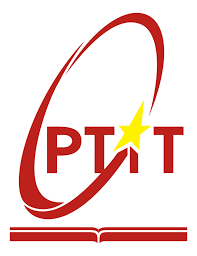
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN II**

 ----

**Tiểu luận môn học: Phân tích và xác định mẫu dữ liệu tấn công**

**Bộ môn** :ANM

**Giảng viên** :Nguyễn Hồng Sơn **Sinh viên :** Trần Quang Linh  **MSSV** : N18DCAT040

**TPHCM 02/2022**

**THÔNG TIN SINH VIÊN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | HỌ | TÊN | MSSV | LỚP |
| 1 | **Trần Quang** | **Linh** | **N18DCAT040** | **D18CQAT02-N** |

# LỜI CẢM ƠN

Để hoàn thành bài lab thực hành này trước hết em xin gửi đến quý thầy,cô giáo trong khoa công nghệ thông tin trường Học Viện Công Nghệ Bưu Chính Viễn Thông lời cảm ơn chân thành.

Đặc biệt, em xin gởi đến thầy Nguyễn Hồng Sơn , người đã tận tình hướng dẫn, giúp đỡ em hoàn thành bài này lời cảm ơn sâu sắc nhất.

**Xin chân thành cảm ơn.**  **TPHCM, 14/10/2022**

Trần Quang Linh

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

**Giảng viên hướng dẫn**

*(Ký và ghi rõ họ tên)*

MỤC LỤC

[LỜI CẢM ƠN ii](#_Toc120138361)

[1.1 Thông tin về lỗ hổng cve 2017-0199 v](#_Toc120138362)

[1.1.1 Thông tin chi tiết v](#_Toc120138363)

[1.1.2 Kịch bản v](#_Toc120138364)

[1.2 Cài đặt thử nghiệm vi](#_Toc120138365)

[1.2.1 Phân tích dấu hiệu của quá trình tấn công ix](#_Toc120138366)

[1.3 Viết tool sử dụng scapy,wireshark phát hiện quá trình tấn công của cve 2020-0199 xii](#_Toc120138367)

[1.3.1 Import module vào chương trình xii](#_Toc120138368)

[1.3.2 Sử dụng windump xii](#_Toc120138369)

[1.3.3 Phân tích file pcap đưa ra file xiii](#_Toc120138370)

[1.3.4 Phân tích và đưa ra màn hình thông điệp xiv](#_Toc120138371)

## Thông tin về lỗ hổng cve 2017-0199

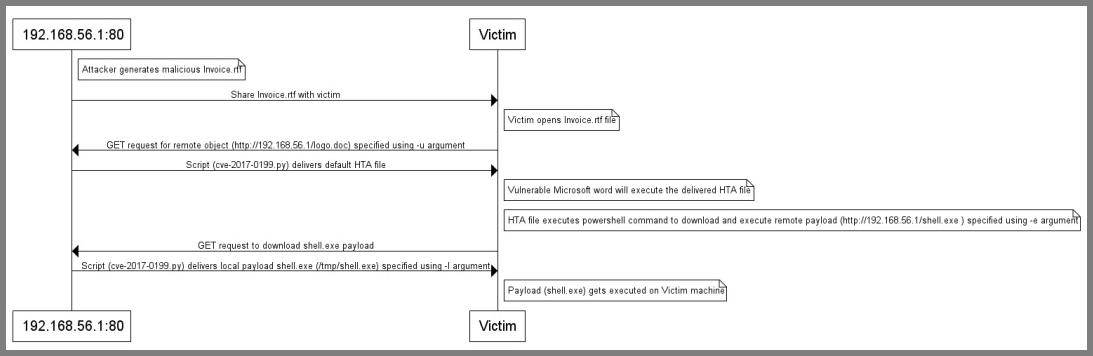
### Thông tin chi tiết

Một lỗ hổng thực thi mã từ xa tồn tại trong cách Microsoft Office và WordPad phân tích cú pháp các tệp được chế tạo đặc biệt. Kẻ tấn công khai thác thành công lỗ hổng này có thể chiếm quyền kiểm soát hệ thống bị ảnh hưởng. Kẻ tấn công sau đó có thể cài đặt các chương trình; xem, thay đổi hoặc xóa dữ liệu; hoặc tạo tài khoản mới với đầy đủ quyền của người dùng.

