BÁO CÁO BÀI TẬP

**Môn học: CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC**

**Tên chủ đề: File Infecting Virus**

*GVHD: Phan Thế Duy*

1. **THÔNG TIN CHUNG:**

Lớp: NT230.M21.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Bảo Hà | 19520067 | 19520067@gm.uit.edu.vn |
| 2 | Lê Thị Hương Giang | 19520499 | [19520499@gm.uit.edu.vn](mailto:19520499@gm.uit.edu.vn) |
| 3 | Nguyễn Thị Hải Hà | 19520506 | 19520506@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Áp dụng kỹ thuật chèn cuối (Appending Virus) hoặc sử dụng trường section .reloc trong tập tin thực thi để tiêm payload của virus | 100% |
| 2 | Áp dụng 02 chiến lược lây nhiễm trong nhóm kỹ thuật Entry-Point Obscuring (EPO) virus – che giấu điểm vào thực thi của mã virus (virus code). Ví dụ: call hijacking EPO virus, và Import Address Tablereplacing EPO virus | 100% |

BÁO CÁO CHI TIẾT

Mức yêu cầu 01 - RQ01 (6đ): Áp dụng kỹ thuật chèn cuối (Appending Virus) hoặc sử dụng trường section .reloc trong tập tin thực thi để tiêm payload của virus.

**Chuẩn bị shellcode bằng tool msfvenom**

**Text

Description automatically generated**

**Để chương trình sau khi chèn virus, ta cần phải thay đổi hướng thực thi của virus. Ban đầu, chương trình virus sẽ đóng sau khi thực thi xong, để có thể khởi động chương trình ban đầu ta sẽ thay đổi 6 byte cuối cùng trong đoạn shellcode.**

**Để tính toán địa chỉ trả về, ta cần phải biết những thông số Original EntryPoint và Image Base**

**Graphical user interface, application

Description automatically generated with medium confidence**

**Sau khi có được các thông số trên, ta tính Return Address = Original EntryPoint + Image Base = 0x739D + 0x1000000 = 0x100739D.**

**Text

Description automatically generated**

**Sử dụng tool** [**defuse.ca**](https://defuse.ca/online-x86-assembler.htm#disassembly) **để đổi mã code asembly thành chuỗi hex**

**Graphical user interface, text, application, email

Description automatically generated**

**Sau đó thay đổi 6 bytes cuối trong shellcode thành chuỗi hex \xB8\x9D\x73\x00\x01\xFF\xD0**

**Text

Description automatically generated**

**Sau khi chuẩn bị shellcode, ta sẽ chèn đoạn shellcode vào chương trình như sau**

**Text

Description automatically generated**

Mức yêu cầu 02 - RQ02 (4đ): Áp dụng 02 chiến lược lây nhiễm trong nhóm kỹ thuật Entry-Point Obscuring (EPO) virus – che giấu điểm vào thực thi của mã virus (virus code). Ví dụ: call hijacking EPO virus, và Import Address Tablereplacing EPO virus

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 .DOCX và .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]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* 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 bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*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)