**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**

**ĐỒ ÁN MÔN HỌC**

**Đề tài: Tìm Hiểu DoS/DDoS**

Nghành: **CÔNG NGHỆ THÔNG TIN**

Lớp: **18DTHB3**

Sinh Viên Thực Hiện : **CHU THANH HẢI**

MSSV : 1811061387

**HOÀNG CÔNG PHÚC**

MSSV : 1811061178

**VÕ MINH TƯỜNG**

MSSV : 1811062038

**Giảng Viên Hướng Dẫn: Th.S Tống Thanh Văn**

TP.Hồ Chí Minh, 04/2021

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**

**ĐỒ ÁN MÔN HỌ**

**Đề tài: Tìm Hiểu DoS/DDoS**

Nghành: **CÔNG NGHỆ THÔNG TIN**

Lớp: **18DTHB3**

Sinh Viên Thực Hiện : **CHU THANH HẢI**

MSSV : 1811061387

**HOÀNG CÔNG PHÚC**

MSSV : 1811061178

**VÕ MINH TƯỜNG**

MSSV : 1811062038

**Giảng Viên Hướng Dẫn: Th.S Tống Thanh Văn**

TP.Hồ Chí Minh ,04,2021

**MỤC LỤC**

[**1. LỊCH SỬ CÁC CUỘC TẤN CÔNG DoS** 3](#_Toc69989125)

[**1.1. Mục tiêu tấn công** 3](#_Toc69989126)

[**1.2. Các cuộc tấn công tiêu biểu** 3](#_Toc69989127)

[**2. Định nghĩa về tấn công DoS** 4](#_Toc69989128)

[**2.1. Các mục đích của tấn công DoS** 4](#_Toc69989129)

[**2.2. Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS** 5](#_Toc69989130)

[**3. CÁC DẠNG TẤN CÔNG DoS** 6](#_Toc69989131)

[**3.1 Các dạng tấn công DoS** 6](#_Toc69989132)

[**3.1.1. Tấn công Smurf** 6](#_Toc69989133)

[**3.1.2. Tấn công Buffer overflow.** 7](#_Toc69989134)

[**3.1.3. Tấn công Ping of Death** 8](#_Toc69989135)

[**3.1.4. Tấn công Teardrop** 8](#_Toc69989136)

[**3.1.5. Tấn công SYN** 9](#_Toc69989137)

[**3.2. Các công cụ tấn công DoS** 11](#_Toc69989138)

[**3.2.1. Tools DoS – Jolt2** 11](#_Toc69989139)

[**3.2.2. Tools DoS: Bubonic.c** 12](#_Toc69989140)

[**3.2.3. Tools DoS: Land and LaTierra** 12](#_Toc69989141)

[**3.2.4. Tools DoS: Targa** 12](#_Toc69989142)

[**3.2.5. Tools DoS Blast 2.0** 13](#_Toc69989143)

[**3.2.6. Tools DoS – Nemesys** 13](#_Toc69989144)

[**3.2.7. Tool DoS – Panther2.** 14](#_Toc69989145)

[**3.2.8. Tool DoS – Crazy Pinger** 15](#_Toc69989146)

[**3.2.9. Tool DoS – Some Trouble** 16](#_Toc69989147)

[**3.2.10. DoS Tools – UDP Flood** 17](#_Toc69989148)

[**3.2.11. Tools DoS – FSMAX** 18](#_Toc69989149)

[**4. MẠNG BOTNET** 19](#_Toc69989150)

[**4.1. Ý nghĩa của mạng BOT** 19](#_Toc69989151)

[**4.2. Mạng BOT** 19](#_Toc69989152)

[**4.3. Mạng BOTNET** 20](#_Toc69989153)

[**4.4. Mục đích sử dụng mạng BOTNETs** 20](#_Toc69989154)

[**4.5. Các dạng của mạng BOTNET** 21](#_Toc69989155)

[**5. TẤN CÔNG DDoS** 22](#_Toc69989156)

[**5.1. Các đặc tính của tấn công DDoS** 23](#_Toc69989157)

[**5.2. Tấn công DDoS không thể ngăn chặn hoàn toàn.** 23](#_Toc69989158)

[**5.3. Kiến trúc tổng quan của DDoS attack-network.** 24](#_Toc69989159)

[**a. Mô hình Agent – Handler** 25](#_Toc69989160)

[**b. Mô hình IRC – Based** 26](#_Toc69989161)

[**5.4. Phân loại tấn công DDoS** 28](#_Toc69989162)

[**a. Những kiểu tấn công làm cạn kiệt băng thông của mạng (BandWith Depletion Attack)** 28](#_Toc69989163)

[**b. Kiểu tấn công làm cạn kiệt tài nguyên: (Resource Deleption Attack)** 31](#_Toc69989164)

[**5.5. Các tools sử dụng để tấn công DDoS** 33](#_Toc69989165)

[**a. Công cụ DDoS dạng Agent – Handler:** 34](#_Toc69989166)

[**b. Công cụ DDoS dạng IRC – Based:** 34](#_Toc69989167)

[**6. Các cách phòng chống DoS/DdoS** 36](#_Toc69989168)

[**KẾT LUẬN** 38](#_Toc69989169)

[KẾT QUẢ THU ĐƯỢC VÀ PHƯƠNG HƯỚNG PHÁT TRIỂN 39](#_Toc69989170)

[TÀI LIỆU THAM KHẢO 40](#_Toc69989171)

[**Kịch Bản Thử Nghiệm** 41](#_Toc69989172)

**1. LỊCH SỬ CÁC CUỘC TẤN CÔNG DoS**

**1.1. Mục tiêu tấn công**

- Mục tiêu các cuộc tấn công thường vào các trang web lớn và các tổ chức thương mại điện tử trên Internet.

**1.2. Các cuộc tấn công tiêu biểu**

- 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.