Việc khai thác lỗ hổng này yêu cầu người dùng phải mở hoặc xem trước tệp được chế tạo đặc biệt với phiên bản Microsoft Office hoặc WordPad bị ảnh hưởng. Trong một tình huống tấn công email, kẻ tấn công có thể khai thác lỗ hổng bằng cách gửi một tệp được chế tạo đặc biệt cho người dùng và sau đó thuyết phục người dùng mở tệp.

Bản cập nhật giải quyết lỗ hổng bảo mật bằng cách sửa cách Microsoft Office và WordPad phân tích cú pháp các tệp được chế tạo đặc biệt và bằng cách bật chức năng API trong Windows mà Microsoft Office và WordPad sẽ tận dụng để giải quyết sự cố đã xác định.

### Kịch bản



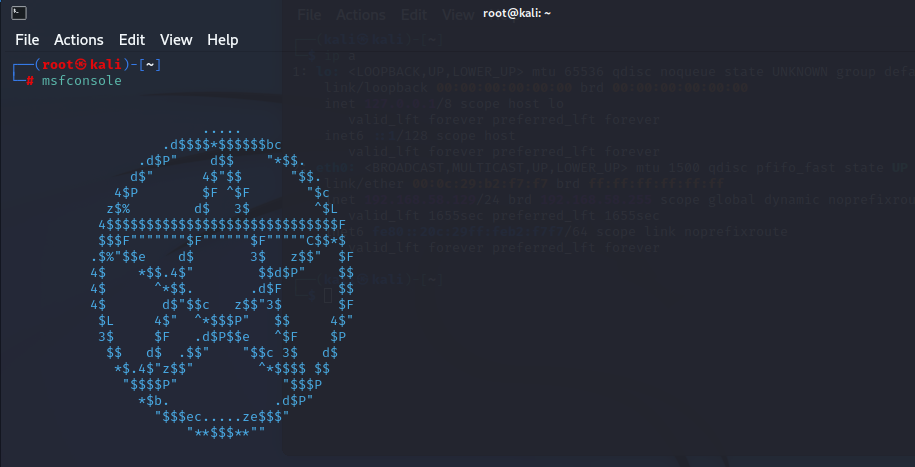
Giải thích sơ đồ :

## Cài đặt thử nghiệm

|  |  |
| --- | --- |
| Tên máy | Địa chỉ ip |
| Kali (ubuntu 20.04) | 192.168.58.129 |
| User (win10) | 192.168.58.1 |

