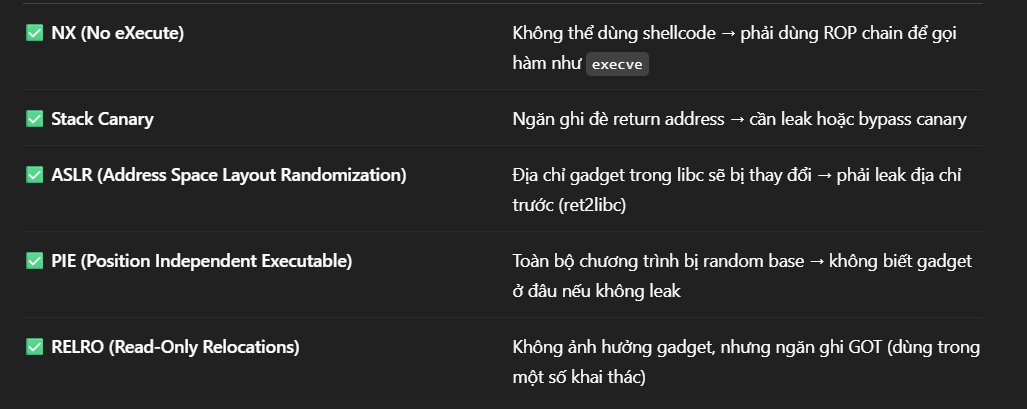
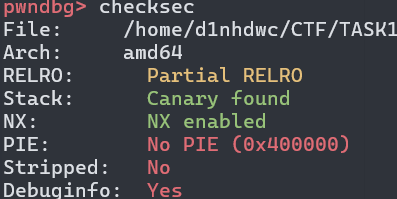
**Challenge: ROPchain\_chall**

**\* ROP Gadget** là một đoạn mã máy nhỏ (thường chỉ vài byte) kết thúc bằng lệnh ret và thực hiện một hành động đơn giản. Ví dụ như: pop rdi ; ret, mov rax, rdi ; ret, syscall, v.v.

\* Ứng dụng của ROPgadget để tìm các đoạn mã (ROPgadgets) trong binary hoặc thư viện để giúp bạn tạo ROPchain thay thế cho shellcode (với những bài không thể thực thi shellcode trên stack do các cơ chế bảo vệ ).

- Các chế độ bảo vệ ảnh hưởng đến ROPgadget:



Với file chall:  


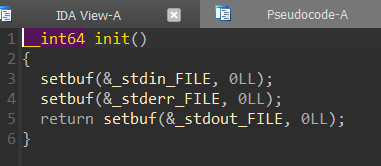
- Canary bật nhưng không hiểu sao debug vẫn buffer overflow đc =)) chắc do lỗi của checksec

- NX enable -> ko thể thực thi shellcode trên stack -> phải nhặt các gadget để thực thi hàm execve

- PIE: No PIE - > ko cần leak địa chỉ do địa chỉ luôn cố định

**\* Xem pseudo code ở IDA xem, chương trình hoạt động ntn:**

- Có chỉ có 2 hàm chính init() và main():

Mô tả chương trình: Đầu tiên khởi tạo các biến v3, v4, v5, v6 và buffer v8[80] sau đó gọi hàm init để khởi tạo các bộ đệm, nhập v8 bằng gets và kết thúc chương trình

A screen shot of a computer

AI-generated content may be incorrect.

**\* Nhận diện ROPchain:**

- Không có sẵn hàm system() hoặc hàm gọi shell trong file binary

- hàm gets() luôn xảy ra lỗi buffer overflow nên có thể dùng buffer overflow để điều khiển thanh ghi rip

- PIE tắt

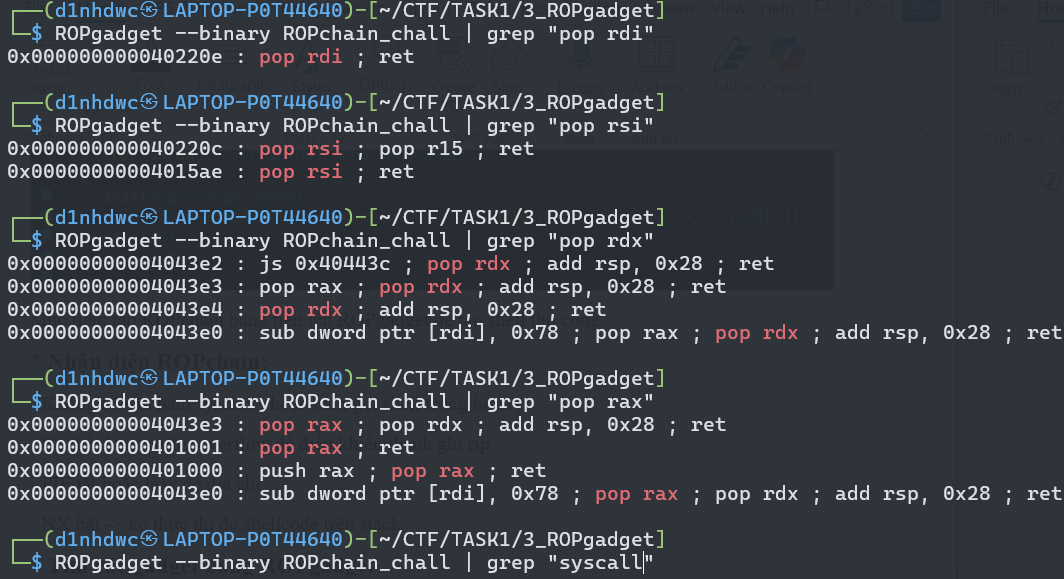
- NX bật -> ko thực thi đc shellcode trên stack

