- Khi truyền giá trị -1 cho hàm malloc(), tham số này sẽ được chuyển đổi thành kiểu size\_t, vốn là số nguyên không dấu. Giá trị -1 chuyển sang size\_t, nó trở thành giá trị lớn nhất có thể biểu diễn, ví dụ: 0xFFFFFFFF (trên hệ thống 32-bit) hoặc 0xFFFFFFFFFFFFFFFF (trên hệ thống 64-bit). Tức là malloc() sẽ nhận tham số 0000 0000 0001 0000 + 1111 1111 1111 1111 = 1 0000 0000 0000 1111. Xảy ra hiện tượng tràn số, nên ta bỏ bit 1 đầu nên kết quả sẽ là 0x000f = 0xf

A screenshot of a computer

Description automatically generated

- Tham số thứ 3 của read là 0xffffffff, tuy nhiên read đọc giá trị số nguyên không dấu nên số byte thật sự read đọc có giới hạn là 4294967295

A screenshot of a computer

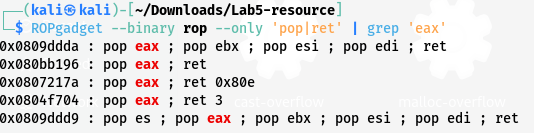
Description automatically generated

- Tham số thứ 3 của read là 0xffffffff, tuy nhiên read đọc giá trị số nguyên không dấu nên số byte thật sự read đọc có giới hạn là 4294967295

A black text on a white background

Description automatically generated

- Sử dụng ROPgadget tìm các địa chỉ của pop eax, pop ebx, pop ecx, pop edx, int 0x80

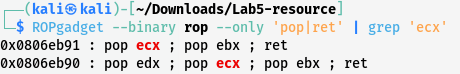


- Ta tìm được địa chỉ của pop eax ; ret là 0x080bb196

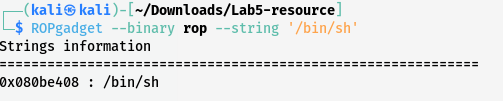
A screenshot of a computer

Description automatically generated

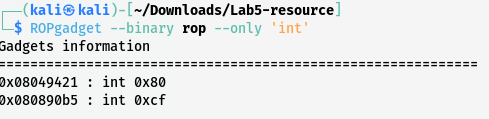
- Ta có địa chỉ của pop ebx; ret là **0x080481c9**



- Ta thấy có một địa chỉ gộp cả ba pop edx ; pop ecx; pop ebx; ret là **0x0806eb90**.



- Tìm thấy vị trí của chuỗi /bin/sh ở 0x080be408



- Cuối cùng ta tìm địa chỉ của system call int 0x80 là **0x08049421**

- Tiếp theo ta sẽ tạo chuỗi thực thi các gadget. Cần xác định địa chỉ trả về để ghi đè

Đặt breakpoint tại gets. Ta thấy địa chỉ ebp là 0xffffcd98, còn địa chỉ bắt đầu sẽ là 0xffffcd2c. Từ đó ta xác định được buffer là 0xffffcd98 – 0xffffcd2c = 108

A close up of a number

Description automatically generated

A computer code with text

Description automatically generated with medium confidence

- Ngoài ra ta cần chèn thêm 4 byte bất kỳ để có thể ghi đè, nên padding là 112 byte

Theo stack thì ta sẽ tạo một file python khai thác như sau

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generated