

NỘI DUNG SÁNG KIẾN KINH NGHIỆM

1. Trình bày khái niệm về DDoS

Tấn công từ chối dịch vụ là sự cố gắng có chủ đích rõ ràng của một người hay nhiều người với mục đích làm gián đoạn, hoặc làm cho hệ thống(dịch vụ từ máy chủ) đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Còn theo định nghĩa từ wikipedia: Là một phương thức tấn công phổ biến kéo theo sự bão hoà máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đáp ứng giao thông hợp pháp, hoặc đáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.

Tấn công từ chối dịch vụ là sự vi phạm chính sách sử dụng internet của IAB (Internet Architecture Board) và những người tấn công hiển nhiên vi phạm luật dân sự.

2. Phương thức hoạt động từ chối dịch vụ trong DDoS : Một cuộc tấn công DDoS yêu cầu kẻ tấn công giành quyền kiểm soát mạng lưới các máy trực tuyến để thực hiện một cuộc tấn công. Máy tính và các máy khác (như thiết bị IoT) bị nhiễm phần mềm độc hại, biến chúng thành bot (hoặc zombie). Kẻ tấn công sau đó có quyền điều khiển từ xa đối với nhóm bot, được gọi là botnet.

Khi botnet đã được thiết lập, kẻ tấn công có thể điều khiển các máy bằng cách gửi các hướng dẫn cập nhật tới từng bot thông qua một phương pháp điều khiển từ xa. Khi địa chỉ IP của nạn nhân bị botnet nhắm mục tiêu, mỗi bot sẽ phản hồi bằng cách gửi yêu cầu đến mục tiêu, có khả năng khiến máy chủ hoặc mạng được nhắm mục tiêu tràn dung lượng, dẫn đến việc từ chối dịch vụ đối với lưu lượng truy cập bình thường. Bởi vì mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng thông thường là rất khó khăn.

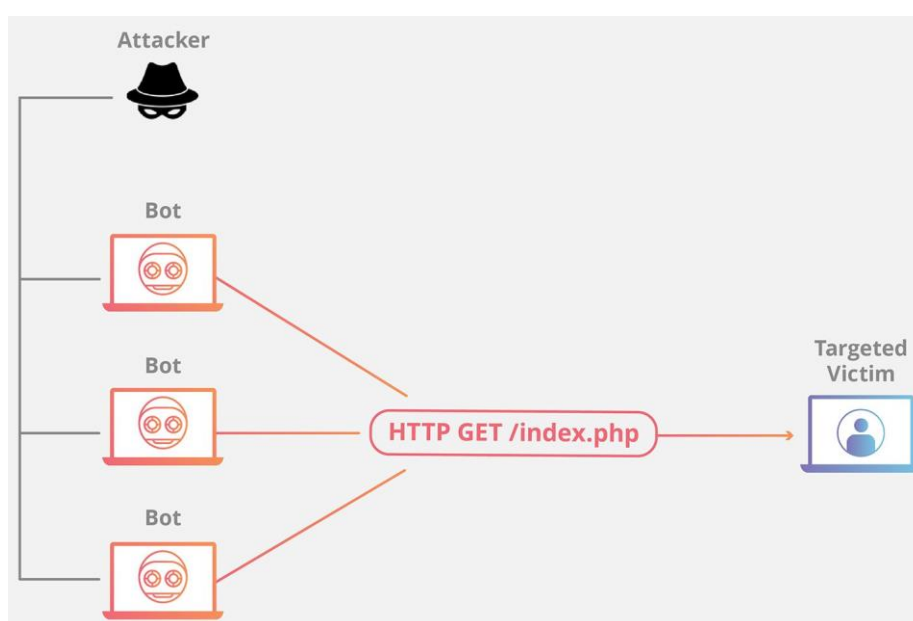
3. Các loại tấn công DDoS phổ biến:

