**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

------------------------------



**BÁO CÁO MÔN CHUYÊN ĐỀ AN NINH MẠNG**

***Đề tài*: Xây Dựng Công Cụ Phân Tích Và Cảnh Báo Phát Hiện Lỗ Hổng Trên Remote Desktop Services**

(CVE-2019-0708)

**Người hướng dẫn : TS. NGUYỄN HỒNG SƠN**

**Sinh viên thực hiện : LÊ QUANG NHƯ**

**Mã số sinh viên : N16DCAT035**

**Lớp : D16CQAT01-N**

**Khoá** **: 2016**

**Hệ** **: ĐẠI HỌC CHÍNH QUY**

**TP.HCM, tháng 11 / 2020**

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

------------------------------



**BÁO CÁO MÔN CHUYÊN ĐỀ AN NINH MẠNG**

***Đề tài*: Xây Dựng Công Cụ Phân Tích Và Cảnh Báo Phát Hiện Lỗ Hổng Trên Remote Desktop Services**

(CVE-2019-0708)

**Người hướng dẫn : TS. NGUYỄN HỒNG SƠN**

**Sinh viên thực hiện : LÊ QUANG NHƯ**

**Mã số sinh viên : N16DCAT035**

**Lớp : D16CQAT01-N**

**Khoá : 2016**

**Hệ : ĐẠI HỌC CHÍNH QUY**

**TP.HCM, tháng 11 / 2020**

**LỜI CẢM ƠN**

Trong lời đầu tiên của bài báo cáo đồ án môn thay thế tốt nghiệp “*Xây Dựng Công Cụ Phân Tích Và Cảnh Báo Phát Hiện Lỗ Hổng Trên Remote Desktop Services(CVE-2019-0708)* ”. Em muốn gửi những lời cảm ơn và biết ơn chân thành tới tất cả những người đã hỗ trợ, và giúp đỡ em về kiến thức và tinh thần trong quá trình thực hiện đồ án.

Em xin chân thành cảm ơn thầy, Tiến sĩ Nguyễn Hồng Sơn, Trưởng Khoa Trường Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở TP.HCM, đã tận tình giải đáp và trao đổi những vấn đề khó khăn, giúp đỡ em trong quá trình học tập, làm đề tài thời gian qua.

Mặc dù bản thân đã rất cố gắng nhưng do thời gian, kiến thức và kinh nghiệm có hạn, và cũng là lần đầu tiên làm đề tài dạng này, nên bài làm của em còn có nhiều thiếu sót trong việc trình bày, đánh giá và đề xuất ý kiến.

Bài báo cáo được thực hiện và thay đổi trong trong suốt quá trình học tập ở trên lớp. Bước đầu đi vào thực tế của em còn hạn chế và còn nhiều bỡ ngỡ nên không tránh khỏi những thiếu sót , em rất mong nhận được những ý kiến đóng góp quý báu của quý Thầy để kiến thức của em trong lĩnh vực này được hoàn thiện hơn đồng thời có điều kiện bổ sung, nâng cao kiến thức của mình.

Em xin chân thành cảm ơn!

**Xây Dựng Công Cụ Phân Tích Và Cảnh Báo Phát Hiện Lỗ Hổng Trên Remote Desktop Services** (CVE-2019-0708)

**Contents**

[DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT 2](#_Toc55723501)

[LỜI NÓI ĐẦU 3](#_Toc55723502)

[1. GIẢI THÍCH LỖ HỔNG CVE-2019-0708: 4](#_Toc55723503)

[2. THỰC NGHIỆM TẤN CÔNG VÀ BẮT DỮ LIỆU: 5](#_Toc55723504)

[3. LẬP TRÌNH CÀI ĐẶT ỨNG DỤNG PHÁT HIỆN: 7](#_Toc55723505)

[4. THỰC NGHIỆM PHÁT HIỆN TẤN CÔNG: 14](#_Toc55723506)

[Phát hiện cuộc tấn công và thông báo địa chỉ IP của máy tấn công 14](#_Toc55723507)

