisations pour lesquelles ils travaillent.
4. **Rapport responsable** : S'assurer que les vulnérabilités sont rapportées aux bonnes parties prenantes de manière sécurisée pour éviter toute fuite d'informations qui pourrait bénéficier à des hackers malveillants.
5. **Mise à jour continue** : Restez à jour avec les dernières tendances en matière de cybersécurité, les techniques de hacking et les technologies de défense pour rester efficaces dans leur rôle.

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Techniques de Hacking

Techniques de Hacking

Pentesting

Les techniques de hacking dans le cadre de tests d'intrusion (pentest) suivent une structure assez standardisée.

- **Reconnaissance (Reconnaissance)**
- **Scanning (Balayage)**
- **Gaining Access (Obtenir l'accès)**
- **Maintaining Access (Maintien de l'accès)**
- **Exploitation**
- **Covering Tracks (Effacement de traces)**

Techniques de Hacking

Pentesting

1. **Reconnaissance (Reconnaissance)**
   - **Objectif :** Recueillir des informations sur la cible pour préparer les étapes suivantes.
   - **Techniques :** Recherche d'informations publiques (OSINT), exploration de réseaux sociaux, analyse de sites web, reconnaissance passive (sans interaction directe avec la cible) et reconnaissance active (balayage de réseau).
2. **Scanning (Balayage)**
   - **Objectif :** Identifier les vulnérabilités et les points d'entrée potentiels dans le système cible.
   - **Techniques :** Scan de ports (pour identifier les services ouverts), scan de vulnérabilités (pour identifier les failles de sécurité), analyse de services (pour comprendre quels services sont en cours d'exécution et leurs versions), et identification des systèmes d'exploitation.

Techniques de Hacking

Pentesting

3. **Gaining Access (Obtenir l'accès)**
   - **Objectif :** Exploiter les vulnérabilités identifiées pour accéder au système cible.
   - **Techniques :** Utilisation d'exploits, attaques par injection SQL, attaques par force brute, attaques par phishing, exploitation de failles logicielles.
4. **Maintaining Access (Maintien de l'accès)**
   - **Objectif :** Installer des moyens pour maintenir l'accès au système même après la détection ou la correction des failles initiales.
   - **Techniques :** Installation de portes dérobées (backdoors), création de comptes utilisateurs, modification de configurations système, installation de rootkits.

Techniques de Hacking

Pentesting

5. **Exploitation**
   - **Objectif :** Réaliser les objectifs de l'attaque tels que le vol de données, la compromission de systèmes supplémentaires ou la perturbation des services.
   - **Techniques :** Escalade de privilèges, extraction de données sensibles, exécution de commandes à distance, déplacement latéral pour compromettre d'autres parties du réseau.
6. **Covering Tracks (Effacement de traces)**
   - **Objectif :** Effacer les traces de l'intrusion pour éviter la détection et les enquêtes post-incident.
   - **Techniques :** Suppression des journaux de connexion, modification des horodatages des fichiers, utilisation de techniques d'obscurcissement, suppression des fichiers temporaires et des logs.

Techniques de Hacking

Pentesting

Documentation :

- **OSSTMM (Open Source Security Testing Methodology Manual) :** Un cadre complet pour les tests de sécurité couvrant divers types de tests (réseaux, applications, humains, etc.).
- **OWASP (Open Web Application Security Project) :** Fournit des guides et des méthodologies spécifiques pour les tests de sécurité des applications web.
- **PTES (Penetration Testing Execution Standard) :** Un standard pour l'exécution de tests d'intrusion, décrivant les phases de planification, de reconnaissance, de balayage, d'exploitation, de post-exploitation et de reporting.
- **NIST SP 800-115 :** Un guide du National Institute of Standards and Technology pour la conduite des tests techniques de sécurité.

Techniques de Hacking

Les techniques d'attaques par catégorie

1. Techniques de Reconnaissance :

- **Footprinting :** Collecte d'informations sur la cible à partir de sources publiques.
- **Whois :** Recherche d'informations sur l'enregistrement de domaines.
- **Reconnaissance DNS :** Extraction d'informations à partir de serveurs DNS.
- **Social Engineering :** Manipulation des personnes pour obtenir des informations sensibles.

2. Techniques de Scanning :

- **Port Scanning :** Identification des ports ouverts sur un réseau ou un système.
- **Vulnerability Scanning :** Utilisation d'outils pour identifier les vulnérabilités dans les systèmes et les applications.
- **Network Mapping :** Création d'une carte des appareils et des services sur un réseau.

Techniques de Hacking

Les techniques d'attaques par catégorie

3. Techniques d'Exploitation

- **Injection SQL :** Insertion de commandes SQL malveillantes dans des requêtes d'application web.
- **Cross-Site Scripting (XSS) :** Injection de scripts malveillants dans des pages web vues par d'autres utilisateurs.
- **Buffer Overflow :** Exploitation d'erreurs de gestion de mémoire pour exécuter du code malveillant.
- **Phishing :** Envoi de courriels ou de messages trompeurs pour obtenir des informations sensibles.
- **Exploits Zero-Day :** Utilisation de vulnérabilités non encore connues du public ou des fournisseurs.

4. Techniques de Maintien de l'Accès

- **Backdoors :** Installation de portes dérobées pour un accès ultérieur non autorisé.
- **Rootkits :** Outils permettant de masquer les processus et les fichiers, rendant l'accès persistant difficile à détecter.