Tấn công từ chối dịch vụ DDoS khác nhau nhắm vào các thành phần khác nhau của kết nối mạng. Để hiểu cách thức các cuộc tấn công DDoS khác nhau hoạt động, cần phải biết cách kết nối mạng được thực hiện. Một kết nối mạng trên Internet bao gồm nhiều thành phần khác nhau hoặc các lớp (layers) khác nhau. Giống như xây dựng một ngôi nhà từ mặt đất lên, mỗi bước trong mô hình có một mục đích khác nhau. Mô hình OSI (phí bên dưới), là một khung khái niệm được sử dụng để mô tả kết nối mạng trong 7 lớp riêng biệt.

3.1. Tấn công lớp ứng dụng

Đôi khi được gọi là một cuộc tấn công DDoS lớp 7 (liên quan đến lớp thứ 7 của mô hình OSI), mục tiêu của các cuộc tấn công này là làm cạn kiệt tài nguyên của mục tiêu. Các cuộc tấn công nhắm vào lớp nơi các trang web được tạo trên máy chủ và được phân phối theo yêu cầu HTTP. Một yêu cầu HTTP duy nhất, đơn giản khi thực hiện ở phía máy khách và có thể tốn kém cho máy chủ mục tiêu đáp ứng vì máy chủ thường phải tải nhiều tệp và chạy các truy vấn cơ sở dữ liệu để tạo trang web. Các cuộc tấn công lớp 7 rất khó để bảo vệ vì lưu lượng có thể khó ngăn cản là độc hại.

Ví dụ về cuộc tấn công lớp ứng dụng:



Cuộc tấn công này tương tự như việc nhấn làm mới trong trình duyệt web nhiều lần trên nhiều máy tính khác nhau – một số lượng lớn yêu cầu HTTP tràn vào máy chủ, dẫn đến từ chối dịch vụ.

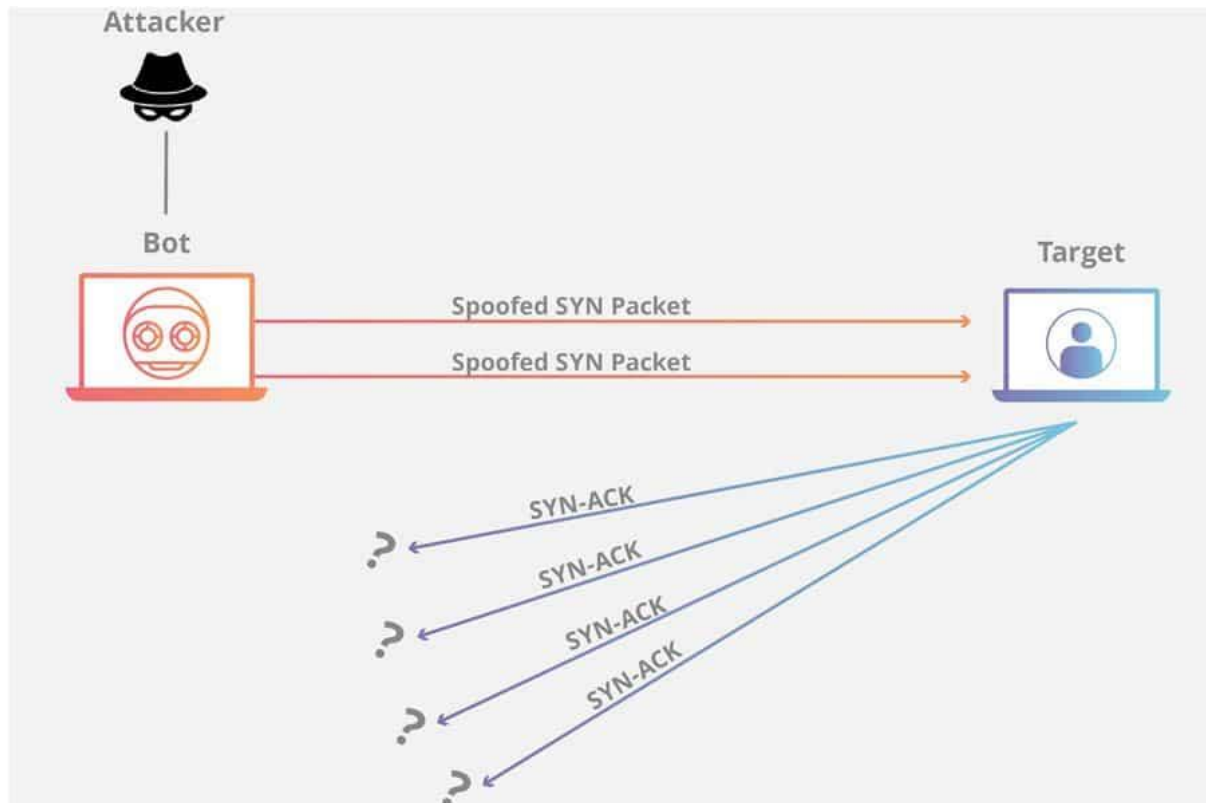
Loại tấn công này từ đơn giản đến phức tạp. Việc triển khai đơn giản hơn có thể truy cập một URL với cùng một phạm vi địa chỉ IP tấn công, người giới thiệu và tác nhân người dùng. Các phiên bản phức tạp có thể sử dụng một số lượng lớn địa chỉ IP tấn công và nhắm mục tiêu các url ngẫu nhiên bằng cách sử dụng các tác nhân người dùng và người dùng ngẫu nhiên.

