Debugging and File Permission

In this task, we’ll be learning the basic of reverse engineering and assembly. Here are some important things to do before starting the task:

* These files have been compiled with the lowest level of optimisation(mức tối ưu hóa thấp nhất) on Unix based machines(machines dựa trên Unix) and are intended to be(được dự định) run on Linux/Mac.
* Make sure you set up a debugger – It would be good to get comfortable with radare2 which can be downloaded from here(<https://github.com/radare/radare2>). You can also use other debuggers like gdb, which come installed in most Unix based operating systems
* When these files have downloaded, change the permissions(quyền) of these files using the command **chmod +x filename**

These tasks will make use of crackme files. The objective(mục tiêu) of these files is to understand the assembly code to uncover(phát hiện ra) the right password for the file.

Here are some of the important things you will learn in this course:

* If statements in assembly
* Loops in assembly
* Standard(tiêu chuẩn) function calls in assembly
* Calling Convention(quy ước) in assembly

Crackme1

This first crackme file will give you an introduction(giới thiệu) to if statements and basic function calling in assembly.

Step1: chmod +x crackme1.bin

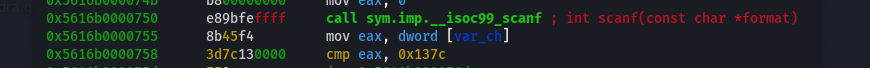
Step2: r2 –d crackme1.bin  
 >>>aaa  
 >>>pdf @main

Password: hax0r

**Crackme2**

This is the second crackme file-unlike the first file, this will involve(liên quan) examining(kiểm tra) registers, how and where values are compared

Step1: chmod +x crackme2.bin

Step2: r2 –d crackme2.bin  
 >>>aaa  
 >>>pdf @main  


Step3: giá trị được scanf sau đó so sánh var\_ch với 0x137c

Step4: dùng rax2 tool: rax2 0x137c   


**Crackme3**

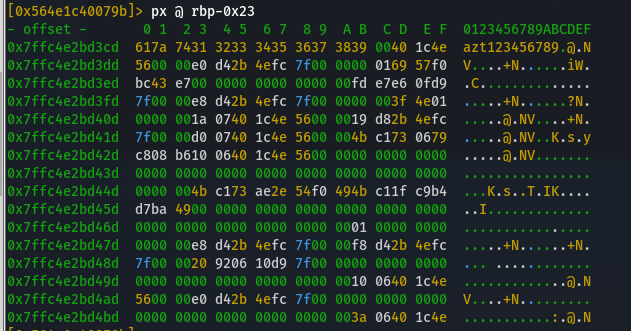
This crackme will be significaltly more challenging(thử thách hơn đáng kể) – it involves learning how loops work and how they are represented(đại diện) in assembly.

Step1: chmod +x crackme1.bin

Step2: r2 –d crackme1.bin  
 >>>aaa  
 >>>pdf @main  


Step3: Set breakpoint to check comparison  
db 0x55712900079b

Step4: Kiểm tra giá trị:

* px @ rbp-0x28  
  
* px @ rbp-0x23  
  

I guess password is “azt”