|  |
| --- |
| ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINHTRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN **KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**  NGÀNH AN TOÀN THÔNG TIN  **Tấn công Slowloris vào ứng dụng Web và biện pháp phòng thủ**  ***Slowloris Attacks on Web Applications and Defensive Measures***  **GIẢNG VIÊN HƯỚNG DẪN**  **NGUYỄN NGỌC TỰ**  VƯƠNG ĐINH THANH NGÂN - 20521649  HÀ TRIỆU YẾN VY - 20522177  NGÔ TRẦN THÁI SƠN - 20521841  **TP. HỒ CHÍ MINH, 2023** |

**Mục lục**

[**I. Giới thiệu:** 2](#_Toc1649)

[**II. Nội dung:** 2](#_Toc11757)

[1. Ngữ cảnh 2](#_Toc6078)

[2. Các bên liên quan 3](#_Toc2739)

[3. Các dạng tấn công slow 3](#_Toc27913)

[a. Tấn công Slowloris: 3](#_Toc28435)

[b. Tấn công Slow POST: 4](#_Toc7621)

[c.Tấn công Slow READ: 5](#_Toc9076)

[4. Hướng thực hiện 6](#_Toc3208)

[5. Phương thức tấn công 6](#_Toc5273)

[6. Phương thức phòng thủ 6](#_Toc23915)

[**III. Thực nghiệm (Demo):** 9](#_Toc7956)

[**IV. Tài liệu tham khảo:** 9](#_Toc2093)

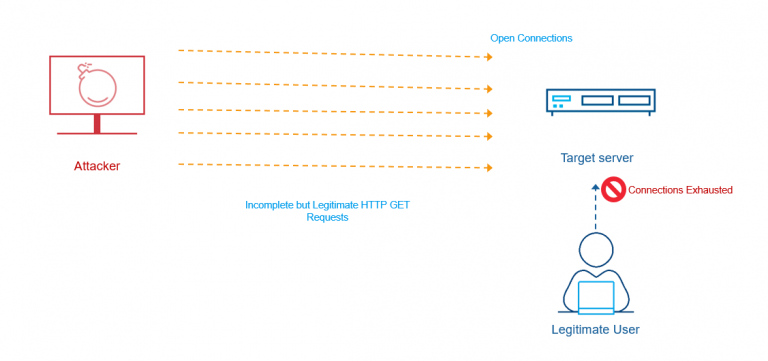
# Giới thiệu:

Các cuộc tấn công từ chối dịch vụ (DoS) chậm và tấn công từ chối dịch vụ phân tán (DDoS) trong các mạng máy tính. Mục đích chính của các cuộc tấn công Từ chối Dịch vụ (DoS) là làm cho dịch vụ mạng mục tiêu không khả dụng đối với người dùng hợp pháp. Các cuộc tấn công DoS đã dần dần phát triển từ các cuộc tấn công tràn tài nguyên đơn giản sang các cuộc tấn công tinh vi hiện nay nhắm mục tiêu vào các giao thức ứng dụng mô hình tham chiếu ISO/OSI, đặc biệt là giao thức truyền tải siêu văn bản (HTTP). Các cuộc tấn công như vậy có thể gây khó khăn cho nhiều cơ chế phát hiện để phân biệt với lưu lượng truy cập hợp pháp. Một trong số đó là các cuộc tấn công DoS slow chẳng hạn như Slowloris, Slow POST và Slow Read.

# Nội dung:

## Ngữ cảnh

Tấn công DDOS ngày càng trở nên tinh vi và trong đó việc tấn công bằng cách gửi các luồng dữ liệu nhỏ và chậm, nhằm giả dạng thành người dùng hợp pháp để làm cạn kiệt tài nguyên của Server gây ra một hậu quả vô cùng to lớn. Trong đó thì việc tấn công vào tài nguyên ứng dựng Web xảy ra phổ biến và gây ra nhiều hậu quả.



## Các bên liên quan

- Hacker: Người truy cập trái phép, muốn phá hoại nhằm ngăn chặn truy cập.