3.2. Tấn công giao thức

Các cuộc tấn công giao thức, còn được gọi là các cuộc tấn công cạn kiệt trạng thái, gây ra sự gián đoạn dịch vụ bằng cách tiêu thụ tất cả dung lượng bảng trạng thái có sẵn của các máy chủ ứng dụng web hoặc tài nguyên trung gian như tường

lừa và cân bằng tải. Các cuộc tấn công giao thức sử dụng các điểm yếu trong lớp 3 và lớp 4 của ngăn xếp giao thức để khiến mục tiêu không thể truy cập được.

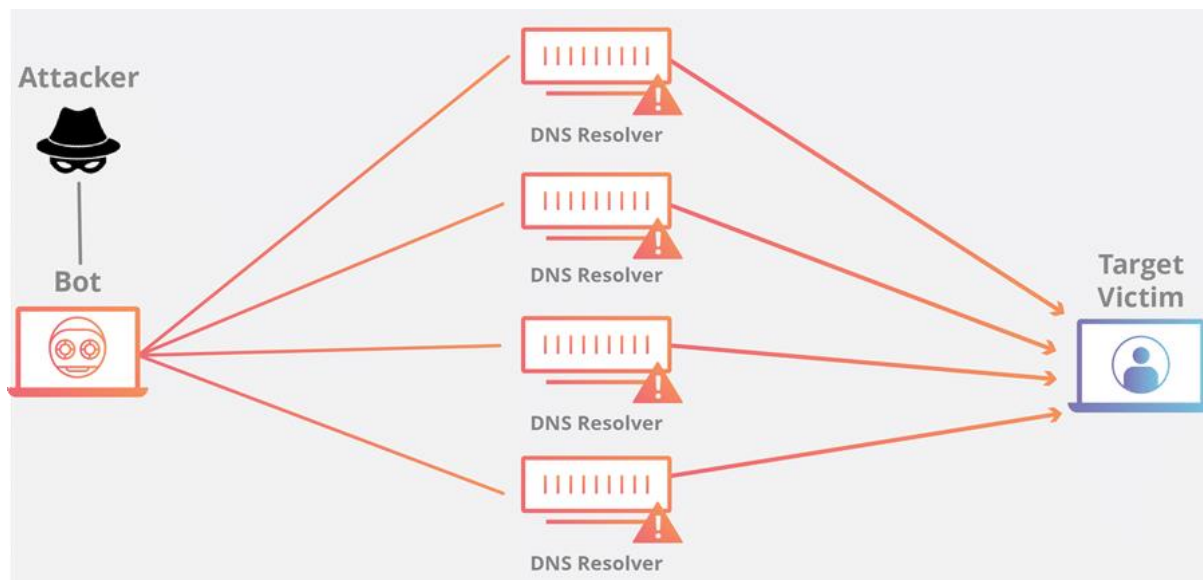
Ví dụ về tấn công giao thức



3.3 Tấn công Volumetric

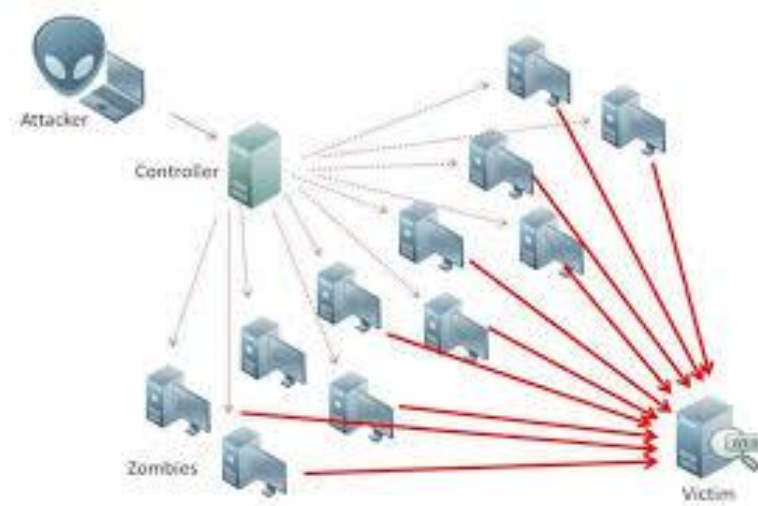
Thẻ loại tấn công này cố gắng tạo ra tắc nghẽn bằng cách tiêu thụ tất cả băng thông có sẵn giữa mục tiêu và Internet lớn hơn. Một lượng lớn dữ liệu được gửi đến mục tiêu bằng cách sử dụng một hình thức khuếch đại hoặc một phương tiện khác để tạo lưu lượng lớn, chẳng hạn như các yêu cầu từ botnet.

Ví dụ khuếch đại:



4. Giới thiệu một số hệ thống mà hacker sử dụng để tấn công từ chối dịch vụ.

Hệ thống 1:



Trong hệ thống 1: Kẻ tấn công sẽ dùng một máy điều khiển và gửi chỉ thị đến tất cả các máy còn lại (các máy trước đó đã bị kiểm soát là các zombies). Máy bị tấn công(victim: máy nạn nhân) là đích đến cuối cùng.

Hệ thống 2:



Trong hệ thống 2: Các Attackers là một nhóm đã được lập lịch trước để chuẩn bị cho một đợt tấn công mới.

5. Thực hiện quá trình 5 bước tấn công từ chối dịch vụ

Bước 1: Thiết lập IP (hệ thống là các máy hệ điều hành Kali Linux)