**2. Định nghĩa về tấn công DoS**

Tấn công DoS là kiểu tấn công vô cùng nguy hiểm, để hiểu được nó ta cần phải lắm rõ định nghĩa của tấn công DoS và các dạng tấn công DoS.  
- Tấn công DoS 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 Denial of Service (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:

**2.1. Các mục đích của tấn công DoS**

- 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.  
- Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó như bị:  
+ Disable Network - Tắt mạng  
+ Disable Organization - Tổ chức không hoạt động  
+ Financial Loss – Tài chính bị mất

**2.2. Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS**

Như chúng ta biết ở bên trên 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 vậy các tài nguyên chúng thường sử dụng để tấn công là gì:  
- Tạo ra sự khan hiếm, những giới hạn và không đổi mới tài nguyên  
- Băng thông của hệ thống mạng (Network Bandwidth), bộ nhớ, ổ đĩa, và CPU Time hay cấu trúc dữ liệu đều là mục tiêu của tấn công DoS.  
- Tấn công vào hệ thống khác phục vụ cho mạng máy tính như: hệ thống điều hoà, hệ thống điện, hệt hống làm mát và nhiều tài nguyên khác của doanh nghiệp. Bạn thử tưởng tượng khi nguồn điện vào máy chủ web bị ngắt thì người dùng có thể truy cập vào máy chủ đó không.  
- Phá hoại hoặc thay đổi các thông tin cấu hình.  
- Phá hoại tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hoà…

# **3. CÁC DẠNG TẤN CÔNG DoS**

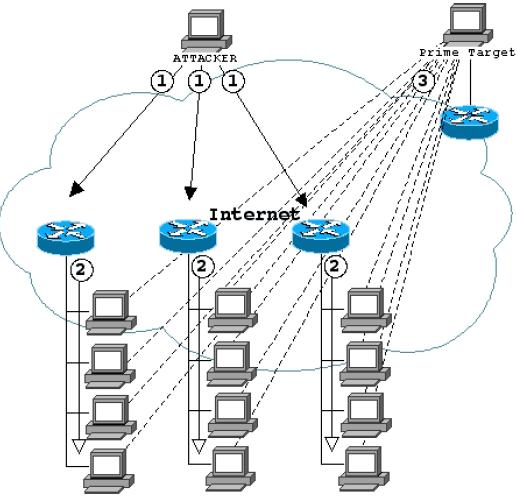
Tấn công Denial of Service chia ra làm hai loại tấn công  
- Tấn công DoS: Tấn công từ một cá thể, hay tập hợp các cá thể.  
- Tấn công DDoS: Đây là sự tấn công từ một mạng máy tính được thiết kế để tấn công tới một đích cụ thể nào đó.

## **3.1 Các dạng tấn công DoS**

- Smurf  
- Buffer Overflow Attack  
- Ping of Death  
- Teardrop  
- SYN Attack

### **3.1.1. Tấn công Smurf**

- Là thủ phạm sinh ra cực nhiều giao tiếp ICMP (ping) tới địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công.  
\* Chúng ta cần lưu ý là: Khi ping tới một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi tôi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại tôi. Nhưng giờ tôi thay đổi địa chỉ nguồn, thay địa chỉ nguồn là máy C và tôi ping tới địa chỉ Broadcast của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ reply lại vào máy C chứ không phải tôi và đó là tấn công Smurf.  
- Kết quả đích tấn công sẽ phải chịu nhận một đợt Reply gói ICMP cực lớn và làm cho mạng bị dớt hoặc bị chậm lại không có khả năng đáp ứng các dịch vụ khác.  
- Quá trình này được khuyếch đại khi có luồng ping reply từ một mạng được kết nối với nhau (mạng BOT).  
- tấn công Fraggle, chúng sử dụng UDP echo và tương tự như tấn công Smurf.



Hình hiển thị tấn công DoS - dạng tấn công Smurf sử dụng gói ICMP làm ngập các giao tiếp khác.

# **3.1.2. Tấn công Buffer overflow.**

- Buffer Overflow xảy ra tại bất kỳ thời điểm nào có chương trình ghi lượng thông tin lớn hơn dung lượng của bộ nhớ đệm trong bộ nhớ.  
- Kẻ tấn công có thể ghi đè lên dữ liệu và điều khiển chạy các chương trình và đánh cắp quyền điều khiển của một số chương trình nhằm thực thi các đoạn mã nguy hiểm. - Tấn công Buffer Overflow tôi đã trình bày cách khai thác lỗi này trong bài viết trước về hacking windows cũng trên trang [VnExperts - Training CCNA, CCNP, CCSP, MCSA, MCSE, MCITP, Linux+, Security+, CEH](http://www.vnexperts.net/).  
- Quá trình gửi một bức thư điện tử mà file đính kèm dài quá 256 ký tự có thể sẽ xảy ra quá trình tràn bộ nhớ đệm.

### **3.1.3. Tấn công Ping of Death**

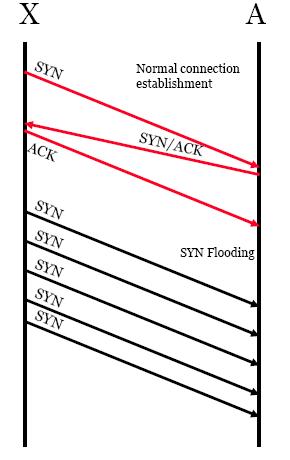


- Kẻ tấn công gửi những gói tin IP lớn hơn số lương bytes cho phép của tin IP là 65.536 bytes.  
- Quá trình chia nhỏ gói tin IP thành những phần nhỏ được thực hiện ở layer II.  
- Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.536 bytes. Nhưng hệ điều hành không thể nhận biết được độ lớn của gói tin này và sẽ bị khởi động lại, hay đơn giản là sẽ bị gián đoạn giao tiếp.  
- Để nhận biết kẻ tấn công gửi gói tin lớn hơn gói tin cho phép thì tương đối dễ dàng.

### **3.1.4. Tấn công Teardrop**

- Gói tin IP rất lớn khi đến Router sẽ bị chia nhỏ làm nhiều phần nhỏ.  
- Kẻ tấn công sử dụng sử dụng gói IP với các thông số rất khó hiểu để chia ra các phần nhỏ (fragment).  
- Nếu hệ điều hành nhận được các gói tin đã được chia nhỏ và không hiểu được, hệ thống cố gắng build lại gói tin và điều đó chiếm một phần tài nguyên hệ thống, nếu quá trình đó liên tục xảy ra hệ thống không còn tài nguyên cho các ứng dụng khác, phục vụ các user khác.

### **3.1.5. Tấn công SYN**

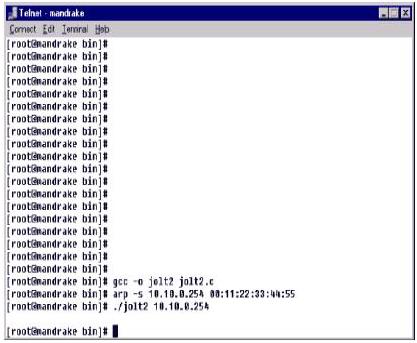


- Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối.  
- Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực 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 – Three-way.  
- 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 và đó chính là tấn công DoS.  
- 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 Three-way handshake 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 Three-way handshake 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 Three-way handshake 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.  
- Với nguyên tắc chỉ chấp nhận gói SYN từ một máy tới hệ thống sau mỗi 75 giây nếu địa chỉ IP nào vi phạm sẽ chuyển vào Rule deny access sẽ ngăn cản tấn công này.