- User: Người dùng dịch vụ

- Sever: Là máy chủ có chức năng cung cấp và lưu trữ thông tin phục vụ Client

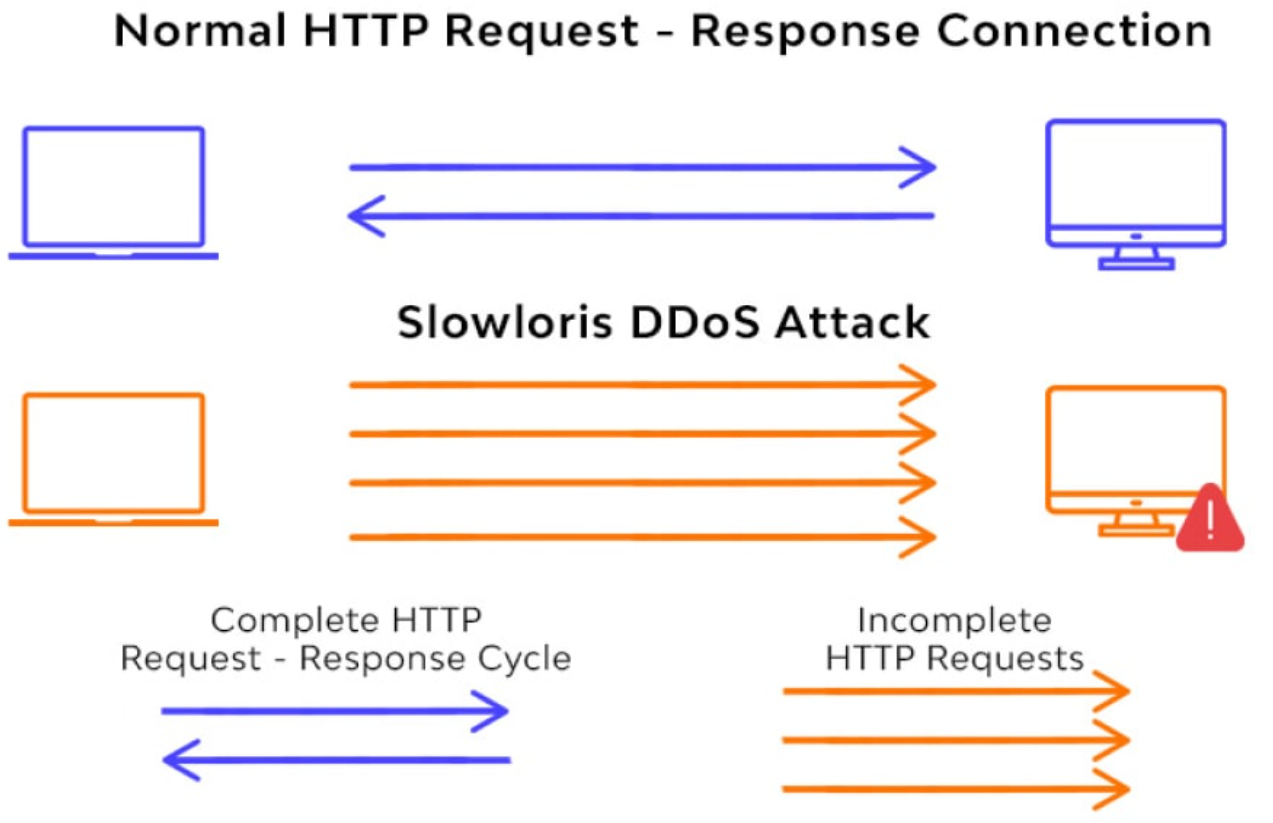
## Các dạng tấn công slow

**Lý do có thể tạo ra việc tấn công từ phương thức gửi các gói HTTP không hoàn chỉnh:** Tất cả các dạng tấn công Slow đều lợi dụng việc gửi nhỏ giọt luồng dữ liệu, chính xác là incomplete HTTP và lý do là vì thông điệp HTTP khi gửi đi sẽ chia thành các packet nhỏ, được đánh các số Seq để khi nhận đủ có thể ghép lại thành thông điệp hoàn chỉnh – dựa vào đây Server sẽ biết được cần phản hồi lại Client như thế nào. Ở cách tấn công này, khi gửi thì chỉ gửi một vài packet (gửi nhỏ gọt) và vì các gói này hợp lệ nên khiến cho Server chờ đợi các gói packet có số Seq tiếp theo để ghép thành thông điệp hoàn chỉnh dẫn tới không thể đóng kết nối. Và với nhiều kết nối như vậy sẽ làm cạn tài nguyên của Server dẫn tới xảy ra tấn công.