Wireless LAN adapter Wi-Fi 4:

```

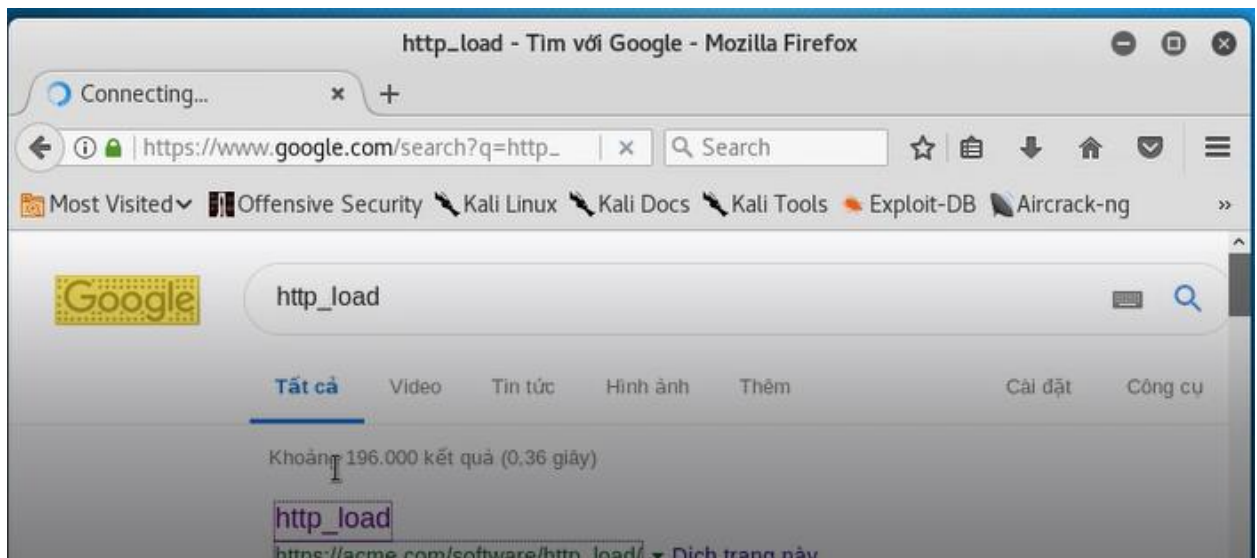
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::9002:34f8:67da:fed9%20
IPv4 Address. . . . . : 192.168.100.26
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%20
                             192.168.100.1