**3.2. Các công cụ tấn công DoS**

- Jolt2  
- Bubonic.c  
- Land and LaTierra  
- Targa  
- Blast20  
- Nemesy  
- Panther2  
- Crazy Pinger  
- Some Trouble  
- UDP Flood  
- FSMax

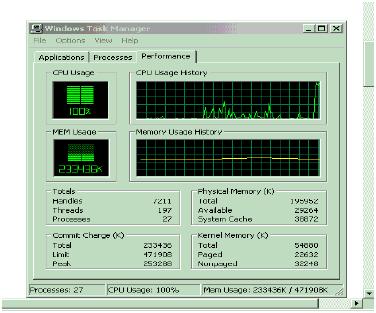
### **3.2.1. Tools DoS – Jolt2**



- Cho phép kẻ tấn từ chối dịch vụ (DoS) lên các hệ thống trên nền tảng Windows  
- Nó là nguyên nhân khiên máy chủ bị tấn công có CPU luôn hoạt động ở mức độ 100%, CPU không thể xử lý các dịch vụ khác.  
- Không phải trên nền tảng Windows như Cisco Router và một số loại Router khác cũng có thể bị lỗ hổng bảo mật này và bị tools này tấn công.

### **3.2.2. Tools DoS: Bubonic.c**

- Bubonic.c là một tools DoS dựa vào các lỗ hổng bảo mật trên Windows 2000  
- Nó hoạt động bằng cách ngẫu nhiên gửi các gói tin TCP với các thiết lập ngẫu nhiên làm cho máy chủ tốn rất nhiều tài nguyên để xử lý vấn đề này, và từ đó sẽ xuất hiện những lỗ hổng bảo mật.  
- Sử dụng bubonic.c bằng cách gõ câu lệnh: bubonic 12.23.23.2 10.0.0.1 100



### **3.2.3. Tools DoS: Land and LaTierra**

- Giả mạo địa chỉ IP được kết hợp với quá trình mở các kết nối giữa hai máy tính.  
- Cả hai địa chỉ IP, địa chỉ nguồn (source) và địa chỉ IP đích, được chỉnh sửa thành một địa chỉ của IP đích khi đó kết nối giữa máy A và máy B đang được thực hiện nếu có tấn công này xảy ra thì kết nối giữa hai máy A và B sẽ bị ngắt kết nối.  
- Kết quả này do địa chỉ IP nguồn và địa chỉ IP đích của gói tin giống nhau và gói tin không thể đi đến đích cần đến.

### **3.2.4. Tools DoS: Targa**

- Targa là một chương chình có thể sử dụng 8 dạng tấn công DoS khác nhau.  
- Nó được coi như một bộ hướng dẫn tích hợp toàn bộ các ảnh hưởng của DoS và thường là các phiên bản của Rootkit.  
- Kẻ tấn công sử dụng một trong các phương thức tấn công cụ thể tới một hệ thống bao giờ đạt được mục đích thì thôi.  
- Targa là một chương trình đầy sức mạnh và nó có khả năng tạo ra một sự nguy hiểm rất lớn cho hệ thống mạng của một công ty.

### **3.2.5. Tools DoS Blast 2.0**

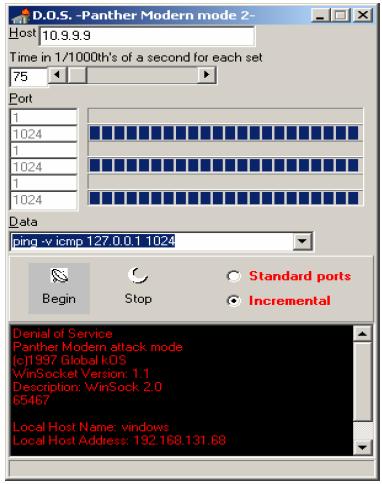
- Blast rất nhỏ, là một công cụ dùng để kiểm tra khả năng của dịch vụ TCP nó có khả năng tạo ra một lưu lượng rất lớn gói TCP và có thể sẽ gay nguy hiểm cho một hệ thống mạng với các server yếu.  
- Dưới đây là cách sử dụng để tấn công HTTP Server sử dụng Blast2.0  
+ Blast 192.168.1.219 80 40 50 /b "GET /some" /e "url/ HTTP/1.0" /nr /dr /v  
- Tấn công máy chủ POP  
+ Blast 192.168.1.219 110 15 20 /b "user te" /e "d" /v

### **3.2.6. Tools DoS – Nemesys**



- Đây là một chương trình sinh ra những gói tin ngẫu nhiên như (protocol, port, etc. size, …)  
- Dựa vào chương trình này kẻ tấn công có thể chạy các đoạn mã nguy hiểm vào máy tính không được bảo mật.

### **3.2.7. Tool DoS – Panther2.**



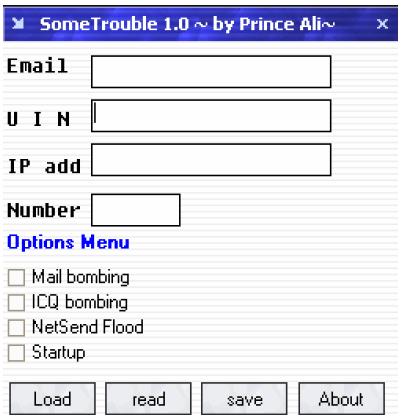
- Tấn công từ chối dịch vụ dựa trên nền tảng UDP Attack được thiết kế dành riêng cho kết nối 28.8 – 56 Kbps.  
- Nó có khả năng chiếm toàn bộ băng thông của kết nối này.  
- Nó có khả năng chiếm băng thông mạng bằng nhiều phương pháp ví như thực hiện quá trình Ping cực nhanh và có thể gây ra tấn công DoS

### **3.2.8. Tool DoS – Crazy Pinger**

- Công cụ này có khả năng gửi những gói ICPM lớn tới một hệ thống mạng từ xa.