a. Tấn công Slowloris:

Tấn công Slowloris còn được gọi là Slow GET hoặc Slow Header. Yêu cầu HTTP GET được gửi đến máy chủ. Yêu cầu này không bị chấm dứt hợp lệ vì nó không chứa ký tự kết thúc \r\n\r\n (ngắt dòng kép). Do đó, máy chủ đợi phần tiếp theo của yêu cầu, phần này sẽ chứa ký tự kết thúc. Sự chờ đợi này bị giới hạn trong cấu hình máy chủ. Sau khi vượt quá thời gian hẹn giờ, máy chủ sẽ đóng kết nối TCP. Tuy nhiên, trước khi hết thời gian này, kẻ tấn công sẽ gửi một phần khác của yêu cầu. Cái gọi là gói giữ nguyên này thường chỉ chứa một vài ký tự ngẫu nhiên.

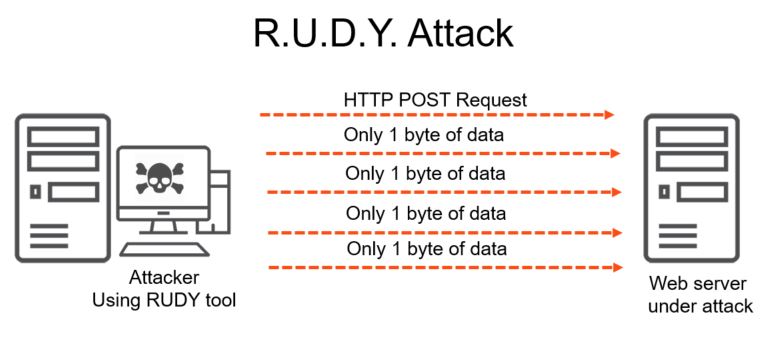
Gói này đặt lại bộ đếm thời gian và sau đó kẻ tấn công lại bị tắt tiếng và toàn bộ quá trình được lặp lại. Bằng cách này, kẻ tấn công cố gắng thiết lập càng nhiều kết nối TCP càng tốt và làm cạn kiệt tất cả các tài nguyên máy chủ miễn phí có thể phục vụ những người dùng hợp pháp khác.



### b. Tấn công Slow POST:

Tấn công Slow POST RUDY (Bạn đã chết chưa?) sử dụng yêu cầu HTTP POST. Loại yêu cầu này thường được sử dụng để gửi dữ liệu được điền vào biểu mẫu Internet. Tiêu đề yêu cầu HTTP chứa trường độ dài, nội dung, chỉ định kích thước của dữ liệu biểu mẫu được truyền sau tiêu đề yêu cầu.

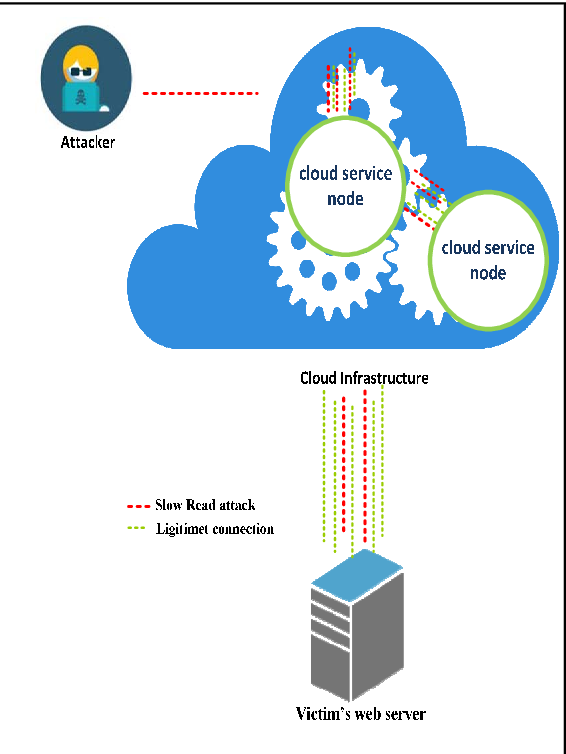
Trong cuộc tấn công này, trường độ dài nội dung chứa một giá trị rất cao, vì vậy máy chủ sẽ nhận được một lượng lớn dữ liệu. Khi đó, tiêu đề của yêu cầu giả mạo sẽ bị chấm dứt hợp lệ và khi đó yêu cầu chứa một phần dữ liệu nhỏ, dữ liệu này thường được biểu thị bằng một vài ký tự ngẫu nhiên. Sau đó, kẻ tấn công sẽ đợi và gửi một đoạn dữ liệu nhỏ khác trước khi hết giờ kết thúc kết nối. Theo cách này, kẻ tấn công giữ cho kết nối hoạt động và tương tự cố gắng thiết lập càng nhiều kết nối càng tốt. Điều này dẫn đến cạn kiệt tất cả tài nguyên máy chủ có sẵn.