[Biểu đồ trên đồ họa 3D hiển thị kết quả sau khi phân cụm: 14](#_Toc55723508)

[5. TỰ ĐÁNH GIÁ 16](#_Toc55723509)

[6. HƯỚNG PHÁT TRIỂN TIẾP THEO 16](#_Toc55723510)

# DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

|  |  |  |  |
| --- | --- | --- | --- |
| **Số trang** | **Ký hiệu** | **Ý nghiã** | **Nick named** |
| Đầu trang | CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability | BlueKeep |

# LỜI NÓI ĐẦU

Trong thời đại ngày nay, thời đại mà công nghệ thay đổi từng ngày từng giờ, phần mềm dữ liệu cũng được cập nhật thay đổi theo. Nhưng bởi vì sự thay đổi liên tục, dẫn đến sự khó kiểm soát được những bản cập nhật, gây ra nhiều lỗ hỏng không mong muốn.

Vì thế việc hạn chế, và cảnh báo sự xâm nhập do các lỗ hỏng là một việc hết sức cần thiết vào lúc này để giảm thiểu rủi ro và có các phản ứng kịp thời. Xây dựng hệ thống cảnh báo sự xâm nhập là mục tiêu không thể thiếu của các doanh nghiệp hiện nay.

An toàn trên lưu lượng mạng, giúp cho người quản trị có thể biết được và yên tâm khi bị xâm nhập, tấn công. Điều này tạo ra xu thuế và làm tiền đề cho các hệ thống bảo mật tiên tiến hơn cho thời đại công nghệ hiện nay. Ở bất kì nơi đâu cũng có thể quản lý hệ thống công ty đã được xây dựng hệ thống phòng thủ bảo mật cặn kẽ.

Chính vì vậy Trong nội dung bài báo cáo này em đã chuẩn bị một số kỹ thuật phân tích và lập trình ứng dụng. Bởi vì xây dựng hệ thống cảnh báo thì rất nhiều loại, Cho nên ở đây em chỉ chọn một lỗ hỏng để thực nghiệm để có những hình dung cách thức làm việc của một hệ thống cảnh báo tấn công, mà bất cứ hệ thống nào cũng cần phải có.

Mục tiêu:

+ Thực hiện xây dựng chức năng lắng nghe và xuất dữ liệu lưu lượng mạng.

+ Hiểu rõ được khái niệm của lỗ hỏng và sư nguy hiểm của nó.

+ Xây dựng chức năng trích xuất dữ liệu thô thành dữ liệu cần thiết cho việc phòng chống lỗ hỏng.

+ Đưa ra được thông tin rõ ràng để cảnh báo chính xác cho người dùng.

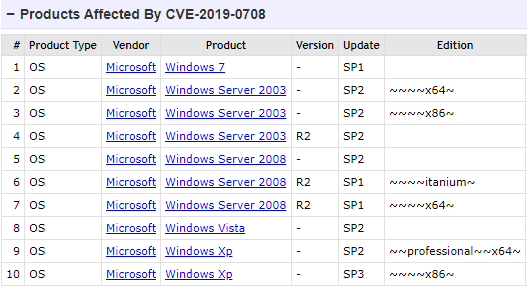
# GIẢI THÍCH LỖ HỔNG CVE-2019-0708:

Nó là lỗ hổng trên nền dịch vụ điều khiển từ xa(remote desktop) của window. Tên gọi là *Remote code execution vulnerablility* nick namelà *bluekeep*.

Lỗ hổng này không cần người dùng tương tác. Kẻ tấn công lợi dụng quá trình bắt tay của giao thức TLSv1 để thực hiện gửi hàng loạt các gói tin có dung lượng lơn để có thể làm cạn kiệt dẫn tới off hệ thống.

Điểm khác biệt giữa DOS thông thường và DOS trên dịch vụ remote desktop là: DOS thông thường vào một ứng dụng web thì nó gây ra trang web không chạy được nhưng máy chủ vẫn có thể hoạt động được cho các hoạt động khác. Còn *cve-2019-0708* thì làm máy vật lý off hẳn.

