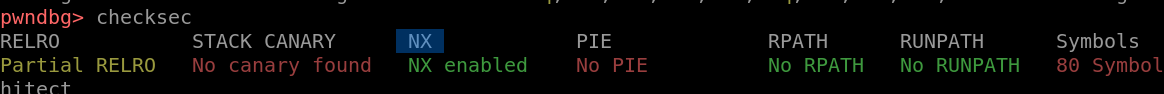
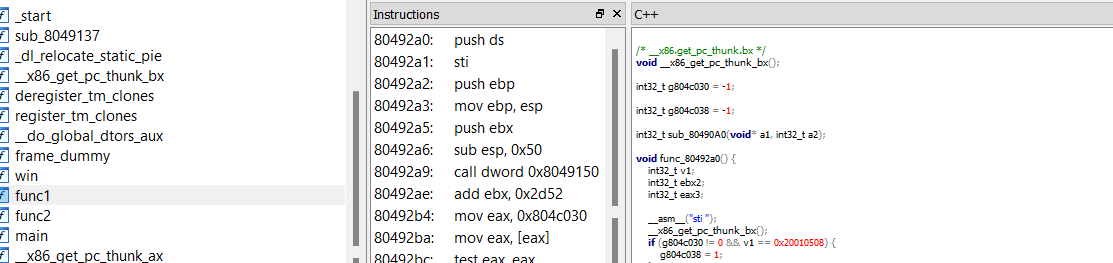
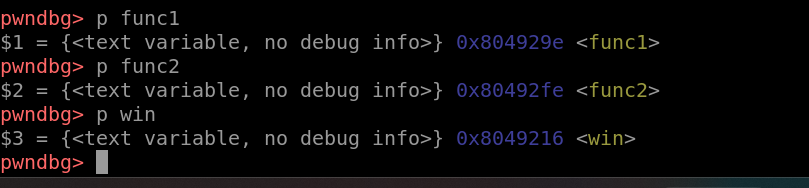
Stack\_Architect



* Khi dùng gdb để checksec thì ta thấy NX đã được bật nghĩa là ta không thể truyền shell code vào



* Dùng ida để tìm địa chỉ của hàm func1, func2, win theo chuỗi để có thể thực hiện ROP attack
* Trong hàm func1 và 2 ta thấy có so sánh giá trị với 0x20010508 nên ta cần truyền giá trị này để làm tham số cho func1 và func2 để sau đó mới có thể đến hàm win



* Địa chỉ của các hàm

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Dùng ROPgadget để tìm địa chỉ của gadget làm thay đổi thanh ghi ebx dùng trong các lệnh để nhập xuất
* Payload:

Ảnh có chứa văn bản

Mô tả được tạo tự động

ShellCode

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta checksec file thì thấy có 1 số trường không được kích hoạt và trường NX disabled thì ta sẽ nghĩ đến thực thi shell code với các phương thức read, write và open

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Kết quả khi thực hiện truyền payload

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động