Techniques de Hacking

Les techniques d'attaques par catégorie

5. Techniques de Post-Exploitation

- **Privilege Escalation :** Obtention de niveaux de privilèges plus élevés sur un système compromis.
- **Pivoting :** Utilisation d'un système compromis pour attaquer d'autres systèmes sur le même réseau.
- **Data Exfiltration :** Vol de données sensibles à partir du système compromis.

6. Techniques d'Effacement de Traces

- **Log Cleaning :** Suppression ou modification des journaux de sécurité pour effacer les traces d'activité.
- **Timestamp Manipulation :** Changement des dates et heures des fichiers pour masquer les actions.
- **Anti-Forensics :** Techniques pour contrecarrer les efforts d'analyse post-incident, comme l'encryption ou l'obfuscation des données.

Techniques de Hacking

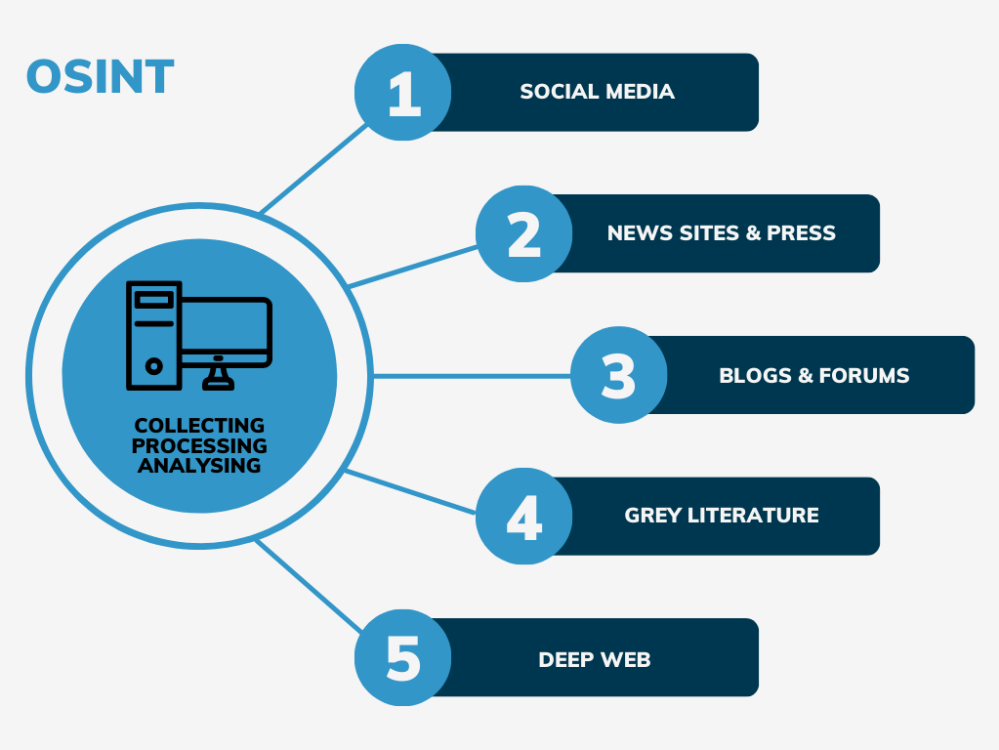
Les techniques d'attaques par catégorie

7. Techniques de Réseaux et de Communications

- **Sniffing :** Capture et analyse du trafic réseau.
- **Man-in-the-Middle (MITM) :** Interception et altération des communications entre deux parties sans qu'elles le sachent.
- **ARP Spoofing :** Usurpation d'adresses IP pour intercepter le trafic réseau.

Techniques de Hacking

Reconnaissance



Techniques de Hacking

Reconnaissance

L'Open Source Intelligence (OSINT) désigne la collecte et l'analyse d'informations disponibles publiquement à partir de sources ouvertes.

1. Recherche sur Internet

- **Moteurs de recherche :** Utilisation de moteurs de recherche comme Google, Bing, ou DuckDuckGo pour trouver des informations.
- **Opérateurs de recherche avancée :** Utilisation d'opérateurs comme site:, filetype:, intext:, intitle:, etc. pour affiner les recherches.
- **Wayback Machine :** Utilisation de l'Internet Archive pour accéder aux versions archivées de pages web.

Techniques de Hacking

Reconnaissance

2. Réseaux sociaux

- **Profilage :** Analyse des profils et des publications sur des plateformes comme Facebook, Twitter, LinkedIn, Instagram.
- **Graph Search :** Utilisation de fonctionnalités de recherche avancée pour découvrir les relations et les connexions entre les utilisateurs.
- **Sentiment Analysis :** Analyse des sentiments des publications pour obtenir des informations sur les opinions et les attitudes.

Techniques de Hacking

Reconnaissance

3. Bases de données et registres publics

- **Whois :** Consultation des informations de registre de domaine.
- **Registres d'entreprises :** Accès aux informations sur les entreprises via des registres comme Infogreffe, Companies House, etc.
- **Documents gouvernementaux :** Recherches dans les bases de données gouvernementales, les archives judiciaires, les rapports financiers, etc.

Techniques de Hacking

Reconnaissance

4. Forums et communautés en ligne

- **Recherche dans les forums :** Participation et surveillance des discussions sur des forums spécialisés comme Reddit, 4chan, etc.
- **Newsgroups :** Utilisation de groupes de discussion comme Google Groups pour trouver des informations spécialisées.

