Audit de sécurité

Penteste avec Msfconsole pour métasploitable & Application Web

Version auditée :

Rapport d’audit technique

26/01/2024

Auditeurs :

WANG PENGCHAO

Ce document est **confidentiel**.

Tous les destinataires sont tenus d’en garantir la confidentialité en en limitant la diffusion aux personnes ayant besoin d’y avoir accès.

Les destinataires de ce document doivent garantir que son transfert et son stockage utilisent les outils de chiffrement mis à disposition par Positive thinking company.

Historique du document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Auteur | Date | Commentaire |
| 1 | WANG PENGCHAO | 26/01/24 | Document intermédiaire |
|  |  |  |  |
|  |  |  |  |

Table des matières

[Formulaire destiné aux équipes de supervision Erreur ! Signet non défini.](#_Toc534383305)

[1 - Démarche d’audit 4](#_Toc534383306)

[1.1 Organisation du document 4](#_Toc534383307)

[1.2 Calcul de la criticité des vulnérabilités 4](#_Toc534383308)

[2 - Listing des constats d’audit 6](#_Toc534383309)

[2.1 Constat n°1 : <FTP Vulnérable> 6](#_Toc534383310)

[2.2 Constat n°2 : <Intrusion Application Web> 12](#_Toc534383311)

# Démarche d’audit

Ce rapport a été conçu dans le cadre d'un exercice pratique du module R508 - Audits de sécurité informatique, dans l'intention de simuler un rapport d'audit réaliste. L'objectif de cet exercice est de perfectionner la compréhension des processus et des meilleures pratiques en matière d'audit de sécurité informatique.

Une simulation d'attaque interne représente un assaut ciblé sur les systèmes informatiques de l'organisation. L'ambition de cette simulation est de reproduire des attaques analogues à celles menées par un hacker, en tentant d'accéder au système ou d'exécuter du code à distance (Remote Code Execution - RCE) sur des machines critiques.

La phase initiale de l'audit visait à passer au crible tous les ports des systèmes sur le réseau pour identifier ceux qui étaient ouverts, déterminer les versions des logiciels utilisés et détecter les failles non corrigées, en particulier celles négligées lors des mises à jour.

## Organisation du document

Nous allons détailler dans les sections qui suivent les différentes étapes de l'audit, y compris la planification, la réalisation et l'évaluation des résultats obtenus.

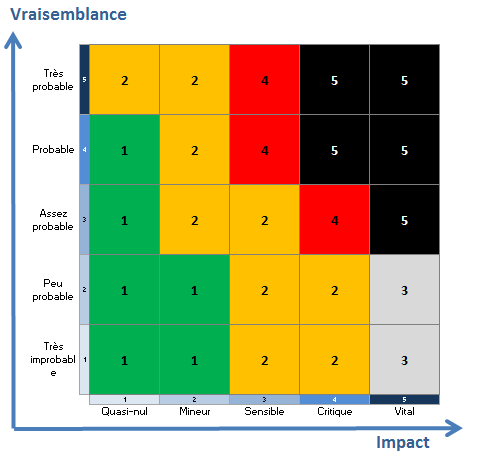
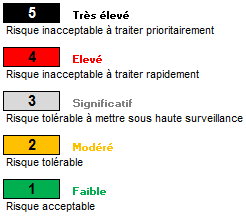
Les déductions faites suite à cet audit apporteront des éléments déterminants pour guider les actions correctives nécessaires.

## Calcul de la criticité des vulnérabilités

Les systèmes avec une manque de mise à jour présentent un risque accru en raison de la prévalence des versions logicielles obsolète, qui sont souvent la cible pour des attaques informatique.

Des vulnérabilités non patchées dans des versions antérieures deviennent des vecteurs d'attaques favoris pour les cyber-agresseurs qui peuvent les exploiter de manière agressive et efficiente, augmentant ainsi la probabilité de compromission, spécialement pour ceux qui ont des intentions malveillantes.

Il est donc essentiel de noter que la vulnérabilité des systèmes non actualisés est en corrélation directe avec l'exposition au risque, soulignant l'importance d'adopter des mesures préventives adéquates face aux menaces de sécurité modernes.



# Listing des constats d’audit

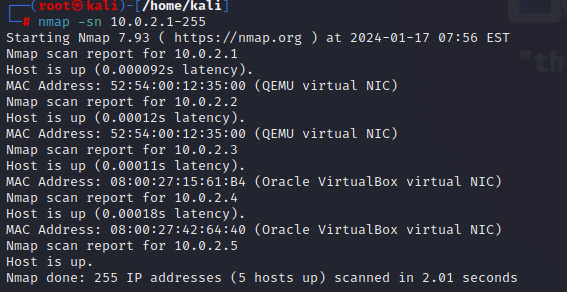
## Constat n°1 : FTP vulnerable HIGH

Description :