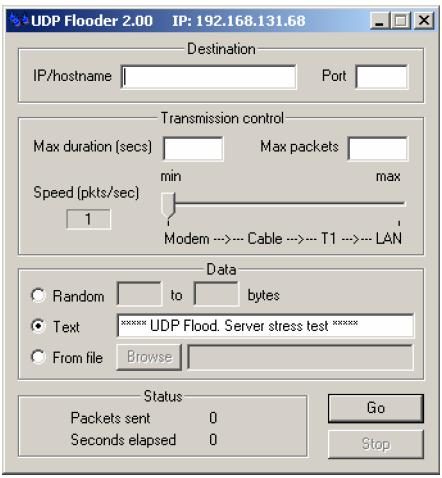


### **3.2.9. Tool DoS – Some Trouble**



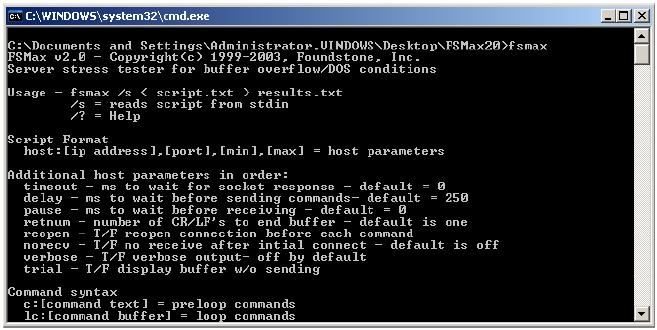
- SomeTrouble 1.0 là một chương trình gây nghẽn hệ thống mạng  
- SomeTrouble là một chương trình rất đơn giản với ba thành phần  
+ Mail Bomb (tự có khả năng Resole Name với địa chỉ mail có)  
+ ICQ Bomb  
+ Net Send Flood

### **3.2.10. DoS Tools – UDP Flood**



- UDPFlood là một chương trình gửi các gói tin UDP  
- Nó gửi ra ngoài những gói tin UDP tới một địac hỉ IP và port không cố định  
- Gói tin có khả năng là một đoạn mã văn bản hay một số lượng dữ liệu được sinh ngẫu nhiên hay từ một file.  
- Được sử dụng để kiểm tra khả năng đáp ững của Server

### **3.2.11. Tools DoS – FSMAX**



- Kiểm tra hiệu năng đáp ứng của máy chủ.  
- Nó tạo ra một file sau đó chạy trên Server nhiều lần lặp đi lặp lại một lúc.  
- Tác dụng của tools này là tìm cách tấn công làm chàn bộ nhớ đệm và tấn công DoS tới máy chủ.

# **4. MẠNG BOTNET**

## **4.1. Ý nghĩa của mạng BOT**

- Khi sử dụng một Tool tấn công DoS tới một máy chủ đôi khi không gây ảnh hưởng gì cho máy chủ - Giả sử ta sử dụng tool Ping of Death tới một máy chủ, trong đó máy chủ kết nối với mạng tốc độ 100Mbps bạn kết nối tới máy chủ tốc độ 3Mbps - Vậy cuộc tấn công đó không có ý nghĩa gì.

- Nhưng hãy thử tưởng tượng có 1000 người cùng một lúc tấn công vào máy chủ kia khi đó toàn bộ băng thông của 1000 người cộng lại tối đa đạt 3Gbps và tốc độ kết nối của máy chủ là 100 Mbps vậy kết quả sẽ ra sao.

- Để tạo ra những máy tính để thực hiện việc tấn công, kẻ tấn công xây dựng một mạng gồm hàng nghìn máy tính kết Internet (có mạng BOT lên tới 400.000 máy). Khi có trong tay mạng BOT kẻ tấn công sử dụng những tool tấn công đơn giản để tấn công vào một hệ thống máy tính. Dựa vào những truy cập hoàn toàn hợp lệ của hệ thống, cùng một lúc chúng sử dụng một dịch vụ của máy chủ.

## **4.2. Mạng BOT**

- BOT từ viết tắt của từ RoBOT

- Internet Relay Chat (IRC) là một dạng truyền dữ liệu thời gian thực trên Internet. Nó thường được thiết kế sao cho một người có thể nhắn được cho một group và mỗi người có thể giao tiếp với nhau với một kênh khác nhau được gọi là – Channels.

- IRCbot – còn được gọi là zombie hay drone.

- Đầu tiên BOT kết nối kênh IRC với IRC Server và đợi giao tiếp giữa những người với nhau.

- Kẻ tấn công có thể điều khiển mạng BOT và sử dụng mạng BOT cũng như sử dụng nhằm một mục đích nào đó.

- Nhiều mạng BOT kết nối với nhau người ta gọi là BOTNET – botnet.

## **4.3. Mạng BOTNET**

- Mạng Botnet bao gồm nhiều máy tính

- Nó được sử dụng cho mục đích tấn công DDoS

- Một mạng Botnet nhỏ có thể chỉ bao gồm 1000 máy tính nhưng bạn thử tưởng tượng mỗi máy tính này kết nối tới Internet tốc độ chỉ là 128Kbps thì mạng Botnet này đã có khả năng tạo băng thông là 1000\*128 ~ 100Mbps – Đây là một con số thể hiện băng thông mà khó một nhà Hosting nào có thể share cho mỗi trang web của mình.

## **4.4. Mục đích sử dụng mạng BOTNETs**

- Tấn công Distributed Denial-of-Service - DDoS

+ Botnet được sử dụng cho tấn công DDoS

- Spamming

+ Mở một SOCKS v4/v5 proxy server cho việc Spamming

- Sniffing traffic

+ Bot cũng có thể sử dụng các gói tin nó sniffer (tóm được các giao tiếp trên mạng) sau khi tóm được các gói tin nó cố gắng giải mã gói tin để lấy được các nội dung có ý nghĩa như tài khoản ngân hàng và nhiều thông tin có giá trị khác của người sử dụng.

- Keylogging

+ Với sự trợ giúp của Keylogger rất nhiều thông tin nhạy cảm của người dùng có thể sẽ bị kẻ tấn công khai thác như tài khoản trên e-banking, cũng như nhiều tài khoản khác.

- Cài đặt và lây nhiễm chương trình độc hại

+ Botnet có thể sử dụng để tạo ra mạng những mạng BOT mới.

- Cài đặt những quảng cáo Popup

+ Tự động bật ra những quảng cáo không mong muốn với người sử dụng.

- Google Adsense abuse

+ Tự động thay đổi các kết quả tìm kiếm hiển thị mỗi khi người dùng sử dụng dịch vụ tìm kiểm của Google, khi thay đổi kết quả nó sẽ lừa người dùng kích vào những trang web nguy hiểm.

