RAPPORT DE TEST D'INTRUSION : R3.Cyber.16

Pierre Famchon

Table des matières :

1.Introduction

Ce document présente les résultats d'un test d'intrusion réalisé dans le cadre d'un contrôle en travaux pratiques sur la découverte du pentesting. L'objectif de cet audit était d'identifier les vulnérabilités potentielles affectant la sécurité du système testé, en évaluant leur impact sur la confidentialité, l'intégrité et la disponibilité des données.

Dans cette démarche, des techniques d'attaque couramment utilisées par les attaquants ont été appliquées de manière méthodique afin d'évaluer la résilience du système face à des menaces réelles. Ce rapport détaille les vulnérabilités identifiées, les preuves associées, ainsi que des recommandations pour renforcer la sécurité.

2.Portée du Test

La portée du test d'intrusion était limitée au serveur hébergeant le blog WordPress de Bug&Blog Ltd et aux services associés. L'objectif était d'identifier les vulnérabilités pouvant compromettre la sécurité du site avant sa mise en ligne.

Éléments inclus dans l'audit

✔ Hôte cible : Une machine virtuelle Ubuntu hébergeant le blog WordPress.
✔ Services analysés :

- WordPress (et ses plugins/thèmes installés).
- Base de données (ex: MySQL, MariaDB).
- Serveur web (ex: Apache, Nginx).
- Accès SSH (limité à un utilisateur restreint).
  ✔ Scénario de test : Approche gray box avec un compte utilisateur restreint.

3.Synthèse de la mission

Le test d'intrusion a été réalisé sur une durée de 4 heures dans le cadre d'un contrôle en travaux pratiques. Il a porté sur une machine virtuelle Ubuntu hébergeant un site WordPress et plusieurs services associés.

L'évaluation a été menée en mode gray box, en combinant analyses automatisées et tests manuels. Les attaques ont été effectuées dans un environnement contrôlé, sans impact sur d'autres systèmes.

Malgré le temps limité, plusieurs vulnérabilités ont été identifiées et analysées.

4.Résumé

Bug&Blog Ltd a sollicité un test d'intrusion afin d'évaluer la sécurité de son futur blog WordPress, avant sa mise en ligne officielle.
L'objectif principal était d'identifier et d'exploiter les vulnérabilités pouvant compromettre la confidentialité, l'intégrité et la disponibilité du système.
L'audit a permis de détecter plusieurs failles, dont certaines critiques, pouvant être exploitées par un attaquant pour accéder à des données sensibles, compromettre l'application ou perturber son bon fonctionnement.

4.1 Surface vulnérable

L'évaluation a révélé que le blog WordPress et ses services associés présentaient des vulnérabilités de différents niveaux de gravité. Certaines failles pourraient permettre une prise de contrôle du serveur ou l'exploitation d'informations sensibles, mettant en danger l'intégrité et la sécurité du système.

Les principaux points d'exposition incluent :
✔ Un WordPress et ses plugins potentiellement vulnérables.
✔ Des services réseau exposés avec des configurations faibles.
✔ Une gestion des accès et des permissions perfectible.

4.2 Table des vulnérabilités

Vulnérabilité	Gravité
Injection SQL sur formulaire de connexion	Critique
Plugin WordPress vulnérable (exécution de code)	Elevée
Mauvaise configuration des permissions système	Moyenne
Service FTP accessible anonymement	Moyenne
Version obsolète de WordPress détectée	Faible

5.Vulnérabilités

5.1 Vulnérabilités des services

5.1.1 Service FTP anonymement accessible

Informations Générales :

- CVE potentielle : CVE-1999-0497 *(Accès anonyme non restreint sur un serveur FTP)*
- Score CVSS estimé : **5.3** (Moyen)
- Résumé **:**
  Un service FTP est accessible anonymement sur la machine cible. Cette configuration peut permettre à un attaquant d'accéder à des fichiers sensibles ou d'exploiter des failles supplémentaires.