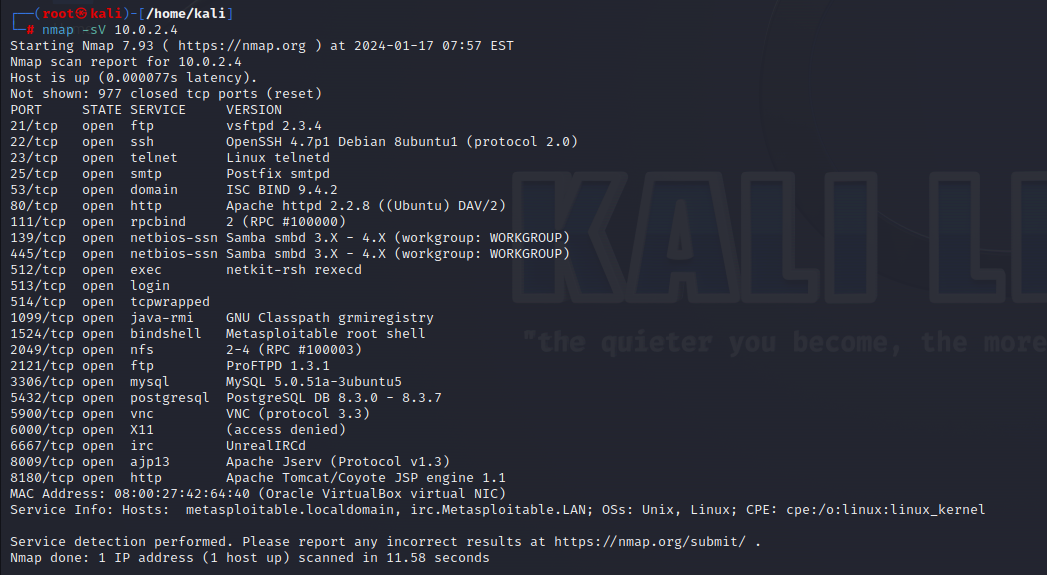
En exploitant une vulnérabilité trouvée dans la version courante du service FTP, il a été possible de gagner l'accès au terminal, ouvrant ainsi la porte aux divers fichiers stockés sur le système.

Preuve :

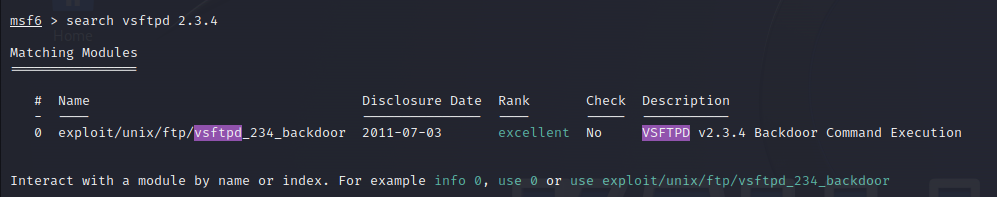
Tout d’abord, nousc allons localiser la machine vulnérable « métasploitable » avec l’outil « Nmap » sur l’ensemble du réseau 10.0.2.0 :



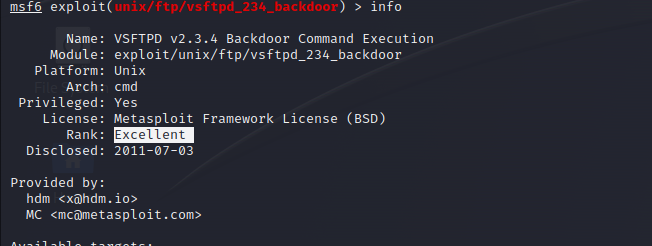
Après avoir identifié la bonne adresse de la machine vulnérable (10.0.2.4), nous allons maintenant scanner les ports existants:

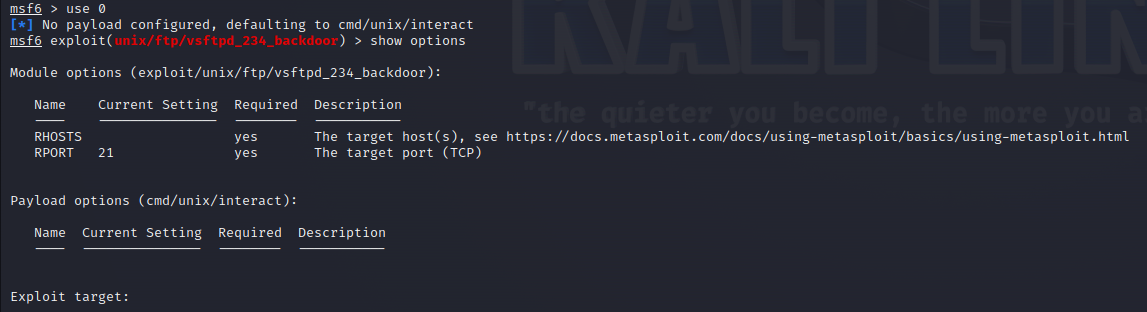


Ensuite, nous allons exploiter une vulnérabilité FTP afin de pouvoir accéder à la session de la machine Metasploitable. Pour cela, nous utiliserons le module vsftpd à l'aide de l'outil 'search' :