Techniques de Hacking

Reconnaissance

5. Médias traditionnels et électroniques

- **Articles de presse :** Lecture et analyse d'articles de journaux, de magazines, et de sites d'information.
- **Communiqués de presse :** Surveillance des communiqués de presse pour des informations officielles.

6. Analyse de documents

- **Metadata :** Extraction et analyse des métadonnées des documents pour obtenir des informations supplémentaires.
- **OCR (Optical Character Recognition) :** Utilisation de la reconnaissance optique de caractères pour extraire du texte à partir d'images ou de PDF scannés.

Techniques de Hacking

Reconnaissance

7. Surveillance des réseaux

- **Analyse de trafic :** Surveillance et analyse du trafic réseau pour détecter des informations sensibles.
- **Sniffing :** Utilisation d'outils de sniffing pour capturer et analyser les paquets de données sur un réseau.

8. Techniques de géolocalisation

- **Analyse de photos :** Utilisation des métadonnées des photos (EXIF) pour obtenir des informations sur l'emplacement et l'heure de la prise de vue.
- **Google Earth/Maps :** Utilisation des outils de cartographie pour analyser des emplacements et des infrastructures.

Techniques de Hacking

Reconnaissance

9. Scraping et automatisation

- **Web scraping :** Utilisation d'outils et de scripts pour extraire des informations de sites web de manière automatisée.
- **Bots :** Développement de bots pour automatiser la collecte d'informations sur différentes plateformes.

10. Analyse des relations

- **Graphes de liens :** Utilisation de logiciels pour créer des graphes de liens entre des entités (personnes, entreprises, événements) pour visualiser et analyser les relations.

Techniques de Hacking

Reconnaissance

- Google hacking :
  https://www.google.com/advanced_search?hl=fr
  https://www.exploit-db.com/google-hacking-database

Techniques de Hacking

Reconnaissance

- Autre moteur de recherche :
  https://www.shodan.io/
  https://tineye.com/

Techniques de Hacking

Reconnaissance

- Autre outils reconnaissance :
  - Spiderfoot
  - nslookup
  - dig
  - Whois
  - ping
  - traceroute

Techniques de Hacking

Reconnaissance

- Autre outils reconnaissance :
  - https://www.iplocation.net
  - https://web.archive.org

Techniques de Hacking

Reconnaissance

- Autre outils reconnaissance :
  - Maltego
  - Recon-ng

Techniques de Hacking

Scanning

- La phase de scanning, ou balayage, est une étape cruciale dans le processus de test d'intrusion (pentest).
- Elle intervient après la phase de reconnaissance (reconnaissance passive et active) et vise à identifier les points d'entrée potentiels que l'attaquant pourrait exploiter.

Techniques de Hacking

Scanning

Le scanning est le processus de collecte d'informations sur les systèmes, les réseaux et les services en ligne pour découvrir des vulnérabilités potentielles. Cela inclut l'identification des hôtes actifs, des ports ouverts, des services en cours d'exécution et des versions de logiciels, ainsi que des configurations de sécurité.

Techniques de Hacking

Scanning

La phase de scanning peut être décomposée en plusieurs sous-étapes :

- **Scanning des ports :** Déterminer quels ports sur un hôte cible sont ouverts ou fermés. Cela aide à identifier les services actifs sur ces ports.
- **Détection de services :** Identifier les services en cours d'exécution et les versions des logiciels sur les ports ouverts.
- **Scanning des vulnérabilités :** Chercher des vulnérabilités connues dans les services et logiciels identifiés.
- **Cartographie du réseau :** Obtenir une vue d'ensemble de l'architecture du réseau cible.

Techniques de Hacking

Scanning

Outils utilisés pour le scanning

Nmap : Pour le scanning des ports, la détection de services, et les scripts NSE pour la détection de vulnérabilités.
Nessus : Pour un scanning de vulnérabilités approfondi.
OpenVAS : Alternative open-source à Nessus.
Masscan : Pour le scanning de ports à très haute vitesse.

Techniques de Hacking

Scanning

Outils utilisés pour le scanning

Masscan : Pour le scanning de ports à très haute vitesse.
Unicornscan : Un scanner de réseau avancé pour une analyse et une reconnaissance plus rapide.
Hping : Un outil de ligne de commande pour assembler et analyser des paquets TCP/IP.
Metasploit : Framework pour tester les vulnérabilités découvertes et pour des scans de vulnérabilité avancés.

Techniques de Hacking

Scanning

Nmap

Nmap (Network Mapper) est un outil de scanner de réseau très puissant et polyvalent, largement utilisé dans le domaine de la sécurité informatique et du hacking éthique. Développé par Gordon Lyon, également connu sous le pseudonyme "Fyodor", Nmap est open source et disponible sous licence GNU GPL.

Techniques de Hacking

Scanning

Nmap

1. **Scanning de ports** :
   - Nmap permet de scanner les ports d'un ou plusieurs hôtes pour déterminer quels ports sont ouverts, fermés ou filtrés. Cela permet aux administrateurs système et aux chercheurs en sécurité de comprendre la topologie du réseau et d'identifier les services exposés.
2. **Détection de services et de versions** :
   - En plus de scanner les ports, Nmap peut détecter les services tournant sur ces ports et même déterminer les versions des logiciels utilisés. Cette fonctionnalité est cruciale pour évaluer la sécurité des systèmes en identifiant les services vulnérables ou obsolètes.

