BÁO CÁO BÀI TẬP

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

**Tên chủ đề: Hijacking Execution Techniques**

*GVHD: Nguyễn Công Danh*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT230.O22.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Nguyên Phúc | 21522469 | 21522469@gm.uit.edu.vn |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Bùi Hoàng Trúc Anh | 21521817 | 21521817@gm.uit.edu.vn |
| 4 | Nguyễn Ngọc Trà My | 21520353 | 21520353@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 1 | 100% |
| 2 | Yêu cầu 2 | 100% |
| 3 | Yêu cầu 3 | 100% |

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

BÁO CÁO CHI TIẾT

1. **Yêu cầu 1: Hiểu và mô tả rõ ràng về mặt lý thuyết kỹ thuật được chọn.**

**DLL hijacking**

Định nghĩa:

* DLL hijacking là một kỹ thuật tấn công mà tin tặc sử dụng để thực thi mã độc hại bằng cách lợi dụng việc tải DLL không an toàn hoặc không được bảo vệ bởi một ứng dụng chính thức. Trong trường hợp này, ta sẽ sử dụng ProcMon để xác định các tập tin DLL bị thiếu được tải bởi một chương trình hợp lệ trên hệ thống Windows.
* Để nâng cao đặc quyền, cơ hội tốt nhất mà chúng ta có là có thể viết một dll mà quy trình đặc quyền sẽ cố tải ở một số nơi mà nó sẽ được tìm kiếm. Do đó, chúng tôi sẽ có thể ghi một dll vào một thư mục nơi dll được tìm kiếm trước thư mục chứa dll gốc (trường hợp lạ) hoặc chúng tôi sẽ có thể ghi vào một số thư mục nơi dll sẽ được tìm kiếm và dll gốc không tồn tại trên bất kỳ thư mục nào.
* Trong bài này, ta sẽ sử dụng DLL Hijacking để thực thi các lệnh độc hại bằng cách trước tiên xác định các tệp DLL thiếu được tải bởi một chương trình hợp lệ trên hệ thống Windows. Việc này có thể được thực hiện với sự trợ giúp của một ứng dụng chính thức của Microsoft là Process Monitor (ProcMon).

Phương pháp thực hiện:

1. Chọn ứng dụng phù hợp: Lựa chọn một ứng dụng có thể bị ảnh hưởng bởi DLL hijacking. Điều này thường là các ứng dụng chính thống được cài đặt trên hệ thống, như trình cài đặt phần mềm, trình giải nén tệp, hoặc các ứng dụng có chức năng tương tự.
2. Xác định DLL cần tải: Tìm hiểu về các DLL mà ứng dụng cần tải để hoạt động. Điều này có thể được thực hiện bằng cách sử dụng các công cụ như Process Monitor (ProcMon) hoặc Dependency Walker.
3. Chọn vị trí chứa DLL độc hại: Lựa chọn một vị trí mà ứng dụng sẽ tìm kiếm DLL để tải vào bộ nhớ. Điều này có thể là thư mục hiện tại của ứng dụng, thư mục hệ thống, hoặc các thư mục khác được chỉ định trong biến môi trường.
4. Tạo DLL độc hại: Tạo một DLL độc hại có cùng tên với DLL mà ứng dụng cần tải. DLL độc hại này có thể chứa mã độc hại để thực thi các hành động không mong muốn hoặc lợi dụng quyền truy cập của ứng dụng.
5. Đặt DLL độc hại vào vị trí chọn lựa: Đặt DLL độc hại vào vị trí đã chọn trước đó, sao cho khi ứng dụng cố gắng tải DLL, nó sẽ tải DLL độc hại thay vì DLL chính thức.
6. Kích hoạt ứng dụng: Chạy ứng dụng để kích hoạt quá trình tải DLL. Khi ứng dụng cố gắng tải DLL, nó sẽ tải và thực thi DLL độc hại.
7. Kiểm tra kết quả: Kiểm tra xem liệu DLL độc hại đã được thực thi thành công và có thực hiện các hành động không mong muốn không.

**DLL Proxying**

DLL proxying là một kỹ thuật để thực hiện mã độc hại một cách ngầm và không gây ra sự cố cho ứng dụng bằng cách chuyển tiếp đến thư viện thực sự.

1. **Yêu cầu 2 & 3: Vận dụng lý thuyết để lập trình mã độc và xây dựng lab đơn giản trên máy ảo Windows 10/11 (Tắt Windows Defender). Chức năng của mã độc: Mở một tiến trình có sẵn trên máy.**

**Môi trường thực nghiệm:**

Máy Kali 2023.3 64 bit có IP là 192.168.30.132

Máy Windows 10 64bit có IP là 192.168.30.137

**Kịch bản thực hiện:**

Tải package mingw-w64 để tạo dll độc hại.

A screenshot of a computer program

Description automatically generated

Đoạn mã dưới là về hàm DllMain trong một DLL trên Windows. Khi DLL được tải vào một quá trình, nó thực thi hai hành động: ghi đầu ra của lệnh whoami vào tệp tin và mở chương trình Calculator.

A screen shot of a computer

Description automatically generated

Lệnh x86\_64-w64-mingw32-g++ -shared --static -o helloworld.dll template.cpp được sử dụng để biên dịch tệp nguồn C++ template.cpp thành một DLL có tên là helloworld.dll bằng trình biên dịch MinGW-W64. Điều này sẽ tạo ra một DLL có thể sử dụng trong các ứng dụng Windows.

A screenshot of a computer screen

Description automatically generated

Thực hiện chạy dịch vụ web để cho nạn nhân có thể tải tập tin reverse shell về máy

A screenshot of a computer

Description automatically generated

Trên máy nạn nhân, mở web browser và truy cập vào đường dẫn <http://192.168.30.132/helloworld.dll> để tải tập tin về máy

A computer screen with white text

Description automatically generated

Lệnh rundll32.exe helloworld.dll, DllMain được sử dụng để gọi hàm DllMain trong DLL có tên là helloworld.dll bằng cách sử dụng tiện ích rundll32.exe trên Windows.

A computer screen with white text

Description automatically generated

Sau khi chạy helloworld.dll, ta thấy file calc.exe được chạy và có file whoami.txt có ghi thông tin của user trong thư mục đã được chỉ định.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Khởi động ProcMon và cấu hình nó để theo dõi sự kiện liên quan đến chương trình mục tiêu. Lọc các sự kiện để tìm kiếm bất kỳ tệp DLL nào được chương trình yêu cầu mà không được tìm thấy.

A screenshot of a computer

Description automatically generated

Ta khởi chạy ứng dụng BurpSuite Community trên Windows thì ta thấy có những file DLL không được tìm thấy như hình dưới:

A screen shot of a computer

Description automatically generated

Ta kiểm tra quyền của thư mục chứa những file DLL đó và ta thấy user admin có đủ quyền.

A computer screen with white text

Description automatically generated

Ta di chuyển file DLL độc hại vào những đường dẫn mà DLL không được tìm thấy. Qua những lần thử nghiệm thì ta thấy khi di chuyển file DLL vào đường dẫn “C:\Users\admin\AppData\Local\BurpSuiteCommunity\USERENV.dll” thì ứng dụng chạy bình thường và file mã độc cũng được thực thi.

A black background with many lines

Description automatically generated with medium confidence

Đây là kết quả sau khi di chuyển file độc hại vào đường dẫn. Ta khởi chạy BurpSuite và ta thấy file calc.exe cũng được khởi chạy và tên của user hiện tại cũng được lưu vô file whoami.txt trong đường dẫn chỉ định.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

---

**HẾT**

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