Intro

Căn phòng này giả định rằng bạn có kiến thức assembly x86 cơ bản. Nếu bạn không có, tôi khuyên bạn nên làm Intro to x86-64 trước khi hoàn thành việc này.  
Căn phòng này cũng không được thiết kế để dạy 100% mọi thứ trên radare2. Nó được thiết kế để dạy cho bạn cách một số thứ phổ biến hơn trong radare2 được sử dụng.  
Các tập tin zip đi kèm có all the binaries bạn sẽ cần cho bài tập này.

Command Line Options

Giới thiệu nhanh về một số command line flags thường được sử dụng cho radare2, một số flags này sẽ cực kỳ hữu ích cho tasks sau này. Bao gồm tất cả các phần của flag bao gồm cả -. All flags có thể được tìm thấy trong the help menu.

+ Flag nào bạn đặt để analyze the binary khi vào r2 console(tương đương với việc chạy aaa khi bạn ở bên trong console)? -a  
+ Làm thế nào để kích hoạt debugger?  
+ Làm thế nào để mở file trong write mode?  
+ Làm thế nào để enter console mà không cần opening a file?

Analyzation

Khi inside the radare console, bạn có vô số tùy chọn để analyze your binary. Nói chung tất cả các analyzation command bắt đầu bằng chữ a. Nếu bạn muốn liệt kê tất cả commands có thể được thực hiện với các chữ cái bắt đầu của bạn, bạn thêm một dấu hỏi vào cuối. Ví dụ a? sẽ xuất ra ab,aa,ac cùng với một description về những gì mỗi command làm.

+ What command 'Analyzes Everything' (all function và their arguments: Giống như chạy với radare với -A)? aaa  
+ What command does basic analysis on function?   
+ Làm thế nào để list ra tất cả function?  
+ Có bao nhiêu function ở trong example1 binary?  
+ What is the name of the secret function in the example1 binary?

Information

i là một command shows general information of the binary. Giống như a nó có nhiều lệnh phụ với mức độ cụ thể khác nhau.

+ What command shows all the information about the file that you're in?    
+ Làm thế nào để bạn có được tất cả các string có mặt trong binary?  
+ Nếu bạn muốn address of the main function?  
+ Bạn thêm ký tự nào vào cuối mỗi lệnh để có được đầu ra ở định dạng JSON?  
+ How do you get the entrypoint(lối vào) of the file?  
+ What is the secret string hidden in the example2 binary?

Navigating Through Memory

s là lệnh được sử dụng để navigate through the memory of your binary. Với nó và các biến thể của nó, bạn có thể nhận được thông tin về where you are in the binary cũng như di chuyển đến các điểm khác nhau trong binary.  
Note: Đối với các function do user created không phải là main, bạn sẽ phải thêm sym. trước chúng, ví dụ: sym.user\_func

+ How do you print out the the current memory address your located at in the binary?  
+ Bạn sử dụng command nào để đi đến một điểm cụ thể trong memory với cú pháp <command> <address>?  
+ What command would you run to **go 5 bytes forward**?  
+ Còn lùi 12 bytes thì sao?   
+ Làm thế nào để undo tìm kiếm trước đó?   
+ Làm thế nào để go to the memory address of the main function?  
+ Điều gì xảy ra nếu bạn muốn đi đến address of the rax register?

Printing

p là một lệnh hiển thị dữ liệu in a myriad of formats(vô số định dạng). This command rất useful khi bạn muốn get information về những gì đang happening trong memory và get some of the data có trong memory. Với p command, it also useful để know about the @ symbol in radare. The @ symbol được use để chỉ định(specify) that something is an address in memory. Ví dụ: nếu bạn muốn specify bạn đang nói about the memory address of the main function, bạn sẽ sử dụng <command>@main

+ How would you print the hex output of where you currently are in memory?  
+ How would you print the disassembly of where you're currently at in memory?  
+ Điều gì sẽ xảy ra nếu bạn muốn disassembly of the main function?  
+ What command prints out the emoji hexdump(not useful)?  
+ Điều gì sẽ xảy ra nếu bạn quyết định(decide) bạn quá tốt cho các hàng và bạn muốn disassembly ở định dạng cột?  
+ What is the value of the first variable in the main function for the example 3 binary?  
+ What about the second variable?