c. Tấn công Slow READ:

Tấn công Slow Read sử dụng giao thức HTTP và TCP. Ban đầu, kẻ tấn công yêu cầu một số dữ liệu lớn hơn, chẳng hạn như hình ảnh, bằng cách gửi yêu cầu GET hợp lệ đến máy chủ.

Kẻ tấn công đặt tham số kích thước cửa sổ trong tiêu đề TCP thành giá trị cửa sổ TCP rất thấp. Tham số này xác định lượng dữ liệu mà máy chủ có thể gửi mà không cần bất kỳ xác nhận nào. Cơ chế này dùng để điều chỉnh và điều chỉnh tốc độ dữ liệu phù hợp với chất lượng kết nối giữa các điểm cuối. Máy chủ buộc phải gửi phản hồi theo từng phần rất nhỏ. Bằng cách này, kẻ tấn công có thể đạt đến trạng thái mà quá trình truyền tệp 1 MB có thể mất vài ngày. Kẻ tấn công sử dụng kỹ thuật này để làm cạn kiệt tất cả tài nguyên máy chủ có sẵn.



## Hướng thực hiện

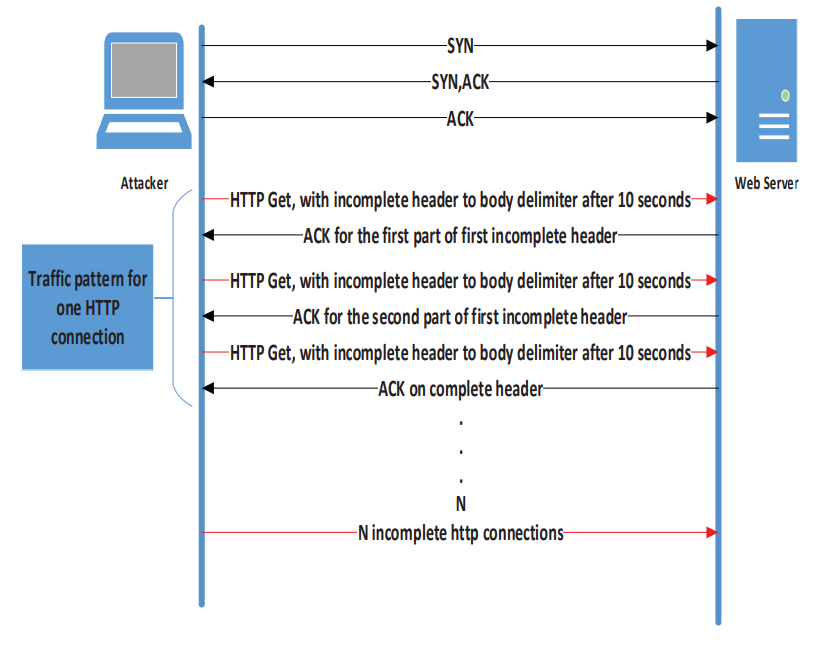
Slow thuộc loại tấn công nhỏ giọt tức là chậm và thấp, vì vậy nó khó để phát hiện. Slowloris dùng để khai thác thông qua giao thức HTTP.

Khi số lượng request chiếm hết tài nguyên của web server thì sẽ dẫn tới tình trạng không giải quyết các yêu cầu mới từ những người dùng bình thường. Vì vậy cần có cái mod an toàn để kiểm soát request, băng thông.