- Tấn công vào IRC Chat Networks

+ Nó được gọi là clone attack

- Phishing

+ Mạng botnet còn được sử dụng để phishing mail nhằm lấy các thông tin nhạy cảm của người dùng.

## **4.5. Các dạng của mạng BOTNET**

Agobot/Phatbot/Forbot/XtremBot

- Đây là những bot được viết bằng C++ trên nền tảng Cross-platform và mã nguồn được tìm trên GPL. Agobot được viết bởi Ago nick name được người ta biết đến là Wonk, một thanh niên trẻ người Đức – đã bị bắt hồi tháng 5 năm 2004 với tội danh về tội phạm máy tính.

- Agobot có khả năng sử dụng NTFS Alternate Data Stream (ADS) và như một loại Rootkit nhằm ẩn các tiến trình đang chạy trên hệ thống

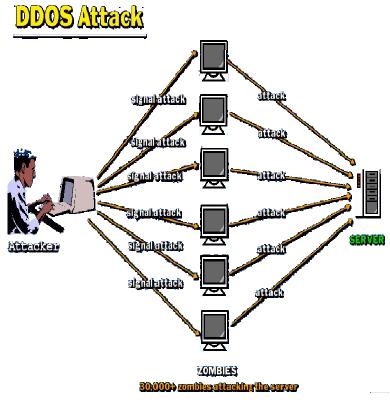
SDBot/Rbot/UrBot/UrXbot

- SDBot được viết bằng ngồn ngữ C và cũng được public bởi GPL. Nó đươc coi như là tiền thân của Rbot, RxBot, UrBot, UrXBot, JrBot

mIRC-Based Bots – GT-Bots

- GT được viết tắt tư fhai từ Global Threat và tên thường được sử dụng cho tất cả các mIRC-scripted bots. Nó có khả năng sử dụng phần mềm IM là mIRC để thiết lập một số script và một số đoạn mã khác.

# **5. TẤN CÔNG DDoS**



Trên Internet tấn công Distributed Denial of Service là một dạng tấn công từ nhiều máy tính tới một đích, nó gây ra từ chối các yêu cầu hợp lệ của các user bình thường. Bằng cách tạo ra những gói tin cực nhiều đến một đích cụ thể, nó có thể gây tình trạng tương tự như hệ thống bị shutdown.

Tấn công DDoS là một biến thể của Foolding DoS (Tấn công từ chối dịch vụ tràn). Mục đích của hình thức này là gây tràn mạng đích. Kẻ tấn công sau đó sẽ sử toàn bộ lượng băng thông khổng lồ của BOTNET để làm tràn website đích. Đó là cách phát động tấn công tốt nhất. Một trong các kiểu tấn công phổ biến nhất được thực hiện thông qua sử dụng giao thức TCP (một giao thức hướng kết nối), gọi là TCP SYN flooding (tràn đồng bộ TCP). Cách thức hoạt động của chúng là gửi đồng thời cùng lúc một số lượng khổng lồ yêu cầu kết nối TCP tới một Web Server (hoặc bất kỳ dịch vụ nào khác), gây tràn tài nguyên server, dẫn đến tràn băng thông và ngăn không cho người dùng khác mở kết nối riêng của họ. Quả là đơn giản nhưng thực sự nguy hiểm! Kết quả thu được cũng tương tự khi dùng giao thức UDP (một giao thức không kết nối).

## **5.1. Các đặc tính của tấn công DDoS**

- Nó được tấn công từ một hệ thống các máy tính cực lớn trên Internet, và thường dựa vào các dịch vụ có sẵn trên các máy tính trong mạng BOTNET

- Các dịch vụ tấn công được điều khiển từ những "primary victim" trong khi các máy tính bị chiếm quyền sử dụng trong BOTNET được sử dụng để tấn công thường được gọi là "zombie".

- Là dạng tấn công rất khó có thể phát hiện bởi tấn công này được sinh ra từ nhiều địa chỉ IP trên Internet.

- Nếu một địa chỉ IP tấn công một công ty, nó có thể được chặn bởi Firewall. Nếu nó từ 30.000 địa chỉ IP khác, thì điều này là vô cùng khó khăn.

- Thủ phạm có thể gây nhiều ảnh hưởng bởi tấn công từ chối dịch vụ DoS, và điều này càng nguy hiểm hơn khi chúng sử dụng một hệ thống BOTNET trên internet thực hiện tấn công DoS và đó được gọi là tấn công DDoS.

## **5.2. Tấn công DDoS không thể ngăn chặn hoàn toàn.**

- Các dạng tấn công DDoS thực hiện tìm kiếm các lỗ hổng bảo mật trên các máy tính kết nối tới Internet và khai thác các lỗ hổng bảo mật để xây dựng mạng BOTNET gồm nhiều máy tính kết nối tới Internet.

- Một cuộc tấn công DDoS tốt được thực hiện sẽ rất khó để ngăn chặn hoàn toàn.

- Những gói tin đến Firewall có thể chặn lại, nhưng hầu hết chúng đều đến từ những địa chỉ IP chưa có trong các Access Rule của Firewall và là những gói tin hoàn toàn hợp lệ.

- Nếu địa chỉ nguồn của gói tin có thể bị giả mạo, sau khi bạn không nhận được sự phản hồi từ những địa chỉ nguồn thật thì bạn cần phải thực hiện cấm giao tiếp với địa chỉ nguồn đó.

- Tuy nhiên một mạng BOTNET bao gồm từ hàng nghìn tới vài trăm nghìn địa chỉ IP trên Internet và điều đó là vô cùng khó khăn để ngăn chặn tấn công.

## **5.3. Kiến trúc tổng quan của DDoS attack-network.**

Giờ đây không một kẻ tấn công nào sử dụng luôn địa chỉ IP để điều khiển mạng BOTNET tấn công tới đích, mà chúng thường sử dụng một đối tượng trung gian dưới đây là những mô hình tấn công DDoS. Nhìn chung DDoS attack-network có hai mô hình chính:

+ Mô hình Agent – Handler

+ Mô hình IRC – Based

**DDoS attack-network**

**Agent -Handler**

**IRC - Based**

Client – Handler

Communication

Secret/private channel

Public channel

TCP

UDP

ICMP

TCP

UDP

ICMP

Client – Handler

Communication

*Sơ đồ chính phân loại các kiểu tấn công DDoS*

### **a. Mô hình Agent – Handler**

Kẻ tấn công sử dụng các handler để điều khiển tấn công

**Attacker**

**Attacker**

**Handler**

**Handler**

**Handler**

**Handler**

**Agent**

**Agent**

**Agent**

**Agent**

**Agent**

**Victim**

*Kiến trúc attack-network kiểu 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

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.