Techniques de Hacking

Scanning

Nmap

3. **Détection d'hôtes actifs** :
    - Nmap peut être utilisé pour détecter quels hôtes sont actifs sur un réseau donné en utilisant des techniques telles que les requêtes ARP, les paquets ICMP, et d'autres méthodes de découverte de réseau.
4. **Scripts Nmap (NSE - Nmap Scripting Engine)** :
    - Nmap inclut un moteur de scripts (NSE) qui permet aux utilisateurs d'automatiser des tâches complexes telles que la découverte de vulnérabilités, l'exploitation de services faibles, la récupération d'informations supplémentaires sur les hôtes, etc. Ces scripts sont écrits en Lua et peuvent être personnalisés pour répondre aux besoins spécifiques de l'utilisateur.

Techniques de Hacking

Scanning

Nmap

5. **Options avancées de scan** :
   - Nmap offre une gamme d'options avancées pour personnaliser les scans, y compris la fragmentation de paquets pour contourner les systèmes de détection d'intrusion (IDS), l'utilisation de faux paquets pour masquer l'origine du scan, le scan de tous les ports (de 1 à 65535), etc.
6. **Utilisation légale et éthique** :
   - Nmap est largement utilisé dans le cadre du hacking éthique pour évaluer la sécurité des réseaux et des systèmes informatiques. Cependant, il est essentiel d'utiliser Nmap de manière éthique et légale, avec l'autorisation appropriée, pour éviter tout problème juridique.

Techniques de Hacking

Scanning

Utilisations courantes de Nmap :

- **Audit de sécurité** : Évaluation des vulnérabilités et des configurations de sécurité des réseaux et des systèmes.
- **Gestion des réseaux** : Découverte de la topologie du réseau et gestion des périphériques connectés.
- **Réponse aux incidents** : Utilisation lors d'incidents de sécurité pour identifier les points d'entrée potentiels et les activités suspectes.
- **Surveillance de la sécurité** : Surveillance continue des ports et des services pour détecter les changements non autorisés.

Techniques de Hacking

Scanning

Scans de base (Nmap) :

1. **Scan de découverte de réseau (Ping Scan)** :
   - **Commande**: `nmap -sn <cible>`
   - **Description**: Cela envoie des paquets ICMP (ping) pour découvrir les hôtes actifs sur le réseau sans scanner les ports.
2. **Scan TCP SYN (Half-open Scan)** :
   - **Commande**: `nmap -sS <cible>`
   - **Description**: Envoie des paquets SYN pour déterminer quels ports sont ouverts sur un hôte. Utile pour contourner les pare-feu.

Techniques de Hacking

Scanning

Scans de base (Nmap) :

3. **Scan TCP Connect** :
   - **Commande**: `nmap -sT <cible>`
   - **Description**: Établit une connexion TCP complète pour déterminer l'état des ports (ouverts, fermés, filtrés).
4. **Scan UDP** :
   - **Commande**: `nmap -sU <cible>`
   - **Description**: Scan des ports UDP pour découvrir les services tournant sur ces ports.

Techniques de Hacking

Scanning

Scans de base (Nmap) :

5. **Scan de versions (Service Version Detection)** :
   - **Commande**: `nmap -sV <cible>`
   - **Description**: Détermine les versions des services tournant sur les ports ouverts.
6. **Scan de script NSE (Nmap Scripting Engine)** :
   - **Commande**: `nmap -sC <cible>`
   - **Description**: Exécute des scripts Nmap préconstruits pour détecter des vulnérabilités, récupérer des informations supplémentaires, etc.

Techniques de Hacking

Scanning

Scans de base (Nmap) :

7. **Scan de sous-réseaux spécifiques (CIDR)** :
   - **Commande**: `nmap <sous-réseau>`
   - **Description**: Scan d'un sous-réseau complet pour découvrir tous les hôtes actifs.
8. **Scan de tous les ports (All Ports)** :
   - **Commande**: `nmap -p- <cible>`
   - **Description**: Scan de tous les 65535 ports TCP pour découvrir les services disponibles.

Techniques de Hacking

Scanning

Exemple de scan avec Nmap :

- **Scan d'un seul port** :
  - **Commande**: `nmap -p <port> <cible>`
  - **Description**: Scan d'un port spécifique sur une cible pour vérifier son état.
- **Scan à partir d'un fichier de listes de cibles** :
  - **Commande**: `nmap -iL <fichier>`
  - **Description**: Scan de plusieurs cibles à partir d'un fichier contenant une liste d'adresses IP ou de noms de domaine.

Techniques de Hacking

Scanning

Remaques !! :

- Assurez-vous d'avoir l'autorisation appropriée avant de scanner un réseau ou un système.
- Utilisez toujours Nmap de manière éthique et légale, en respectant la politique de sécurité de votre organisation ou les lois locales.
- Pour des scans plus complexes ou des configurations spécifiques, consultez la documentation officielle de Nmap et explorez les options avancées de l'outil.

Techniques de Hacking

Scanning

Remaques !! :

- Assurez-vous d'avoir l'autorisation appropriée avant de scanner un réseau ou un système.
- Utilisez toujours Nmap de manière éthique et légale, en respectant la politique de sécurité de votre organisation ou les lois locales.
- Pour des scans plus complexes ou des configurations spécifiques, consultez la documentation officielle de Nmap et explorez les options avancées de l'outil.

Techniques de Hacking

Scanning

Nmap
Nikto

Techniques de Hacking

Scanning

Comment se premunir contre le scanning de réseau ?