Các phiên bản chứa lỗ hỏng



# THỰC NGHIỆM TẤN CÔNG VÀ BẮT DỮ LIỆU:

Ta chuẩn bị 3 máy:

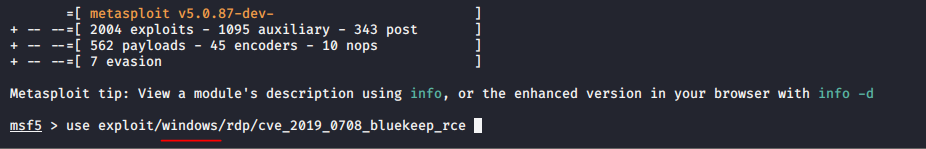
+ 1 máy ảo kali làm máy tấn công

+ 1 máy ảo window 2007 packet 1 làm máy nạn nhân.

+ Máy thật dùng để chạy chương trình bắt gói.

**Bước 1: sử dụng máy kali mở chương trình metasploit và cài đặt tấn công**

Sử dụng module là: **exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce**



Lần lượt set các option sau:

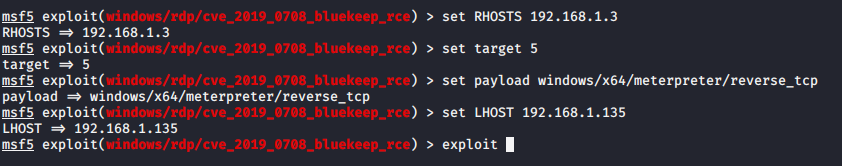
**RHOSTS** <ip máy nạn nhân> **192.168.1.3**

**Target** <chọn version của ứng dụng máy ảo VMW>

**Payload** <chọn payload tương ứng>

**LHOSTS** <ip máy tấn công> **192.168.1.135**

**Exploit** : dùng để bắt đầu khai thác



**Bước 2: Chạy chương trình bắt lưu lượng mạng đã viết.**

Cài đặt câu lệnh windump trong chương trình python sử dụng subprocess:

# option: -i 3: ethernet || -i 1: wifi || -i 2 interface VMNET 8

WinDump.exe  -i 2 -c 1000 -w <pathFile.pcap>

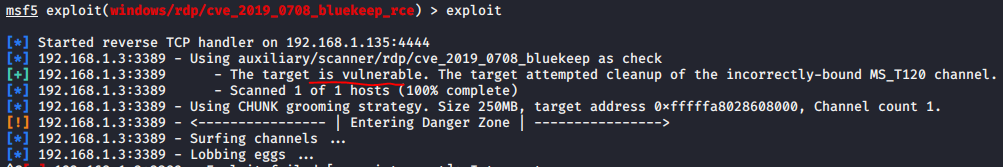
**Trong đó:**

**-i 2:** là interface của máy ảo cá nhân.

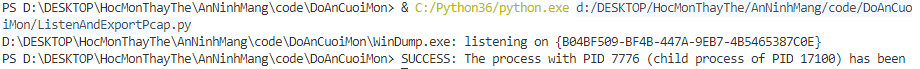
**-c 1000:** là số lượng gói tin muốn bắt

**-w <pathFile.pcap>:** đường dẫn file data *.pcap*

Bắt đầu tấn công!



Mở chương trình lắng nghe



Ta thu được file:



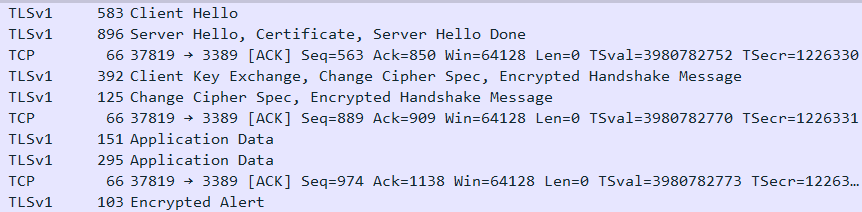
# LẬP TRÌNH CÀI ĐẶT ỨNG DỤNG PHÁT HIỆN:

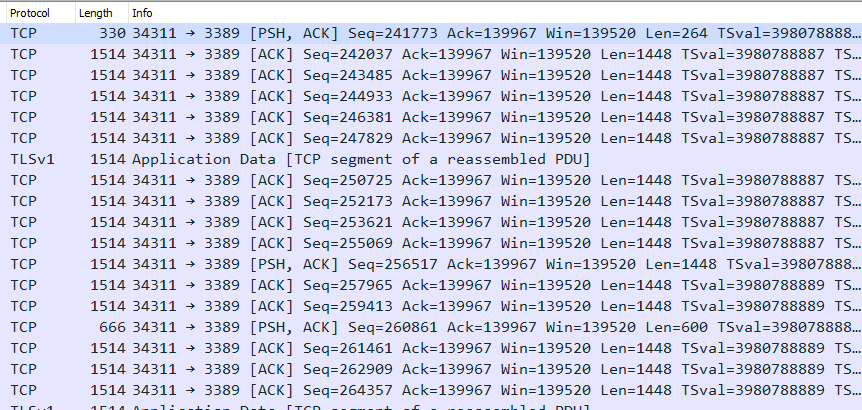
- Để tạo ra được ứng dụng này ta phải đi tìm hiểu phân tích những thông tin sau:

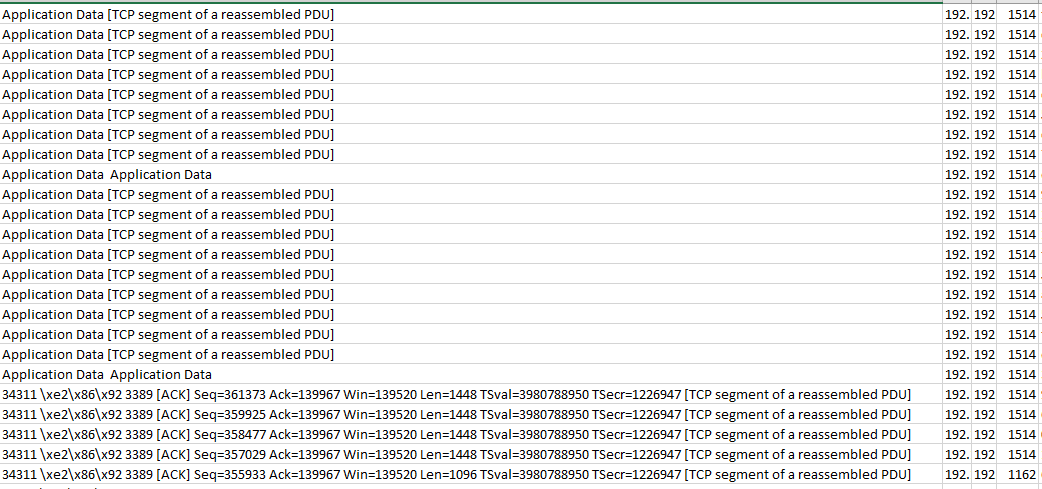
**Đầu tiên ta phải tìm hiểu. công cụ này gửi những gói tin có đặc điểm như thế nào để khai thác lỗ hỏng này?.**

Từ đó, để ta nhận biết được, những thông tin cần thiết cho việc phân biệt, lọc các gói tin, tạo thành DataSet liên quan của lỗ hỏng này.

*Hình ảnh cho việc bắt gói.*







**Phân tích tiến trình tấn công của tool:**

Bước 1: Attacker thực hiện gửi thủ tục bắt tay của giao thức TLS

Bước 2: Và ở giữa quá trình bắt tay thì liên tục gửi các gói “TCP segment of a reassembled PDU” để làm đầy dung lượng bộ đệm của máy nạn nhân.

Bước 3: Máy nạn nhân sẽ gửi gói “TCP window update” và “TCP ZeroWindow” với length bằng 0 để báo hiệu rằng bộ đệm nhận thông tin liên lạc đã đầy và không thể nhận dữ liệu nữa.