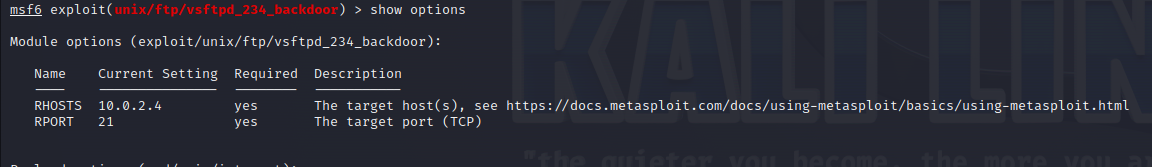
Par la suite, nous procéderons à un exploit pour utiliser ce module. De plus, avec la commande 'info', nous pouvons obtenir des informations telles que le nom de l'exploit, le module, la plateforme, l'architecture, les privilèges, la licence, le rang, la date de divulgation et les auteurs :



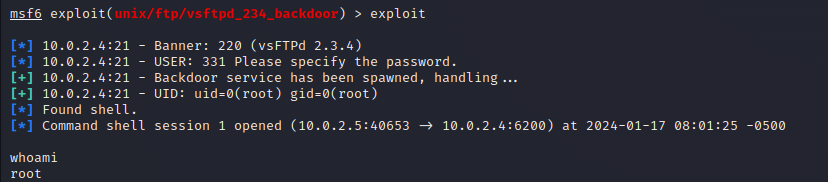
Nous pouvons également effectuer un 'show options' pour voir les informations à paramétrer afin de réaliser cet exploit : 

Nous remarquons que cet exploit nécessite uniquement une adresse IP ; pour cela, nous allons renseigner l'adresse IP de la machine vulnérable :

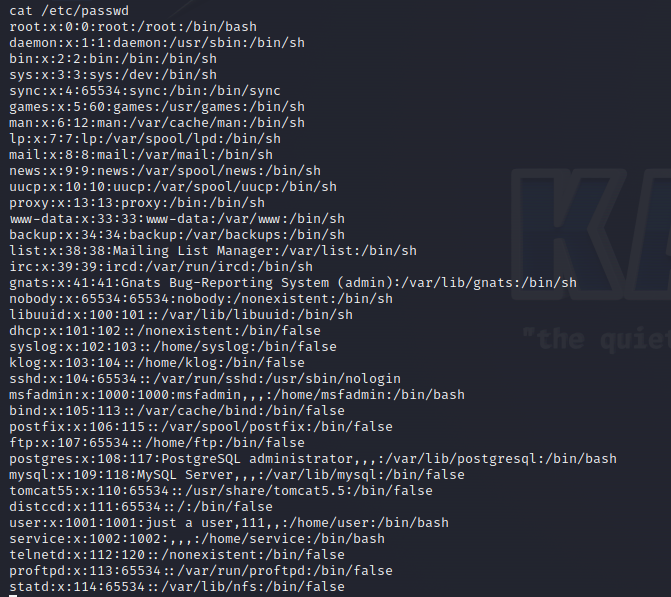




Nous allons maintenant lancer l’exploit pour avoir accès à la session de la machine vulnérable :

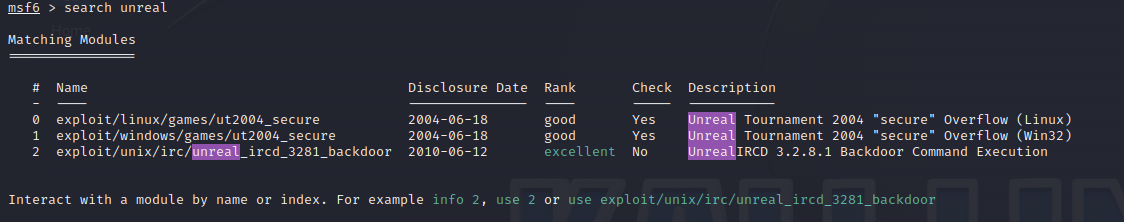


Enfin, nous allons lire le contenu du fichier /etc/passwd de la machine vulnérable :

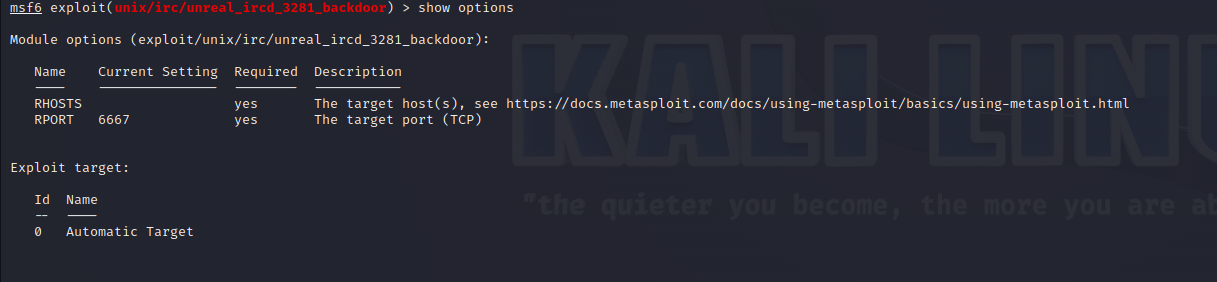


**Voici une autre vulnérabilité de la machine métasploitable :**

Nous allons utiliser une vulnérabilité dans UnreallRCd qui permet d’avoir un backdoor pour obtenir un accès non autorisé au serveur IRC :