- Se prémunir contre le scanning de réseau comme Nmap est un défi, car ces outils sont conçus pour être très efficaces dans la détection des services et des ports ouverts.
- Cependant, il existe plusieurs mesures que vous pouvez prendre pour rendre le scanning plus difficile et pour protéger vos systèmes contre des intrusions potentielles

Techniques de Hacking

Scanning

Comment se premunir contre le scanning de réseau ?

- Utilisation de pare-feu
- Utilisation d'IDS/IPS
- Utilisation de port knocking
- Changement de ports par défaut
- Surveillance et Analyse de Logs
- Réduction de la surface d'attaque
- Utilisation de honeypots

Techniques de Hacking

Scanning

Exemple de Configuration de Pare-Feu avec iptables (Linux)

```
# Bloquer tout le trafic entrant par défaut
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Autoriser le trafic entrant sur les ports nécessaires (par exemple, SSH et HTTP)
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# Autoriser le trafic local (loopback)
iptables -A INPUT -i lo -j ACCEPT

# Autoriser le trafic entrant sur les connexions établies
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Techniques de Hacking

Exploitation

- L'exploitation ou le gain d'accès dans le cadre du hacking éthique se réfère à l'étape du processus de test de pénétration où l'attaquant simule une intrusion pour identifier et exploiter les vulnérabilités d'un système.
- L'objectif est de démontrer comment ces vulnérabilités peuvent être utilisées pour obtenir un accès non autorisé à des ressources sensibles.

Techniques de Hacking

Exploitation

1. **Identification des vulnérabilités**

- **Recherche des failles :** Utilisation d'outils automatisés et de techniques manuelles pour trouver des failles de sécurité dans le système, telles que des failles de sécurité logicielles, des mauvaises configurations ou des faiblesses dans les politiques de sécurité.
- **Collecte d'informations :** Recueil d'informations sur le système cible pour comprendre sa structure, ses composants et les points faibles potentiels.

Techniques de Hacking

Exploitation

2. **Exploitation des vulnérabilités**

- **Développement ou utilisation d'exploits :** Création ou utilisation d'exploits existants pour tirer parti des vulnérabilités identifiées. Cela peut inclure des scripts, des outils ou des techniques spécifiques à la vulnérabilité.
- **Exécution des exploits :** Lancer les exploits sur le système cible pour obtenir un accès non autorisé. Cela peut inclure des attaques de type injection SQL, exploitation de failles de configuration, ou attaques de type "buffer overflow".

Techniques de Hacking

Exploitation

3. **Escalade des privilèges**

- **Obtention de privilèges élevés :** Une fois un accès initial obtenu, l'attaquant tente d'obtenir des privilèges plus élevés pour accéder à des ressources sensibles ou prendre un contrôle complet du système.
- **Exploration latérale :** Mouvement latéral dans le réseau pour trouver d'autres systèmes vulnérables ou obtenir des données supplémentaires.

Techniques de Hacking

Exploitation

3. **Escalade des privilèges**

- **Obtention de privilèges élevés :** Une fois un accès initial obtenu, l'attaquant tente d'obtenir des privilèges plus élevés pour accéder à des ressources sensibles ou prendre un contrôle complet du système.
- **Exploration latérale :** Mouvement latéral dans le réseau pour trouver d'autres systèmes vulnérables ou obtenir des données supplémentaires.

Techniques de Hacking

Exploitation

Quels outils pour la phase d'exploitation ?

- **Metasploit Framework :** Un outil de test de pénétration qui permet aux utilisateurs de découvrir, de valider et d'exploiter des vulnérabilités. Il offre une vaste bibliothèque d'exploits.
- **BeEF (Browser Exploitation Framework) :** Un outil axé sur l'exploitation des vulnérabilités des navigateurs web.
- **SQLMap :** Un outil automatisé pour détecter et exploiter les vulnérabilités d'injection SQL dans les applications web.

Techniques de Hacking

Exploitation

Le Metasploit Framework

Le Metasploit Framework est l'un des outils les plus utilisés pour le test de pénétration et l'exploitation de vulnérabilités. Développé par Rapid7, Metasploit fournit une plateforme flexible pour tester la sécurité des systèmes en simulant des attaques réelles.

Techniques de Hacking

Exploitation

Fonctionnalités Principales de Metasploit

1. **Bibliothèque d'Exploits :**

- Metasploit contient une vaste collection d'exploits pour diverses vulnérabilités connues dans les systèmes, les applications web, et les services réseau.
- Les exploits sont constamment mis à jour par la communauté et par Rapid7.

Techniques de Hacking

Exploitation

