**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

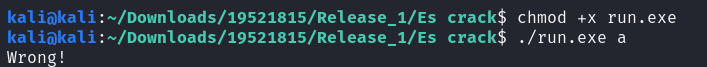
**RE CHALLENGES: ES CRACK**

|  |  |  |  |
| --- | --- | --- | --- |
| **Giảng viên hướng dẫn** | **Phạm Văn Hậu** | | **ĐIỂM** |
| **Sinh viên thực hiện 1** | **Trần Đức Lương** | **19521815** |  |

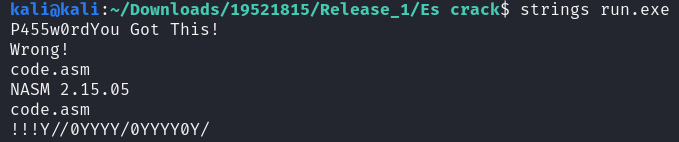
Đây là file ELF 32bit chạy trên nền Linux.

https://raw.githubusercontent.com/ducluongtran9121/RE-WriteUp/main/19521815/Release_1/Es%20crack/file.png?token=AOZ4VHK4QNAEPGBMVMDDNKDAUOGGK

Thực hiện cấp quyền và chạy chương trình trên terminal ./run.exe với tham số đầu vào là “a” thì chương trình trả về kết quả “Wrong!”. Ý tưởng của bài này chắc cũng chỉ là nhập một chuỗi và check xem chuỗi đó có giống với flag hay chuỗi chương trình đã cho để trả về kết quả tương ứng.



Chạy câu lệnh strings run.exe để tìm ra tất cả các strings có trong file run.exe. Nhìn nhanh qua có thể thấy một chuỗi khá đáng nghi “P455w0rd”, đây có thể chính là tham số cần nhập vào để pass chương trình này.



Thực thi chương trình với tham số là “P455w0rd” thì thấy chương trình trả về kết quả là “You Got This!” , tức là chuỗi trên chính là flag cần tìm.

