

NỘI DUNG SÁNG KIẾN KINH NGHIỆM

1. Trình bày khái niệm về DDoS

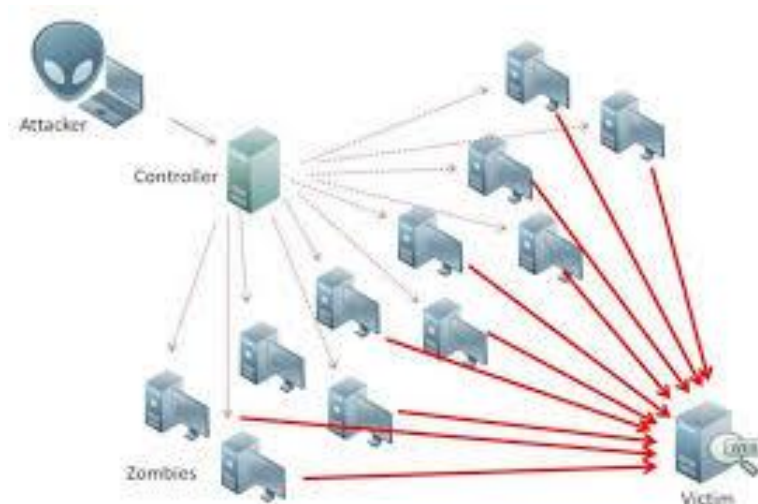
Tấn công từ chối dịch vụ là sự cố gắng có chủ đích rõ ràng của một người hay nhiều người với mục đích làm gián đoạn, hoặc làm cho hệ thống(dịch vụ từ máy chủ) đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

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. 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.

3. 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)

