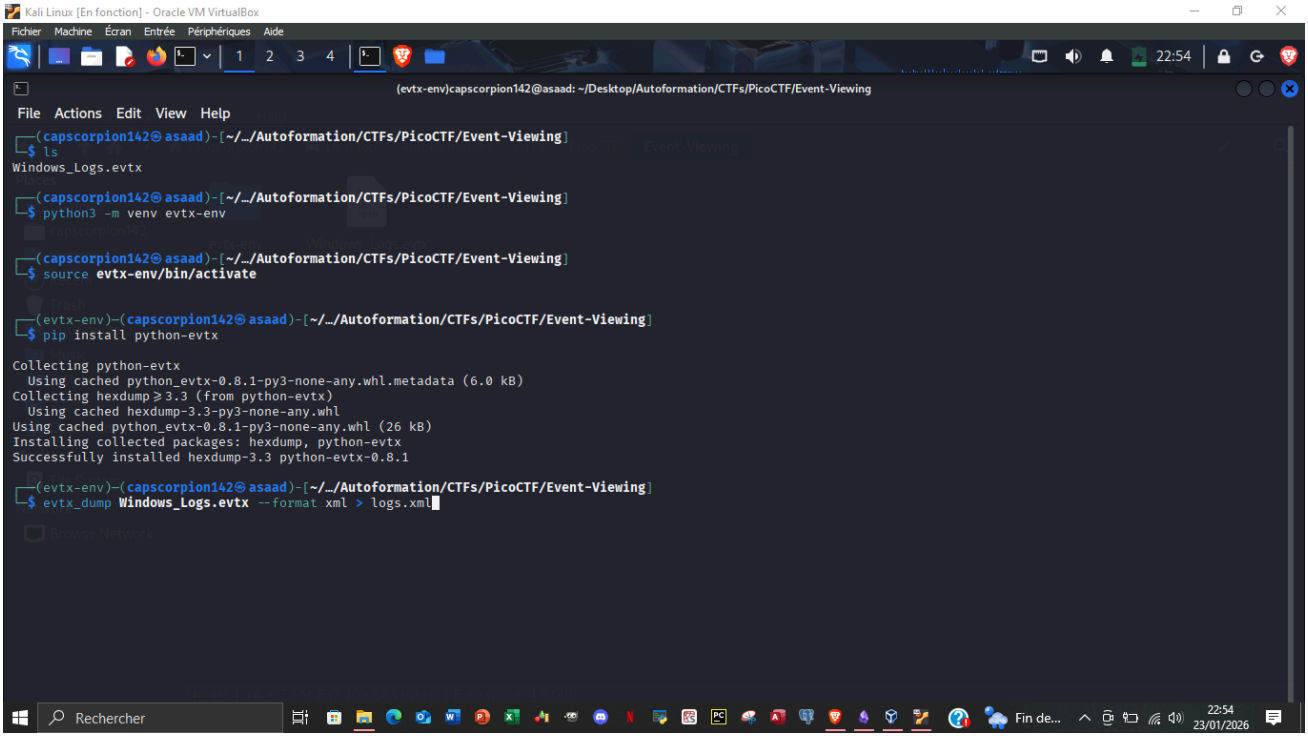
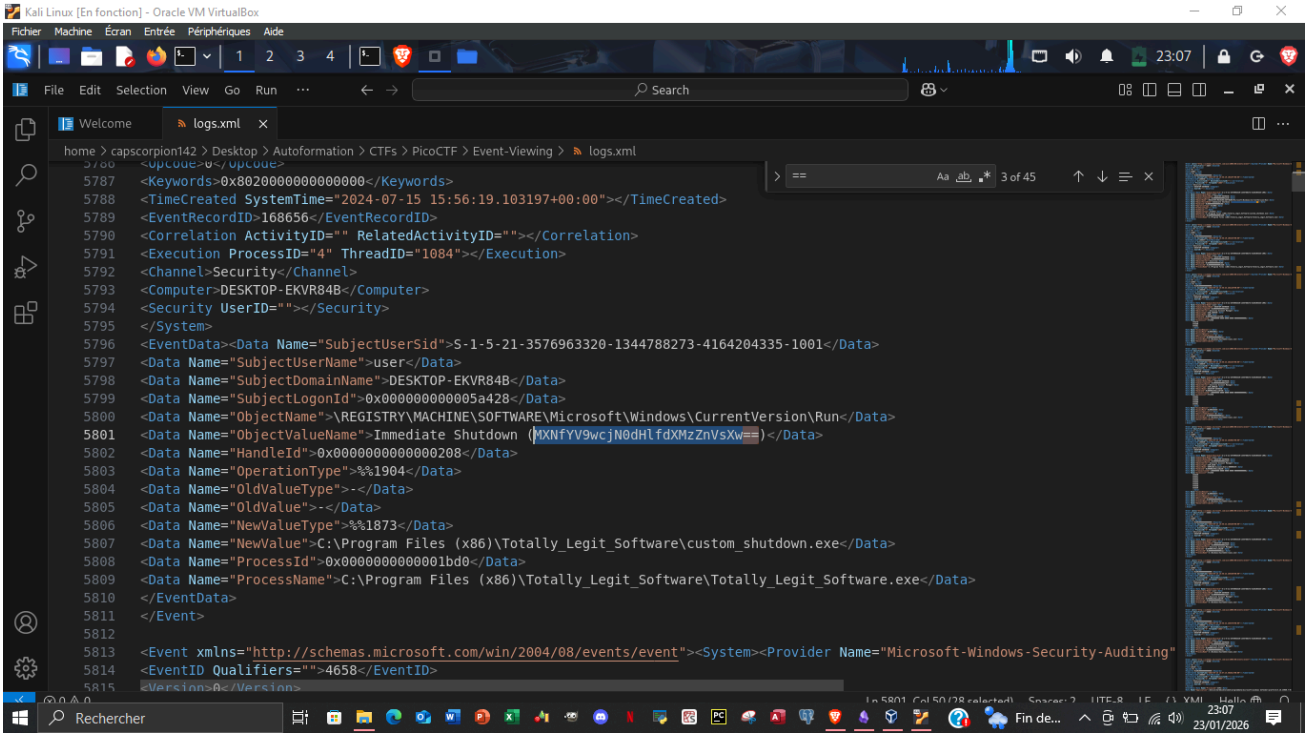
Event-Viewing

