**ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**🙣 🕮 🙡**



**ĐỒ ÁN MÔN HỌC**

**AN TOÀN VÀ BẢO MẬT DỮ LIỆU   
TRONG HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI:**

**TÌM HIỂU CÁC PHƯƠNG PHÁP TẤN CÔNG   
TỪ CHỐI DỊCH VỤ**

**Nhóm 14**

**Sinh viên thực hiện:**

|  |  |
| --- | --- |
| **3119410215** | **Võ Hoàng Kiệt** |
| **3119410204** | **Trần Hữu Khương** |
| **3119410254** | **Lê Thái Thanh Sơn** |

***Thành phố Hồ Chí Minh, tháng 4 năm 2022***

**MỤC LỤC**

[CHƯƠNG 1: SƠ LƯỢC VỀ TẤN CÔNG DOS 5](#_Toc102725673)

[1.1. Khái niệm: 5](#_Toc102725674)

[1.2. Mục đích của tấn công DoS 5](#_Toc102725675)

[1.3. Hậu quả của tấn công DoS 6](#_Toc102725676)

[1.4. Lịch sử của DoS và một số vụ tấn công nổi tiếng: 7](#_Toc102725677)

[CHƯƠNG 2: TẤN CÔNG DOS 9](#_Toc102725678)

[2.1. Các dạng tấn công DoS 9](#_Toc102725679)

[a. Tấn công SYN Flood 10](#_Toc102725680)

[b. Tấn công Smurf 11](#_Toc102725681)

[c. Tấn công Ping Of Dead 12](#_Toc102725682)

[d. Tấn công UDP Flood: 13](#_Toc102725683)

[e. Tấn công Http Flood 14](#_Toc102725684)

[2.2. Phương pháp phát hiện tấn công DoS 15](#_Toc102725685)

[2.3. Phương pháp phòng chống tấn công DoS 16](#_Toc102725686)

[CHƯƠNG 3: THỰC HIỆN TẤN CÔNG DOS 18](#_Toc102725687)

[3.1. Sử dụng phương thức HTTP Flood ( Application Layer Attack ): 18](#_Toc102725688)

[3.2. Sử dụng phương thức SYN Flood ( Protocol Attacks ): 21](#_Toc102725689)

[3.3. Sử dụng phương thức UDP Flood ( Volumetric Attack ): 24](#_Toc102725690)

[3.4. Phương pháp phòng chống 25](#_Toc102725691)

[KẾT LUẬN 28](#_Toc102725692)

[TÀI LIỆU THAM KHẢO 29](#_Toc102725693)

**TỔNG QUAN VỀ ĐỀ TÀI**

1. **Lý do chọn đề tài:**

Mạng Internet ngày càng phát triển và mở rộng trên phạm vi toàn thế giới. Có thể nói các cổng thông tin điện tử, dịch vụ mạng là sự sống còn của từng cá nhân, tổ chức. Việc những hệ thống đó bị quá tải, không truy cập được trong một khoảng thời gian dù ngắn hay dài cũng có thể gây ra những tổn thất không nhỏ và hậu quả mà nó mang lại là không thể lường trước được.

Từ vấn đề thực tế trên, kiểu tấn công từ chối dịch vụ phân tán, DoS (Denial Of Service) đã xuất hiện từ rất sớm – khoảng những năm 90 của thế kỷ 20. Kiểu tấn công này hướng tới làm cạn kiệt tài nguyên của hệ thống, khiến người quản trị, người sử dụng không thể truy cập được hệ thống thông tin trên internet.

Trong những năm qua, không chỉ Việt Nam mà cả thế giới, các cuộc tấn công DoS liên tục diễn ra. Các cuộc tấn công này xuất phát từ nhiều mục đích khác nhau: kinh tế, cá nhân, thậm chí mang cả màu sắc chính trị; điển hình như 2 ông lớn Mỹ - Trung những năm gần đây. Do vậy, nghiên cứu Dos không bao giờ là cũ, mà trái lại cần phải luôn cập nhật cùng với việc nâng cấp các thiết bị, kỹ thuật công nghệ thông tin mới.

1. **Mục tiêu:**

Tìm hiểu về DoS, bao gồm các kiến thức liên quan đến lịch sử hình thành cũng như cách phát hiện, kịch bản tấn công và phòng thủ trong thực tế. Từ đó giúp khái quát hoá cũng như bổ sung kiến thức cho sinh viên trước khi tiếp xúc với thực tế công việc.

1. **Phạm vi:**

Tìm hiểu, xây dựng kịch bản tấn công và phòng thủ trước những đợt DoS trên môi trường ảo hoá.

# CHƯƠNG 1: SƠ LƯỢC VỀ TẤN CÔNG DOS

## Khái niệm:

Tấn công DoS là kiểu tấn công vô cùng nguy hiểm, để hiểu được nó ta cần phải nắm rõ định nghĩa của tấn công DoS và các dạng tấn công DoS.

* Tấn công DoS (Denial of Service) là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.
* Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công DoS.
* Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đích của tấn công DoS.

## Mục đích của tấn công DoS

Tấn công DOS là một kiểu tấn công phá hoại. Do đó người tấn công bằng phương pháp này không thực sự xâm nhập vào hệ thống hay truy cập được vào dữ liệu của hệ thống. Vì thế phương pháp này thường dùng trong việc “cạnh tranh không lành mạnh”. Nạn nhân của các cuộc tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội. Mặc dù DoS khó để đánh cắp thông tin quan trọng, nhưng chúng có thể khiến nạn nhân phải mất rất nhiều thời gian và tiền bạc để giải quyết hậu quả. Bởi vì một cuộc tấn công DoS có thể dễ dàng được thực hiện từ bất kỳ đối tượng nào, việc tìm kiếm người chịu trách nhiệm rất khó khăn.

VD: Bạn là chủ công ty A chuyên bán hàng online mua từ Trung Quốc về Việt Nam để kiếm lời. Một ngày đẹp trời công ty B cũng làm điều tương tự, tuy nhiên do nhảy vào làm sau cho nên không thể cạnh tranh lại bạn. Thế là anh chủ của công ty B quyết định thuê các hacker DDOS vào server của bạn một tháng trời. Khách hàng của bạn không thể đăng nhập vào trang của bạn để mua hàng thì nhảy sang trang của anh B mua. Thế là khách của bạn “nhảy” hết sang anh B.

Tóm lại mục đích của DoS thường là:

* Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
* Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
* Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó.
* Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.

## Hậu quả của tấn công DoS

Tấn công DoS xảy ra khi kẻ tấn công sử dụng hết tài nguyên của hệ thống và hệ thống không thể đáp ứng cho người dùng bình thường được. Hậu quả mà DoS để lại là vô cùng lớn:

* Hệ thống, máy chủ bị DoS sẽ bị ảnh hưởng hiến quá trình vận hành của các website và mạng nội bộ thường xuyên gặp sự cố.
* Doanh nghiệp sở hữu máy chủ, hệ thống sẽ bị mất doanh thu, chưa kể đến khoản chi phí cần phải bỏ ra để khắc phục sự cố.
* Khi mạng sập, mọi công việc yêu cầu mạng đều không thể thực hiện, làm gián đoạn công việc, ảnh hưởng đến hiệu suất công việc.
* Nếu người dùng truy cập website khi nó bị sập sẽ ảnh hưởng đến danh tiếng của công ty, nếu website sập trong thời gian dài thì có thể người dùng sẽ bỏ đi, lựa chọn dịch vụ khác thay thế.

## Lịch sử của DoS và một số vụ tấn công nổi tiếng:

* Các tấn công DoS bắt đầu vào khoảng đầu những năm 90. Đầu tiên, chúng hoàn toàn “nguyên thủy”, bao gồm chỉ một kẻ tấn công khai thác băng thông tối đa từ nạn nhân, ngăn những người khác được phục vụ. Điều này được thực hiện chủ yếu bằng cách dùng các phương pháp đơn giản như ping floods, SYN floods và UDP floods. Sau đó, các cuộc tấn công trở nên phức tạp hơn, bằng cách giả làm nạn nhân, gửi vài thông điệp và để các máy khác làm ngập máy nạn nhân với các thông điệp trả lời. (Smurf attack, IP spoofing…).
* Các tấn công này phải được đồng bộ hoá một cách thủ công bởi nhiều kẻ tấn công để tạo ra một sự phá huỷ có hiệu quả. Sự dịch chuyển đến việc tự động hoá sự đồng bộ, kết hợp này và tạo ra một tấn công song song lớn trở nên phổ biến từ 1997, với sự ra đời của công cụ tấn công DDoS đầu tiên được công bố rộng rãi, Trinoo. Nó dựa trên tấn công UDP flood và các giao tiếp master-slave (khiến các máy trung gian tham gia vào trong cuộc tấn công bằng cách đặt lên chúng các chương trình được điều khiển từ xa). Trong những năm tiếp theo, vài công cụ nữa được phổ biến – TFN (tribe flood network), TFN2K, vaf Stacheldraht.
* Tuy nhiên, chỉ từ cuối năm 1999 mới có những báo cáo về những tấn công như vậy, và đề tài này được công chúng biết đến chỉ sau khi một cuộc tấn công lớn vào các site công cộng tháng 2/2000.

+ 30 / 7 – 2 -2000 Yahoo! ( Một trang web nổi tiếng ) đã bị tấn công từ chối dịch vụ và ngưng trệ hoạt động trong vòng 3 giờ đồng hồ. Website Mail Yahoo và GeoCities đã bị tấn công từ 50 địa chỉ IP khác nhau với những yêu cầu chuyển vận lên đến 1 gigabit /s.

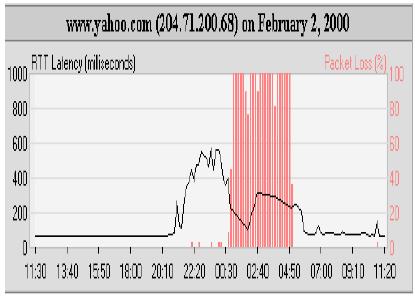
+ 8 -2 nhiều Website lớn như Buy.com, Amazon.com, eBay, Datek, MSN, và CNN.com bị tấn công từ chối dịch vụ.

+ Lúc 7 giờ tối ngày 9-2/2000 Website Excite.com là cái đích của một vụ tấn công từ chối dịch vụ, dữ liệu được luân chuyễn tới tấp trong vòng 1 giờ cho đến khi kết thúc, và gói dữ liệu đó đã hư hỏng nặng.

Từ đó các cuộc tấn công DoS thường xuyên xảy ra ví dụ:

- Vào ngày 15 tháng 8 năm 2003, Microsoft đã chịu đợt tấn công DoS cực mạnh và làm gián đoạn websites trong vòng 2 giờ.

