Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

daffainfo feat: grouped the challs e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month

README.md

coup de réseau

> Too late. The network admin's system was compromised and we can't access our network anymore. Investigate the memory dump.

> Too late. The network admin's system was compromised and we can't access our network anymore. Investigate the memory dump.

> Memory Dump Link: https://drive.google.com/file/d/1LbElkzno-FophYpkTLPL5ic2BnZgn-UN/view?usp=sharing

> Amour Plastique will be visible after solving this challenge.

About the Challenge

We were given a dump memory file called `dump2.mem` and we need investigate the memory dump file

How to Solve?

In this case im using `strings` and `grep` to get the flag

```
root@ubuntu-s-1vcpu-2gb-sgp1-01:~/dump1# strings dump2.mem | grep "nite{"
C:\Users\napoleon\AppData\Roaming\Microsoft\Windows\Recent\nite{8_bit_synths}.lnk
nite{8_bit_synths}.mp3
main input debug: Creating an input for 'nite{8_bit_synths}'
nite{8_bit_synths}.lnk
nite{8_bit_synths}.lnk
nite{can
nite{8_bit_synths}.mp3
C:\Users\admin\Music\nite{8_bit_synths}.mp3
main input source debug: creating demux: access='file' demux='any' location='/C:/User
nite{8_bit_synths}
#EXTINF:3545,nite{8_bit_synths}
C:\Users\admin\Music\nite{8_bit_synths}.mp3
#nite{cant_catch_me}
nite{8_bit_synths}.mp3
```

```
nite{cant_catch_me}
```