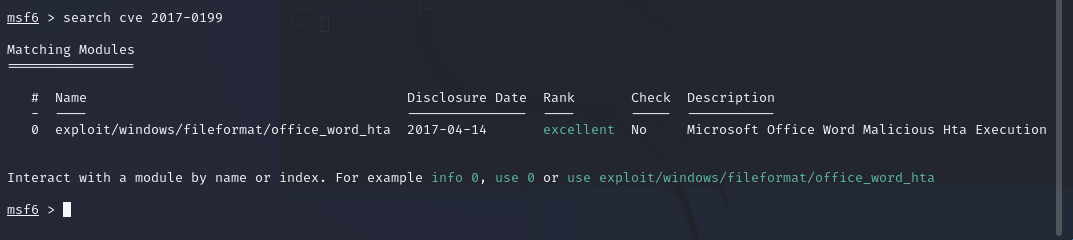
Bước 1: mở msfconsole bằng lệnh

Msfconsole trên máy kali

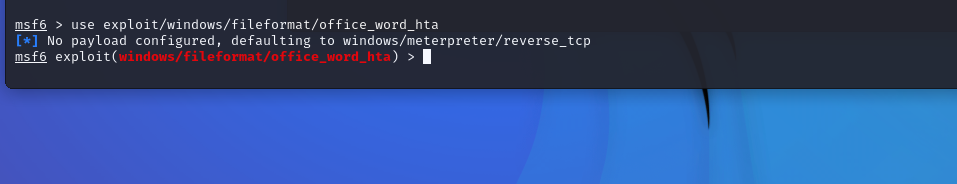


Bước 2: tìm cve bằng lệnh

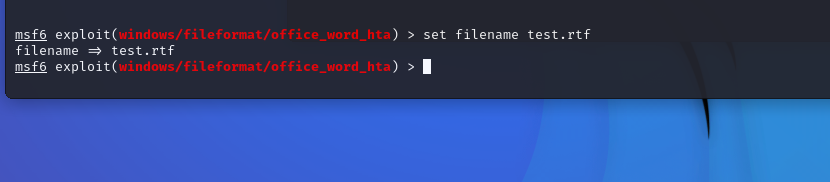
Search cve 2017-0199



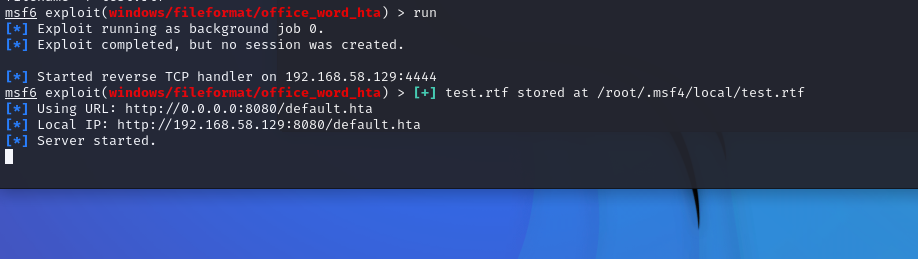
Bước 3: sử dụng cve này



Bước 4: tạo file test.rtf



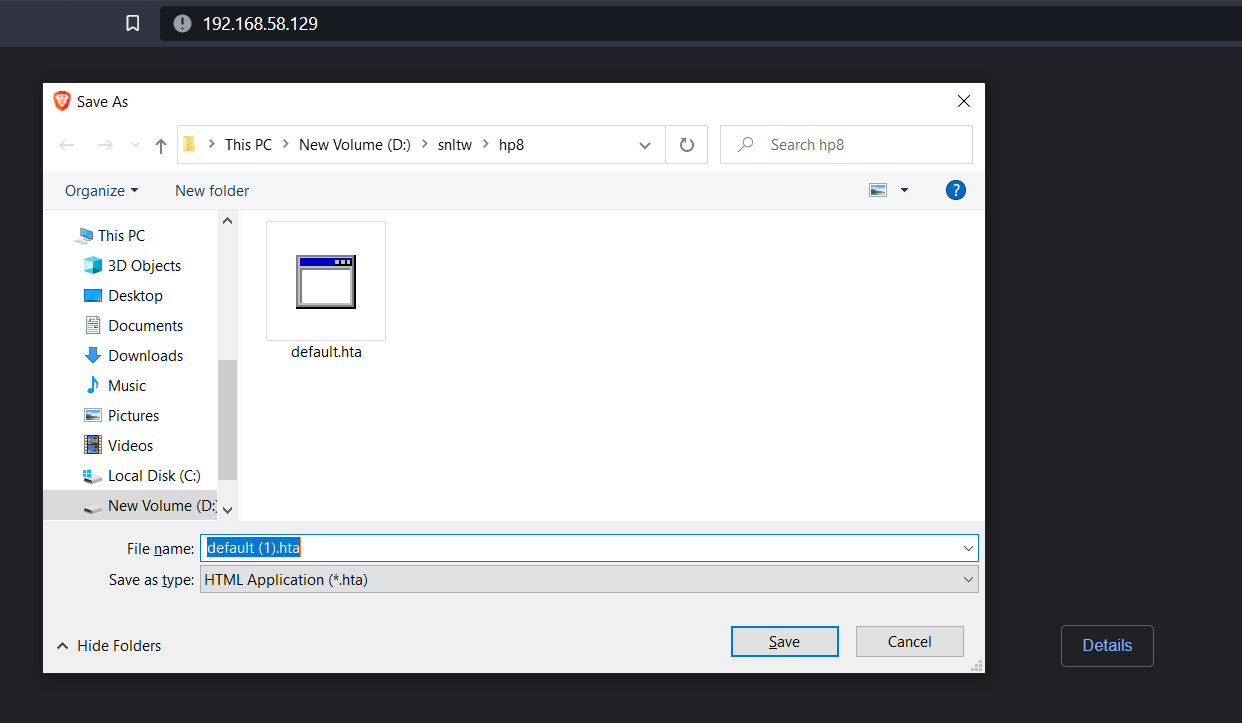
Bước 5: run



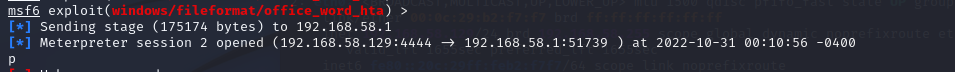
Bước 6: truy cập vào server để tải file đã tạo từ máy victim