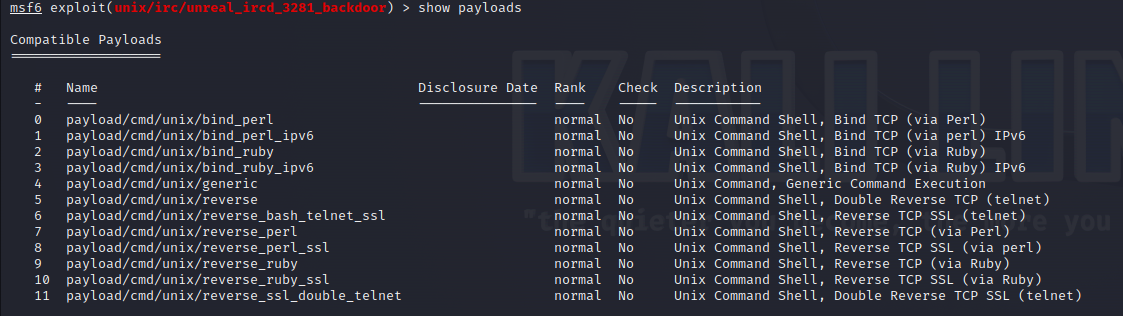
Nous allons regarder les options proposées :



On fourni l’adresse IP de la machine vulnérable :



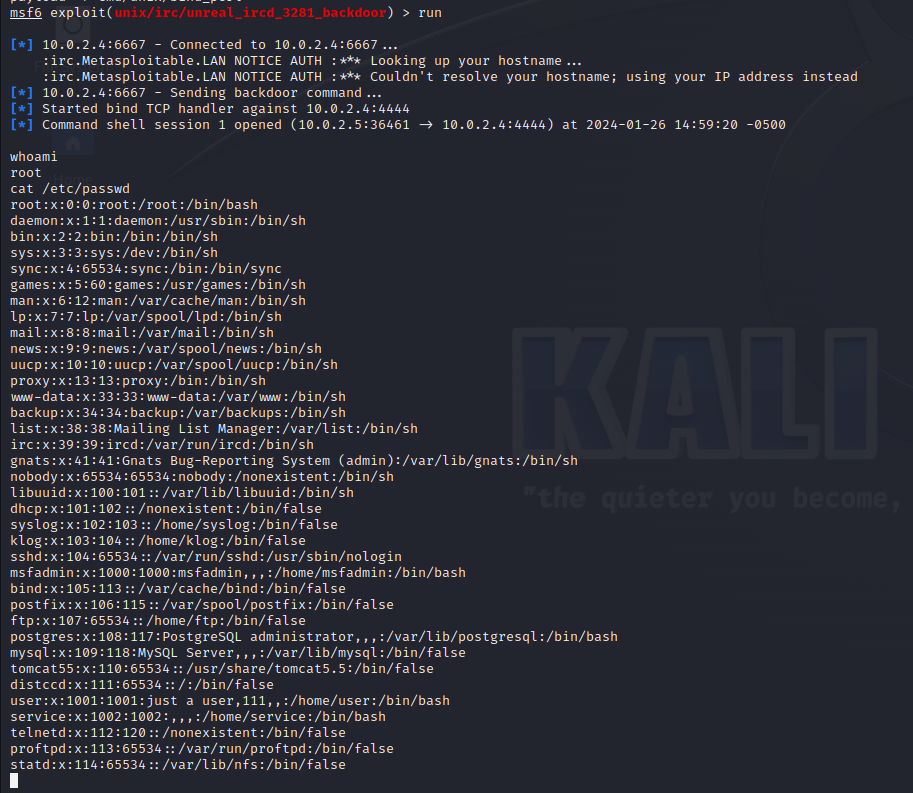
Il faut aussi fournir un payload, nous allons voir les listes disponible :



Nous allons utiliser ce payload :



Nous allons maintenant lancer l’attaque :



Recommendations :

**Vulnérable FTP :**

* S'assurer que le service FTP est configuré de manière sécurisée, avec des mots de passe forts, des connexions cryptées, et limiter l'accès FTP aux utilisateurs qui en ont strictement besoin.
* Privilégier l'utilisation de protocoles FTP sécurisés comme SFTP ou FTPS qui offrent une couche de sécurité supplémentaire via le chiffrement.
* Maintenir à jour le logiciel serveur FTP pour s'assurer que toutes les failles de sécurité connues sont corrigées. Appliquez régulièrement les patches de sécurité dès qu'ils sont disponibles.