Détection et Preuve :

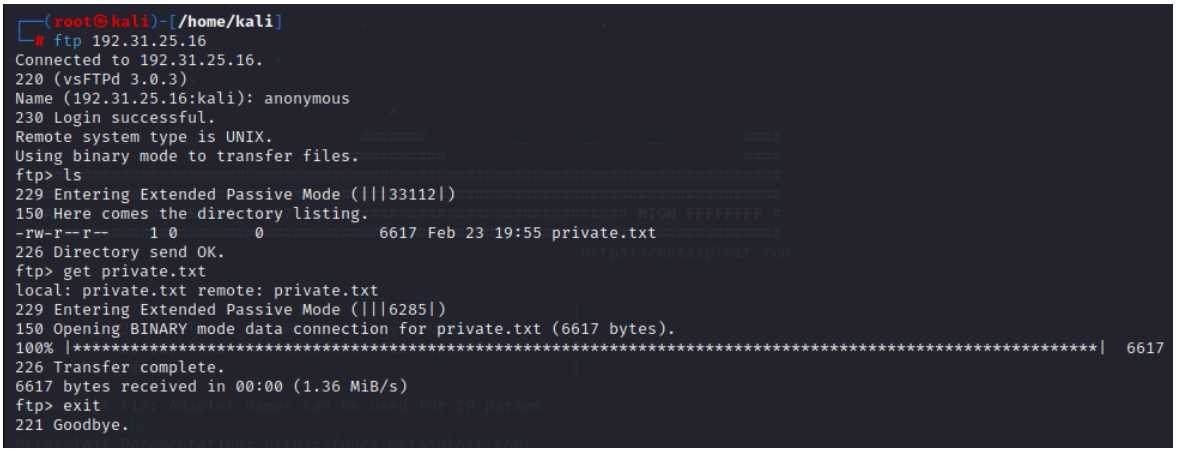
- Scan avec Nmap **:**

Le service FTP autorise la connexion anonyme.nmap -p 21 –script ftp-anon 192.31.25.16

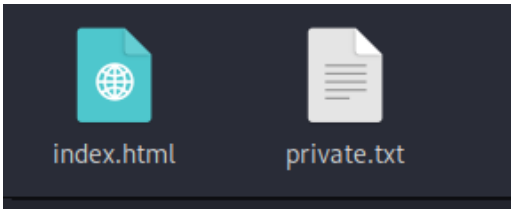
- Exploitation avec les commandes **:**

  - ftp 192.31.21.16

Résultat : Accès réussi avec un compte anonyme.



- get private.txt



Impact et Risques :

- Impact sur la confidentialité **:** Un attaquant peut récupérer des fichiers sensibles.
- Impact sur l'intégrité **:** Possibilité d'écrire ou modifier des fichiers si les permissions sont mal configurées.
- Impact sur la disponibilité **:** FTP pourrait être utilisé pour transférer des fichiers malveillants et compromettre le serveur.

Recommandations :

- Désactiver l'accès anonyme **:** dans la configuration FTP (/etc/vsftpd.conf ou autre selon le serveur).
- Remplacer FTP par SFTP (FTP sécurisé via SSH) **:** pour le transfert de fichiers.
- Restreindre l'accès au service FTP **:** uniquement aux utilisateurs authentifiés.
- Utiliser un pare-feu (iptables ou UFW) **:** pour limiter les connexions FTP aux seules adresses IP autorisées.

5.1.2 Exposition d'informations sensibles

Informations Générales :