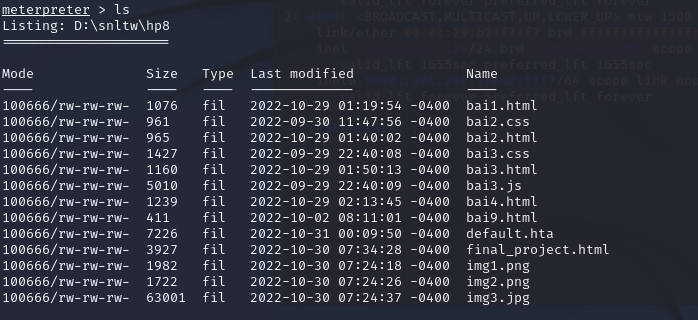
Máy chủ trả về tệp template.doc dưới dạng nội dung ứng dụng / hta mà Word sẽ xử lý như vậy, không phải dưới dạng

Tệp RTF, nhưng dưới dạng tệp HTA.



Bước 7: kết quả với cve này ta đã chiếm quyền được vào hệ thống





### Phân tích dấu hiệu của quá trình tấn công

Đứng từ phía máy client (window 10): 192.168.58.1

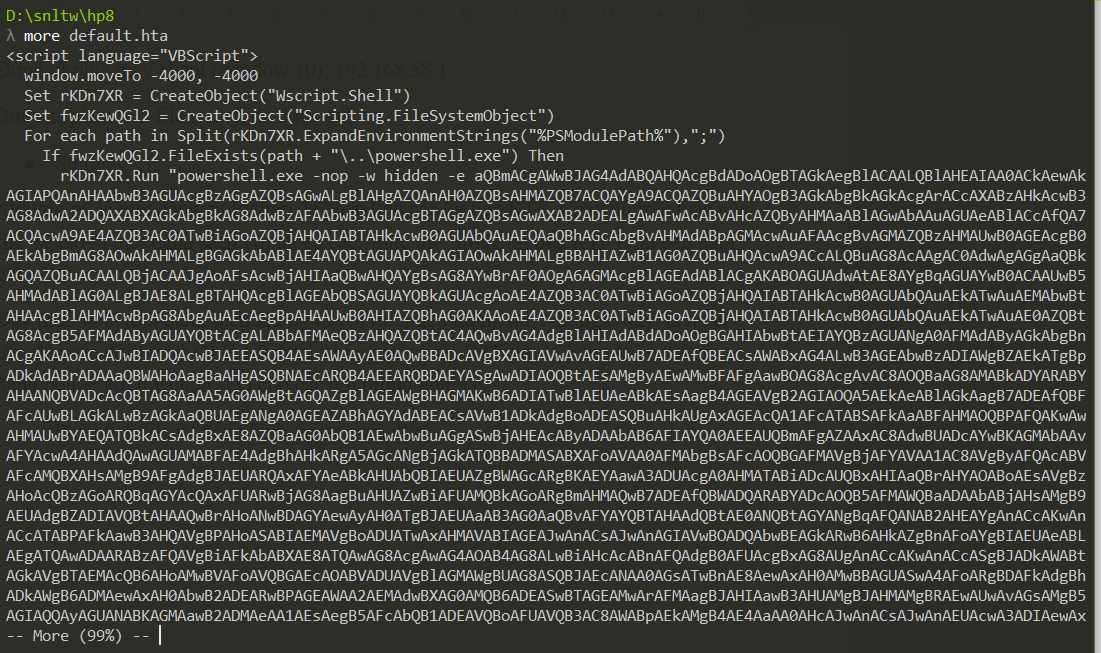
Bước 1: phân tích file test.rft đã được gửi