- Vào lúc 15:09 giờ GMT ngày 27 tháng 3 năm 2003: toàn bộ phiên bản tiếng anh của website Al-Jazeera bị tấn công làm gián đoạn trong nhiều giờ.



*Tấn công DDoS vào Yahoo.com năm 2000*

Ngoài ra ở Việt Nam thì gần đây nhất cũng có 2 vụ tấn công DDOS lớn đó là:

* DDoS vào VCCrop gây chấn động an ninh mạng ở Việt Nam trong thời gian gần đây, hacker phá hoại server gây lỗi data center hàng loạt website báo mạng như: Dân trí, Kênh 14, Soha v.v.v (chưa tìm ra thủ phạm ).
* Và vụ thứ 2 là DDoS vào diễn đàn công nghệ thông tin VN-Zoom vào lúc 19 giờ ngày 26/10/2015 với dung lượng gần 400MB/giây.

# CHƯƠNG 2: TẤN CÔNG DOS

## Các dạng tấn công DoS

Với tấn công DOS thì chia ra làm 3 loại:

* **Tấn công Volumetric (tấn công băng thông):**

Tấn công băng thông làm bão hòa băng thông mà hệ thống bị nhắm đến sử dụng. Đây là kỹ thuật thường gặp nhất và cũng là dễ thực hiện nhất. Thường thì những kẻ tấn công sẽ vận dụng các kỹ thuật khuếch đại để sinh ra các request mà không cần dùng đến một lượng lớn tài nguyên.

VD: ICPM Flood, Ipsec Flood, UDP Flood,…

* **Tấn công Protocol Attacks:** (tấn công vào layer 3 4 với những request “độc hại”).

Các cuộc tấn công giao thức tận dụng các lỗ hổng ở Layer 3 hoặc Layer 4 của mô hình OSI, nghĩa là chúng sẽ sử dụng hết bộ nhớ, các lõi xử lý, hoặc làm quá tải nguồn thiết bị hoặc các mạng lưới giữa hệ thống bị nhắm đến và user ở đầu kia.

VD: SYN floods, Ping of Death, Smurf DdoS,…

* **Tấn công** **Application Layer Attack** (tấn công tầng thứ 7).

Tấn công tầng ứng dụng là loại hình tấn công hiệu quả nhất và rất khó để phát hiện và giảm thiểu. Những cuộc tấn công kiểu này không cần dùng lượng lớn request như các loại hình tấn công khác. Mục tiêu của tấn công DDoS là một khía cạnh của máy chủ hoặc ứng dụng. Tất cả các request đều có vẻ bình thường nên ứng dụng sẽ cố gắng phản hồi từng request một, dẫn đến việc bị quá tải.

VD: HTTP Flood,…

**Các phương pháp tấn công phổ biến hiện nay:**

### Tấn công SYN Flooddos3

* **Khái niệm:**

SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (DDoS). Tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp. Bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Người tấn công có thể áp đảo tất cả các cổng trên Server. Làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp.

* **Cách thức hoạt động:**

SYN Flood khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều.

Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối.

Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện Request TCP SYN và lúc này máy chủ không còn khả năng đáp lại – kết nối không được thực hiện.

Đây là kiểu tấn công mà kẻ tấn công lợi dụng quá trình giao tiếp của TCP theo quy tắc bắt tay 3 bước.

Các đoạn mã nguy hiểm có khả năng sinh ra một số lượng cực lớn các gói TCP SYN tới máy chủ bị tấn công, địa chỉ IP nguồn của gói tin đã bị thay đổi.

Hình bên trên thể hiện các giao tiếp bình thường với máy chủ và bên dưới thế hiện khi máy chủ bị tấn công gói SYN đến sẽ rất nhiều trong khi đó khả năng trả lời của máy chủ lại có hạn và khi đó máy chủ sẽ từ chối các truy cập hợp pháp.

Quá trình TCP bắt tay 3 bước được thực hiện: Khi máy A muốn giao tiếp với máy B.

(1) máy A bắn ra một gói TCP SYN tới máy B.

(2) máy B khi nhận được gói SYN từ A sẽ gửi lại máy A gói ACK đồng ý kết nối.

(3) máy A gửi lại máy B gói ACK và bắt đầu các giao tiếp dữ liệu.

Máy A và máy B sẽ dữ kết nối ít nhất là 75 giây, sau đó lại thực hiện một quá trình TCP bắt tay 3 bước lần nữa để thực hiện phiên kết nối tiếp theo để trao đổi dữ liệu.

Thật không may kẻ tấn công đã lợi dụng kẽ hở này để thực hiện hành vi tấn công nhằm sử dụng hết tài nguyên của hệ thống bằng cách giảm thời gian yêu cầu bắt tay 3 bước xuống rất nhỏ và không gửi lại gói ACK, cứ bắn gói SYN ra liên tục trong một thời gian nhất định và không bao giờ trả lời lại gói SYN&ACK từ máy bị tấn công.

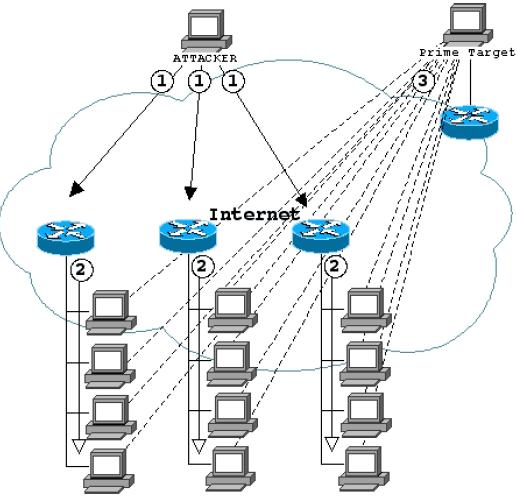
### Tấn công Smurf

* **Khái niệm:**

Tấn công Smurf là một dạng của tấn công từ chối dịch vụ phân tán (DDoS). Những kẻ tấn công sẽ nhắm đến server bằng gói tin Internet Control Message Protocol (ICMP) theo cách gửi các yêu cầu bởi IP giả mạo máy chủ của nạn nhân và gửi gói tin đến các máy trong cùng 1 mạng. Các máy này sau khi nhận được yêu cầu thì sẽ phản hồi lại gói tin trả lời đến máy của nạn nhân và sẽ mở rộng cuộc tấn công này lên. Dẫn đến máy chủ quá tải và từ chối dịch vụ xảy ra.

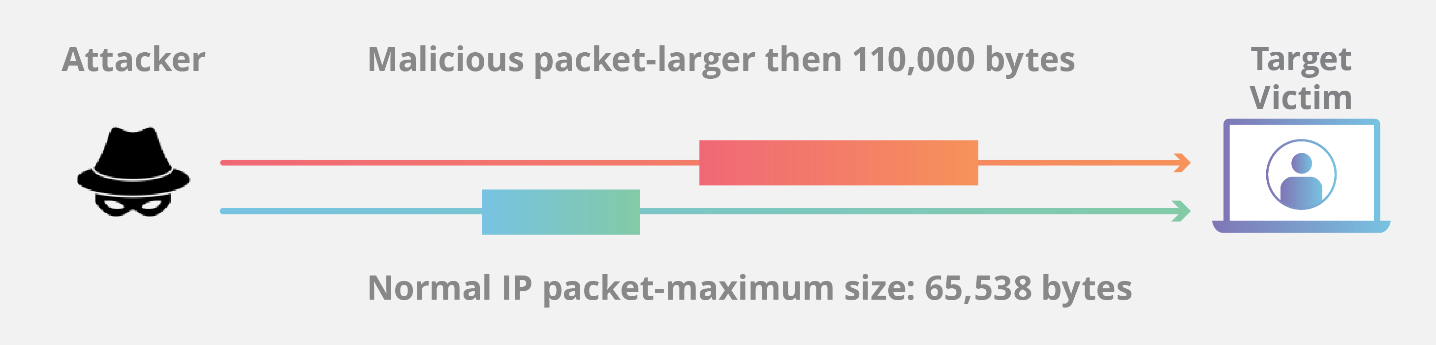
* **Cách thức hoạt động:**

Đầu tiên smurf malware tạo ra một gói tin mà địa chỉ nguồn là địa chỉ của máy nạn nhân.Gói tin được gửi broadcast đến router hoặc firewall. Router/firewall sẽ gửi tiếp gói broadcast này đến tất cả các máy trong vùng broadcast để tăng số lượng máy nhân được request.Mỗi thiết bị nhận được gói tin sẽ gửi phản hồi về địa chỉ nguồn của gói tin. Địa chỉ này đã được giả mạo thành địa chỉ của máy nạn nhân.Nạn nhân nhận được gói tin ICMP Echo Reply với số lượng quá lớn có thể dẫn đến hết tài nguyên và từ chối dịch vụ.



*Tấn công Smurf sử dụng gói ICMP làm ngập các giao tiếp khác.*

### Tấn công Ping Of Dead



*Mô phỏng tấn công Ping Of Death*

* **Khái niệm:**

Ping of death (hay còn gọi là PoD) là một dạng tấn công DoS, trong đó kẻ tấn công vào hệ thống máy tính bằng việc gửi lệnh ping không đúng định dạng hoặc độc hại đến một máy tính. Khiến hệ thống mất ổn định, đóng băng hoặc làm sập hệ thống trong một khoảng thời gian nhất định.

* **Cách thức hoạt động:**

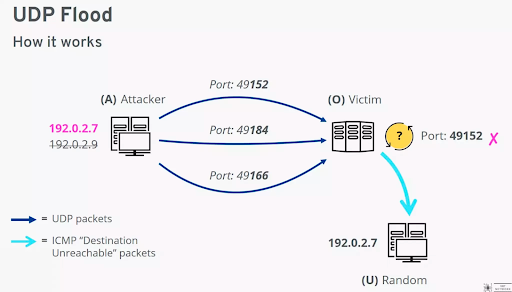
Kỹ thuật tấn công Ping of death thực hiện tấn công bằng cách dùng giao thức ICMP. Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của tin IP là 65.536 bytes Gói ICMP này sẽ được chia nhỏ ra để gửi đến máy tính của nạn nhân.Quá trình chia nhỏ gói tin IP thành những phần nhỏ được thực hiện ở layer II.Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.536 bytes. Những gói tin nhỏ này khi đến máy chủ sẽ lắp ráp lại thành một gói tin có kích thước quá lớn làm cho máy tính nhận được không quản lý nổi và như thế sẽ bị treo, một số máy sẽ bị ngưng hoạt động, bị reboot hoặc crash.

### Tấn công UDP Flood:

* **Khái niệm:**

Tấn công UDP FLood chính là một kiểu tấn công DDoS. Trong đó một số lượng lớn các packets User Datagram Protocol (UDP) được gửi đến server. Mục tiêu nhằm áp đảo khả năng xử lý và phản hồi của thiết bị. Firewall bảo vệ server mục tiêu cũng có thể bị cạn kiệt do UDP Flood. Dẫn đến DDoS với lưu lượng 1 cách hợp pháp.