## Phương thức tấn công

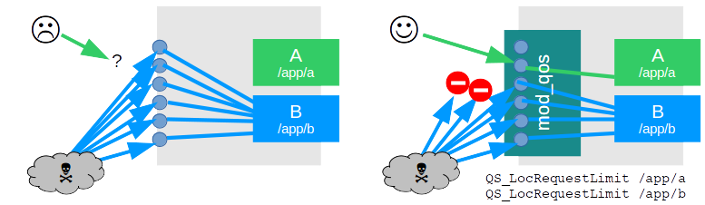
Mở nhiều kết nối đến máy chủ, gửi các header incomplete HTTP request. Sau khi server mở một luồng cho mỗi yêu cầu, ta định kỳ gửi một phần tiêu đề yêu cầu tới mục tiêu để giữ cho yêu cầu tồn tại, nếu server muốn giải phóng các tài nguyên bị giữ thì sẽ lại tiếp tục bị attacker gửi các gói theo định kì để không bị timeout nhằm giữ các tài nguyên lâu nhất có thể

Máy chủ không thể giải phóng tài nguyên, dẫn tới sẽ không thể phản hồi các yêu cầu bổ sung (từ chối dịch vụ)

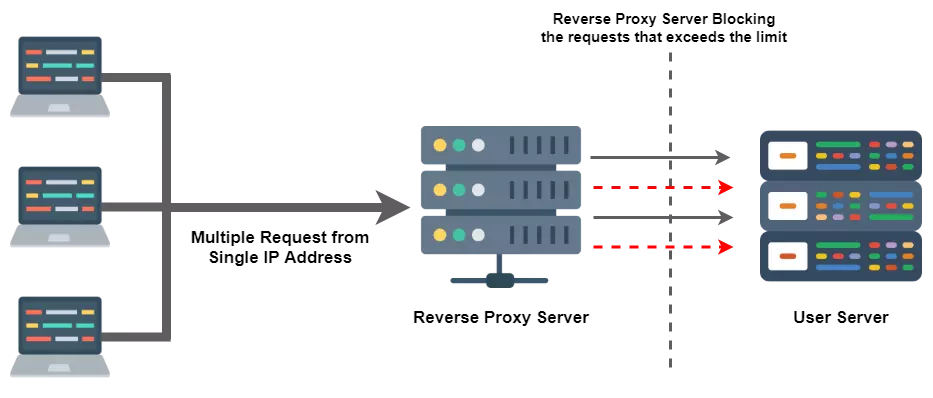


## Phương thức phòng thủ

Trước đó, ta đã có một số phương thức đã ngăn chặn các cuộc tấn công như vậy bằng cách sử dụng các mô-đun an toàn: mod\_noloris, mod\_antiloris, mod\_qos. Tuy nhiên các mod như vậy không còn tác dụng trong các cuộc tấn công tinh vi gần đây



Máy chủ proxy hay gọi là proxy là máy chủ đặt trước một nhóm máy khách. Khi các máy khách đó thực hiện yêu cầu đến các trang web và dịch vụ trên internet, proxy sẽ chặn các yêu cầu đó và sau đó giao tiếp với máy chủ web theo kiểu thay mặt còn gọi là thay mặt , giống như là một nguồn trung gian nhằm ngăn kết nối trực tiếp giữa các máy chủ và trang web



Proxy ngược cũng gần tương tự như máy chủ proxy thuận hay proxy bình thường vẫn sử dụng, nhưng không phải chặn trước các máy khách mà là chặn trước các máy chủ web, chặn yêu cầu từ máy khách. Với proxy ngược khi máy khách gửi yêu cầu đến máy chủ gốc của một trang web, những yêu cầu đó sẽ bị chặn ở biên mạng bởi máy chủ proxy ngược. Sau đó proxy ngược sẽ gửi yêu càu đến và nhận phản hồi từ máy chủ gốc. Quan trọng là tại sao lại sử dụng proxy ngược lại được sử dụng trong trường hợp này thay vì proxy thuận:

- Thứ nhất, proxy ngược có cơ chế Load Balancing (Cân bằng tải). Có thể hiểu việc khi bị tấn công ddos thì các web bị nhồi quá nhiều request tới các port rồi dẫn tới việc các từ chối dịch vụ. Nhưng khi có cân bằng tải thì việc đó lại có thể được hóa giải bằng cách cân bằng tải nhằm phân phân đều lưu lượng đến các máy chủ khác nhau nhằm ngăn bất kì máy chủ nào bị quá tải và dẫn tới từ chối dịch vụ. Việc này có giảm chi phí khi chúng ta có thể sử dụng nhiều máy chủ nhỏ lẻ thay vì một máy chủ khổng lồ với chi phí quá đắt đỏ