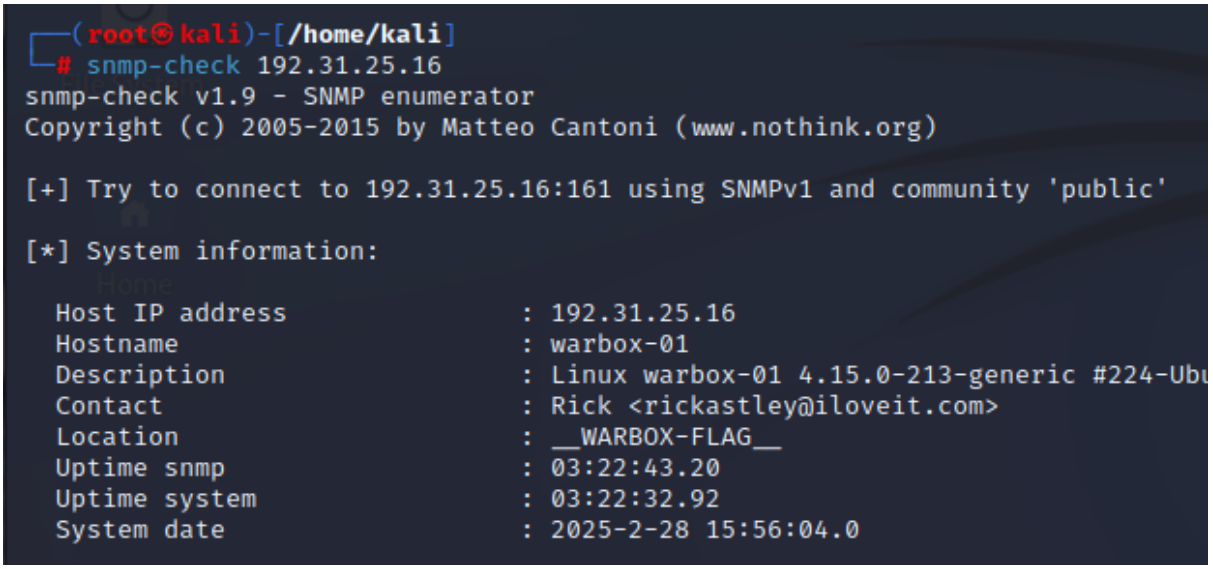
- CVE potentielle : CVE-1999-0517
- Score CVSS estimé : **6.0** (Moyen)
- Résumé **:**
  Un service SNMP est configuré avec une chaîne de communauté simple (public), cette configuration peut permettre à un attaquant d'accéder à des fichiers sensibles ou d'exploiter des failles supplémentaires.

Détection et Preuve :

- Vérification avec les commandes :
  - snmpwalk -v1 -c public 192.31.25.16
  - snmp-check 192.31.25.16

Résultat : La machine répond avec des données, elle est vulnérable.

```
┌──(root㉿kali)-[/home/kali]
└─# snmpwalk -v1 -c public 192.31.25.16
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Linux warbox-01 4.15.0-213-generic #224-Ubuntu
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (1276443) 3:32:44.43
iso.3.6.1.2.1.1.4.0 = STRING: "Rick <rickastley@iloveit.com>"
iso.3.6.1.2.1.1.5.0 = STRING: "warbox-01"
iso.3.6.1.2.1.1.6.0 = STRING: "__WARBOX-FLAG__"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (36) 0:00:00.36
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
```



Impact et Risques :

- Un attaquant peut cartographier le réseau et identifier des cibles pour d'autres attaques (pivot, exploitation de services vulnérables).

- Si SNMP permet l'écriture (RW au lieu de RO), un attaquant peut modifier la configuration du système à distance (changer les routes, désactiver des interfaces, etc.).

Recommandation :

- Désactiver SNMP si non utilisé.
- Changer la chaîne de communauté SNMP (`public` ➜ `"ChaîneComplexe123!"`).
- Restreindre l'accès SNMP aux IPs de confiance via le pare-feu
- Mettre à jour le logiciel SNMP

5.2 Vulnérabilités des systèmes
5.2.1 Bruteforce SSH réussi

Informations Générales :

- CVE potentielle : CVE-2018-15473 *(Vulnérabilité d'énumération d'utilisateur SSH sur OpenSSH)*
- Score CVSS estimé : **7.5** (Élevé)
- Résumé **:**
  Un bruteforce SSH a permis d'obtenir un accès valide à un compte utilisateur sur la machine cible. Cette vulnérabilité expose le système à un risque de compromission par des attaquants.