The Mid-term

Chúc mừng đến điểm này, bây giờ bạn đã biết đủ để vượt qua the mid-term exam. Tất cả questions trong this task sẽ liên quan đến các command đã có trong các previous task vì vậy nếu bạn bỏ qua một, tôi khuyên bạn nên quay lại và thực hiện nó. Như bạn có thể đoán từ tên tệp, tất cả các bài tập trong task này sẽ được thực hiện bằng cách sử dụng tệp the midterm binary.

+ How many functions are in the binary?  
+ What is the value of the hidden string?  
+ What is the return value of secret\_func()?  
+ What is the value of the first variable set in the main function(in decimal format)?  
+ What about the second one(also in decimal format)?  
+ What is the next function in memory after the main function?  
+ How do you get a hexdump of four bytes of the memory address your currently at?

Debugging

Hãy nhớ rằng trong task 'Command Line Options', bạn đã học được rằng –d flag có radare enter debug mode.Debug mode allows you set breakpoints và cung cấp(offers) a lot of options để không chỉ navigate through your binary, mà còn analyze the data đi vào và ra khỏi registers.

+ How do you set a breakpoint?  
+ What command is used to print out the values of all the registers?  
+ Làm thế nào để bạn chạy qua chương trình cho đến khi chương trình kết thúc hoặc bạn nhấn điểm ngắt tiếp theo?  
+ Điều gì xảy ra(what) if you want to step through the binary one line at a time(tại 1 thời điểm)?  
+ How do you go forth 2 lines in the binary?  
+ Làm thế nào để bạn list out các chỉ mục(indexes) và memory address của tất cả các breakpoint?  
+ Go back through all previous binaries và mess around with debug mode

Visual Mode

Mặc dù visual mode(chế độ trực quan) không cần thiết và vốn sẽ không dạy cho bạn bất cứ điều gì mới về binary bạn hiện đang chạy. Nó cho phép assembly để con người dễ đọc hơn và cung cấp more options để tăng cường(enhance) the visual appeal(sự hấp dẫn trực quan) của radare và chắc chắn có thể impprove sự hiệu quả. Vì vậy, tôi sẽ nói rằng đó là một công cụ có giá trị mà bạn nên biết cách sử dụng. Tất cả commands liên quan đến visual mode bắt đầu bằng v

+ Làm thế nào để enter 'graph mode' cái mà cho phép mọi thứ được sắp xếp trong các hộp có thể đọc được tốt đẹp(Also note that the second character is uppercase) ?  
+ What character do you press to run normal radare commands inside visual mode?  
+ How do you go back to the regular(thông thường)radare shell(leaving visual mode)?  
+ What if you want to step through the binary inside Visual mode?  
+ How do you add a comment?  
Nhìn qua bất kỳ nhị phân nào trong chế độ trực quan và xem mọi thứ đẹp hơn trông như thế nào.

Write Mode

Đôi khi bạn có thể kết thúc trong một tình huống, nơi một task là không thể giải quyết với current intructions. Ví dụ: Take this code

int val = 4;

if(val == 5){

printf("%s","You win!");

}

Bạn sẽ không bao giờ có thể có được nó để print out “You win!” Bởi vì trong những trường hợp normal, val sẽ không bao giờ được set bằng 5. Đây là nơi write mode đi kèm, nó cho phép bạn thay đổi instructions để bạn có thể có được một số điều kiện nhất định để execute. All commands liên quan đến write mode bắt đầu bằng w

+ How do you write a string to current memory address?  
+ What command lists all write changes?  
+ What command modifiles an instruction at the current memory address?  
+ Get the example4 binary to show the You win! Message

The Final Exam

Xin chúc mừng bạn đã làm cho nó đến this point. Bây giờ bạn có thể giải quyết một crackme! Sử dụng tất cả các công cụ bạn đã học và get that password! Binary để sử dụng cho task này là the\_final\_exam!