- First we create a Python Environment...
- Then we convert the evtx file into a logs.xml file using this tool we installed:

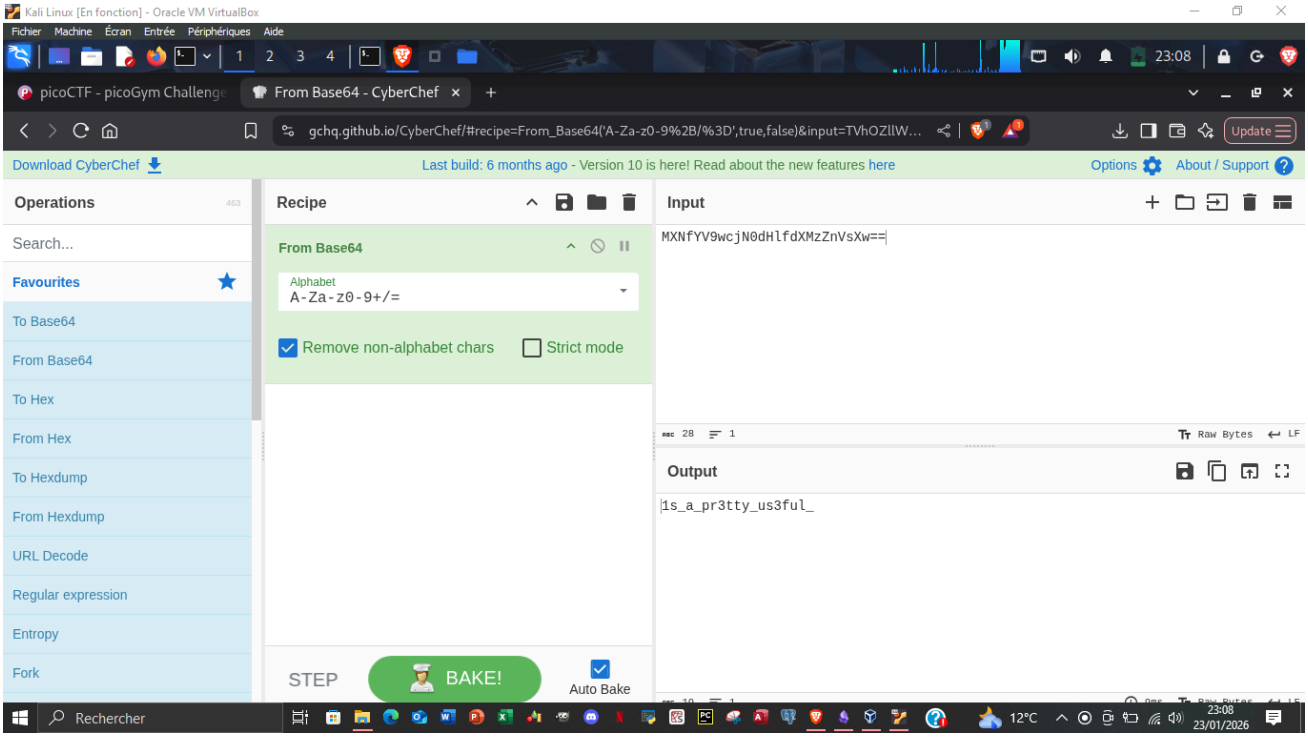


- Then we open that file xml:

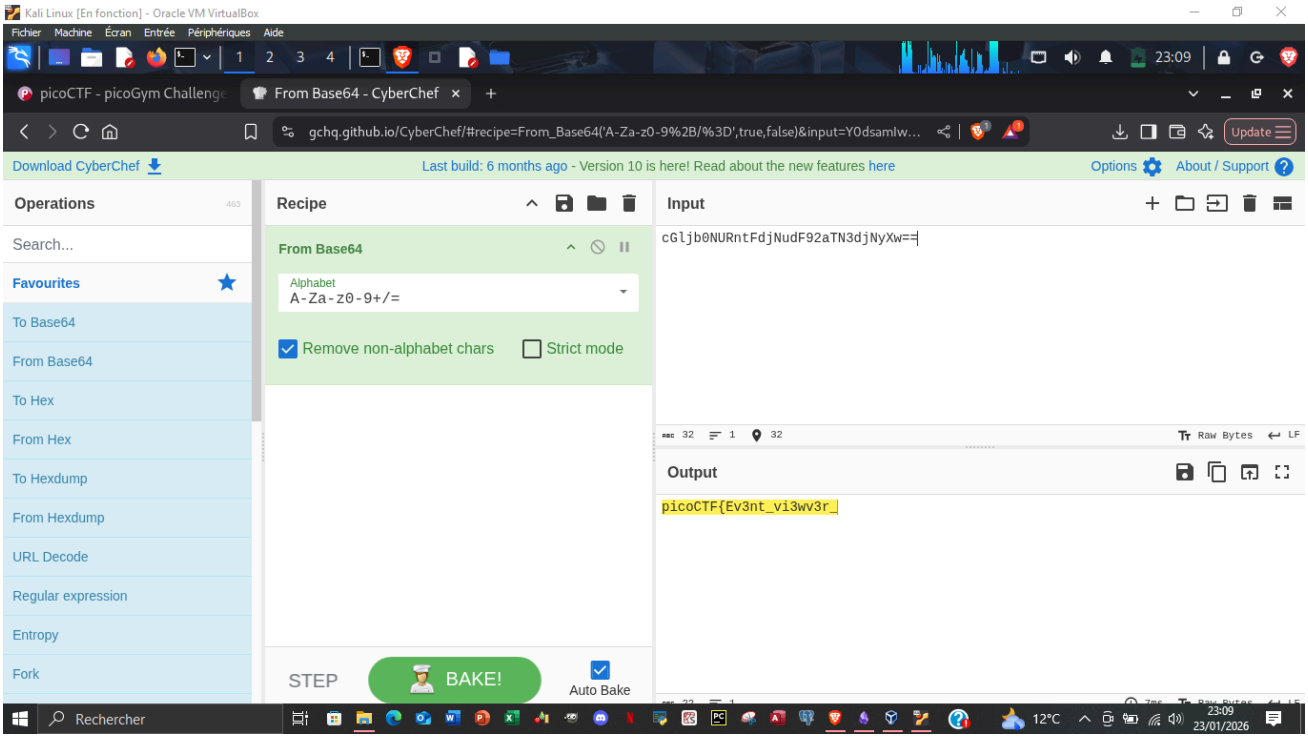


- And so, we investigate that file for anything suspicious...
- As we know, the flag is divided in three pieces...

