BÁO CÁO BÀI TẬP

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

**Kỳ báo cáo: Buổi 04 (Session 04)**

**Tên chủ đề:**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 08/05/2023*

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/Câu hỏi 01 | 100% |  |
| 2 | Kịch bản 02 | 100% |  |
| 3 | Kịch bản 03 | 100% |  |
| 4 | Kịch bản 04 | 100% |  |
|  |  |  |  |

**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

## Kịch bản 02

Câu trả lời là có vì chương trình được cài đặt dưới dạng module kernel (có thể chạy ở phân quyền nhân – kernel priviledge level) từ đó có thể mở được các port TCP dùng để backdoor. Qua thao tác trên có thể cấp quyền truy cập cho kẻ tấn công từ xa thông qua bind shell hoặc reverse shell

## Kịch bản 03

Ngoài ra thay vì add trên thiết bị ta có thể add trên master boot loader giúp cho việc có thể chạy trước khi bật hệ điều hành. Ngoài ra có thể thực hiện chiếm quyền kiểm soát hệ thống sau đó tạo bind shell và cấu hình nó như việc 1 chương trình chạy nền, từ đó rootkits có thể che giấy thông tin bind shell.

## Kịch bản 04

1. Nếu chương trình muốn sử dụng các certain routines trong kernel thì nó phải gọi API kallsyms\_\*() và gọi tên symbol để lấy các con trỏ của hàm đó. Vì vậy để thực hiện điều trên thì nó cần phải có con trỏ hàm
2. Để thực hiện quá trình che giấu, chúng ta cần đến việc khả năng đọc ghi và thực hiện, nhưng khi làm việc này vấn đề phát sinh là kernel sẽ không cho phép ta thực hiện bằng cách kernel sẽ thực hiện read only ở kernel mode. Như vậy sẽ có 1 exception được thành lập nếu như cố sửa.

Vậy để vượt qua việc chặn này (page protection) của kernel ta sẽ thực hiện

Bước 1 tắt tính năng chống ghi

Bước 2 ghi đè

Bước 3 bật tính năng chống ghi

Trong ngữ cảnh này bit chống ghi có trong cr0

Do đó ta cần thực hiện các thao tác trên để thực hiện ghi đè hàm

## Kịch bản 05

Thay vì add trên thiết bị ta có thể add trên master boot loader giúp cho việc có thể chạy trước khi bật hệ điều hành. Ngoài ra có thể thực hiện chiếm quyền kiểm soát hệ thống sau đó tạo bind shell và cấu hình nó như việc 1 chương trình chạy nền, từ đó rootkits có thể che giấy thông tin bind shell.

## Kịch bản 06

---

***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)