* Sử dụng rft

rtfdump.py là một công cụ Python để phân tích các tài liệu RTF. Chạy nó trên mẫu của file sẽ tạo ra một danh sách với tất cả các "thực thể" trong tài liệu RTF (văn bản nằm giữa {}):

Đây thường là một danh sách khổng lồ với rất nhiều thông tin. Nhưng ở đây, ta quan tâm đến các đối tượng OLE 1.0 được nhúng trong tệp RTF này. Chúng ta có thể sử dụng bộ lọc với tùy chọn -f O cho các đối tượng như vậy:

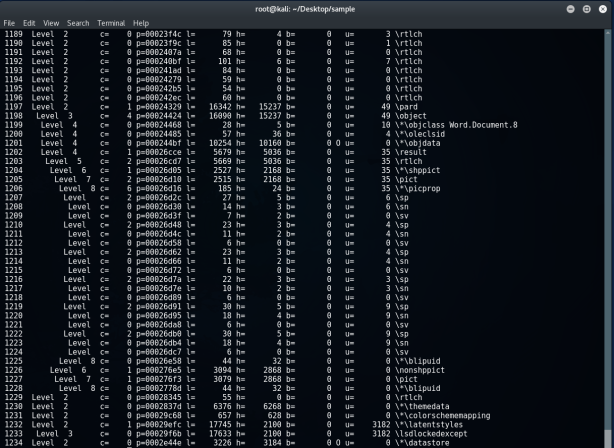
* Phân tích file rtf bằng lệnh :more nameflie



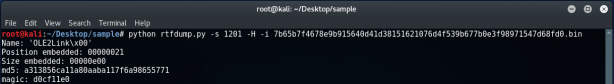
=>Đối tượng này chứa một URL trỏ đến thành phần tiếp theo, trình tải xuống HTA.

Trong một số trường hợp, liên kết ban đầu được chèn dưới dạng tệp bên ngoài được nhúng vào tiêu đề của tài liệu:

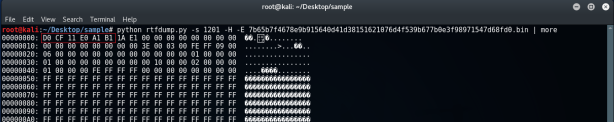
Sử dụng rtfdump, sau khi parse file, công cụ phát hiện có object data được nhúng tại vị trí 1201:



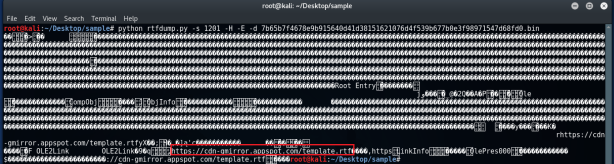
Tiếp tục dùng rtfdump, lựa chọn vị trí 1201 để dump, thêm tùy chọn –H để decode và xem dưới dạng hexa, -i để in ra các thông tin liên quan tới object tại vị trí được lựa chọn:



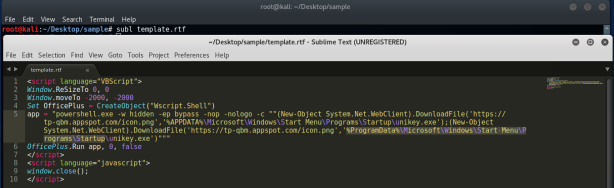
Theo thông tin thì object được nhúng có định dạng là OLE file:



Sử dụng tùy chọn –d để dump, ta có được thông tin:

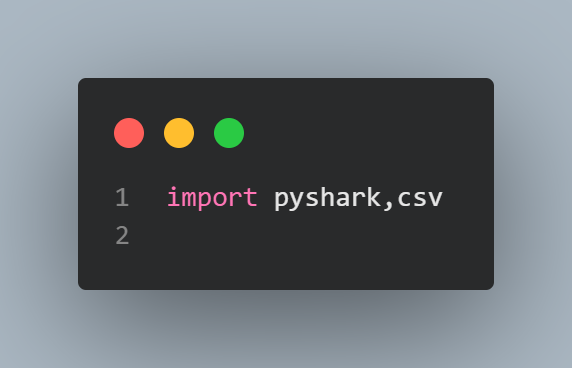


Mở file bằng một trình Text Editor, thấy đây là một VBScript, thực hiện việc gọi powershell để download file tại hxxps://tp-qbm.appspot.com/icon.png và lưu với tên là unikey.exe tại hai thư mục là “%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup” và “%ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup”:

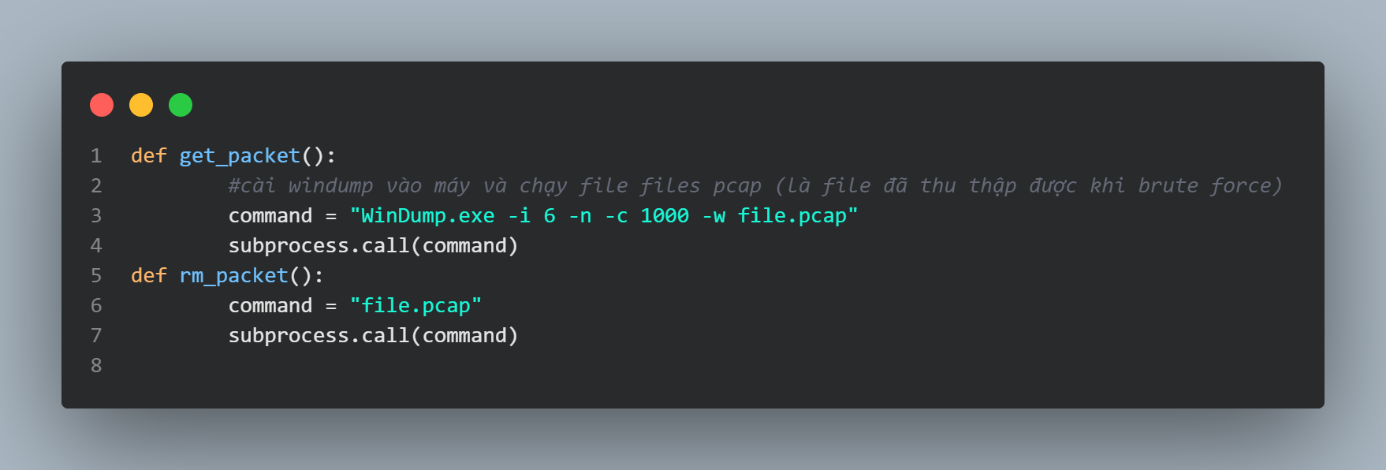


## Viết tool sử dụng scapy,wireshark phát hiện quá trình tấn công của cve 2020-0199

### Import module vào chương trình



### Sử dụng windump



### Phân tích file pcap đưa ra file



### Phân tích và đưa ra màn hình thông điệp



* Phát hiện tấn công thành công