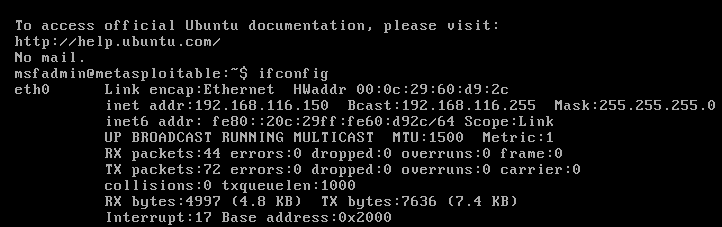
- Thứ hai, Caching (Bộ nhớ đệm), proxy ngược có thể lưu nội dung vào cache, giúp hiệu suất nhanh hơn. Tại vì khi sử dụng cache thì lần truy cập đầu tiên sẽ được tạm thời lưu, và dẫn tới khi truy câp các lần truy cập tiếp theo sẽ được nhận các phiên bản được lưu trong các bộ nhớ cache cục bộ từ máy chủ proxy ngược.

- Thứ ba, bảo vệ tránh sụp đổ trang khi có tấn công ddos, khi tấn công ddos chúng ta cần có địa chỉ IP của mục tiêu cần tấn công proxy ngược có cơ chế không tiết lộ IP của trang web vì đã làm ủy quyền giữa web và user nhằm tránh các truy cập trực tiếp giữa 2 phái này nhằm lộ ra IP. Thay vào đó, attacker chỉ có thể chuyển hướng qua các proxy, nhưng các proxy ngược này lại có nhiều tài nguyên và có nền tảng bảo mật chặt chẽ hơn một hosting bất kì nào làm cho việc ddos trở nên cực kì khó khăn.

- Cuối cùng là có Mã Hóa SSL: Mã hóa thông tin liên lạc SSL (hoặc TLS) cho từng máy khách có thể tốn kém về mặt tính toán cho mỗi máy chủ gốc. Một proxy ngược có thể được cấu hình để giãi mã tất cả các yêu cầu đến và mã hóa tất cả phản hồi gửi đi, nhằm giải phóng tài nguyên có giá trị trên máy chủ gốc.

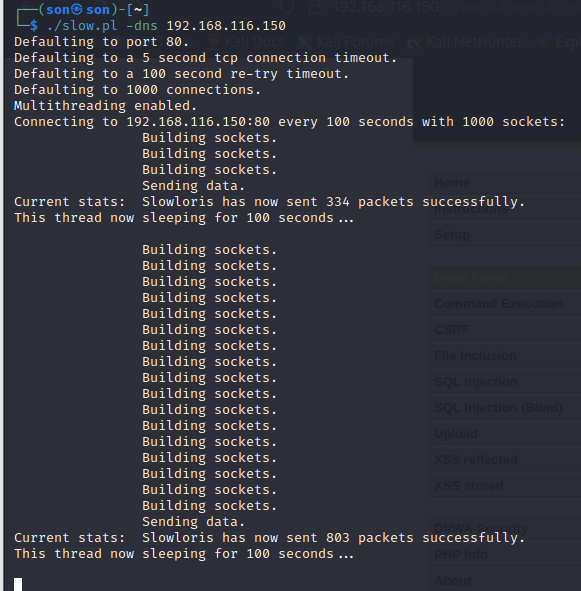
# Thực nghiệm (Demo):

Sử dụng web server local dựa trên máy ảo metasploitable có ip là 192.168.116.150 làm mục tiêu để thực hiện tấn công.





Thực hiện tấn công đến port 80, liên tục khởi tạo hàng trăm yêu cầu HTTP hợp lệ và giữ kết nối bằng cách gửi một phần (bổ sung nhỏ giọt).



Làm treo máy chủ, không thể tiếp nhận các kết nối từ người dùng hợp lệ.

# Tài liệu tham khảo:

[1] Sikora, M., Krivulcik, A., Fujdiak, R., & Blazek, P. (2020, October). Design of Advanced Slow Denial of Service Attack Generator. In 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 99-104). IEEE.

[2] Fitri, N. R., Budi, A. H. S., Kustiawan, I., & Suwono, S. E. (2020, May). Low interaction honeypot as the defense mechanism against Slowloris attack on the web server. In IOP Conference Series: Materials Science and Engineering (Vol. 850, No. 1, p. 012037). IOP Publishing.