### **b. Mô hình IRC – Based**

Kẻ tấn công sử dụng các mạng IRC để điều khiển, khuyếch đại và quản lý kết nối với các máy tính trong mạng Botnet.

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.

**Attacker**

**Attacker**

**Agent**

**Agent**

**Agent**

**Agent**

**Agent**

**Victim**

*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.

## **5.4. Phân loại tấn công DDoS**

Nhìn chung, có rất nhiều biến thể của kỹ thuật tấn công DDoS nhưng nếu nhìn dưới góc độ chuyên môn thì có thể chia các biến thề này thành hai loại dựa trên mụch đích tấn công: Làm cạn kiệt băng thông và làm cạn kiệt tài nguyên hệ thống. Dưới đây là sơ đồ mô tả sự phân loại các kiểu tấn công DDoS.

DDoS attack

Bandwith DeleptionDeleption

Resource Deleption

Flood Attack

Amplification

Attack

UDP

Random

Port

Attack

Smuft

attack

Protocol

Exploit

Attack

Malformed Paclket attack

Static

Port

Attack

ICMP

Spoof

Source

Attack

Flaggle

Attack

Direct

Attack

Loop

Attack

TCP SYS

Attack

Spoof

source

Attack

PUSH

+ACK

SYN

Attack

IP @

Attack

IP Packet Options

Attack

Spoof

source

Attack

Spoof

source

Attack

Spoof

source

Attack

*Sơ đồ phân loại tấn công DDoS.*

## **a. Những 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 địch 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.

**Attacker/Agent**

**VICTIM**

**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.

## **b. 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.

**TCP**

**Client**

Client Port

1024-65535

**TCP**

**Server**

Service Port

1-1023

**SYS**

ACK

**SYN/ACK**

80

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.

**Malicious**

**TCP**

**Client**

**Victim**

**TCP**

**Server**

SYS packet with a deliberately fraudulent (spoofed) source IP return address

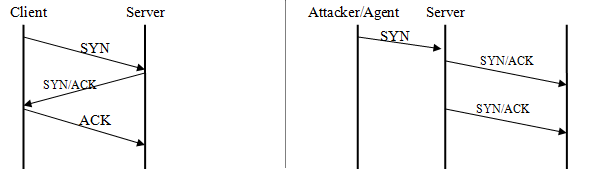
SYS/ACK

**SYN**

80

**?**

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.

## **5.5. Các tools sử dụng để tấn công DDoS**

Dựa trên nền tảng chung của phần trên, đã có nhiều công cụ được viết ra, thông thường các công cụ này là mã nguồn mở nên mức độ phức tạp ngày càng cao và có nhiều biến thể mới lạ.

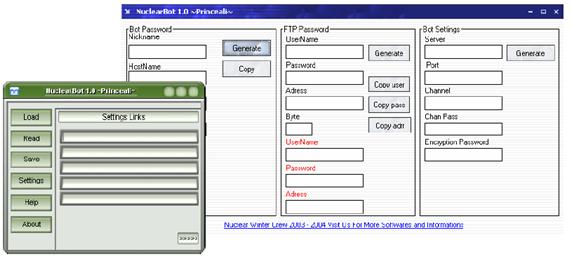
Trong toàn bộ các tools được giới thiệu trong bài này hầu hết là các tools cũ và không hiệu quả, và chỉ mang tính chất sư phạm để có thể hiểu về dạng tấn công DDoS hơn mà thôi. Dưới đây là các Tools tấn công DDoS.

- Trinoo -    Tribe flood Network (TFN) -    TFN2K -    Stacheldraht -    Shaft

- Trinity -    Knight -    Mstream -   Kaiten

Các tools này hoàn toàn có thể Download miễn phí trên Internet và lưu ý là chỉ để thử đây là các tools yếu và chỉ mang tính Demo về tấn công DdoS mà thôi.

- **Nuclear Bot**: là một tool cực mạnh "Multi Advanced IRC BOT" có thể sử dụng để Floods, Managing, Utilities, Spread, IRC Related, tấn công DDoS và nhiều mục đích khác.



### **a. Công cụ DDoS dạng Agent – Handler:**

- **TrinOO:** là một trong các công cụ DDoS đầu tiên được phát tán rộng rãi. TrinOO có kiến trúc Agent – Handler, là công cụ DDoS kiểu Bandwidth Depletion Attack, sử dụng kỹ thuật UDP flood. Các version đầu tiên của TrinOO không hỗ trợ giả mạo địa chỉ IP. TrinOO Agent được cài đặt lợi dụng lỗi remote buffer overrun. Hoạt động trên hệ điều hành Solaris 2.5.1 à Red Hat Linux 6.0. Attack – network giao tiếp dùng TCP (attacker client và handler) và UDP (Handler và Agent). Mã hóa giao tiếp dùng phương pháp mã hóa đối xứng giữa Client, handler và Agent.

- **Tribe Flood Network (TFN):** Kiểu kiến trúc Agent – Handler, công cụ DDoS hoễ trợ kiểu Bandwidth Deleption Attack và Resourse Deleption Attack. Sử dụng kỹ thuật UDP flood, ICMP Flood, TCP SYN và Smurf Attack. Các version đầu tiên không hỗ trợ giả mạo địa chỉ IP, TFN Agent được cài đặt lợi dụng lỗi buffer overflow. Hoạt động trên hệ điều hành Solaris 2.x và Red Hat Linux 6.0. Attack – Network giao tiếp dùng ICMP ECHO REPLY packet (TFN2K hỗ trợ thêm TCP/UDP với tính năng chọn protocol tùy ý), không mã hóa giao tiếp (TFN2K hỗ trợ mã hóa).

- **Stacheldraht**: là biến thể của TFN có thêm khả năng updat Agent tự động. Giao tiếp telnet mã hóa đối xứng giữa Attacker và Handler.

- **Shaft**: là biến thể của TrinOO, giao tiếp Handler – Agent trên UDP, Attacker – Hendle trên Internet. Tấn công dùng kỹ thuật UDP, ICMP và TCP flood. Có thể tấn công phối hợp nhiều kiểu cùng lúc. Có thống kê chi tiết cho phép attacker biết tình trạng tổn thất của nạn nhân, mức độ quy mô của cuộc tấn công để điều chỉnh số lượng Agent.