Bước 4: Máy attacker tiếp tục gửi các gói “TCP Window Update” với size bằng 0 để thăm dò và yêu cầu tăng kích thước bộ đệm máy nạn nhân .

Bước 5: Lặp lại bước 2 đến khi nào máy nạn nhân bị sập.

**Đặc điểm nhận dạng tấn công:**

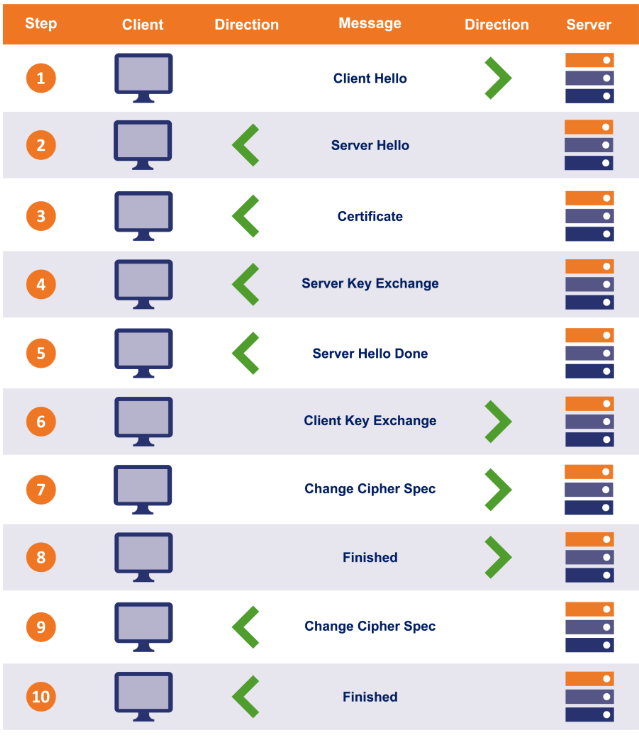
+ Ta thấy máy tấn công đang thực hiện quá trình bắt tay với máy nạn nhân trên nền dịch vụ remote service với port **3389**.

+ Thông qua quá trình handshake của giao thức TCP(*TLSv1*)

+ "TCP segment of a reassembled PDU": tức là một phần của gói tin. Nó gửi hàng loạt các gói tin có dung lượng lớn và không đầy đủ, để máy nạn nhân tốn tài nguyên để lắp ráp các gói tin này.

+ Ở đây ta thấy gói tin có info là : *Client Hello, Server Hello, Client key Exchange, Encrypted Alert*. Là thông tin của quá trình handshake của TLS protocol.

*Đây là 1 session handshake của giao thức TLS*



Bởi vì lỗ hỏng này lợi dụng trong lúc bắt tay của giao thức TLS để gửi hàng loạt các gói tin. Chính vì vậy số lượng hoàn thành được một phiên bắt tay là không nhiều.

**Kết luận:** Thông tin quan trọng ở đây để biết được đây là dạng tấn công nhắm vào lỗ hỏng cve-2019-0708. Đó là gói tin có info là: [*TCP segment of a reassembled PDU]*, càng nhiều gói [*TCP segment of a reassembled PDU]* được gửi có dung lượng lớn, trong thời gian ngắn, trong quá trình handshake **TLS** protocol thì mới chứng tỏ được đây là 1 cuộc tấn công **blue keep DOS**.

**Từ đây ta xây dựng code lọc gói tin như sau:**

Bước 1: Ta loại bỏ các gói tin ping



Bước 2: Kiểm tra xem có sự tồn tại của quá trình bắt tay của giao thức TLS (remote desktop sử dụng loại giao thức này) hay không?