* **Cách thức hoạt động:**



*Quy trình tấn công UDP Flood*

* Một kẻ tấn công sẽ gửi các gói tin UDP từ một địa chỉ IP giả mạo đến các port ngẫu nhiên trên máy chủ mục tiêu. Quy trình sau đây phải được lặp lại cho mỗi gói tin đến.
* Lúc này, máy chủ sẽ kiểm tra các ứng dụng với cổng và thấy rằng không có ứng dụng nghe ở cổng nên sẽ trả lời với một gói ICMP “không thể truy cập".
* Hệ thống bị buộc phải nhận nhiều gói tin ICMP nên sẽ mất khả năng xử lý các yêu cầu của người dùng thực hoặc khách hàng truy cập hợp pháp khác.

### Tấn công Http Flood

* **Khái niệm:**

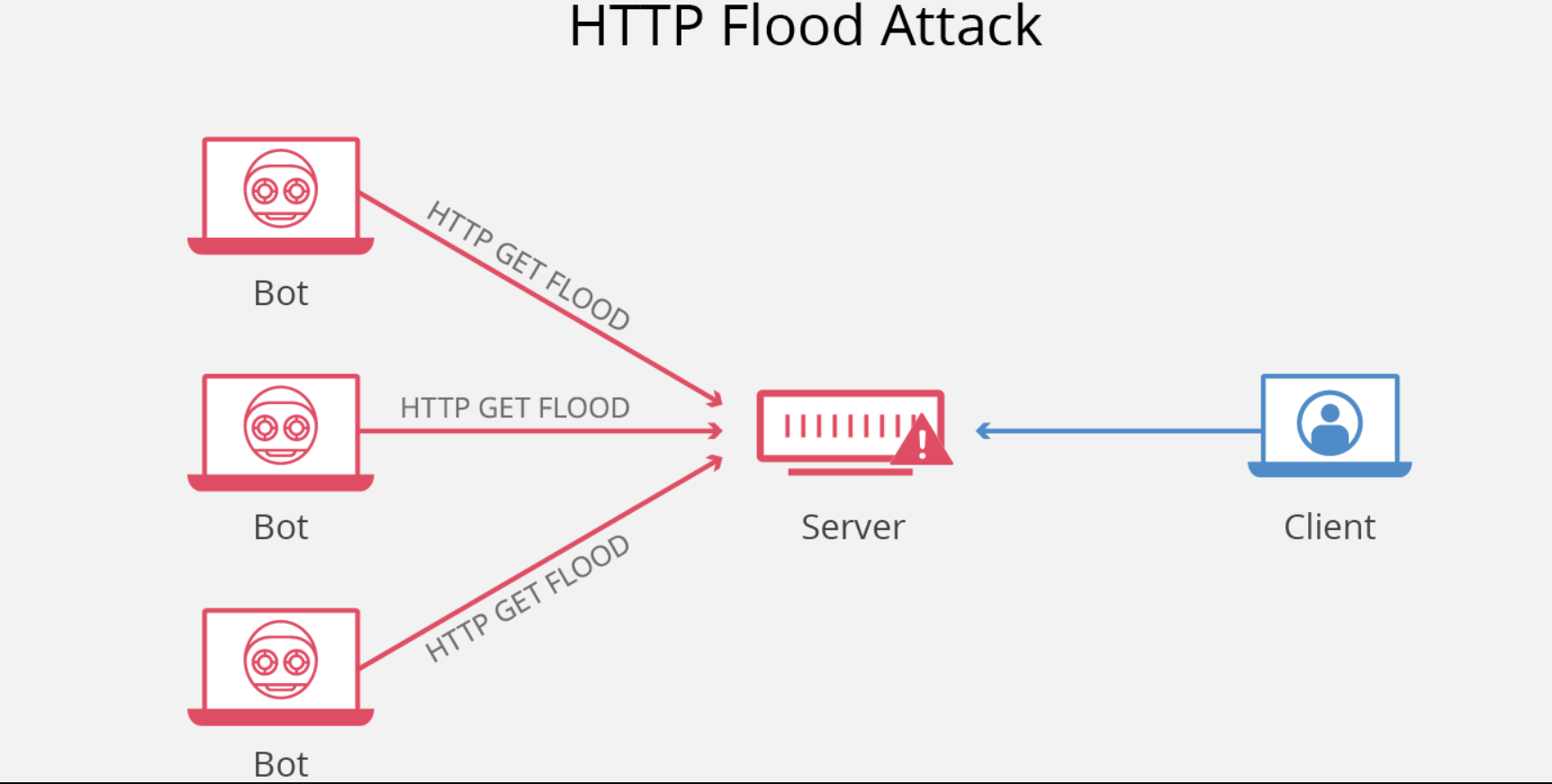
HTTP flood là một kiểu tấn công Distributed Denial of Service (DDoS - từ chối dịch vụ phân tán), trong đó kẻ tấn công khai thác các yêu cầu HTTP GET hoặc POST có vẻ hợp pháp để tấn công máy chủ web hoặc ứng dụng.

* **Cách thức hoạt động:**

Các cuộc tấn công HTTP flood là một loại tấn công “layer 7”. “layer 7” là một ứng dụng của [mô hình OSI](https://bkhost.vn/posts/mo-hinh-osi-la-gi) và liên quan đến các giao thức trên internet như HTTP, HTTPS, … Cụ thể, HTTP chính là cơ sở của các yêu cầu trên internet dựa vào trình duyệt và được dùng để tải các website,…

Khi một client HTTP như trình duyệt web “giao tiếp” với ứng dụng web hoặc máy chủ thì nó sẽ gửi một yêu cầu HTTP và thường là một trong hai loại yêu cầu: GET hoặc POST.

* **GET flood:**Yêu cầu GET thường được sử dụng để truy xuất các nội dung tĩnh như hình ảnh. Thông thường, điều này gây ra yêu cầu tải tương đối thấp trên máy chủ.
* **POST flood:** Các yêu cầu POST có nhiều khả năng yêu cầu máy chủ thực hiện một số loại xử lý để truy cập các tài nguyên động, chẳng hạn như tìm kiếm các mục trong cơ sở dữ liệu. Do đó, các cuộc tấn công HTTP POST flood thường yêu cầu tải cao hơn lên máy chủ.



*Mô hình tấn công Http Flood*

Cuộc tấn công HTTP flood sẽ có hiệu quả khi nó buộc máy chủ hoặc ứng dụng web **cung cấp tài nguyên tối đa** để có thể đáp ứng các yêu cầu. Vì vậy, kẻ tấn công sẽ nhắm tới mục đích làm “tràn ngập” máy chủ hoặc ứng dụng web với số lượng lớn yêu cầu, mỗi yêu cầu phải càng sử dụng nhiều tài nguyên thì cuộc tấn công càng lớn mạnh.

## Phương pháp phát hiện tấn công DoS

Có nhiều cách để phát hiện và phòng tránh tấn công DoS/DDoS. Dưới đây là những dấu hiệu nhận biết:

**+** Băng thông sụp giảm nghiêm trọng.

+ Website, hệ thống bị sập hoàn toàn.

+ Lưu lượng truy cập bất thường.

+ Mất kết nối đột ngột với các thiết bị cùng mạng.

## Phương pháp phòng chống tấn công DoS

Nhìn chung, tấn công từ chối dịch vụ không quá khó thực hiện, nhưng rất khó phòng chống do tính bất ngờ và thường là phòng chống trong thế bị động khi sự việc đã rồi. Việc đối phó bằng cách tăng cường “phần cứng” cũng là giải pháp tốt, nhưng thường xuyên theo dõi để phát hiện và ngăn chặn kịp thời cái gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất.

* Sử dụng các CDN để giảm thiểu ảnh hưởng của tấn công Dos.
* Nâng cấp dịch vụ Hosting.
* Mô hình hệ thống cần phải được xây dựng hợp lý, tránh phụ thuộc lẫn nhau quá mức. Bởi khi một bộ phận gặp sự cố sẽ làm ảnh hưởng tới toàn bộ hệ thống
* Thiết lập các mức xác thực đối với người sử dụng cũng như các nguồn tin trên mạng. Đặc biệt, nên thiết lập chế độ xác thực khi cập nhật các thông tin định tuyến giữa các router.
* Xây dựng hệ thống lọc thông tin trên router, firewall… và hệ thống bảo vệ chống lại SYN flood.
* Chỉ kích hoạt các dịch vụ cần thiết, tạm thời vô hiệu hoá và dừng các dịch vụ chưa có yêu cầu hoặc không sử dụng.
* Xây dựng hệ thống định mức, giới hạn cho người sử dụng, nhằm mục đích ngăn ngừa trường hợp người sử dụng ác ý muốn lợi dụng các tài nguyên trên server để tấn công chính server hoặc mạng và server khác.
* Sử dụng các biện pháp kiểm tra hoạt động của hệ thống một cách liên tục để phát hiện ngay những hành động bất bình thường.
* Xây dựng và triển khai hệ thống dự phòng.
* Dùng tính năng lọc dữ liệu của router/firewall để loại bỏ các packet không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.
* Nếu bị tấn công do lỗi của phần mềm hay thiết bị thì nhanh chóng cập nhật các bản sửa lỗi cho hệ thống đó hoặc thay thế.
* Giới hạn số kết nối website tại một thời điểm: Khi một khách truy cập vào website thì sẽ tạo ra một truy vấn kết nối với cơ sở dữ liệu (CSDL) lấy thông tin và trả về thông qua hiển thị của website. Mỗi máy chủ sẽ có phép bao nhiêu truy vấn kết nối là hạn định và khi vượt quá hạn mức này thì việc truy cập sẽ khó khăn hoặc không thể truy xuất được. Các tin tặc lợi dụng vào điều này để tạo ra các truy cập ảo, kết nối ảo thông qua proxy hay chuyên nghiệp hơn là mạng botnet nhằm đánh sập trang web và phá hỏng CSDL website. Để hạn chế điều này ta có thể chủ động giới hạn số kết nối truy vấn tin (lượt truy cập) cùng một thời điểm.

# CHƯƠNG 3: THỰC HIỆN TẤN CÔNG DOS

Có rất nhiều phương thức tấn công Dos như đã viết ở trên. Trong báo cáo này sẽ sử dụng 3 phương thức chính để tấn công gồm: HTTP Flood, UDP Flood, SYN Flood.