**Vulnérable UnreallRCd 3.2.8.1 Backdoor :**

* Il est impératif de mettre à jour le logiciel UnrealIRCd vers la dernière version qui corrige la vulnérabilité de la backdoor. Si la mise à jour n'est pas possible, envisagez de désactiver temporairement le service jusqu'à ce que le correctif puisse être appliqué.
* Effectuez un audit de sécurité complet pour vérifier s'il y a eu compromission. Examinez les journaux (logs) pour toute activité suspecte et vérifiez l'intégrité des systèmes.
* Renforcez les mesures de sécurité réseau, y compris l'utilisation de pare-feu pour filtrer le trafic non autorisé et l'application de règles de segmentation réseau strictes pour minimiser l'impact potentiel d'une compromission.

En général, il faut adopter une politique de sécurité proactive et effectuer des évaluations régulières des vulnérabilités permettra de réduire significativement le risque d'exploitation de failles de sécurité.

## Constat n°2 : Intrusion Application Web

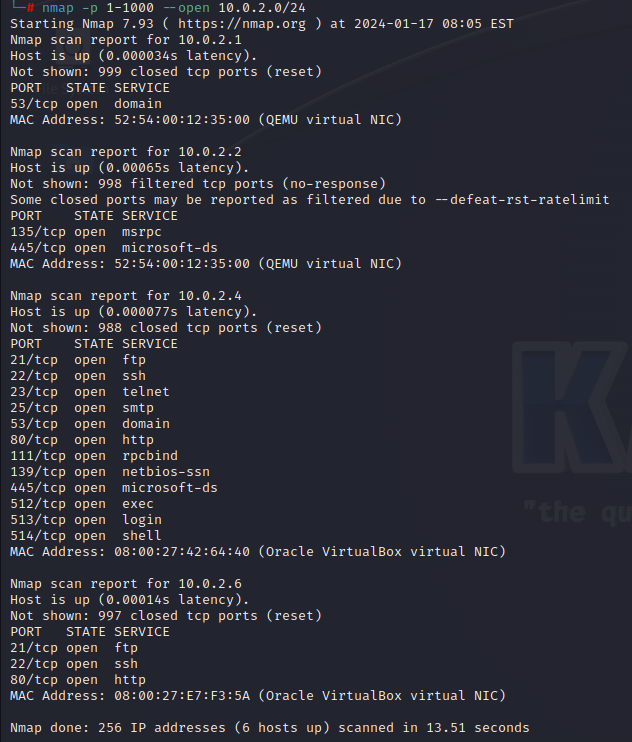
Description :

En utilisant l'outil Nmap de Kali Linux, nous allons identifier une machine suspecte sous Debian et tenter de nous y introduire en exploitant une vulnérabilité dans des applications web sur le système de type Unix.

Preuve :

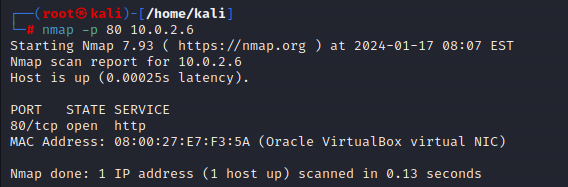
On va utiliser la commande suivante pour scanner les ports de 1-1000 sur le réseau 10.0.2.0/24 :

On peut apercevoir que l’adresse 10.0.2.6 est suspect



Nous allons maintenant trouver le port du service web

Le port du service web est le port 80



A présent, nous allons utiliser la commande **dirbuster**

*Dirb http://****<ip de la machine cible>*** */usr/share/wordlists/dirb/common.txt -o sortie.txt*

Cette commande va enregistrer les informations de common.txt dans le fichier sortie.txt.



Ensuite, nous allons accéder à la page de connexionetUtiliser la commande wpscan :

Cela permet de faire un test de séccurité des installations WordPress.