```

C:\Users\ADMIN>

Hình 2: Set địa chỉ IP

Bước 2: Tải phần mềm cài đặt tại đường dẫn <https://acme.com/Software>



Hình 2: Tải phần mềm dành cho tấn công DDoS

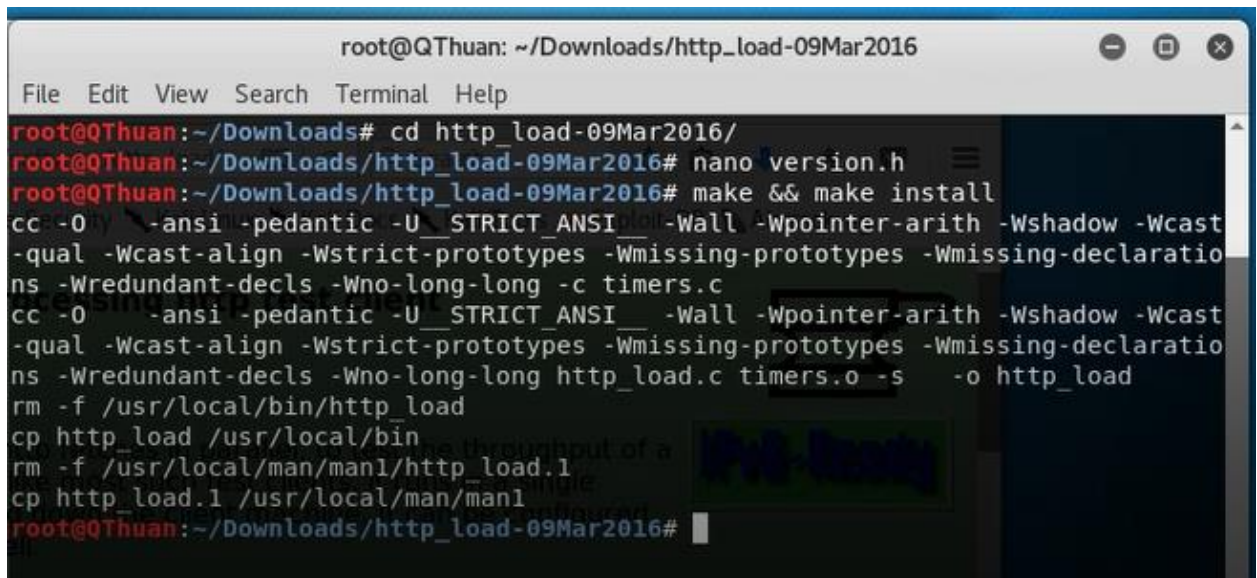
Bước 3: Cấu hình tập tin version.h

Cho phép chỉnh sửa nội dung tập tin hệ thống VERSION.H



Hình 3: Thiết lập thông số cho tập tin version.h

Bước 4: Cài đặt thông số http_loads

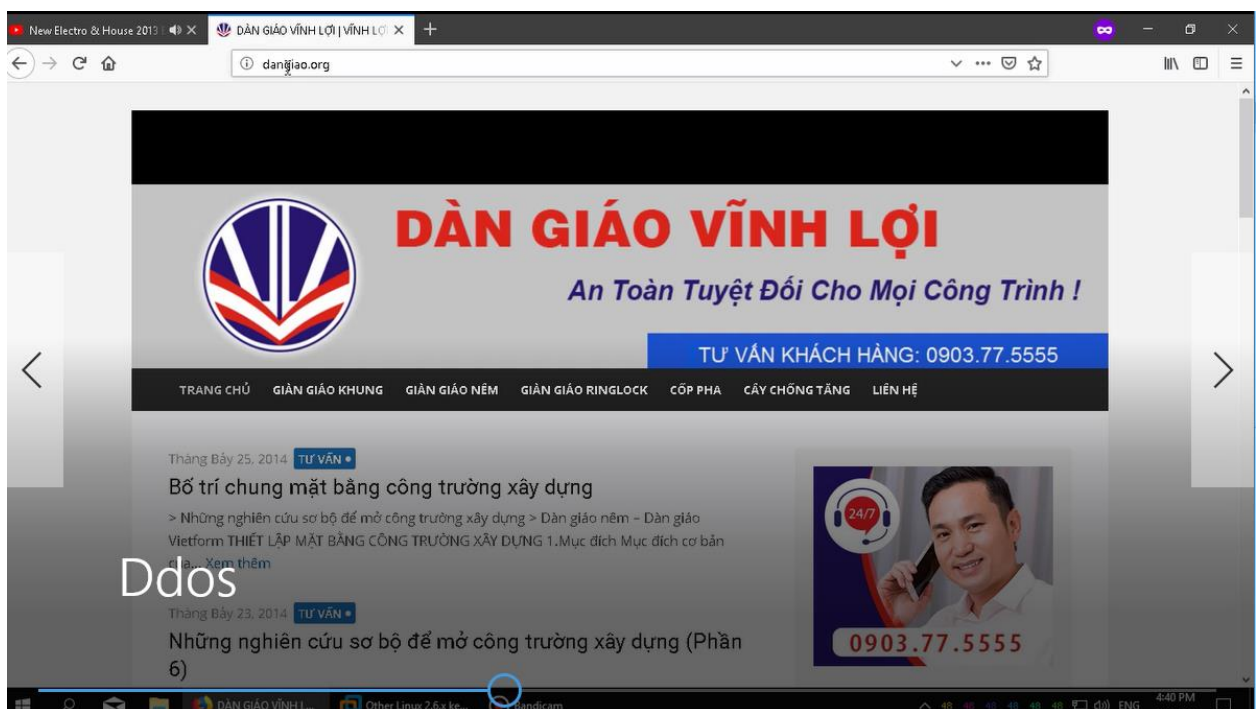


```
root@QThuan: ~/Downloads/http_load-09Mar2016
File Edit View Search Terminal Help
root@QThuan:~/Downloads# cd http_load-09Mar2016/
root@QThuan:~/Downloads/http_load-09Mar2016# nano version.h
root@QThuan:~/Downloads/http_load-09Mar2016# make && make install
cc -O2 -ansi -pedantic -U__STRICT_ANSI__ -Wall -Wpointer-arith -Wshadow -Wcast-qual -Wcast-align -Wstrict-prototypes -Wmissing-prototypes -Wmissing-declarations -Wredundant-decls -Wno-long-long -c timers.c
cc -O2 -ansi -pedantic -U__STRICT_ANSI__ -Wall -Wpointer-arith -Wshadow -Wcast-qual -Wcast-align -Wstrict-prototypes -Wmissing-prototypes -Wmissing-declarations -Wredundant-decls -Wno-long-long http_load.c timers.o -s -o http_load
rm -f /usr/local/bin/http_load
cp http_load /usr/local/bin
rm -f /usr/local/man/man1/http_load.1
cp http_load.1 /usr/local/man/man1
root@QThuan:~/Downloads/http_load-09Mar2016#
```

