CTF Episode 5: Hide your ass

Câu chuyện hôm nay sẽ bắt đầu bằng trò chơi trốn tìm phiên bản số, trò chơi như sau: Mỗi người trong các bạn sẽ nhận được một chuỗi kí tự bí mật, các bạn được giao cho một thế giới giả lập có thể tạo ra và sử dụng bất cứ thứ gì để giấu chuỗi đó đi , nhiệm vụ của đối phương là tìm ra chuỗi bí mật đó bằng cách đi vào thế giới gỉa lập của các bạn . Trong trò chơi này cả người giấu và người đi tìm sẽ bị giới hạn về mặt thời gian và tài nguyên, từ đó ràng buộc họ phải chọn ra một chiến lược phù hợp nhất để đảm bảo tính hiệu quả và chiến thắng của bản thân.
Liệu có bao nhiêu chiến lược có thể thực hiện trong trò chơi này?
Trước hết, để tìm đạt được mục tiêu (tìm ra chuỗi bí mật của đối phương) sẽ có 2 giai đoạn:
Giai đoạn 1, xác định vị trí của chuỗi bí mật kia.
Giai đoạn 2, vào thế giới giả lập của đối phương để tới địa điểm đã xác định và lấy chuỗi bí mật.
Đồng nghĩa với điều đó, người giấu cũng cần vạch ra cho mình một chiến lược phù hợp bao gồm:

1. Tập trung vào sự phức tạp của thế giới giả lập để tung hoả mù kẻ đi tìm: ví dụ như các bạn có thể xây dựng 1 toà tháp rồi clone ra thành hàng ngàn cái như vậy, giấu chuỗi vào 1 trong những toà tháp đó nhằm khiến cho đối phương sẽ rối trí và mất phương hướng khi lọt vào thế giới của bạn.

2. Tập trung vào sự phức tạp của việc đi đến nơi lấy chuỗi bằng cách tạo ra các chướng ngại vật phức tạp nhằm ngăn cản bước tiến của đối phương, hòng khiến họ bỏ cuộc vì quá khó khăn hoặc không đủ thời gian để vượt qua: ví dụ đặt những trạm gác có sử dụng quái vật bắt buộc đối phương phải đánh bại trước khi vượt qua.

3. Dĩ nhiên luôn có phương án trộn lẫn giữa 2 thứ trên.

Nhưng luôn nhớ rằng trò chơi này bắt buộc người giấu phải chứng minh được người tìm có khả năng chiến thắng, đó sẽ là điều ràng buộc căn bản nhất để trò chơi được thực thi.

Chúng ta sẽ chơi trò này với chương trình chat của các bạn ở bài tập trước, hãy kiếm cách giấu một lỗi buffer overflow ví dụ ở phần trước vào chương trình đó bằng cách đọc nội dung của người chat và thực hiện những yêu cầu dưới đây:

1. Tạo ra một menu với nhiều sự lựa chọn để đối phương có thể chọn và giấu lỗi vào 1 trong những sự lựa chọn đó.

2. Tạo ra một menu với ít sự lựa chọn, tuy nhiên với mỗi sự lựa chọn lại dẫn tới một menu khác.

3. Tạo ra thêm 1 vai trò của người quản trị song song với vai trò của người chơi, tạo ra một lỗi off-by-one để giúp người chơi lấy quyền người quản trị và giấu lỗi buffer overflow vào trong role của người quản trị.

4. Tạo ra một chương trình cho nhiều người song song cùng chat với nhau trong một room chat sử dụng thread, tạo ra một vùng nhớ sử dụng chung giữa các thread để chứa chuỗi do người chơi gửi vào.

5. Tự nghĩ ra một cách khác để giấu lỗi vào dựa trên những ý tưởng trên.

Complile 5 chương trình của các bạn và gửi lại cho mình, mình sẽ giao cho các bạn binary đã compile của một bạn khác, nếu các bạn tìm ra lời lỗi trong binary đó thì coi như hoàn thành Episode 5.

Episode 6: Let your hand dirty.

Bài tập bên lề, để chuẩn bị cho Episode 9, các bạn hãy học cách sử dụng Google Scraper (https://github.com/NikolaiT/GoogleScraper) viết một script chạy song song download từ Internet về khoảng 100000 file pdf đặt tên chúng dưới dạng $(md5_file).pdf đồng thời lưu vào một database khác tên file và URL tới file đó.