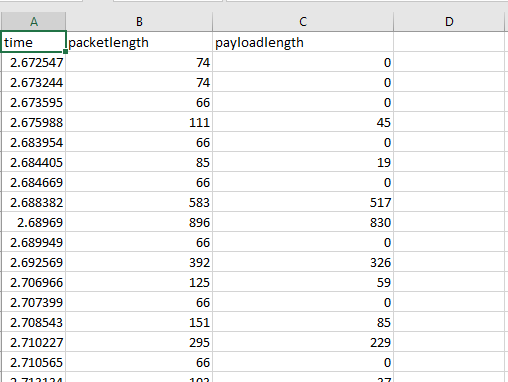
Bước 3: Kiểm tra xem kết quả ở bước 2. Nếu có sự tồn tại TLS protocol thì bắt đầu thu thập gói tin. Thu thập dựa trên gói tin nào có port **3389** hoặc info là **: [*TCP segment of a reassembled PDU].***

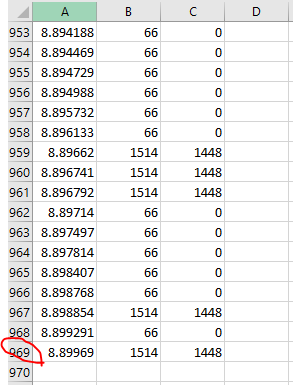


Bước 4: Thu thập gói tin và ghi vào file csv.

File data set:





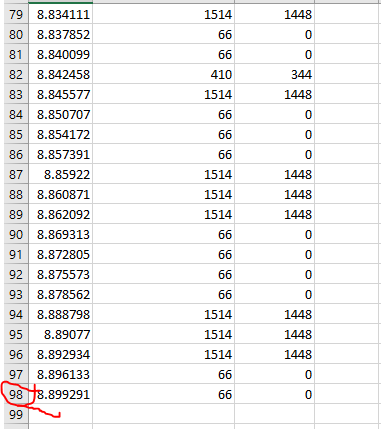


* Có tổng cộng **969 gói tin / 1000** gói bắt được cho là của cuộc tấn công.

**Thứ hai, ta gôm các dữ liệu có một số đặc điểm giống nhau thành 1 point dữ liệu:**

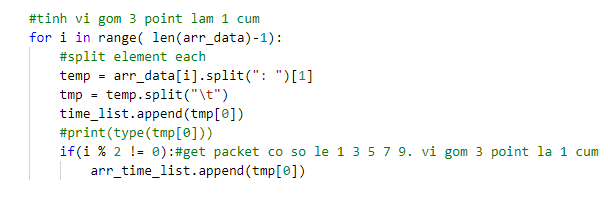
Ở đây ta gôm 10 gói tin có thời gian gần nhau thành 1 point dữ liệu.





* Sau khi gôm cụm các gói tin với số lượng dữ liệu là **98** point**/ 969** gói tin

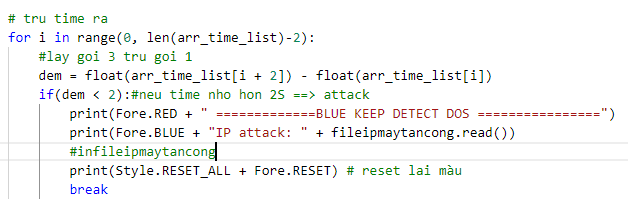
Ta xây dựng hệ thống cảnh báo tấn công: với 3 point(30 gói tin) liên tiếp là 1 cụm để phát hiện.