Détection et Preuve :

- Test de connexion SSH avec **metasploit :**
  - use auxiliary/scanner/ssh/ssh_login

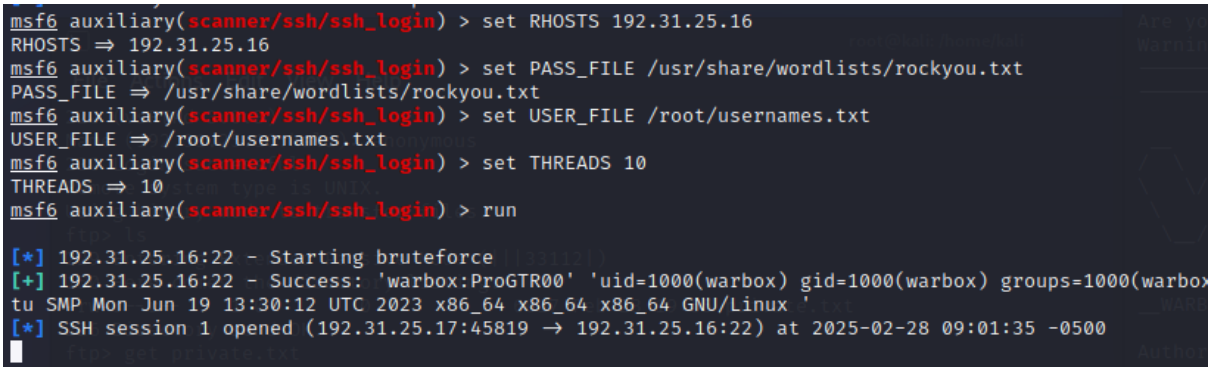
    set RHOSTS 192.31.25.16

    set PASS_FILE /usr/share/wordlists/rockyou.txt

    set USER_FILE /root/usernames.txt *

    set THREADS 10 run

Résultat : Un couple nom utilisateur/mot de passe valide a été trouvé, permettant un accès non autorisé au serveur SSH.



Impact et Risques :

- Impact sur la confidentialité **:** Un attaquant peut accéder aux fichiers et données sensibles de l'utilisateur compromis.
- Impact sur l'intégrité **:** Un compte compromis peut être utilisé pour modifier ou supprimer des fichiers critiques.
- Impact sur la disponibilité **:** Une attaque prolongée pourrait mener à un blocage de service ou une prise de contrôle complète du serveur.

Recommandations :

- Désactiver l'authentification par mot de passe **:** et utiliser l'authentification par clé SSH).
- Mettre en place une politique de mots de passe forts **:** empêchant l'utilisation de mots de passe faibles ou communs.
- Configurer un mécanisme de blocage d'IP après plusieurs échecs d'authentification avec Fail2Ban **:** bloque les ip après plusieurs essais infructueux.
- Surveiller les logs SSH **:** pour détecter d'éventuelles tentatives de bruteforce

5.2.2 Mots de passe identiques pour root et user

Informations Générales :

- CVE potentielle : CVE-2019-14287
- Score CVSS estimé : **9.8** (Élevé)

Détection et Preuve :

- Connexion en SSH avec l'utilisateur compromis :
  - ssh warbox@192.31.25.16
- Elévation de privilèges avec le même mot de passe :
  - su root

Résultat : Un couple nom utilisateur/mot de passe valide compromis plus suite au bruteforce a été trouvé, permettant un accès en root total au serveur SSH.