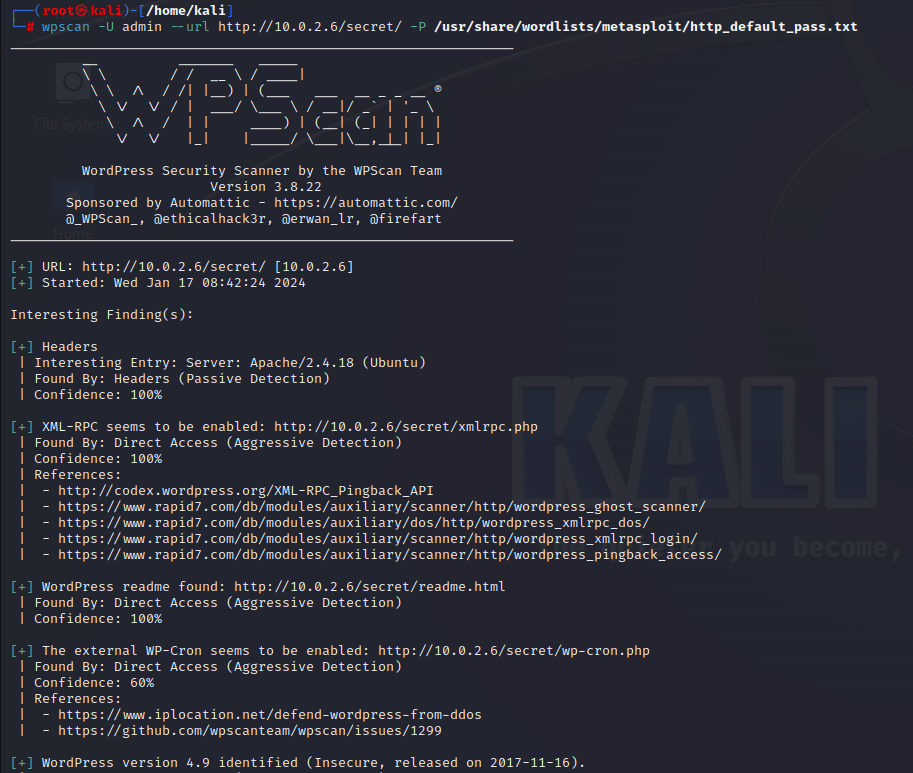
****

On peut donc voir l’analyse du wpscan :

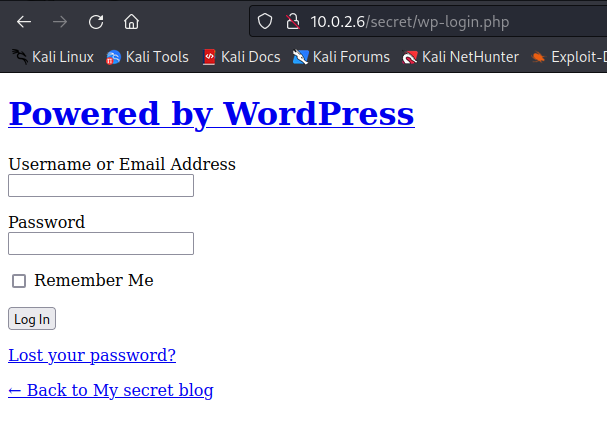
* La présence d'Apache 2.4.18 et de WordPress 4.9 suggère que le système peut être dépassé. Ces versions ne sont peut-être plus prises en charge et peuvent contenir des vulnérabilités de sécurité non corrigées.
* WordPress 4.9 a été identifié et est marqué comme non sécurisé, il est probable que des vulnérabilités connues existent pour cette version qui pourraient être exploitées.
* L'accessibilité directe des fichiers xmlrpc.php et wp-cron.php peut indiquer que des fonctionnalités potentiellement exploitables sont actives. XML-RPC a été fréquemment exploité dans le passé pour des attaques par amplification, tandis que WP-Cron peut être utilisé pour exécuter des tâches automatisées qui pourraient être détournées par un attaquant.
* La disponibilité publique du fichier readme.html expose des détails qui pourraient aider un attaquant dans ses efforts pour compromettre le site.

Nous allons maintenant lancer ensuite la commande :

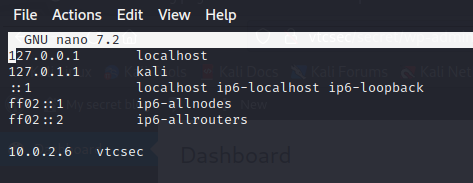
wpscan -U admin --url [http://<ip de la machine cible>/](http://vtcsec/secret)  -P /usr/share/wordlists/metasploit/http\_default\_pass.txt

****

Nous allons maintenantpasser le formulaire d’authentification



Puis on va mettre dans le localhost l’adresse IP de la cible et la page web.

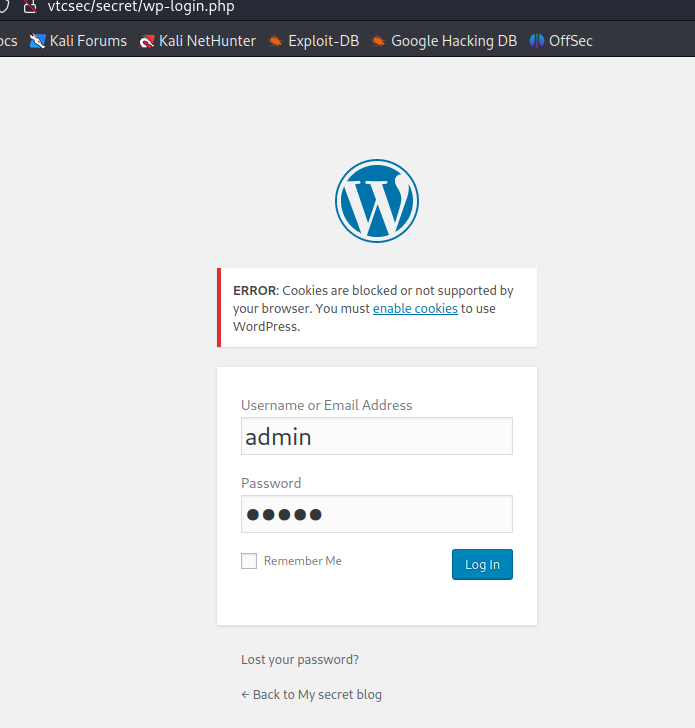


Ensuite, on peut apercevoir que le site a changer.