### **b. Công cụ DDoS dạng IRC – Based:**

Công cụ DDoS dạng IRC-based được phát triển sau các công cụ dạng Agent – Handler. Tuy nhiên, công cụ DDoS dạng IRC phức tạp hơn rất nhiều, do tích hợp rất nhiều đặc tính của các công cụ DDoS dạng Agent – Handler.

- **Trinity:** là một điển hình của công cụ dạng này. Trinity có hầu hết các kỹ thuật tấn công bao gồm: UDP, TCP SYS, TCP ACK, TCP fragment, TCP NULL, TCP RST, TCP random flag, TCP ESTABLISHED packet flood. Nó có sẵn khả năng ngẫu nhiên hóa địa chỉ bên gởi. Trinity cũng hỗ trợ TCP flood packet với khả năng ngẫu nhân tập CONTROL FLAG. Trinity có thể nói là một trong số các công cụ DDoS nguy hiểm nhất.

- Ngoài ra có thể nhắc thêm về một số công cụ DDoS khác như Knight, được thiết kế chạy trên Windows, sử dụng kỹ thuật cài đặt của troijan back Orifice. Knight dùng các kỹ thuật tấn công như SYV, UDP Flood và Urgent Pointer Flooder.

- Sau cùng là Kaiten, là biến thể của Knight, hỗ trợ rất nhiều kỹ thuật tấn công như: UDP, TCP flood, SYN, PUSH + ACK attack. Kaiten cũng thừa hưởng khả năng ngẫu nhiên hóa địa chỉ giả mạo của Trinity.

# **6. Các cách phòng chống DoS/DdoS**

Trước khi thiết lập chính sách cho tường lửa, chúng ta cần lập tài liệu đánh giá phân tích rủi ro có thể sảy ra đối với các ứng dụng của tổ chức khi bị tấn công từ chối dịch vụ. Kết quả của sự phân tích này sẽ bao gồm một danh sách các ứng dụng, và phương pháp bảo vệ các ứng dụng này như thế nào. Rủi ro là mặt đối lập của bảo mật nên chúng ta thường cố gắng loại trừ nó. Tuy nhiên, thực tế cho thấy các rủi ro không bao giờ loại trừ hết được.

Các chính sách chống lại tấn công từ chối dịch vụ:

**Đặc quyền tối thiểu:** đây là nguyên tắc an ninh căn bản nhất. Mọi đối tượng tượng (người dùng, người quản trị, chương trình, hệ thống...) chỉ nên có đủ đặc quyền để đối tượng thực hiện nhiệm vụ của chúng. Ví dụ trong firewall ta nên thiết lập rule mặc định là chặn tất cả các gói tin đi từ mạng bên trong ra bên ngoài và ngược lại, sau đó thiết lập dịch vụ nào được chạy, những user nào có quyền được làm gì… Để hạn chế sự mở rộng của tấn công và tác hại của chúng.

**Kiểm soát dịch vụ:**  Xác định kiểu dịch vụ nào có thể được truy nhập (vào/ra). Ví dụ: Dịch vụ web, mail, FTP, telnet, SHH …

**Kiểm soát hướng:** Khi mở 1 dịch vụ sẽ cho request từ mạng nào vào (tin cậy hoặc không tin cây)

Ví dụ: Một mạng định nghĩa có 3 miền: interner, externer, DMZ. Trong miền DMZ cấu hình dịch vụ chia sẻ file FTP, chỉ cho phép những request từ miền interner và drop những request từ miền khác. Firewall kiểm soát hướng vào ra của gói tin.

**Kiểm soát số lượng connections trên 1 IP trong 1 đơn vị thời gian**: Hay nói các khác là giới hạn các gói SYN. Ví dụ chỉ cho phép 5 gói SYN tới server trong 3 giây nhiều hơn firewall sẽ chặn để giảm tải cho server không phải xử lí nhiều. Cách này là phương pháp tốt nhất để ngăn chặn SYN attack.

**Ngăn chặn Virus, Trojan, Worm**: đây là cách làm hạn chế quy mô của BOTNET và tạo sự an toàn cho mạng nội bộ. Một công cụ mà bất cứ ai sử dụng ISA Server đều phải sử dụng nó, đó là GFI’s Download Security. Đặc điểm chính của công cụ này, nó được tích hợp vào ISA Firewall và nó ngăn chặn các tập tin tự chạy .exe, kiểm soát các tập tin được download từ Internet về, kiểm tra ActiveX trong trình duyệt và đưa ra cảnh báo cho các user. Hoặc sử dụng công cụ từ các hảng bảo mật như BitDefender for ISA, Symantec AntiVirus for ISA Server,… Những kẻ tấn công có thể lợi dụng virus hay trojan này để điều khiển các máy trong mạng làm zombie để thực hiện tấn công DDOS. Khi tấn công xảy ra có thể làm nghẽn băng thông của mạng của tổ chức.

**Chuyển sang IPv6**: Nếu chuyển sang IPv6 thì 90% những kẻ hở của giao thức trong IPv4 sẽ bị loại bỏ và bởi thế, DDoS cũng bị loại bỏ 1 phần lớn.

Một trong những tính năng quan trọng của IPv6 là IPSec hoàn toàn được hỗ trợ (natively). Vì tính năng này, những dạng DDoS sử dụng reflection không thể thực hiện được vì các packets refection không có giá trị. Những dạng DDoS sử dụng spoof addresses như với IPv4 sẽ không thực hiện được với IPv6. Các dạng DDoS sử dụng biện pháp spoofing và reflection chiếm tỉ lệ rất lớn ở IPv4.

Khi chuyển sang IPv6, mỗi thiết bị được gán cho 1 IP riêng và nếu IP ấy dùng để DDoS thì nó sẽ bị ban vĩnh viễn. Giúp loại bỏ tác nhân DDoS.

Không may, với IPv6, dạng flood bằng TCP, UDP và ICMP vẫn không thể triệt tiêu vì cơ chế "bắt tay" vẫn không thay đổi. Tuy nhiên, vì IPv6 có thừa IP để cấp cho mỗi thiết một IP tĩnh riêng biệt cho nên nếu sử dụng biện pháp ban IP vi phạm thì chỉ ảnh hưởng có 1 người thay vì ban 1 IPv4 IP như hiện nay có thể ban hàng chục, hàng trăm hay hàng ngàn người (vì sử dụng proxy, nat....).

# **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.

DDOS đang và sẽ là vấn nạn nguy hại lớn cho nền Internet toàn cầu. 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.