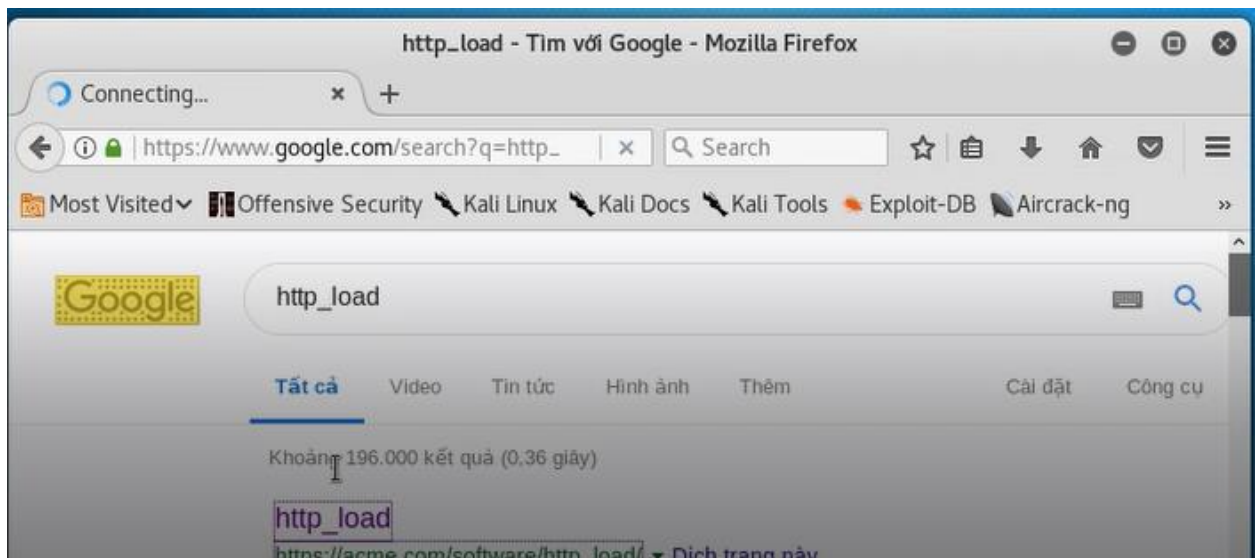
Wireless LAN adapter Wi-Fi 4:

```
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>



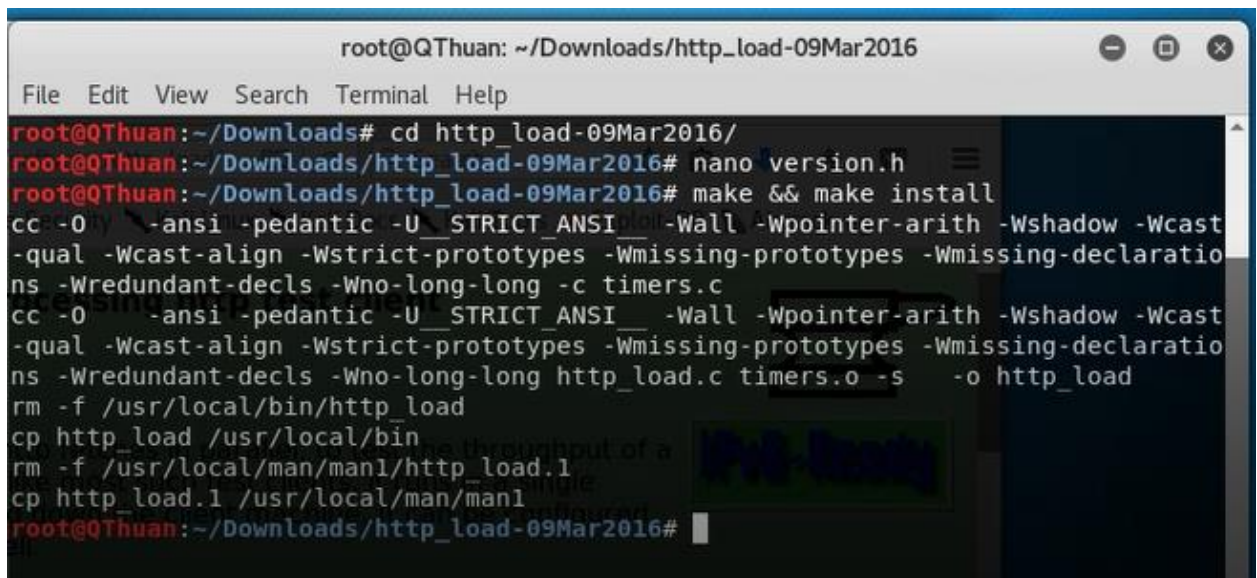
Hình 2: Tải phần mềm dành cho tấn công DDoS

Bước 3: Cấu hình tập tin version.h



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

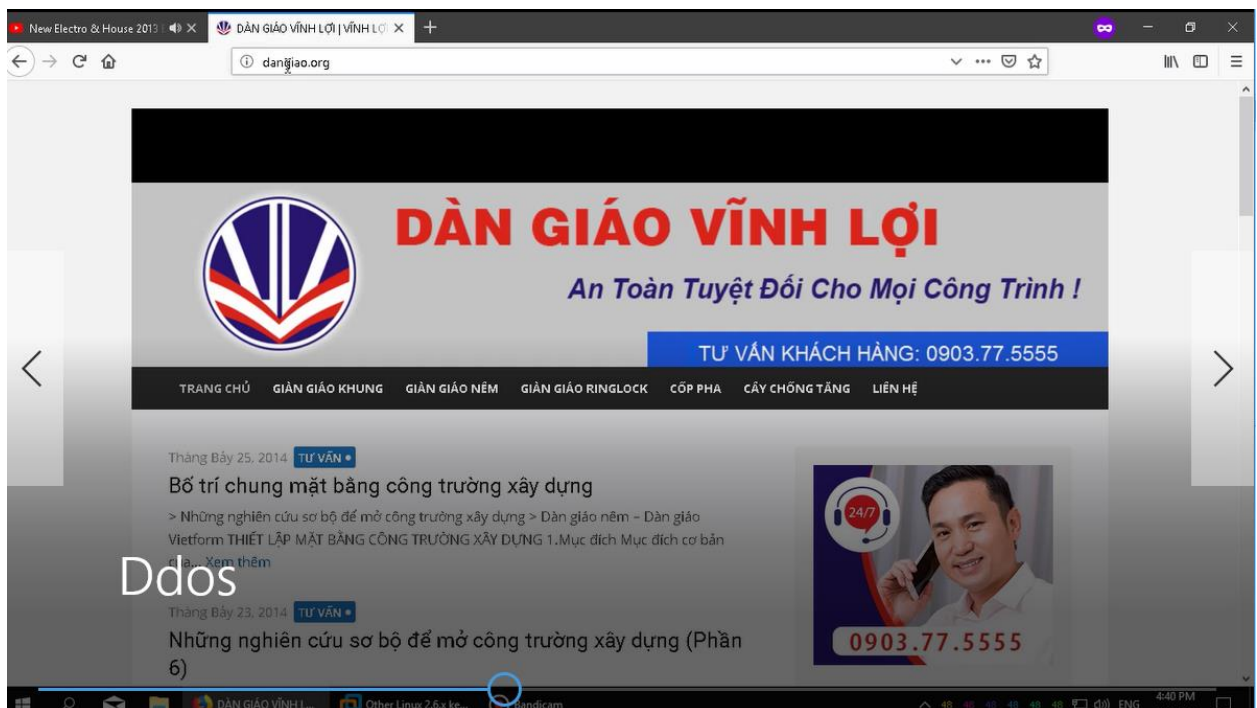
Bước 4: Cài đặt thông số http_loads



```
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



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)