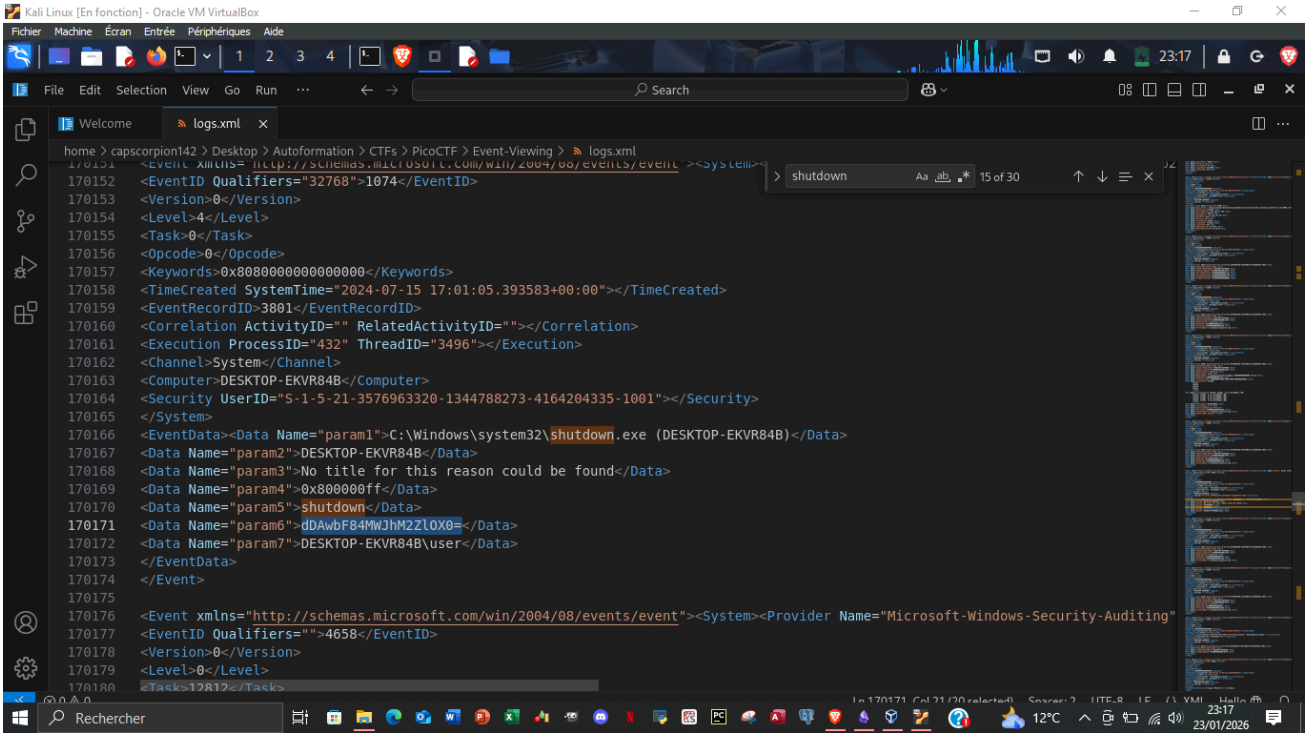
- We decode the first piece:

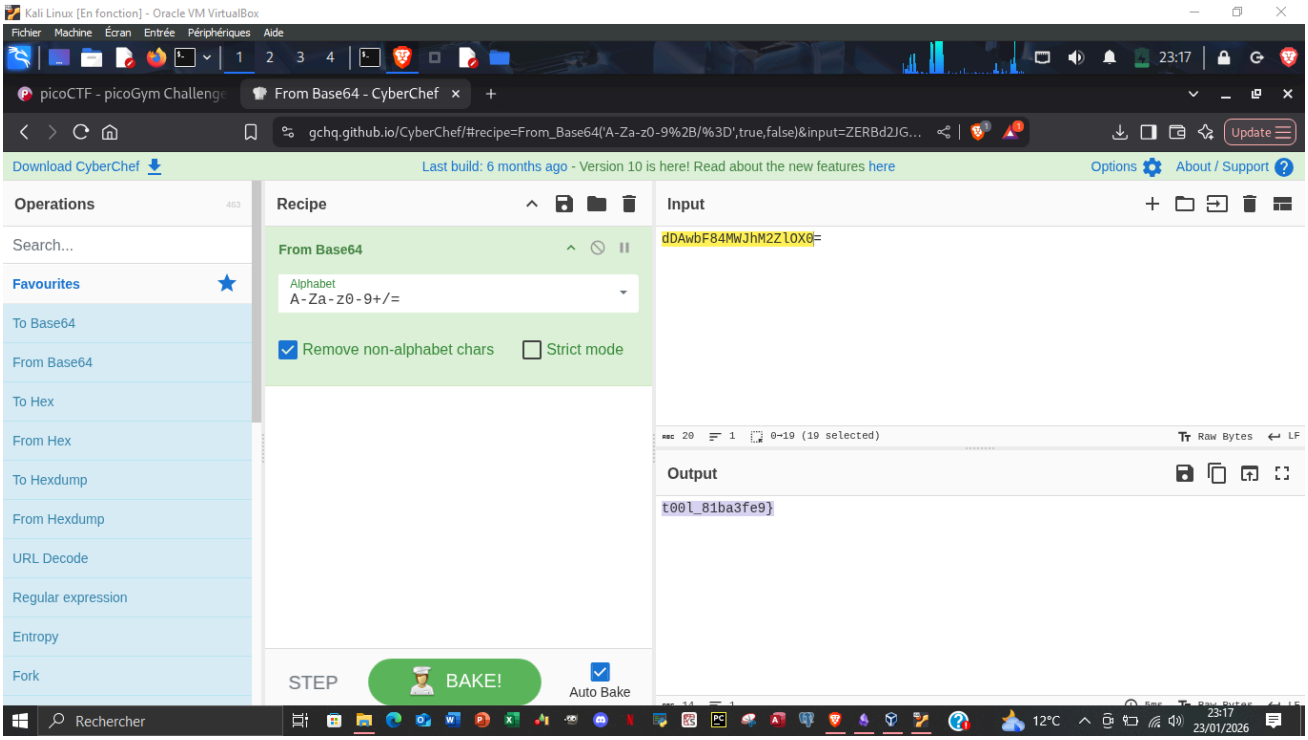


- here's the second piece:

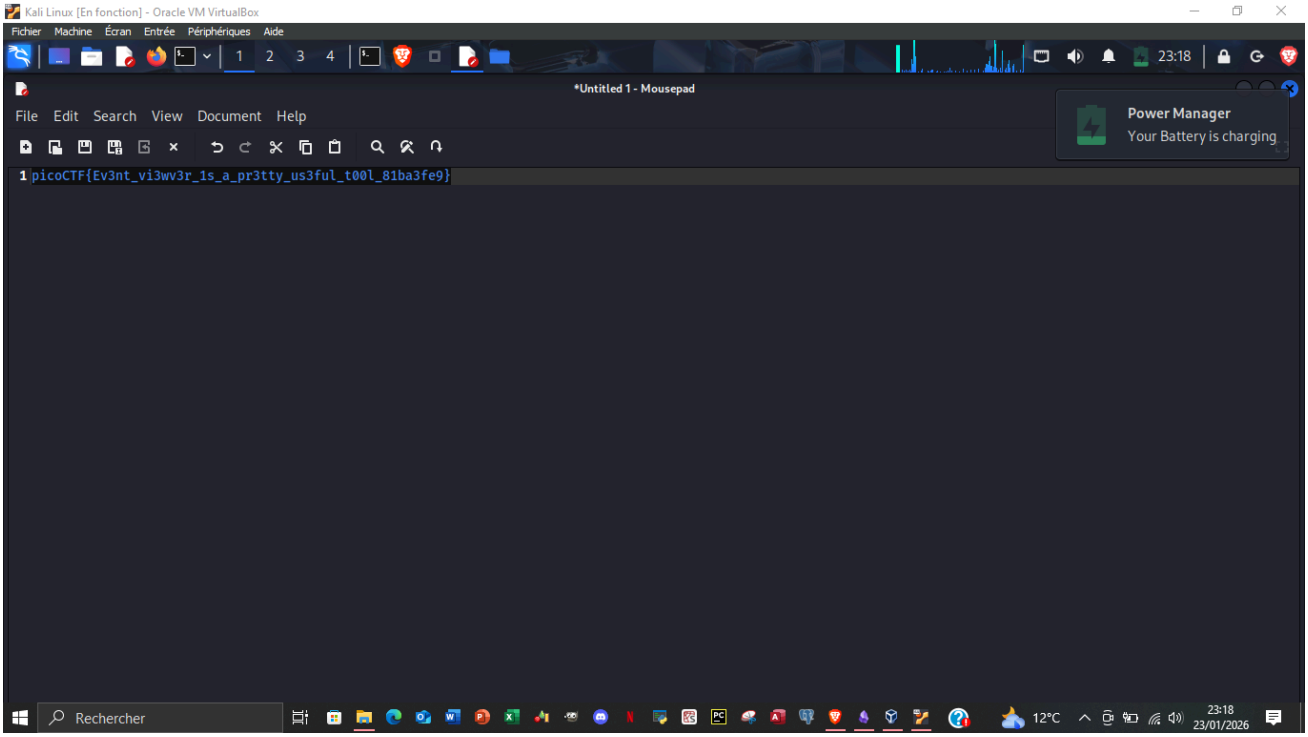


- The last piece after I filtered with "shutdown":





- The flag :


Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
*Untitled 1 - Mousepad
File Edit Search View Document Help
Power Manager
Your Battery is charging
1 picoCTF{Ev3nt_vi3wv3r_1s_a_pr3tty_us3ful_t00l_81ba3fe9}
Rechercher
12°C
23:18
23/01/2026