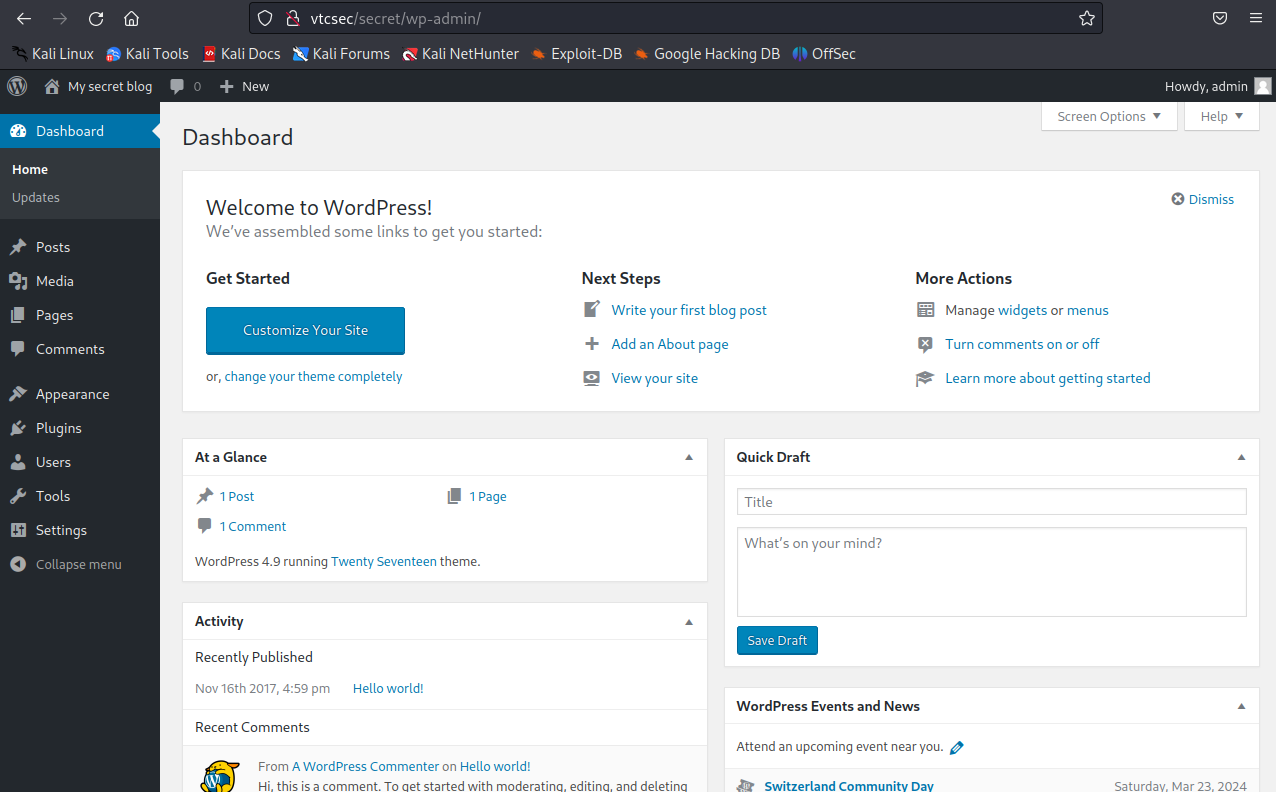
Voici les identifiants :

ID : admin

Mdp : admin



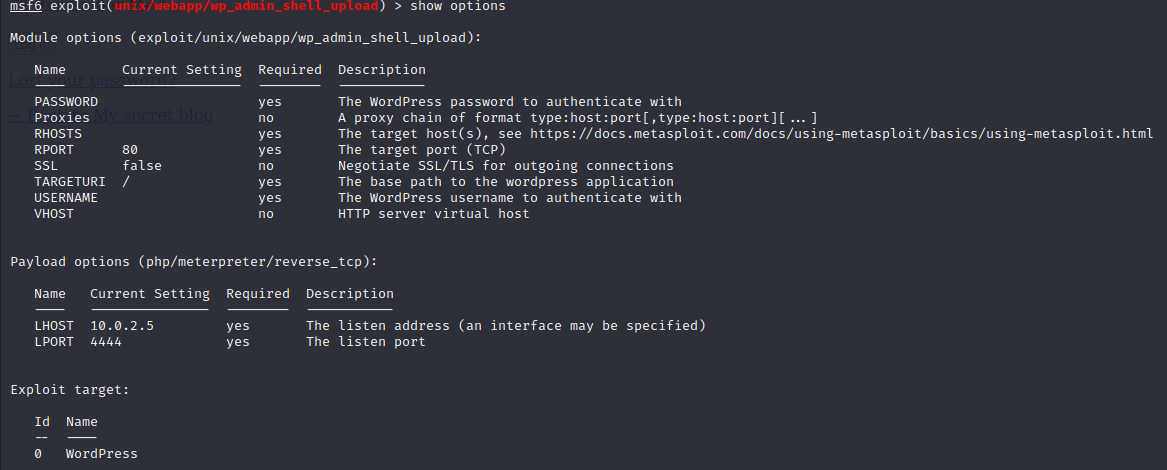
On peut apercevoir qu’on peut bien accéder au site web :