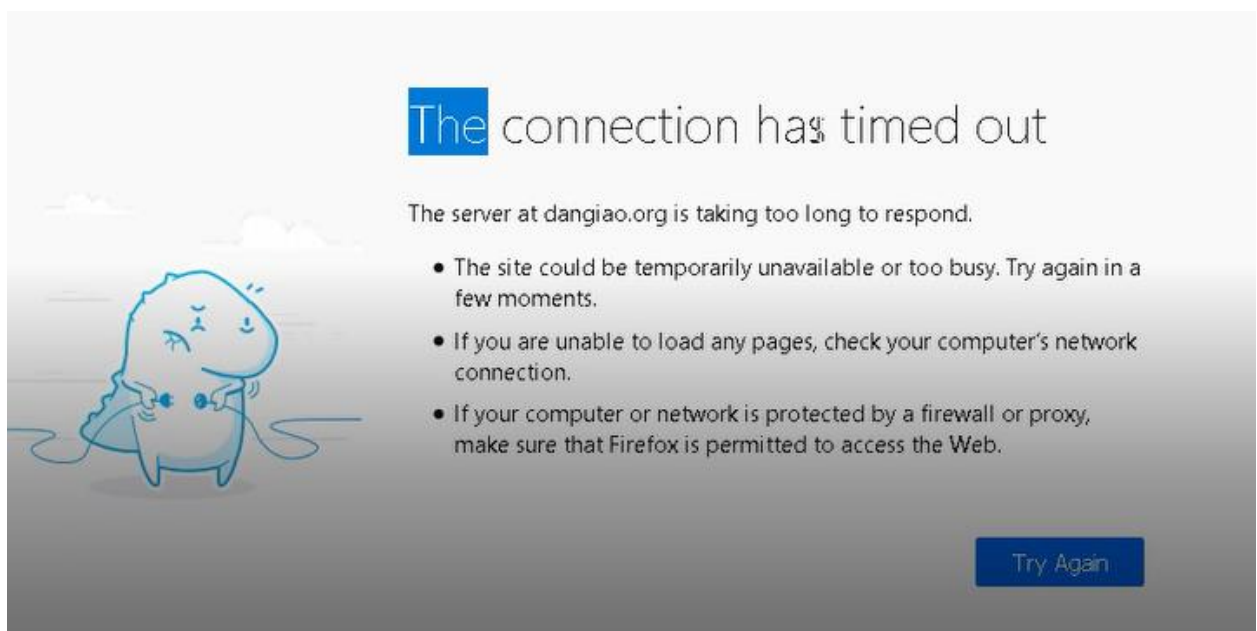
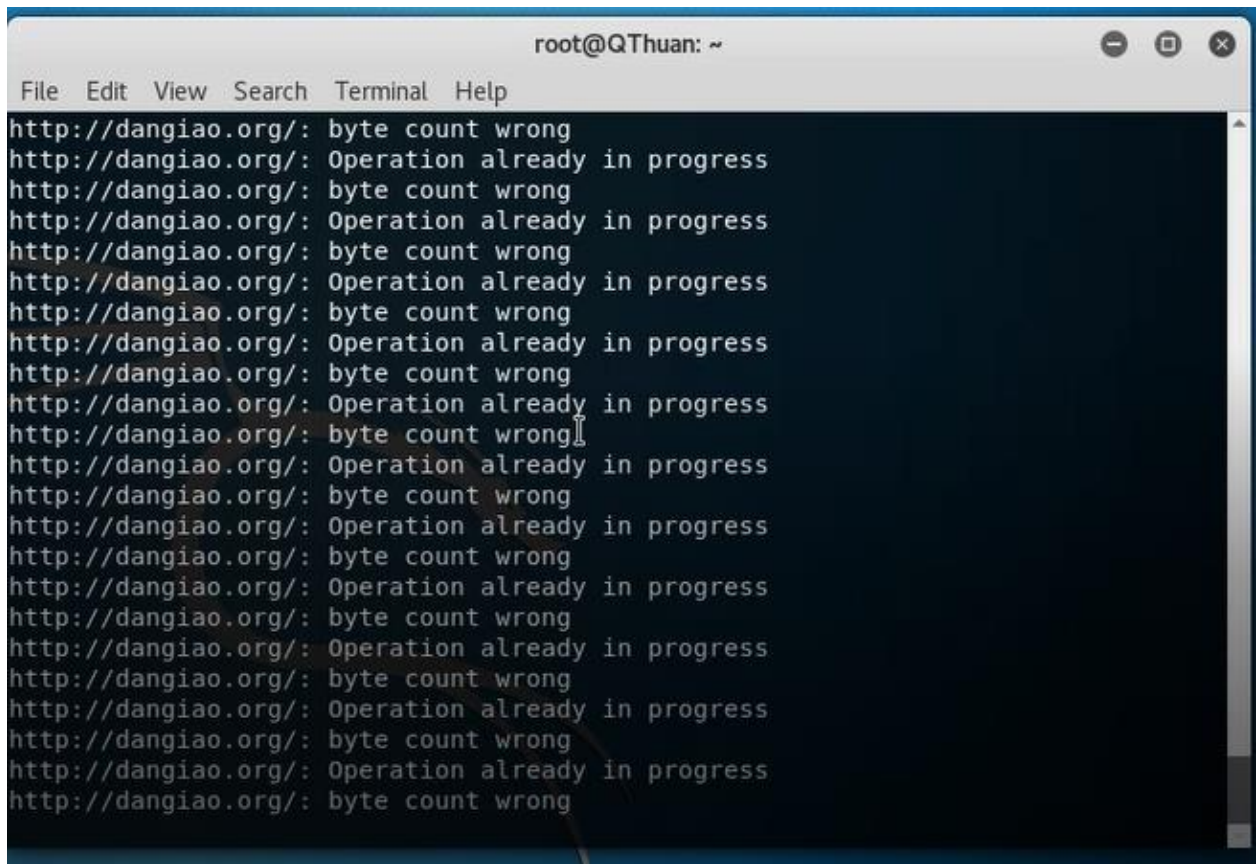
Hình 4: Cài đặt http_loads

Bước 5: Chọn đối tượng tấn công bằng DDoS

Để minh họa cụ thể cho kiểu tấn công từ chối dịch vụ DDoS, đối tượng được chọn là website **dangiao.org**.



Hình 5: (Để đảm bảo cho bài viết, trang này chỉ mang tính chất minh họa. Mục tiêu của đối tượng là trang dangiao.org)



Trong hình trên, website **dangiao.org** là không thể truy cập được nữa.

