**Câu 1: Tạo Shellcode thực hiện hiển thị MessageBoxA với yêu cầu như sau:**

|  |  |
| --- | --- |
| **Yêu cầu hiển thị MessageBoxA** | **Ví dụ:** |
| Tiêu đề: ATHDH\_KT2  Nội dung: Hiển thị 2 dòng:  Dòng 1: <Họ và tên>  Dòng 2:<Lớp> |  |

**Câu 2: Thực hiện các yêu cầu sau:**

1. ***Viết và biên dịch thành file thực thi đoạn chương trình sau:***

#include <stdio.h>

main()

{

printf("Chuc mung ban.\nBan da thuc thi file thanh cong.");

}

Lưu lại với tên file có định dạng: **<TenLop>.c**

*(Chú ý: Tên file viết liền không dấu, và phải đúng yêu cầu)*

1. ***Đoạn chương trình sau có lỗ hổng tràn bộ đệm:***

#include <string.h>

#include <stdio.h>

main()

{

char name[200];

printf("Your name? ");

scanf("%s", name);

bo(name, "uname -a");

}

int bo(char \*name, char \*cmd)

{

char c[10];

char buffer[10];

strcpy(c, cmd);

strcpy(buffer, name);

printf("Goodbye, %s!\n", buffer);

printf("Executing command: %s\n", c);

fflush(stdout);

system(c);

}

Khai thác lỗ hổng của đoạn chương trình trên để thực thi được file đã biên dịch ở ý a.

**Câu 3. Khai thác lỗ hỏng tràn bộ đệm theo đề được phân.**