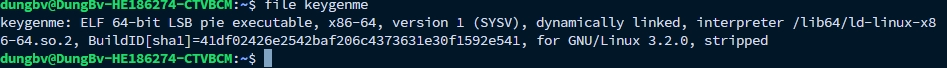
Write up cho key gen me :

File này đã bị stripped k còn thông tin debug



Địa chỉ ở ghidra sau khi disassembly k thể dùng đẻ debug đặt breakpoint bên gdb

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

Vấn đè là phải đặt breakpoint ở ví trị sau khi austack38 đã hoàn thiện

Austack38 chính là 9 kí tự cuối trong flag

A white background with black text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Chỉ cần có thể có địa chỉ đặt breakpoint là được

K h thẻ tìm đc base address :

Nên dùng starti để đi load chương trình

Sau đó dùng : info proc mappings đẻ sem thông tin về địa chỉ base address các vùng nhớ mà chương trình sử dụng

Xác định được base address là dòng 2 có vẻ đây là .text sections

A screenshot of a computer program

AI-generated content may be incorrect.

Sau đó disassebly đoạn này đẻ có code đọc và tìm phần khở tạo cho austack38 là nơi lưu flag

A computer screen shot of a program code

AI-generated content may be incorrect.

Đây chính là phần khở tạo cho austack38 (9 kí tự cuối )bên ghidra

A screen shot of a computer program

AI-generated content may be incorrect.

Việc của mình là sem string tại địa chỉ $sbp – 0x15 và đặt breakpoint sau khí nó đã tạo xong tại 5414 HAY sau nữa 5419 : 

Ta thấy rằng min adress của ghidra dùng đây là 100000 và ofset là 1419 vậy tương tự

Ta thấy min address của gdb là 0x555555554000 ta cũng cộng với offset này ra địa chỉ tương ứng

0x555555554000 + 0x1419 = 0x555555555419 :

Chú ý nhập 36 kí tự input cho đầu vào yêu cầu :

A screenshot of a computer

AI-generated content may be incorrect.



Lắp 9 kí tự này với key gốc : picoCTF{br1ng\_y0ur\_0wn\_k3y\_"9d74d90d}

A screen shot of a computer code

AI-generated content may be incorrect.

->> flag : " picoCTF{br1ng\_y0ur\_0wn\_k3y\_"