Impact et Risques :

- Accès root **:** immédiat après un bruteforce réussi sur l'utilisateur standard.
- Compromission totale du serveur.
- Possibilité d'installer **:** des portes dérobées, de voler des données ou d'endommager le système

Recommandations :

- Modifier immédiatement le mot de passe **:** root
  - Désactiver la connexion SSH pour root en modifiant /etc/ssh/sshd_config
- Imposer des mots de passe **:** différents et complexes pour chaque compte utilisateur.
- Activer l'authentification **:** par clé SSH et désactiver les mots de passe
- Surveiller les connexions **:** et tentatives de connexion root

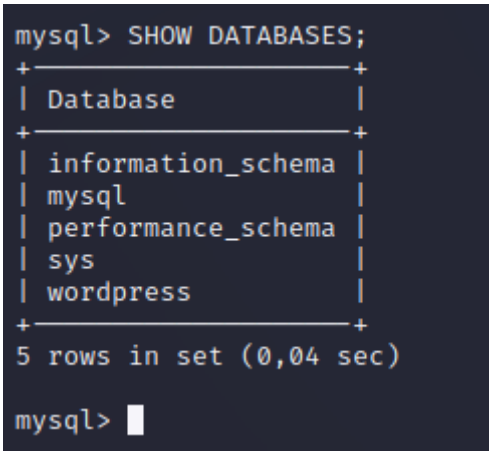
5.3 Vulnérabilité Web
5.3.1 Accès non restreint à la base de données WordPress

Informations Générales :

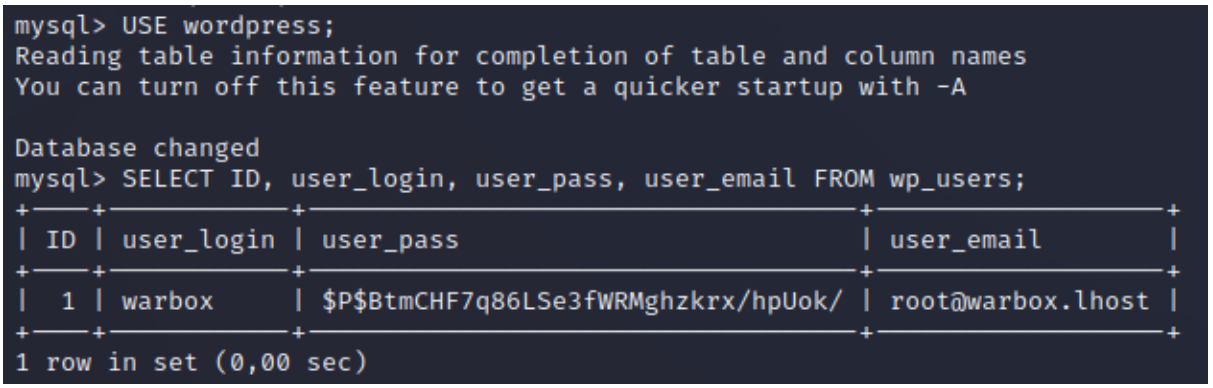
- CVE potentielle : CVE-2017-1000367
- Score CVSS estimé : **7,5** (Élevé)

Détection et Preuve :

- Accéder à MySQL :
  - mysql -u root -p
- Lister les bases de données :
  - SHOW DATABASES;



- Sélectionner la base de données WordPress :
  - USE wordpress;
- Récupérer les utilisateurs et leurs informations :
  - SELECT ID, user_login, user_pass, user_email FROM wp_users;



- Modifier le mot de passe d'un admin pour prendre le contrôle :
    - UPDATE wp_users SET user_pass = MD5('NewPassword123!') WHERE user_login = 'admin';

Impact et Risques :

- Confidentialité **:** Un attaquant peut récupérer des informations sensibles sur les utilisateurs et l'administration du site.
- Intégrité **:** Il peut modifier ou supprimer des données, altérant le fonctionnement du site.
- Disponibilité **:** Il peut supprimer ou corrompre la base de données, rendant le site inutilisable.

Recommandations :

- Restreindre l'accès à la base de données **:** Modifier la configuration MySQL pour n'autoriser que les connexions locales.
- Sécuriser les identifiants **:** Utiliser des mots de passe forts et uniques pour les comptes de base de données.
- Protéger wp-config.php **:** Restreindre les permissions
- Surveiller les connexions suspectes **:** Configurer un journal des accès.
- Mettre en place un IDS (Intrusion Detection System) comme Fail2Ban pour bloquer les tentatives de connexion répétées.