

Comparaison

20

Challenge 188 résolutions

## Comparaison

20

algorithmique hardware

Cette épreuve fait partie de la série qui utilise la machine virtuelle du FCSC 2023, plus d'informations sur celle-ci ici : <https://www.france-cybersecurity-challenge.fr/vm>

Afin de se familiariser avec la machine virtuelle et son langage assembleur, vous devez écrire dans cette épreuve un code assembleur qui effectue une comparaison.

La machine est initialisée avec deux valeurs aléatoires dans les registres **R5** et **R6**. À la fin du programme, **R0** doit contenir **1** si les valeurs sont différentes, **0** sinon.

Le code machine (bytecode) sera envoyé sous un format hexadécimal, qu'on pourra générer à l'aide de l'assembleur fourni (fichier **assembly.py**).

nc challenges.france-cybersecurity-challenge.fr 2300

assembly....

machine.py

challenge...

Flag

Submit

challenge.py > ...

```
43
44 if __name__ == "__main__":
45
46     # try:
47     print("Enter your ASM instructions")
48     asm = []
49     "XOR R0, R0, R0",
50     "CMP R5, R6", #Z=1 si R5 = R6 et sinon Z=0 ; si R5
51     "JZA end",
52     "MOV R0, #1", #si égal, R0 = 1 sinon ret direct R0 = 0
53     "end:",
54     "STP"
55     ]
56     code = assembly(asm)
57     print(code)
58     correctness(code)
59     # except:
60     #     print("Please check your inputs.")
61
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL Python + - [ ] [X] ... ^ X

bytes generated : 4400066588000006800000011400

4400066588000006800000011400

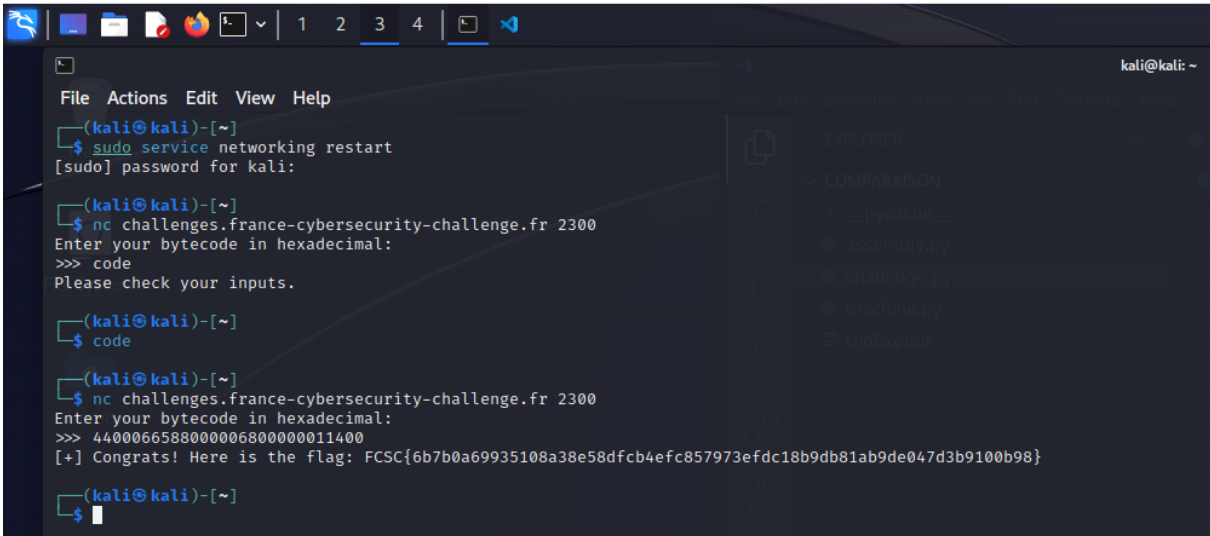
Traceback (most recent call last):

File "/home/kali/Documents/FCSC2023/INTRO/Comparaison/challenge.py", line 61, in <module>

correctness(code)

File "/home/kali/Documents/FCSC2023/INTRO/Comparaison/challenge.py", line 41, in correctness

flag = open("flag.txt").read().strip()



The screenshot shows a Kali Linux terminal window with a dark theme. The terminal displays the following commands and output:

```
(kali@kali)-[~]
$ sudo service networking restart
[sudo] password for kali:

(kali@kali)-[~]
$ nc challenges.france-cybersecurity-challenge.fr 2300
Enter your bytecode in hexadecimal:
>>> code
Please check your inputs.

(kali@kali)-[~]
$ code

(kali@kali)-[~]
$ nc challenges.france-cybersecurity-challenge.fr 2300
Enter your bytecode in hexadecimal:
>>> 4400066588000006800000011400
[+] Congrats! Here is the flag: FCSC{6b7b0a69935108a38e58dfcb4efc857973efdc18b9db81ab9de047d3b9100b98}

(kali@kali)-[~]
$
```

On the right side of the terminal window, a file explorer pane is visible, showing a directory structure with files like `EXPLODER`, `COMPARAISON`, `__pycache__`, `assembly.py`, `challenge.py`, `machine.py`, and `OldExploit`.