Để thực hiện cuộc tấn công DoS, ta sử dụng 1 máy attacker Kali Linux có địa chỉ IP: 192.168.255.128 tấn công vào Server Victim của máy Centos 7 có địa chỉ IP: 192.168.255.129 được mô tả như hình sau:



* Thông tin thêm:

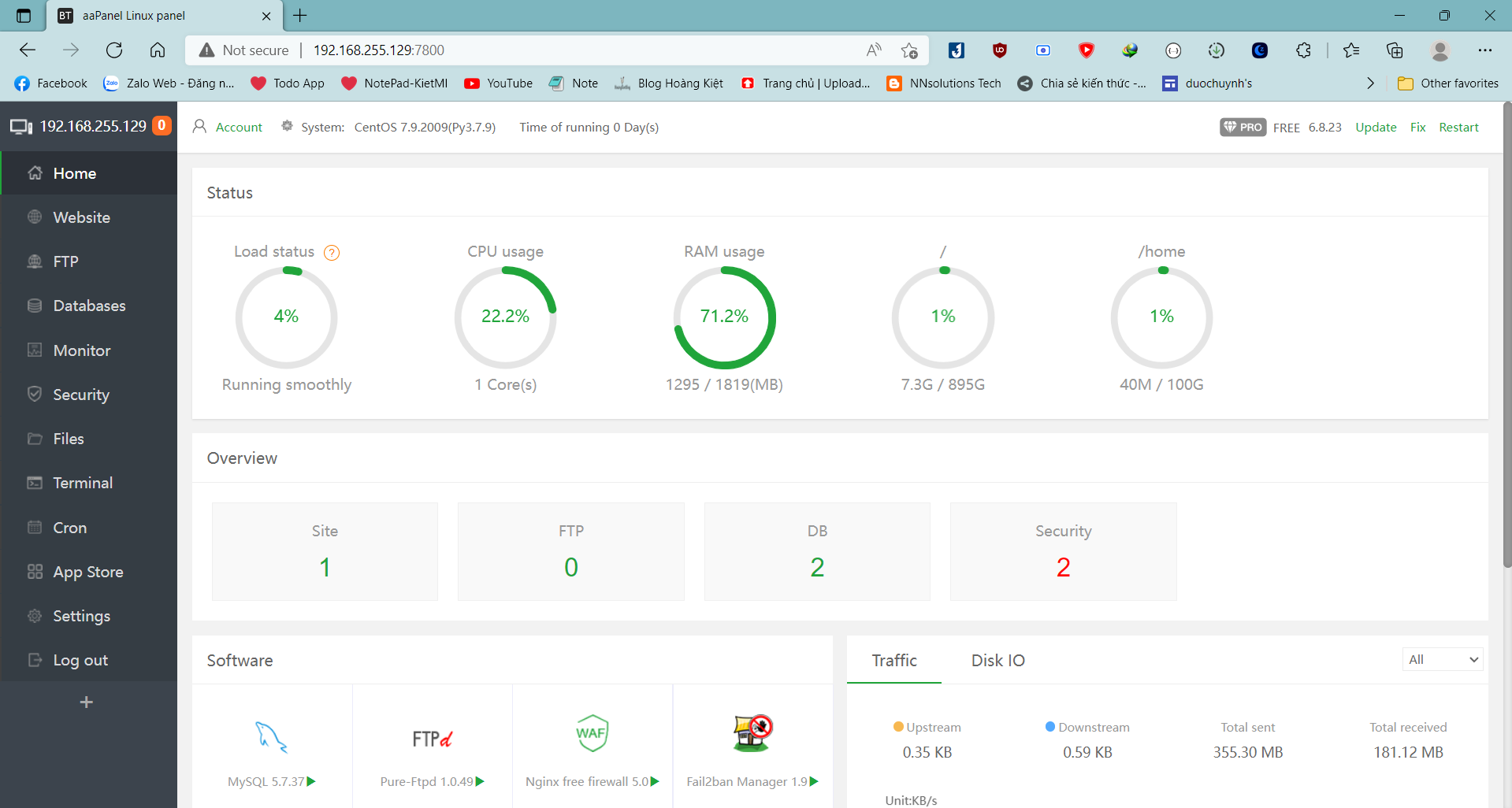
+ Máy Attacker và máy VicTim được kết nối cùng mạng.

+ Máy Attacker cài phần mềm WireShark để tìm ra địa chỉ IP của mục tiêu.

+ Máy VicTim cài dịch vụ web và quản lý bằng aaPanel.

## Sử dụng phương thức HTTP Flood ( Application Layer Attack ):

* Hiện tại có rất nhiều phần mềm hỗ trợ tấn công HTTP Flood, để đạt được hiệu quả cao sẽ sử dụng công cụ Overload Layer 7 của [7zx](https://github.com/7zx/overload) (<https://github.com/7zx/overload>).



*Hình ảnh Server nạn nhân trước khi bị tấn công*

Thực hiện tấn công trên máy attacker Kali linux:

B1: Tải Overload từ github về sử dụng lệnh git

git clone <https://github.com/7zx/overload>

B2: Các bạn vào thư mục của Overload bằng cách nhập

cd overload

B3: Ghi lệnh sau để tải PIP cần thiết:

pip3 install -r requirements.txt

B4: Sử dụng Overload:

Cú pháp câu lệnh:

python3 overload.py [-h] [--target <URL>] [--method <HTTP>] [--time <time>]  
[--threads <threads>]

