BÁO CÁO BÀI TẬP

**Môn học: Cơ chế hoạt động của mã độc**

**Kỳ báo cáo: Buổi 05 (Session 05)**

**Tên chủ đề: DLL Injection**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 25/5/2023*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Kịch bản 01 | 100% |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
|  |  |  |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Kịch bản 01

Link video: <https://youtu.be/A7l9G-Bvt3M>

Giải thích code source:

Bước 1: Ở phần code Source thì ta thấy được là đầu tiên thực hiện get các thông tin về các tiến trình

A picture containing text, screenshot, software

Description automatically generated

Bước 2: Sau đó thực hiện đọc và thao tác trên bộ nhớ

A screen shot of a computer code

Description automatically generated with low confidence

Bước 3: tác động đến các giá trị biến từ đó có thể thay đổi được các giá trị biến trong trò chơi

A picture containing text, screenshot, font

Description automatically generated

Giải thích code Injector:

Bước 1: Tương tự như source, injector cũng thực hiện một số thao tác get các thông tin về tiến trình

A screen shot of a computer code

Description automatically generated with low confidence

Bước 2: thực hiện đọc và thao tác trên bộ nhớ

A screen shot of a computer program

Description automatically generated with low confidence

Bước 3: chương trình sẽ tạo ra các thread để thực hiện việc hỗ trợ truyền các DLL độc hại vào trong chương trình trò chơi

A computer code on a black background

Description automatically generated with low confidence

Như vậy để có thể thực hiện được việc nhấn F6 tăng điểm, ta sẽ thực hiện chỉnh sửa DLL

Đầu tiên ta sẽ sử dụng code source bỏ vào DLL

A picture containing text, screenshot, software, display

Description automatically generated

Thực hiện một số chỉnh sửa, thực hiện đổi tên hàm

A picture containing text, screenshot, software, font

Description automatically generated

Ngoài ra ta sẽ chuyển đổi phần nhập liệu thành lấy giá trị hiện tại cộng thêm 100

A picture containing text, screenshot, font

Description automatically generated

Thêm việc thực hiện hàm khi nhấn F6

A picture containing text, screenshot, font

Description automatically generated

Sau đó ta sẽ thực thi chạy trò chơi

A screenshot of a video game

Description automatically generated

Thực hiện chạy file Injector

A screenshot of a computer

Description automatically generated

Quay lại trò chơi nhấn F6 và lúc này ta nhận được thông báo nhấn F6

A screenshot of a computer

Description automatically generated

Cuối cùng ta thấy thức ăn tăng lên 100 thành 300 so với 200 ban đầu đã có sự thay đổi

A screenshot of a video game

Description automatically generated

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)