Hackfest CTF 2020 pwning challenges

salt

montrehack

17 March 2021

Presentation of the challenges

- Challenge 1
  - Estimated difficulty : Easy
  - Number of solves : 20
- Challenge 2
  - Estimated difficulty : Intermediate
  - Number of solve : 1 (so it's harder than expected !)

Prerequisite

- Basic knowledge of assembly (x64)
- One programming language (Python)
- Basic skills of reverse engineering and debugging
- Recommended tools : pwntools, gdb, ghidra

Presentation

- nc 138.197.158.98 1234
- You need to download chal1 and reverse it to understand how the secret number is generated

Hint

- The time zone in the server is maybe different in your machine
- It is advised to use the same randomization library of the program

Presentation

- nc 138.197.158.98 5678
- You need to download chal2 and exploit the binary

Hint 1

- The first step is to find a way to control the RIP
- Think about how an array works

Hint 2

- You need to find a way to bypass the ASLR
- The leak is very classic and trivial

Hint 3

- You need to find a way to load your shellcode
- Where in the program is there enough space ?
- Bad character will oblige you to build your shellcode