**Trong đó**

-**h** hay **-help**: hiển thị mục help của overload

**-target <URL>**: mục tiêu mà bạn muốn nhắm tới

**-method <HTTP>**: kiểu tấn công

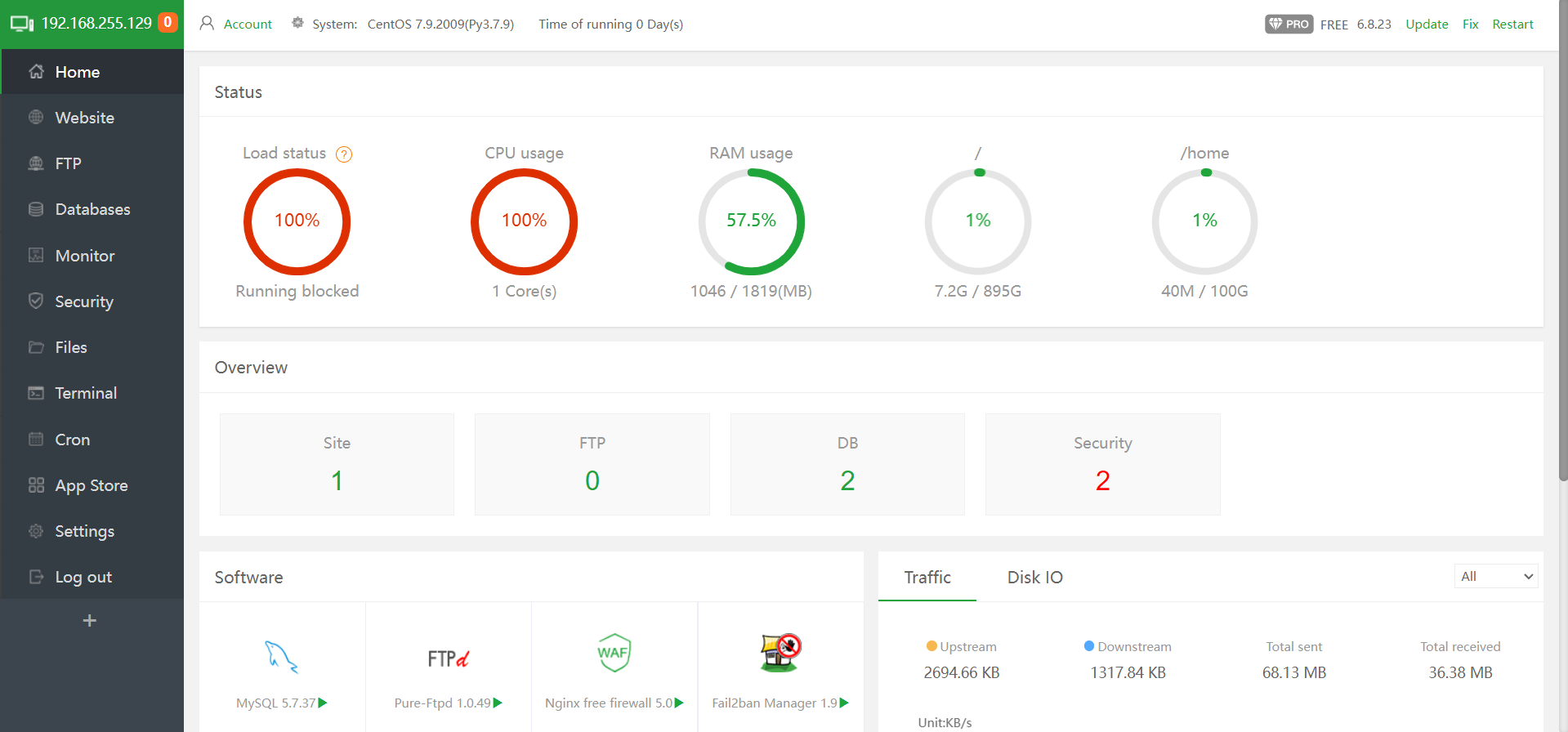
**-time <giây>**: Thời gian chạy tool

**--thread <luồng>**: số luồng trên giây

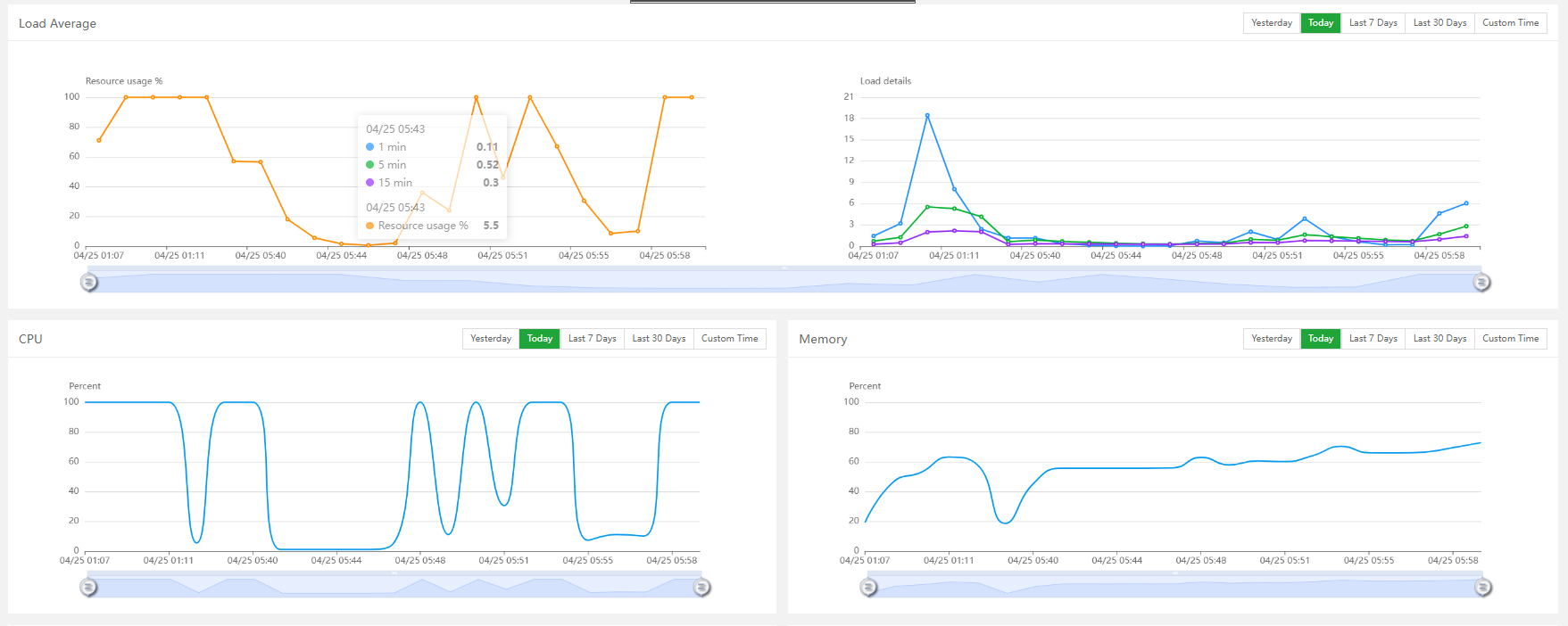
Ví dụ ở đây ta tấn công VicTim có IP: 192.168.255.129 với kiểu tấn công HTTP, thời gian chạy tool là 500 giây, số luồng là 10000 thì câu lệnh như sau

python3 overload.py --time 5000 --threads 10000 --target http://192.168.255.129/ --method HTTP

Kết quả là server nạn nhân sẽ quá tải:

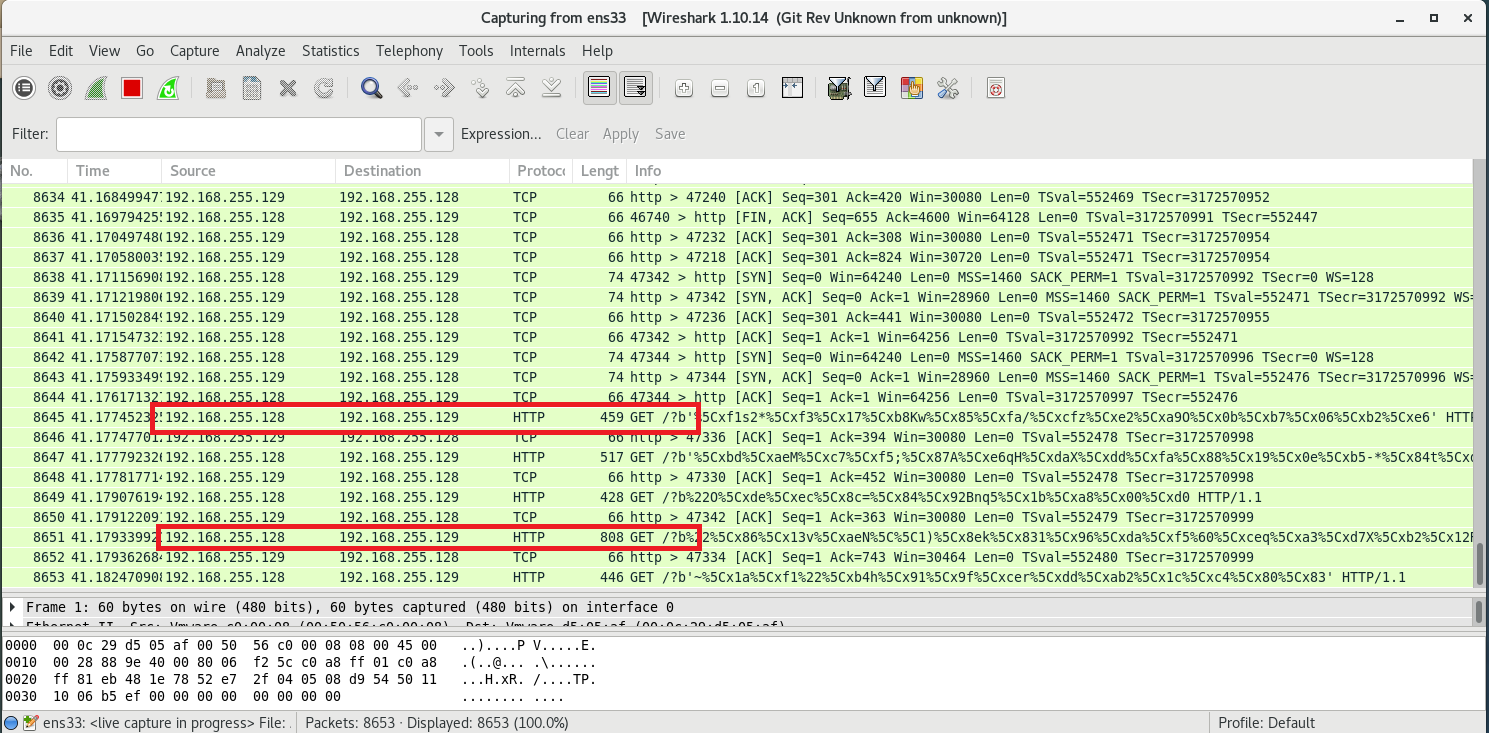


*Hình ảnh Server nạn nhân đang bị tấn công*

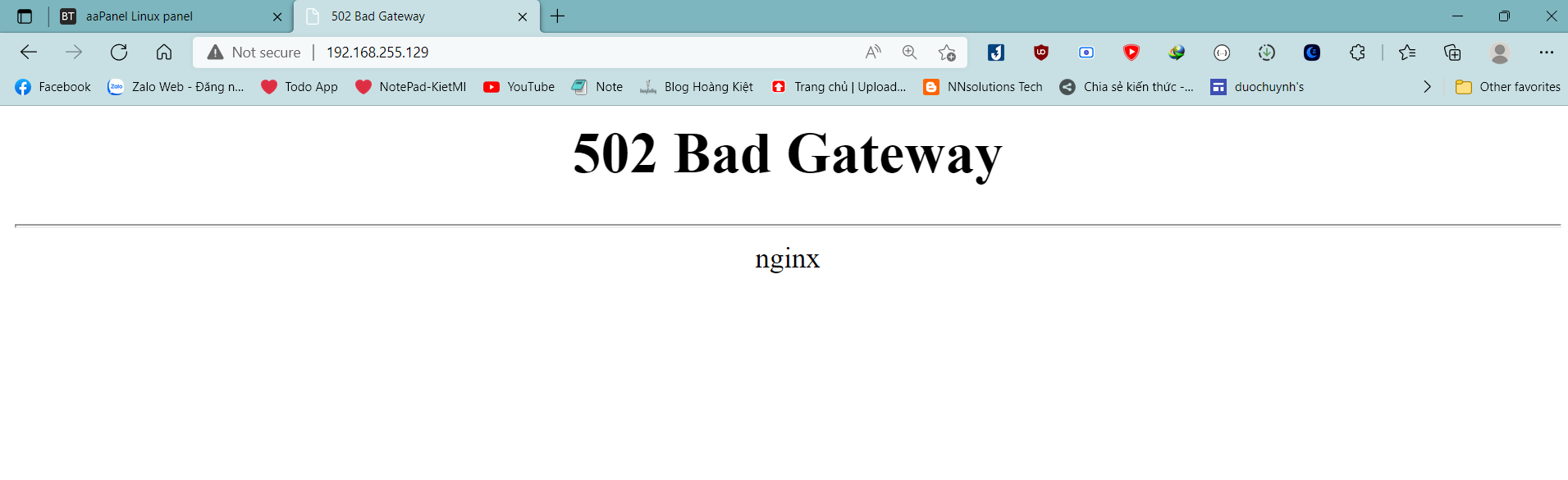


*Hình ảnh Server nạn nhân đang bị tấn công*

Dùng WireShark trên máy VICTIM để kiểm tra kết quả ta thấy rất nhiều gói tin được gửi từ IP của máy Attacker sang máy nạn nhân Victim làm quá tải hệ thống gây ra vượt quá số lượng HTTP request nó thì có thể gây ra gián đoạn trong việc truy cập website của người dùng hay cụ thể là không thể kết nối tới trang Web. Khi đó máy chủ sẽ phản hồi với lỗi những lỗi 5XX. Các lỗi 5XX có thể gặp bao gồm: 500 tới 505.



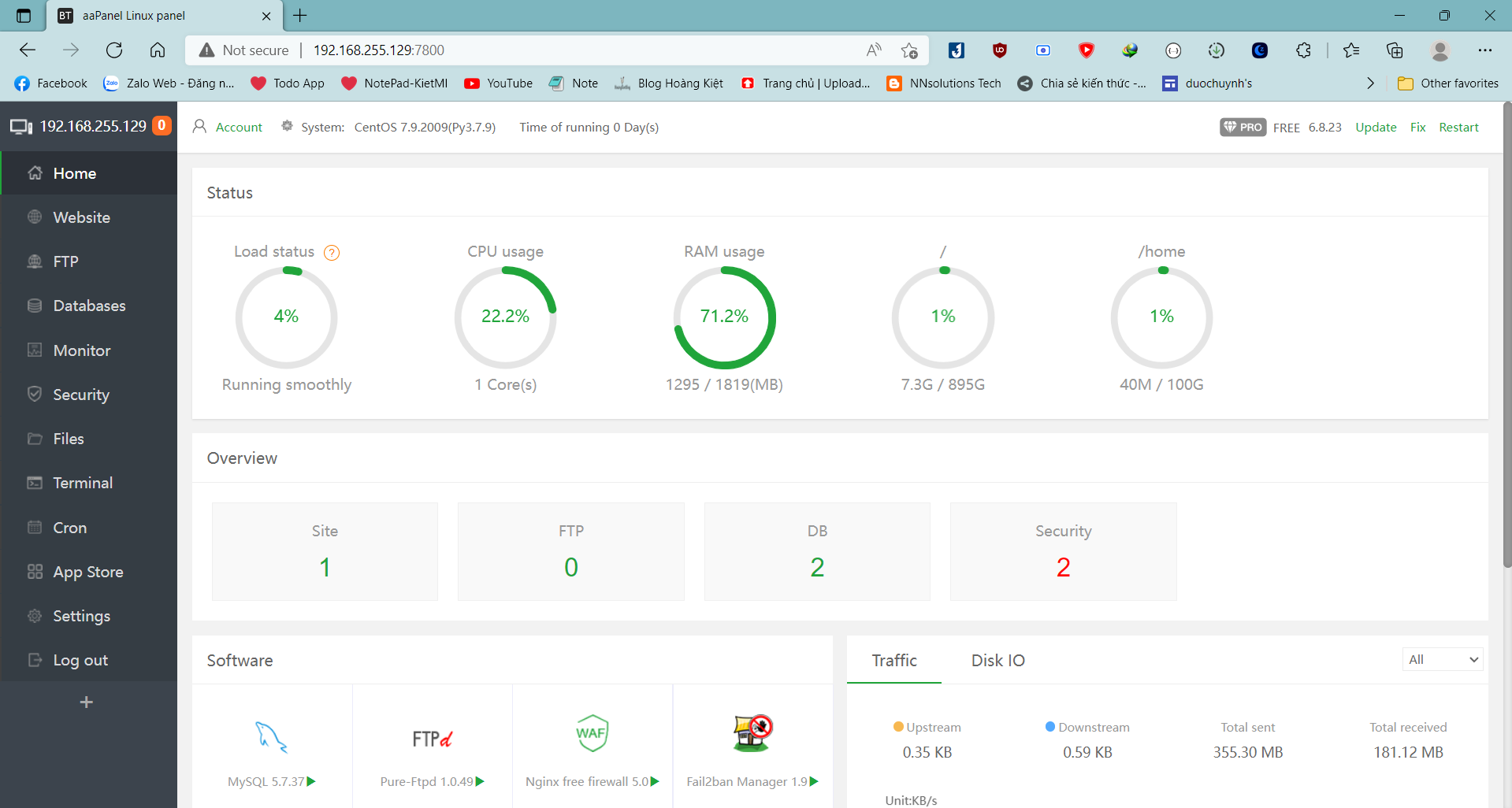
*HÌnh ảnh dùng WireShark bắt gói tin trên máy VicTim*