Fonctionnalités Principales de Metasploit

2. **Payloads :**

- Payloads Statiques : Incluent des commandes simples à exécuter sur la machine cible.
- Meterpreter : Un payload avancé qui permet un contrôle interactif sur la machine compromise, offrant des fonctionnalités comme l'escalade de privilèges, le dumping de mots de passe, et l'accès à la webcam.

Techniques de Hacking

Exploitation

Fonctionnalités Principales de Metasploit

2. **Payloads :**

- Payloads Statiques : Incluent des commandes simples à exécuter sur la machine cible.
- Meterpreter : Un payload avancé qui permet un contrôle interactif sur la machine compromise, offrant des fonctionnalités comme l'escalade de privilèges, le dumping de mots de passe, et l'accès à la webcam.

Techniques de Hacking

Exploitation

Fonctionnalités Principales de Metasploit

3. **Encoders et NOPS :**

- Encoders : Utilisés pour éviter la détection par les systèmes de détection d'intrusion (IDS) en obfusquant le payload.
- NOPS : Utilisés pour stabiliser les exploits en remplissant l'espace mémoire avec des instructions NOP (No Operation).

Techniques de Hacking

Exploitation

Fonctionnalités Principales de Metasploit

4. **Auxiliary Modules :**

- Incluent une variété d'outils pour les tâches comme le scanning de vulnérabilités, le fuzzing, le sniffing, et le DoS (Denial of Service).

5. **Post-Exploitation Modules :**

- Permettent de maintenir l'accès, d'extraire des informations sensibles, et de pivoter vers d'autres systèmes dans le réseau.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Brute force

- Le brute force (force brute en français) est une méthode d'attaque informatique qui consiste à essayer toutes les combinaisons possibles pour trouver une information secrète, comme un mot de passe ou une clé de chiffrement.
- Cette méthode repose sur la puissance de calcul et la capacité à effectuer un grand nombre de tentatives en un laps de temps relativement court.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Fonctionnement de l'attaque par force brute

1. **Essai de toutes les combinaisons possibles :**

L'attaquant utilise un logiciel qui génère et teste systématiquement toutes les combinaisons possibles de caractères jusqu'à ce que la combinaison correcte soit trouvée.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Fonctionnement de l'attaque par force brute

2. **Types de force brute :**

- **Force brute pure :** Essai de toutes les combinaisons possibles sans aucune optimisation.
- **Force brute optimisée :** Utilisation de techniques pour réduire le nombre de tentatives nécessaires, comme l'utilisation de dictionnaires de mots de passe courants (attaque par dictionnaire).
- **Force brute hybride :** Combinaison des deux méthodes précédentes, souvent en utilisant des variations des mots de passe trouvés dans un dictionnaire (par exemple, ajouter des chiffres ou des symboles).

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Fonctionnement de l'attaque par force brute

3. **Exécution de l'attaque :**

- **Dictionnaire :** Une liste précompilée de mots de passe communs est utilisée pour essayer chaque mot de passe de la liste.
- **Attaque incrémentale :** Chaque combinaison possible de caractères est générée et testée, généralement commençant par les mots de passe les plus courts et simples.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Outils de force brute

- **Hydra :** Un outil rapide de force brute qui supporte de nombreux protocoles et services.
- **John the Ripper :** Un outil de craquage de mots de passe qui utilise diverses techniques de force brute et d'attaque par dictionnaire.
- **Hashcat :** Un outil avancé de craquage de mots de passe qui supporte les attaques par force brute sur les hashes.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Protection contre les attaques par force brute

Complexité des mots de passe :

- Utiliser des mots de passe longs et complexes (mélange de lettres majuscules et minuscules, chiffres et symboles) rend les attaques par force brute plus difficiles.

Limitation des tentatives :

- Mettre en place des mécanismes de limitation des tentatives de connexion, comme le verrouillage du compte après un certain nombre de tentatives infructueuses.

Authentification multi-facteurs (MFA) :

- Ajouter une couche supplémentaire de sécurité en exigeant une deuxième forme d'authentification, comme un code envoyé par SMS ou une application d'authentification.

Techniques de Hacking

Exploitation

Le hacking de mot de passe : Protection contre les attaques par force brute

Captchas :
Utiliser des captchas pour empêcher les scripts automatisés de tester un grand nombre de combinaisons de mots de passe.