**Time = gói thứ 3 - gói thứ 1**

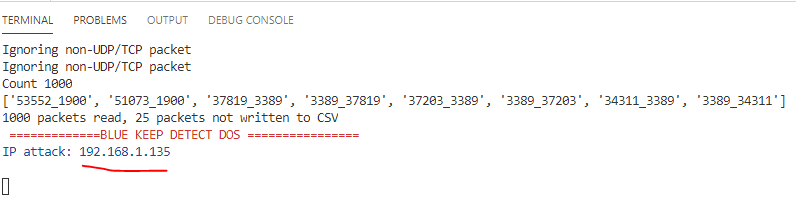
Và ta lấy

Nếu **time < 2s** thì suy ra đây là cuộc tấn công DOS dạng **Blue Keep**

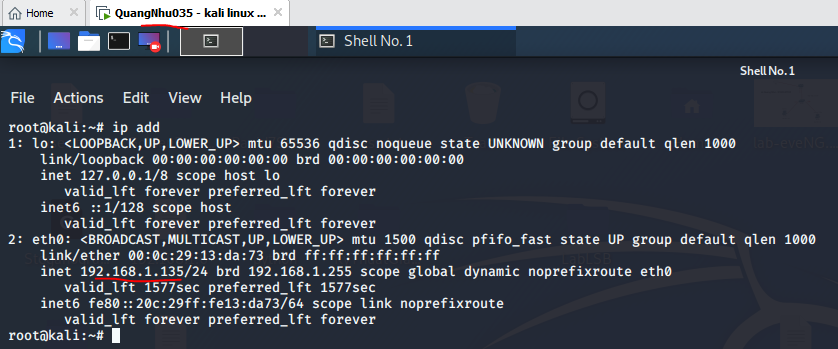


# THỰC NGHIỆM PHÁT HIỆN TẤN CÔNG:

Phát hiện cuộc tấn công và thông báo địa chỉ IP của máy tấn công.



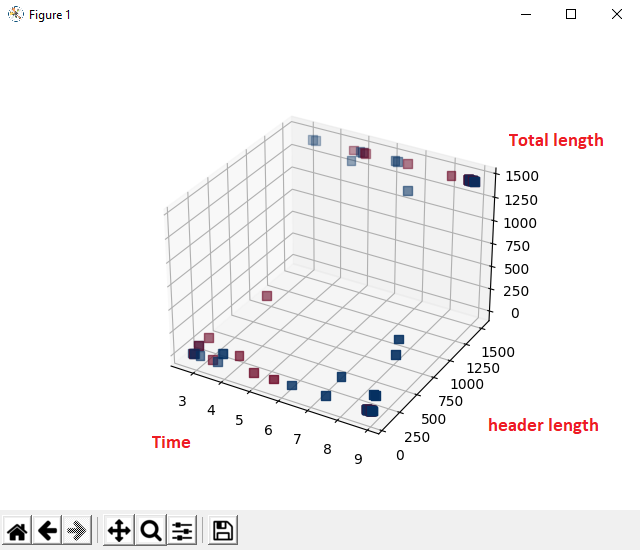
Ip máy kali:



Kết quả: Đã phát hiện thành công cuộc tấn công và đưa ra được địa chỉ ip của máy tấn công!!.

Biểu đồ trên đồ họa 3D hiển thị kết quả sau khi phân cụm: giúp ta có cái nhìn tổng quan hơn

Để biết được cuộc tấn công này rơi vào khoảng thời gian nào nhiều nhất, và độ lớn gói tin như thế nào ?



**Qua biểu đồ ta thấy:**

+ Cuộc tấn công này rơi vào khoảng thời gian 2 – > 3, 8 -> 9. Trong khoảng thời gian rất ngắn mà có rất nhiều điểm dữ liệu.

+ Chiều dài gói tin rơi vào mức 1200 🡪 1400. Khá lớn so với gói tin thông thường

**Kết Luận**: Đây là dấu hiệu của cuộc tấn công. Công cụ đã chạy đúng.

# TỰ ĐÁNH GIÁ

Đồ án xây dựng công cụ phát hiện và cảnh báo tấn công do lỗ hỏng *CVE-2019-0708*.

Qua đồ án, giúp nắm được một số kỹ năng tìm hiểu phân tích, nhận dang các lỗ hỏng và cách lập trình để tạo ra các ứng dụng có thể áp dụng vào thực tế.

Đồ án cơ bản đã được xử lý tất cả các chức năng theo nội dung được yêu cầu và đã thử nghiệm, cho kết quả như mong muốn.

# HƯỚNG PHÁT TRIỂN TIẾP THEO

Hướng phát triển tiếp theo của đồ án là xây dựng thêm các chức năng mở rộng, để có thể phát hiện nhiều loại tấn công hơn. Phát hiện được các loại **DOS** khác như TCP SYN flood**,** Slowloris**, …… .**

**DANH MỤC TÀI LIỆU THAM KHẢO**

**Danh mục các Website tham khảo:**

1. <https://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html>
2. <https://plotly.com/python/v3/3d-point-clustering/>