*Hình ảnh máy Server nạn nhân quá tải gây ra lỗi 502 Bad Gateway*

## Sử dụng phương thức SYN Flood ( Protocol Attacks ):

Chúng ta sẽ dùng Kali Linux để tấn công máy nạn nhân Centos 7 (192.168.255.128) bằng Metasploit Framework. Cũng dùng bộ lọc WireShark để kiểm tra gói tin trên máy nạn nhân.



*Hình ảnh Server nạn nhân trước khi bị tấn công.*

Quy trình tấn công:

B1: Sử dụng lệnh **nmap** để quét các port đang mở trên máy nạn nhân. Chúng ta sẽ quét port 21:

nmap –p 192.168.255.128

B2: Nhập lệnh “**msfconsole**” để khởi chạy **Metasploit framework**

B3: Nhập dòng lệnh “**use auxiliary/dos/tcp/synflood**”

B4: Nhập các dòng lệnh sau:

set RHOST 192.168.255.128

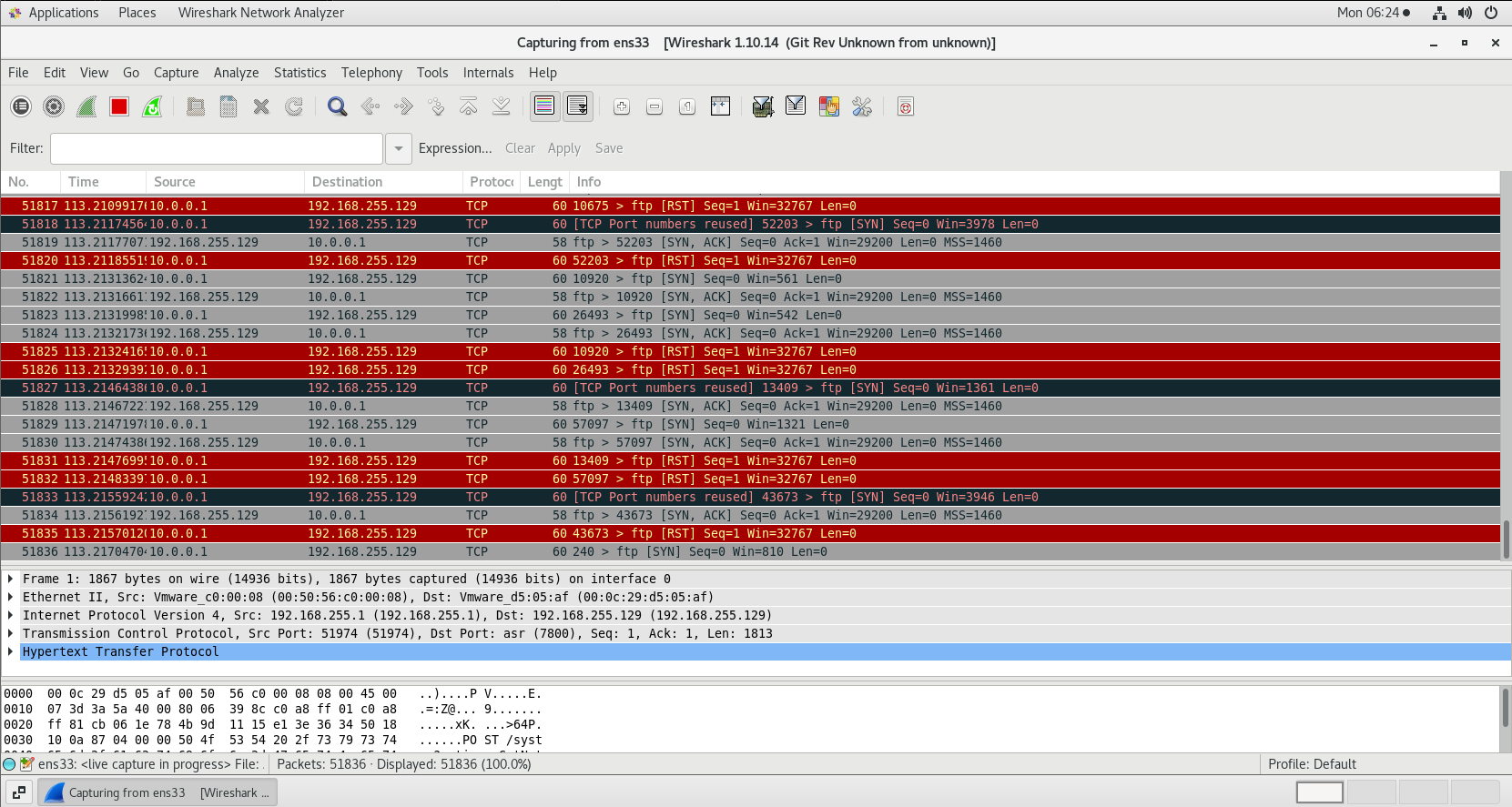
set RPORT 21

set SHOST 10.0.0.1

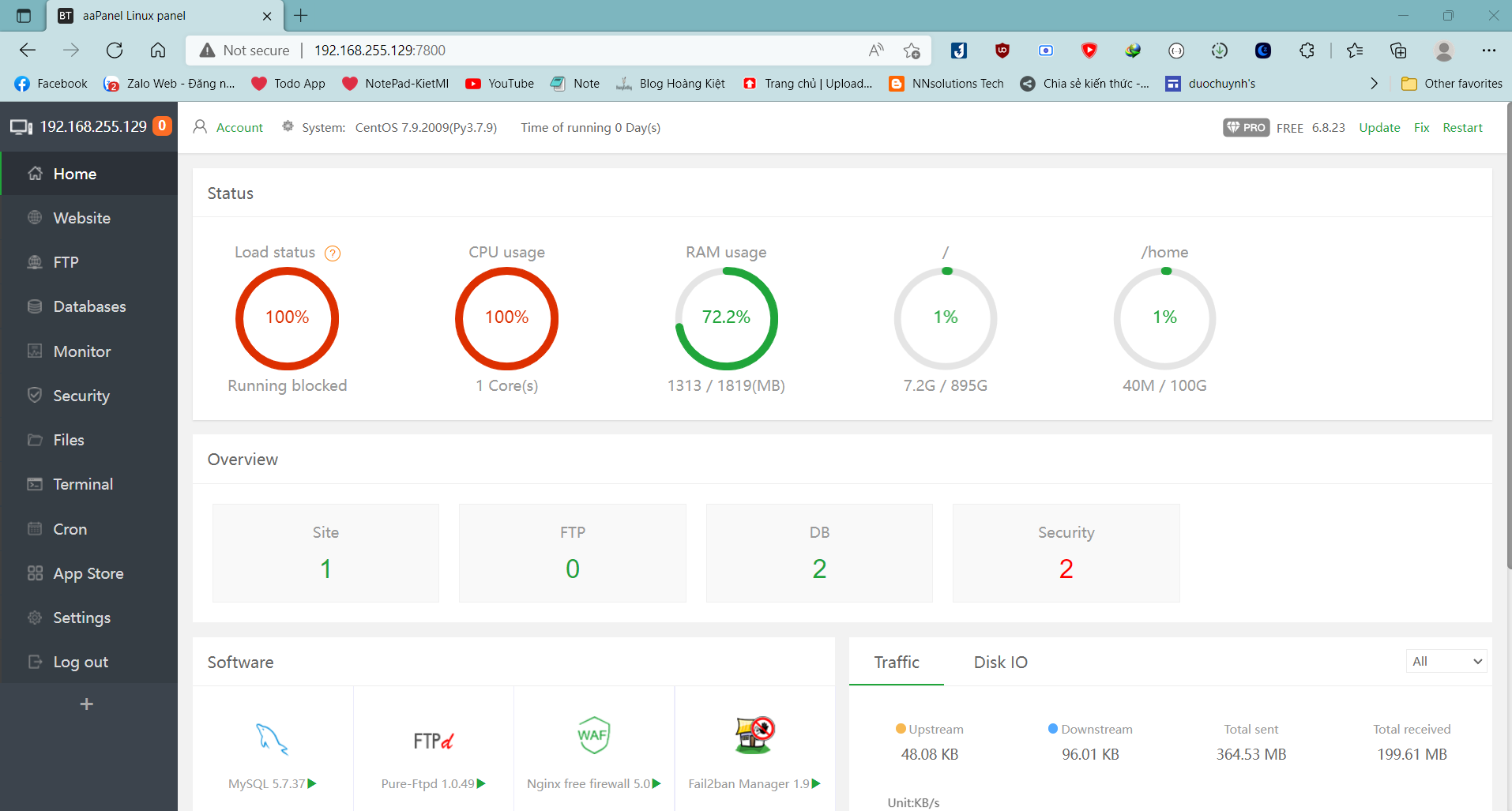
set TIMEOUT 30000

B5: Nhập dòng lệnh “**exploit**”. Tấn công tràn SYN đã được bắt đầu.