-> Mục tiêu: tạo ROPchain bằng tiện ích ROPgadget để tạo shell thủ công

**\* Tìm các gadget bằng ROPgadget**

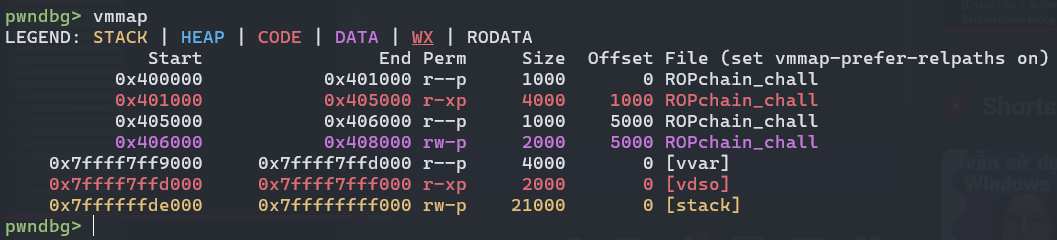
- Tìm các gadget của pop rax, pop rdi, pop rsi, pop rdx và syscall tương ứng với các argument của hàm execve()

- Phải tìm gadget tại các pop vì pop dùng để đưa giá trị từ stack vào thanh ghi, giúp bạn điều khiển tham số của hàm hoặc syscall mà bạn muốn gọi.



-> viết vào script

- Sau đó, ta sẽ tìm 1 địa chỉ có thể write đc của file chall này

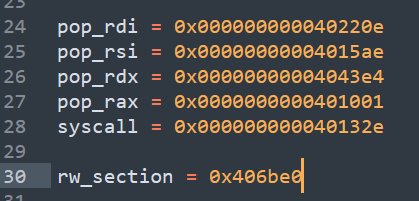


- ta thấy có địa chỉ 0x406000 có thể read và write đc nên ta dùng lệnh x/50xg 0x406000 để tìm 1 địa chỉ trống chưa có giá trị để write vào

A screenshot of a computer screen

AI-generated content may be incorrect.

-> Chọn 1 trong các địa chỉ trống rồi viết vào script



**\*Viết Payload:**

- Trước tiên ta sẽ tính offet từ hàm gets đến return

A screenshot of a computer code

AI-generated content may be incorrect.

-> ta sẽ truyền vào 88 byte rác vào trước sau đó thiết lập thanh ghi rdi với địa chỉ có thể write vào payload



-> overwrite rip thành gadget pop rdi, sau đó pop cái địa chỉ có thể ghi đc sau đó đến địa chỉ của hàm gets() để ta nhập chuỗi ‘/bin/sh’

- Sau đó ta sẽ viết tiếp payload để thực thi luôn hàm execve(“/bin/sh”, 0, 0) với 3 argument:

rdi = con trỏ trỏ tới địa chỉ “/bin/sh” , rsi = 0, rdx = 0 và syscall numer rax = 0x3b

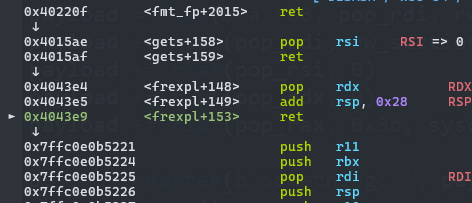


Script:

A screen shot of a computer code

AI-generated content may be incorrect.

- Kiểm tra bằng debug động:



- Ở đây ta thấy lệnh add rsp, 0x28 sau khi pop rsi rdx, ta cần cộng thêm 0x28 byte rác để nhảy trúng pop rax

A computer screen shot of white text

AI-generated content may be incorrect.

- Debug động kiểm tra lại 1 lần nữa

A screen shot of a computer program

AI-generated content may be incorrect.

-> đã đúng script

- Giờ giử solve.py lên:

A screen shot of a computer

AI-generated content may be incorrect.-> đã chiếm đc shell