**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

Logo

Description automatically generated  
  
  
 **Tìm hiểu bài thực hành: ptit-code-analysis**

Sử dụng công cụ IDA để dịch mã nguồn

**Giảng viên:** Đinh Trường Duy

**Môn học:** Kiểm thử xâm nhập

**Thành viên:**

|  |  |
| --- | --- |
| Lường Thế Vinh | – B20DCAT201 |
| Nguyễn Hoài Ngọc | – B20DCAT133 |
| Nguyễn Quốc Quân | – B20DCAT149 |
| Doãn Hà Ly | – B20DCAT117 |
| Nguyễn Thị Yên | – B20DCAT205 |

**Nội dung và hướng dẫn bài thực hành**

* 1. ***Mục đích***
     + Giúp sinh viên tìm hiểu về việc sử dụng phần mềm IDA để phân tích ngược một chương trình mẫu có tên là ***shell.exe***.
     + Sau khi hoàn thành bài thực hành, sinh viên sẽ có thấy được những khó khăn khi phân tích ngược chương trình về mã nguồn gốc
  2. ***Yêu cầu đối với sinh viên***
     + Có kiến thức cơ bản về ngôn ngữ lập trình Assembly.
     + Biết và sử dụng phần mềm IDA.
  3. ***Nội dung thực hành***
     + Khởi động bài lab: Vào terminal trong thư mục labtainer-student, gõ:

*labtainer ptit-code-analysis*

* + - Có thể thực hiện lại bài thực hành bằng lệnh:

*labtainer –r ptit-code-analysis*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong một terminal ảo sẽ xuất hiện, và là đại diện cho máy chứa phần mềm IDA. Ở thư mục "home" có chứa file cài đặt của IDA và, hãy chạy để cài đặt chương trình

*./idafree70\_linux.run*

Sinh viên sử dụng IDA để xem xét chương trình có tên "shell.exe" ở thư mục "home".

Các nhiệm vụ cần phải thực hiện:

Để kiểm tra kết quả, sinh viên cần lưu file phân tích này dưới dạng html <.html> và thực hiện grep kết quả từ file này.

* Nhiệm vụ 1: Xác định hàm kiểm tra sandbox

🡪 Để hoàn thành nhiệm vụ này sinh viên cần phải thực hiện tìm kiếm và chuyển đổi qua các hàm trong IDA để tìm ra hàm này.

*Sau khi hoàn thành nhiệm vụ này sinh viên kiểm tra kết quả tại mục sandbox trong checkwork.*

* Nhiệm vụ 2: Kiểm tra kết nối mạng: xác định địa chỉ IP, cổng kết nối.

🡪 Để hoàn thành nhiệm vụ này sinh viên cần phải thực hiện tìm kiếm và chuyển đổi qua các hàm trong IDA để tìm ra hàm này

Để kiểm tra kết quả, sinh viên cần lưu file phân tích này dưới dạng html <.html> và thực hiện grep kết quả từ file này.

*Sau khi hoàn thành nhiệm vụ này sinh viên kiểm tra kết quả tại mục IP, socket trong checkwork.*

* Nhiệm vụ 3: Xác định URL đáng nghi thực hiện tải file

🡪 Để hoàn thành nhiệm vụ này sinh viên cần phải thực hiện tìm kiếm và chuyển đổi qua các hàm trong IDA để tìm ra hàm này

Để kiểm tra kết quả, sinh viên cần lưu file phân tích này dưới dạng html <.html> và thực hiện grep kết quả từ file này.

*Sau khi hoàn thành nhiệm vụ này sinh viên kiểm tra kết quả tại mục url trong checkwork.*

* Nhiệm vụ 4: Nhận dạng hàm main trong IDA.

🡪 Để hoàn thành nhiệm vụ này sinh viên cần phải thực hiện tìm ra hàm đầu tiên chứa các hàm quan trọng để chương trình này có thể hoạt động.

Để kiểm tra kết quả, sinh viên cần lưu file phân tích này dưới dạng html <.html> và thực hiện grep kết quả từ file này.

*Sau khi hoàn thành nhiệm vụ này sinh viên kiểm tra kết quả tại mục main trong checkwork.*

* + - Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab ptit-code-analysis*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Kiểm tra các bài tập phải làm trong bài thực hành:

*Checkwork*