Dùng WireShark để bắt gói tin trên máy nạn nhân ta thu được kết quả:

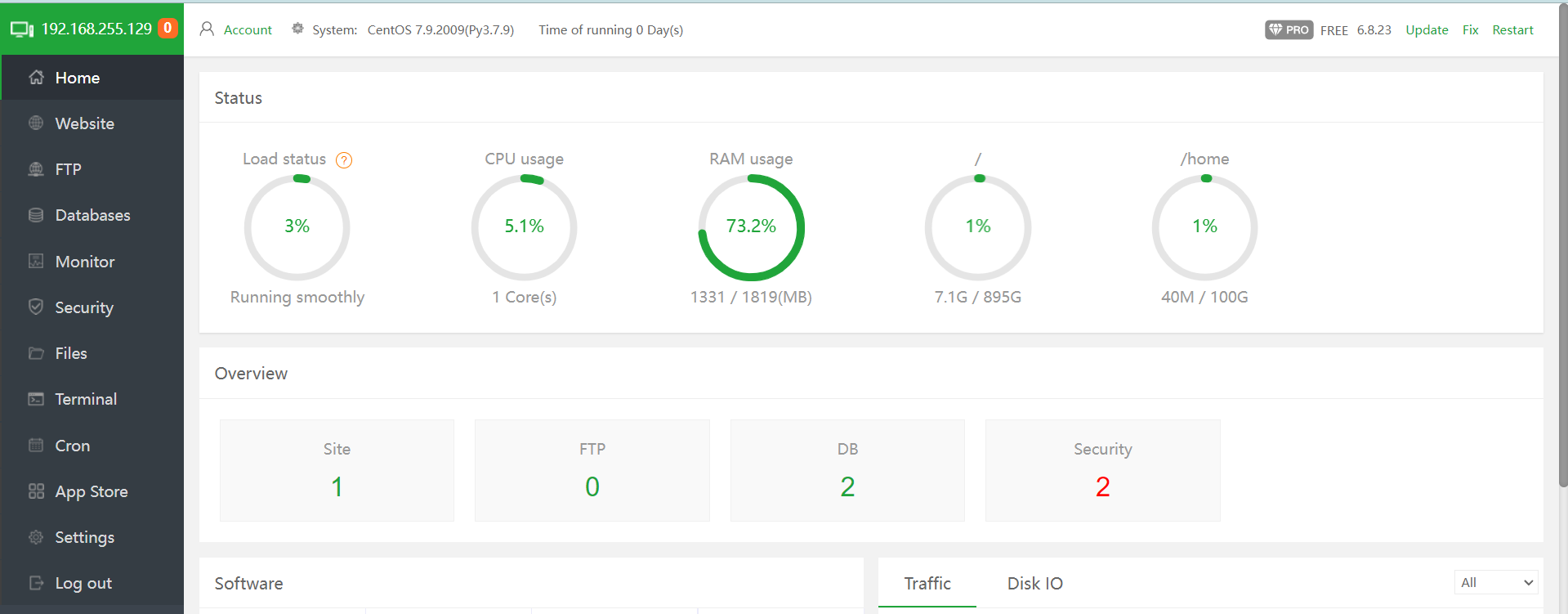


*Hình ảnh WireShark máy nạn nhân đang bị tân công bằng SYN Flood*



*Hình ảnh máy nạn nhân sau khi bị tấn công*

## Sử dụng phương thức UDP Flood ( Volumetric Attack ):

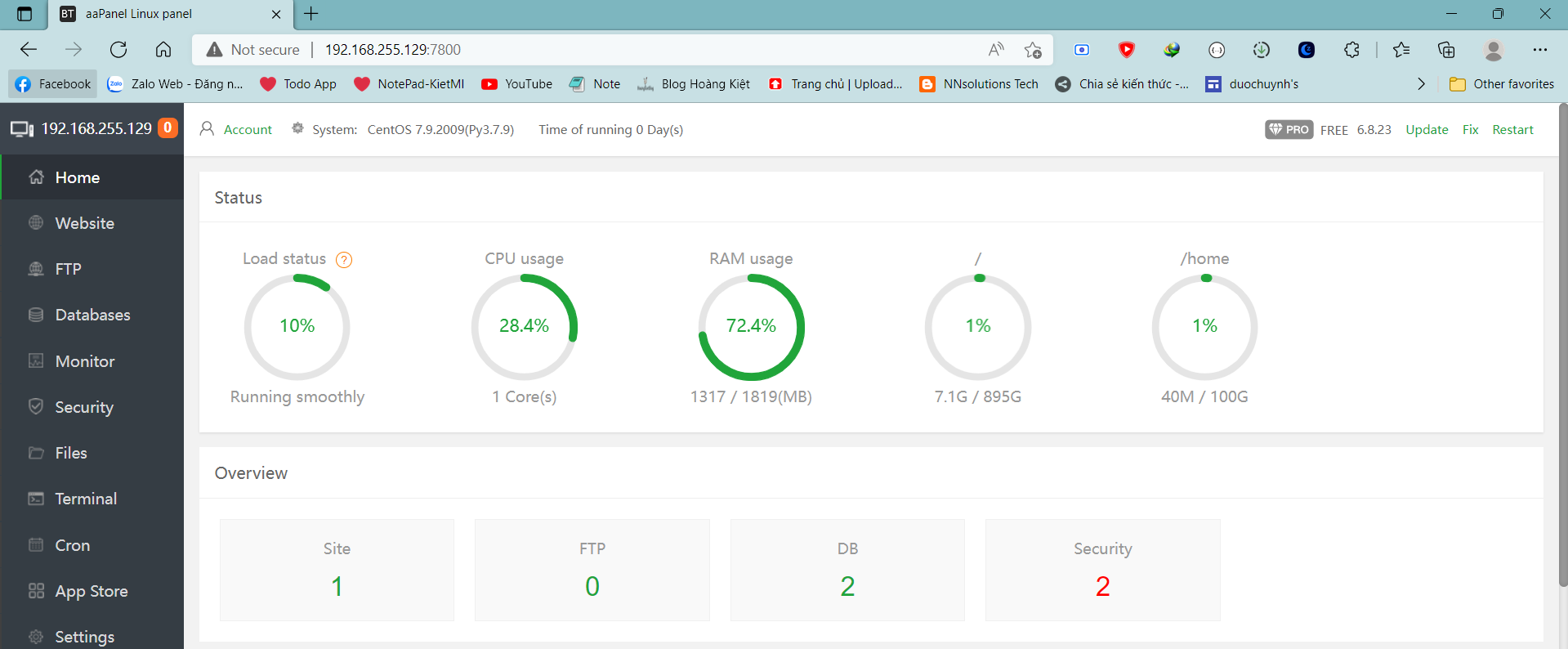
****

*Hình ảnh Server nạn nhân trước khi tấn công*

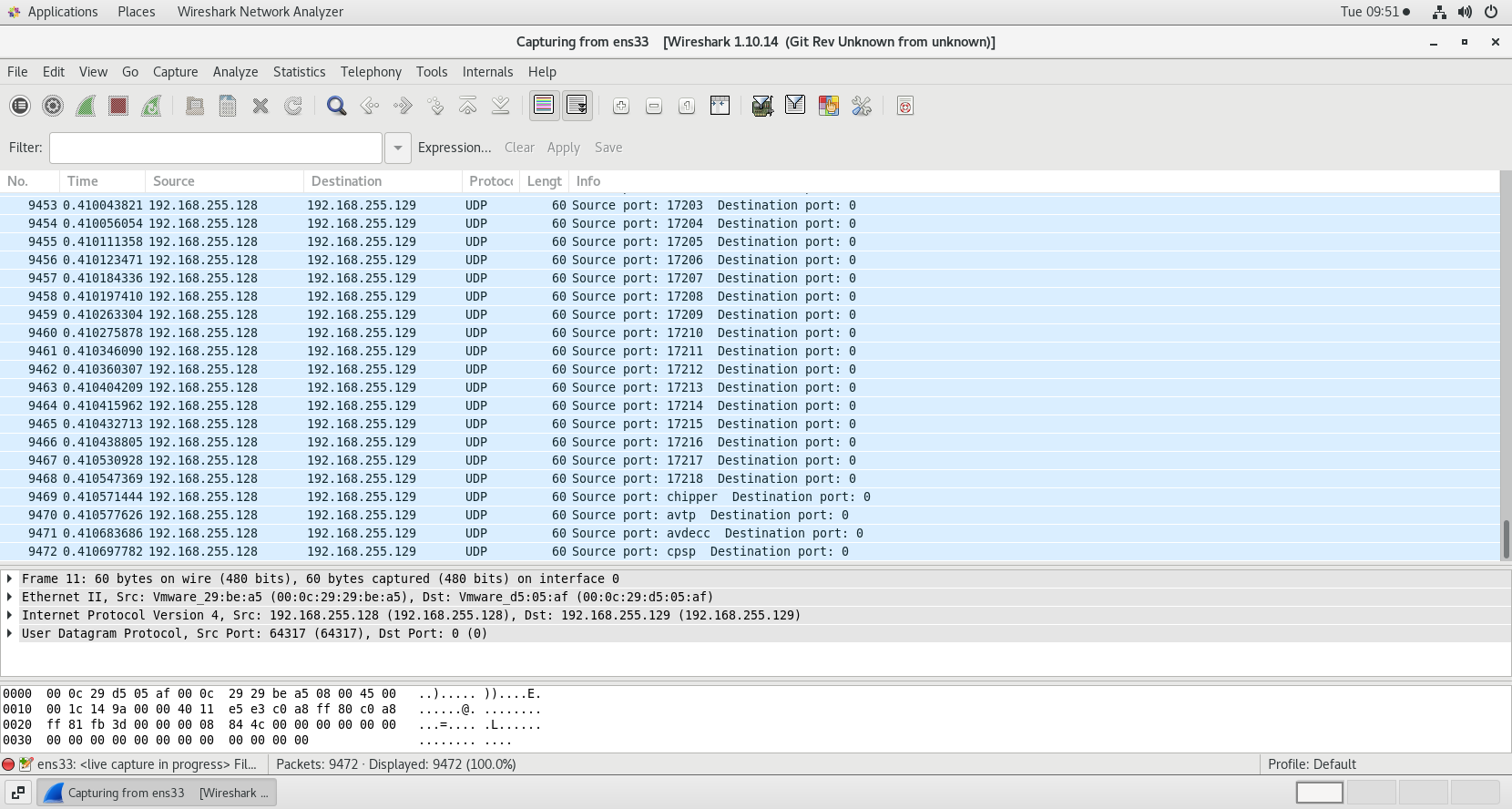
B1: Mở Kali Linux Terminal.

B2: Nhập lệnh “**hping3 -2 -–flood 192.168.255.129**”

B3: UPD đã bắt đầu.