Surveillance et alerte :
Mettre en place des systèmes de surveillance pour détecter les tentatives de connexion suspectes et alerter les administrateurs.

Techniques de Hacking

Exploitation

Attaques par Interception : Man-in-the-Middle, MitM

- L'attaque décrite est connue sous le nom d'attaque de type "Man-in-the-Middle" **(MITM)**. Dans ce scénario, l'attaquant intercepte et éventuellement modifie les communications entre deux parties sans que celles-ci s'en aperçoivent.
- L'objectif de l'attaquant peut être d'espionner, de voler des informations sensibles ou de manipuler les données échangées entre les deux parties.
- Pour se protéger contre ce type d'attaque, il est important d'utiliser des protocoles de communication sécurisés comme HTTPS, des certificats SSL/TLS, et des méthodes de chiffrement robustes.

Techniques de Hacking

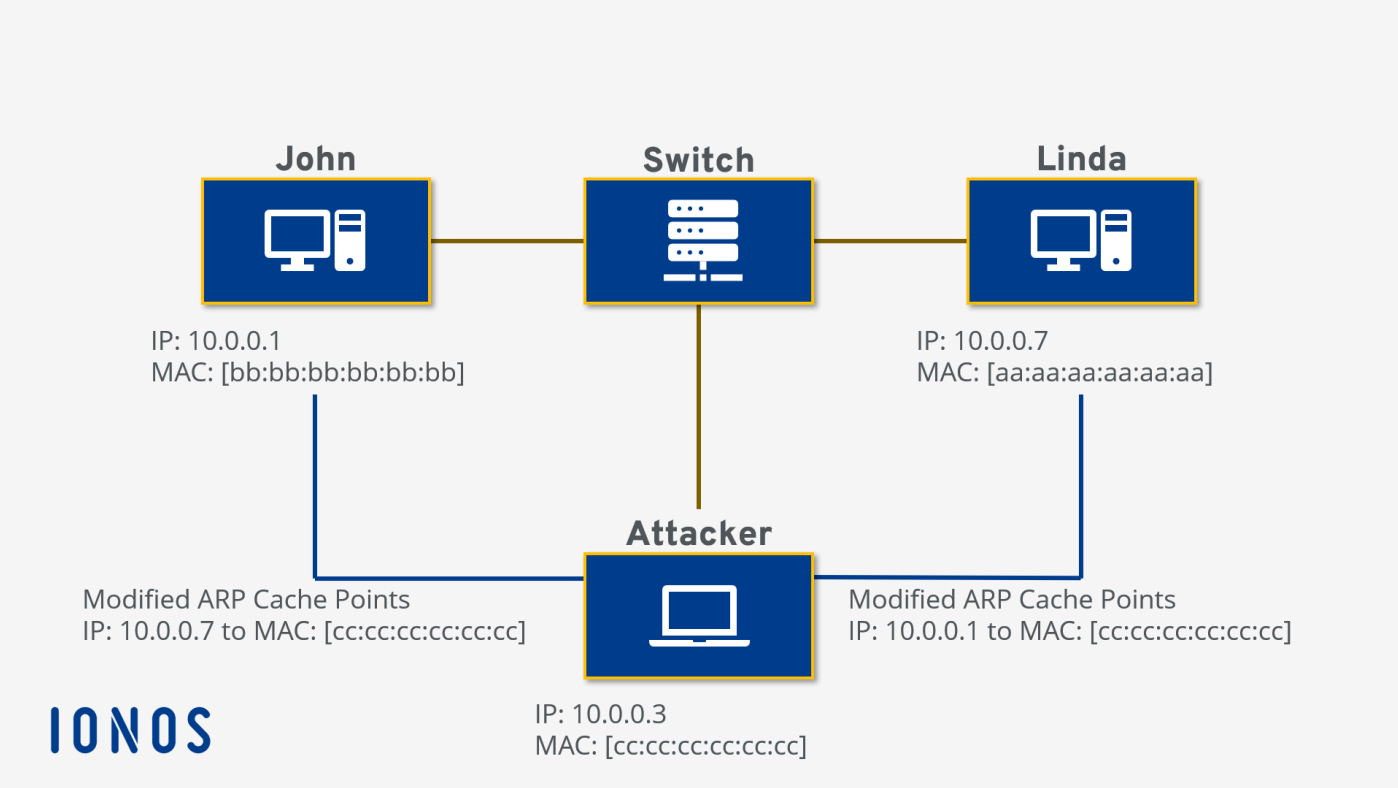
Exploitation

Attaques par Interception (MITM): ARP Poisoning

- **Address Resolution Protocol (ARP) :** ARP est un protocole utilisé pour résoudre les adresses IP en adresses MAC sur un réseau local.
- **ARP poisoning :** L'attaquant envoie des messages ARP falsifiés sur le réseau local. Ces messages contiennent de fausses associations entre les adresses IP et les adresses MAC. Par exemple, l'attaquant pourrait associer sa propre adresse MAC à l'adresse IP d'un routeur ou d'un autre dispositif réseau.
- **Interception et modification :** Une fois que les dispositifs sur le réseau ont accepté les associations ARP falsifiées, les paquets de données destinés à l'adresse IP légitime (comme celle du routeur) sont envoyés à l'attaquant. L'attaquant peut alors intercepter, lire, modifier ou rediriger ces paquets avant de les retransmettre à leur véritable destination.

Techniques de Hacking

Exploitation



Techniques de Hacking

Exploitation

Attaques par Interception (MITM): Les contre-mesures

- **Utiliser des ARP statiques :** Configurer des entrées ARP statiques sur les dispositifs critiques pour éviter les modifications non autorisées.
- **Activer le filtrage ARP :** Utiliser des switches avec des fonctionnalités de sécurité avancées comme le Dynamic ARP Inspection (DAI).
- **Chiffrement des communications :** Utiliser des protocoles sécurisés (comme HTTPS, SSH, VPN) qui chiffrent les données, même si elles sont interceptées.
- **Surveillance du réseau :** Utiliser des systèmes de détection d'intrusion (IDS) pour surveiller les activités suspectes sur le réseau.

Techniques de Hacking

Exploitation

Attaques par Injection: Injection XSS

- Le **Cross-Site Scripting (XSS)** est une vulnérabilité de sécurité informatique qui permet à un attaquant d'injecter des scripts malveillants dans des pages web consultées par d'autres utilisateurs.
- Cette injection de code peut être utilisée pour voler des informations sensibles, contourner des contrôles d'accès ou manipuler le contenu affiché sur la page web.

Techniques de Hacking

Exploitation

Attaques par Injection: Types de XSS

1. **XSS Stocké (Persistant) :**

- Le script malveillant est injecté directement dans une application web et est stocké dans une base de données. Chaque fois qu'un utilisateur accède à la page compromise, le script est exécuté.
- **Exemple :** Une zone de commentaires où l'attaquant injecte un script. Chaque utilisateur qui lit le commentaire exécute involontairement le script.

Techniques de Hacking

Exploitation

Attaques par Injection: Types de XSS

2. **XSS Réfléchi (Non-persistant) :**

- Le script malveillant est injecté via une entrée utilisateur (comme un paramètre d'URL) et est immédiatement renvoyé dans la réponse de la page web. Ce type d'attaque nécessite que l'utilisateur clique sur un lien malveillant pour que le script soit exécuté.
- Exemple : Un lien envoyé par e-mail contenant un script dans un paramètre d'URL. Lorsque l'utilisateur clique dessus, le script s'exécute.

Techniques de Hacking

Exploitation

Attaques par Injection: Types de XSS

3. **XSS Basé sur le DOM (Document Object Model) :**

- Cette forme d'attaque modifie le DOM de la page web à l'aide de scripts côté client, généralement via JavaScript, sans toucher directement la réponse HTTP initiale.
- Exemple : Une application web qui manipule le DOM en fonction des paramètres d'URL sans vérifier ou échapper correctement ces paramètres.

Techniques de Hacking

Exploitation

Attaques par Injection: Conséquences d'une attaque XSS

- **Vol de Cookies et Sessions :** Les attaquants peuvent voler des cookies de session pour usurper l'identité d'un utilisateur.
- **Défacement de Site :** Les attaquants peuvent modifier le contenu affiché aux utilisateurs.