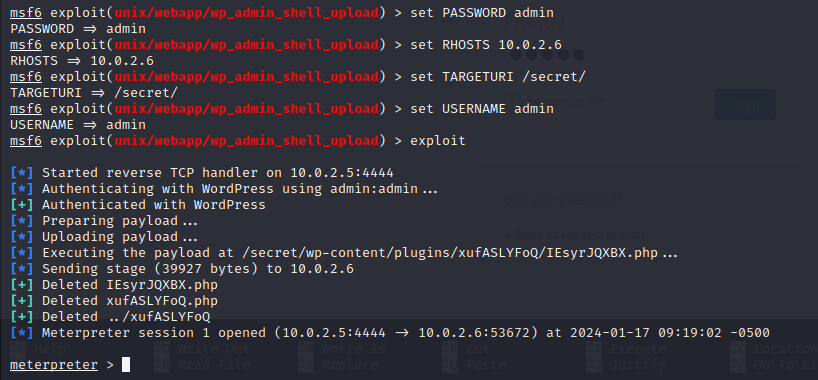


Enfin, nous allonsouvrir metasploit et utilisez l’exploit :

*exploit/unix/webapp/wp\_admin\_shell\_upload*

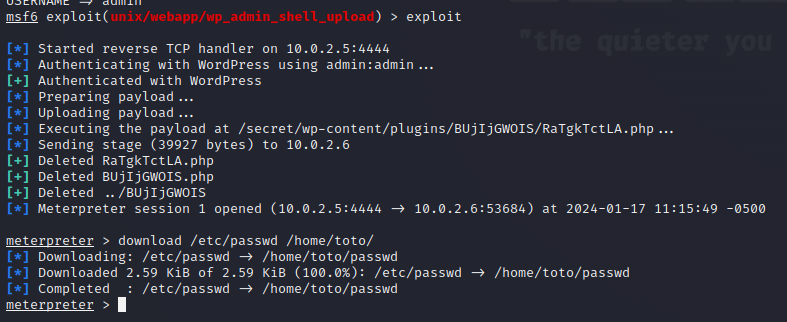






Grâce aux informations obtenu aux étapes précédente et l’exploit ci dessus, on peut prendre le contrôle de la machine.

Enfin, nous allons exporter le fichier /etc/passwd dans un répertoire :



Recommendations :

* Mises à jour régulières de WordPress, ses thèmes et ses plugins sont toujours à jour. Les développeurs de WordPress publient régulièrement des correctifs de sécurité pour remédier aux vulnérabilités connues.
* Suppression des thèmes et plugins inutilisés ,désactivez et supprimez les thèmes et plugins que vous n'utilisez pas. Moins de code signifie moins de points d'attaque potentiels.
* Complexité des mots de passe : Utilisez des mots de passe forts pour les comptes WordPress, y compris celui de l'administrateur. Évitez les mots de passe faciles à deviner, comme "admin" ou "password". Utilisez des combinaisons de lettres majuscules, minuscules, de chiffres et de caractères spéciaux.
* Limitation des tentatives de connexion : Utilisez un plugin de limitation des tentatives de connexion pour bloquer automatiquement les adresses IP après un certain nombre de tentatives infructueuses.
* Contrôle d'accès aux fichiers sensibles : Restreignez l'accès aux fichiers sensibles tels que wp-config.php et .htaccess en utilisant des règles de sécurité appropriées dans votre configuration de serveur web.
* Firewall d'application web (WAF) : Mettez en place un pare-feu d'application web pour surveiller et bloquer les attaques avant qu'elles n'atteignent votre site WordPress.
* Surveillance des journaux : Surveillez régulièrement les journaux d'activité du site WordPress pour détecter toute activité suspecte. Les plugins de sécurité peuvent vous aider à automatiser cette tâche.
* Sauvegardes régulières : Effectuez des sauvegardes régulières de votre site WordPress afin de pouvoir le restaurer en cas de compromission.
* Formation en sécurité : Assurez-vous que les personnes qui ont accès à l'administration de WordPress sont informées des meilleures pratiques en matière de sécurité, notamment en évitant de télécharger des plugins ou des thèmes non fiables.
* Authentification à deux facteurs (2FA) : Activez l'authentification à deux facteurs pour les comptes d'administration WordPress, ce qui ajoute une couche de sécurité supplémentaire.