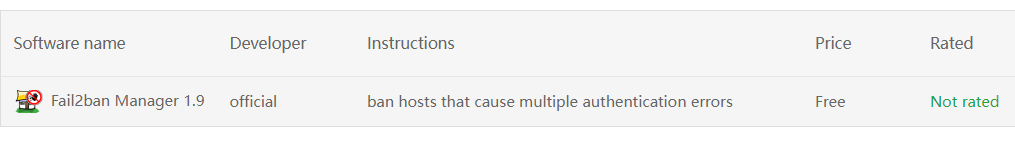
*Hình ảnh Server sau khi bị tấn công*



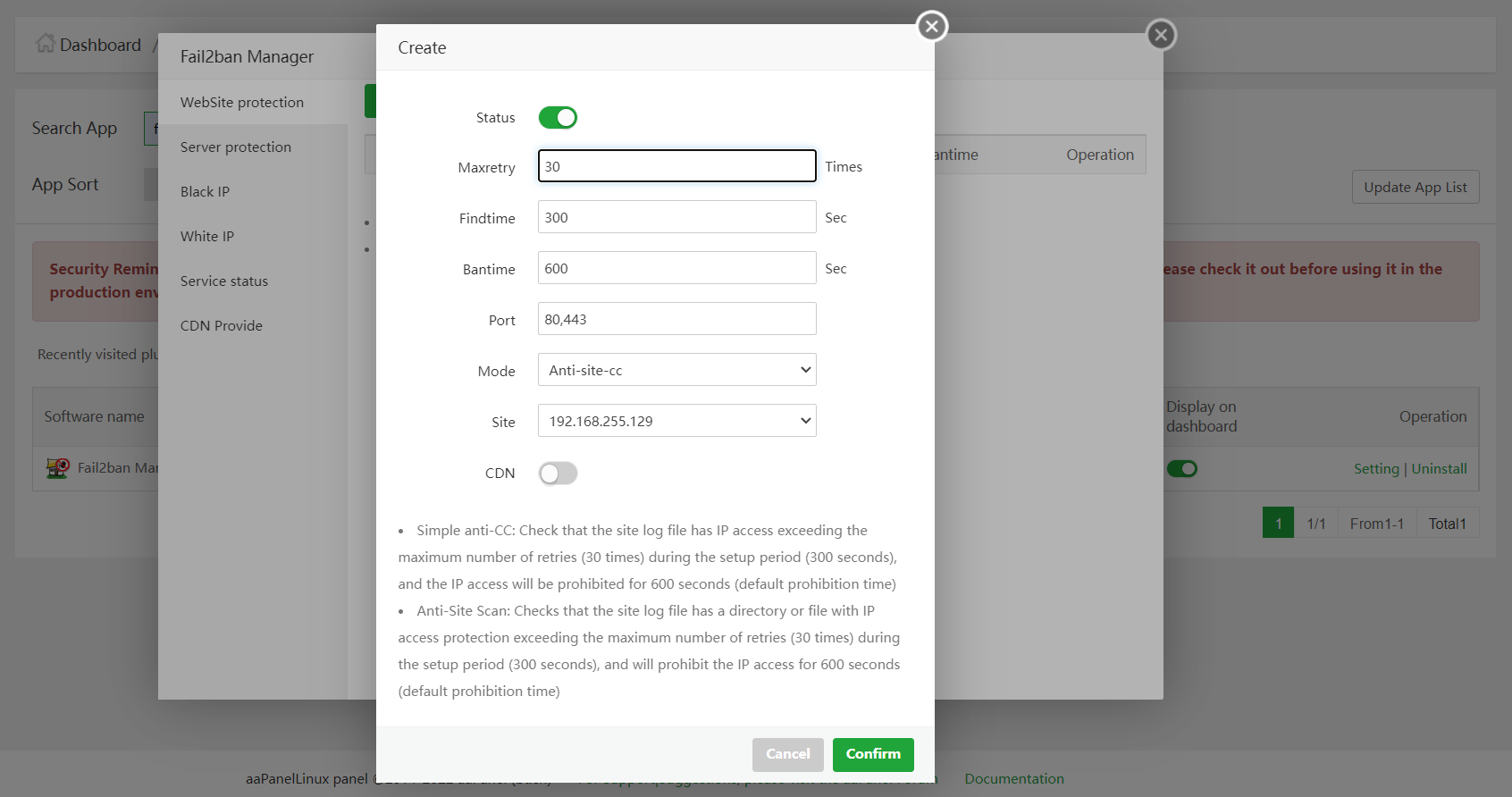
*Hình ảnh WireShark máy nạn nhân đang bị tân công bằng UDP Flood*

## Phương pháp phòng chống

**Không có phương pháp phòng chống nào là tốt nhất**, tuy nhiên để hạn chế việc tấn công dos ta cài phần mềm có sẵn trên aapanel đó là **Fail2Ban**:



Chúng ta sẽ tạo 1 role dành cho website:



Status: trạng thái ( Bật / tắt ).

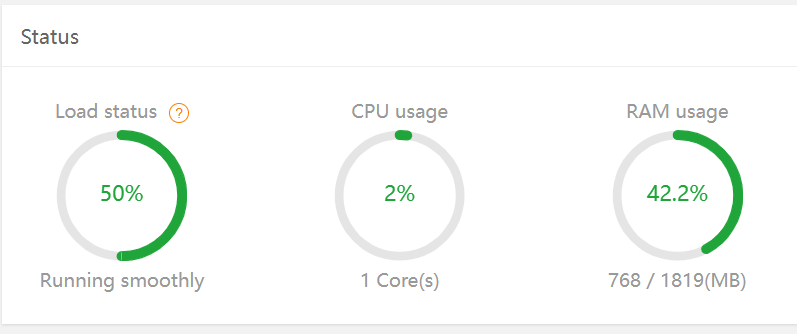
Maxretry: Số lần truy cập.

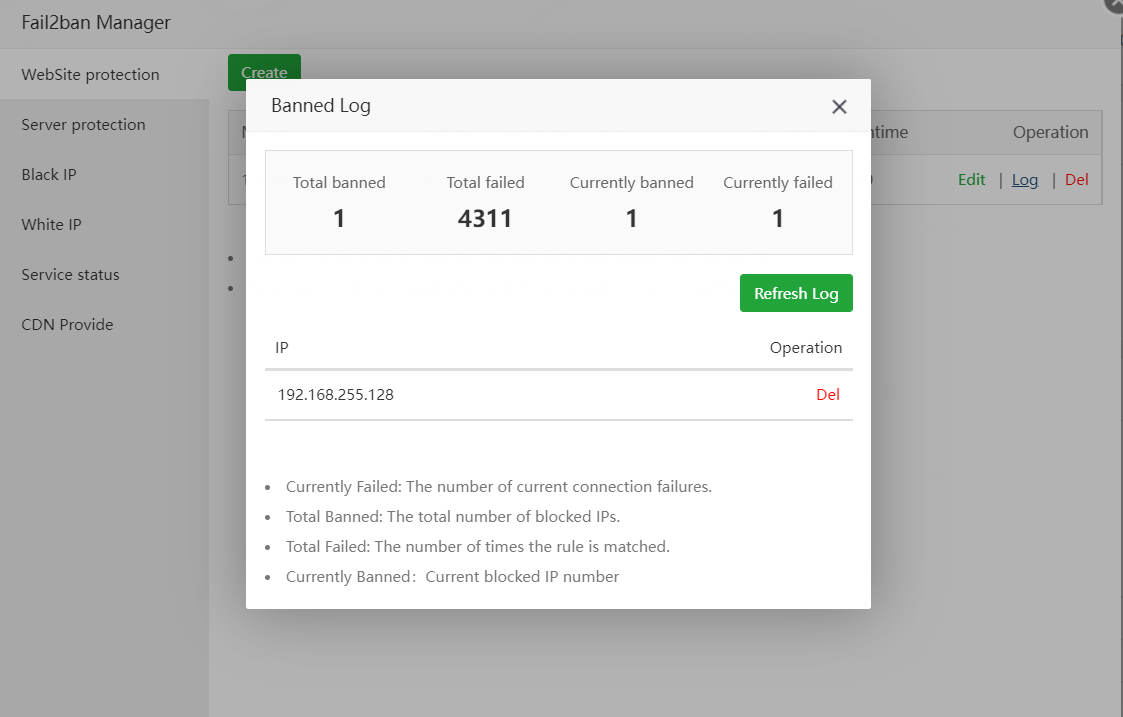
Bantime : Thời gian chặn try cập

Port: Các port áp dụng

Site: Lựa chọn trang web cần phòng chống

Sau đây là là hình ảnh Fail2Ban ngăn chặn tấn công **HTTP Flood** dựa trên công cụ **OverLoad**:





*IP máy Attacker đã được chặn bởi Fail2Ban.*

# KẾT LUẬN

Nhìn chung, tấn công từ chối dịch vụ không quá khó thực hiện, nhưng rất khó phòng chống do tính bất ngờ và thường là phòng chống trong thế bị động khi sự việc đã rồi. Việc đối phó bằng cách tăng cường “phần cứng” cũng là giải pháp tốt, nhưng thường xuyên theo dõi để phát hiện và ngăn chặn kịp thời cái gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất.

Tùy mô hình, quy mô cụ thể của hệ thống mà có các biện pháp bảo vệ, phòng chống khác nhau.

DoS, DDoS, DRDoS đang và sẽ là vấn nạn nguy hại lớn cho nền Internet toàn cầu. Tuy nhiên có thể loại trừ nó ra khỏi mạng internet hiện nay là rất khó. Có rất nhiều việc phải làm và chuẩn bị để kiểm soát được DDoS. Chúng ta phải có những bước đi cụ thể & mạnh mẽ hơn để cùng khống chế loại hình tấn công nay.

# TÀI LIỆU THAM KHẢO

[1] viettelidc, "Tìm hiểu về tấn công từ chối dịch vụ DoS," [Online]. Available: https://viettelidc.com.vn/tin-tuc/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos. [Accessed 22 4 2022].

[2] Wikipedia, "Tấn công từ chối dịch vụ," [Online]. Available: https://vi.wikipedia.org/wiki/T%E1%BA%A5n\_c%C3%B4ng\_t%E1%BB%AB\_ch%E1%BB%91i\_d%E1%BB%8Bch\_v%E1%BB%A5. [Accessed 22 4 2022].

[3] blogchiasekienthuc, "Dos – DDos là gì? Hacker tấn công DDos bằng cách nào?," [Online]. Available: https://blogchiasekienthuc.com/dan-cong-nghe/dos-ddos-la-gi-hacker-tan-cong-ddos-bang-cach-nao.html. [Accessed 22 4 2022].

[4] quantrimang, "Tấn công từ chối dịch vụ DoS và DDoS là gì? Tác hại của chúng ra sao?," [Online]. Available: https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926. [Accessed 22 4 2022].