- **Redirections Malveillantes :** Les utilisateurs peuvent être redirigés vers des sites de phishing ou malveillants.
- **Exécution de Keyloggers :** Les scripts peuvent enregistrer les frappes des utilisateurs et voler des informations sensibles comme des mots de passe.

Techniques de Hacking

Exploitation

Attaques par Injection: Prévention des attaques XSS

- **Échappement des Entrées Utilisateur :** Toujours échapper les entrées utilisateur avant de les rendre sur une page web.
- **Validation des Entrées :** Vérifier et nettoyer les entrées utilisateur pour s'assurer qu'elles ne contiennent pas de code malveillant.
- **Utilisation de Content Security Policy (CSP) :** Implémenter CSP pour restreindre les sources de contenu exécutables.
- **Encodage des Données :** Utiliser des méthodes d'encodage appropriées pour les données rendues dans HTML, JavaScript, et URL.

Techniques de Hacking

Exploitation

Attaques par Injection: Injection SQL

- L'injection SQL (SQL Injection ou SQLi) est une vulnérabilité de sécurité qui permet à un attaquant d'interférer avec les requêtes qu'une application effectue sur sa base de données.
- En insérant du code SQL malveillant dans des champs de saisie, l'attaquant peut manipuler les requêtes SQL, ce qui peut entraîner des conséquences graves comme la divulgation d'informations sensibles, la modification de données, et même la prise de contrôle totale du serveur de la base de données.

Techniques de Hacking

Exploitation

Attaques par Injection: Types d'Injection SQL

1. **Injection SQL Classique (In-band SQLi) :**

- Les données injectées sont directement visibles dans la réponse de la base de données.
- Exemple : L'attaquant obtient des informations en ajoutant du code SQL malveillant dans un champ de saisie.

Techniques de Hacking

Exploitation

Attaques par Injection: Types d'Injection SQL

2. **Blind SQL Injection :**

- Les résultats des requêtes injectées ne sont pas directement visibles pour l'attaquant, mais des réponses booléennes ou temporelles peuvent être utilisées pour extraire des informations.
- **Exemple :** L'attaquant pose des questions à la base de données, comme "Si cette condition est vraie, attend 5 secondes", et en fonction de la réponse, il peut déduire des informations.

Techniques de Hacking

Exploitation

Attaques par Injection: Types d'Injection SQL

3. **Error-based SQL Injection :**

- Utilise les messages d'erreur de la base de données pour obtenir des informations sur la structure de la base de données.
- **Exemple :** L'attaquant provoque des erreurs intentionnellement pour récupérer des informations détaillées.

Techniques de Hacking

Exploitation

Attaques par Injection: Conséquences d'une attaque XSS

- **Vol de données sensibles :** Les attaquants peuvent accéder à des informations confidentielles comme les noms d'utilisateur, mots de passe, adresses e-mail, etc.
- **Modification des données :** Les attaquants peuvent insérer, mettre à jour ou supprimer des données dans la base de données.
- **Exécution de commandes administratives :** Les attaquants peuvent effectuer des opérations administratives sur la base de données, comme arrêter le serveur.
- **Compromission de l'intégrité des données :** Les attaquants peuvent corrompre les données, rendant l'application inutilisable.
- **Prise de contrôle du serveur :** Dans certains cas, les attaquants peuvent utiliser SQLi pour exécuter des commandes sur le système d'exploitation sous-jacent.

Techniques de Hacking

Exploitation

Attaques par Injection: Prévention des Attaques par Injection SQL

1. **Utilisation de Requêtes Préparées :**

- Les requêtes préparées (ou requêtes paramétrées) séparent le code SQL des données, rendant les injections inefficaces.

```
$stmt = $pdo->prepare("SELECT * FROM users WHERE username = :username AND password = :password");
$stmt->execute(['username' => $username, 'password' => $password]);
```

Techniques de Hacking

Exploitation

Attaques par Injection: Prévention des Attaques par Injection SQL

2. **Échappement des Entrées Utilisateur :**

- Utiliser des fonctions spécifiques à chaque SGBD pour échapper correctement les entrées utilisateur.

3. **Validation et Nettoyage des Données :**

- Valider et nettoyer toutes les données entrantes pour s'assurer qu'elles respectent les formats attendus.

Techniques de Hacking

Exploitation

Attaques par Injection: Prévention des Attaques par Injection SQL

4. **Moins de Privilèges :**

- Utiliser des comptes de base de données avec les privilèges les plus bas nécessaires à l'application.

5. **Surveillance et Audits :**

- Mettre en place des systèmes de surveillance pour détecter les activités suspectes et réaliser des audits réguliers de la sécurité de l'application.