# KẾT QUẢ THU ĐƯỢC VÀ PHƯƠNG HƯỚNG PHÁT TRIỂN

* Hiểu rõ bản chất, sự nguy hại của tấn công từ chối dịch vụ.
* Đối với tấn công DDOS với sự tham gia của nhiều máy tính. Người quản trị sẽ phải cấu hình Firewall chặn nhiều IP một cách thủ công dẫn tới không hiệu quả và có thể là tự từ chối dịch vụ của chính mình.Nên phương hướng phát triển tiếp theo là kết hợp giữa IDS đưa ra hành động và giới hạn thời gian chặn và Firewall thực hiện tạo thành IPS.

# TÀI LIỆU THAM KHẢO

**[1]** DoS và DDoS toàn tập

http://vnexperts.net/bai-viet-ky-thuat/security/664-dos-va-ddos-toan-tp-phn-i.html

**[2]** Distributed Reflection Denial of Service - Tấn công từ chối dịch vụ bằng phương pháp phản xạ nhiều vùng

http://www.hvaonline.net/hvaonline/posts/list/156.hva

**[3]** [DLD00] S. Dietrich, N. Long, and D. Dittrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case," Proceedings of 14th USENIX Systems Administration Conference (LISA 2000), December 2000, pp. 329–339, http://www.adelphi.edu/~spock/lisa2000-shaft.pdf.

**[4]** D. Dittrich, "Analysis of the "Power" Bot," August 2001, http://staff.washington.edu/dittrich/misc/power.analysis.txt

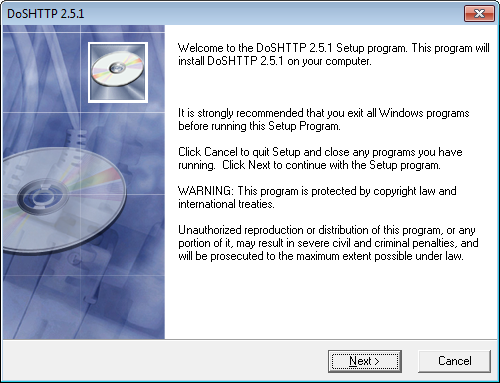
**[5]** K. J. Houle, G. M. Weaver, N. Long, and R. Thomas, Trends in Denial of Service Attack Technology, Technical Report, CERT Coordination Center, October 2001, http://www.cert.org/archive/pdf/DoS\_trends.pdf.

**[6]** [Dith] D. Dittrich, "The Tribe Flood Network Distributed Denial of Service Attack

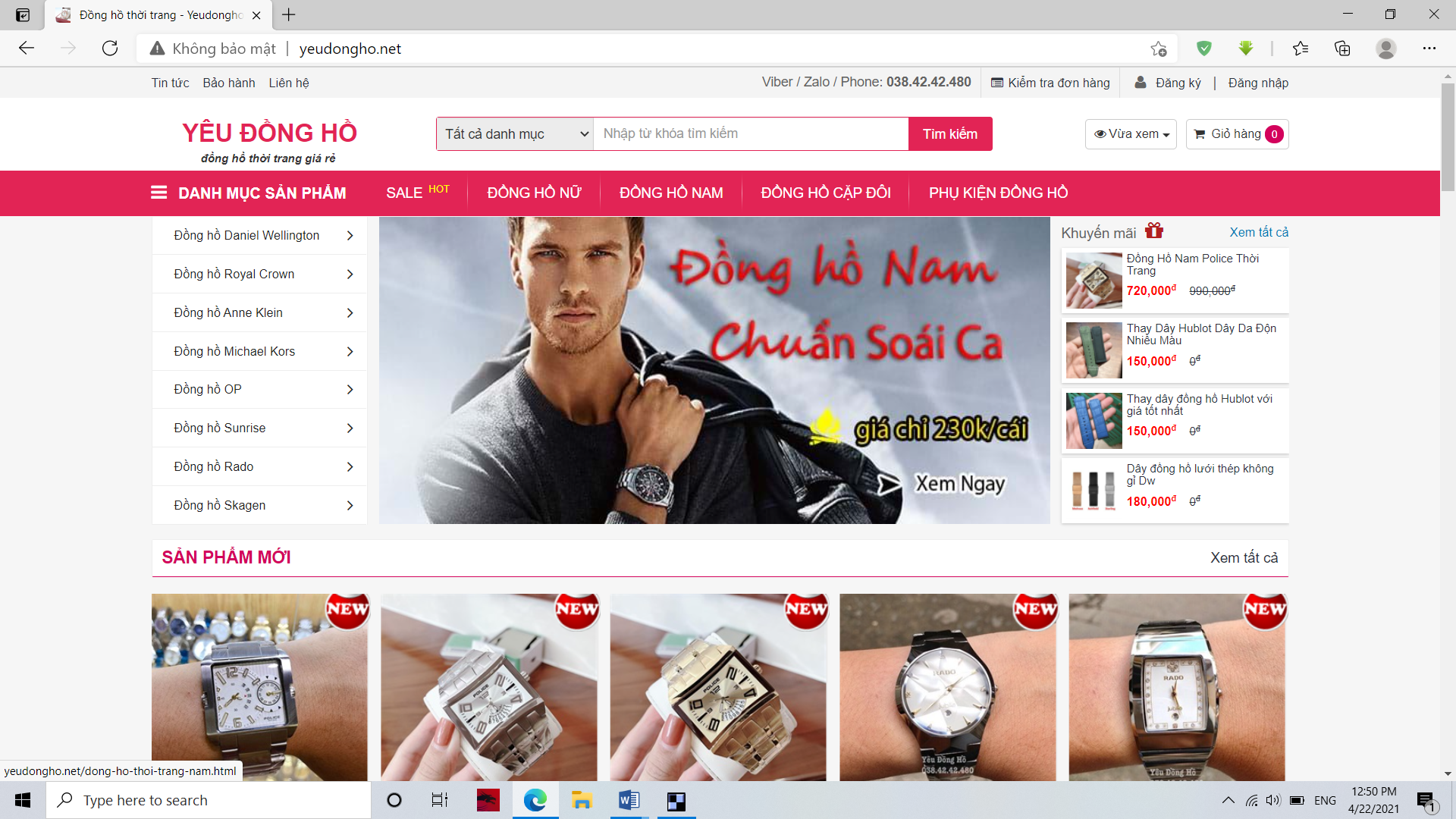
Tool," October 1999, http://staff.washington.edu/dittrich/misc/tfn.analysis.txt.

# **Kịch Bản Thử Nghiệm**

**Bước 1:** Cài đặt DoSHTTP 2.5.1

****

**Bước 2:** Vào Website mục tiêu để kiểm tra **: yeudongho.net**



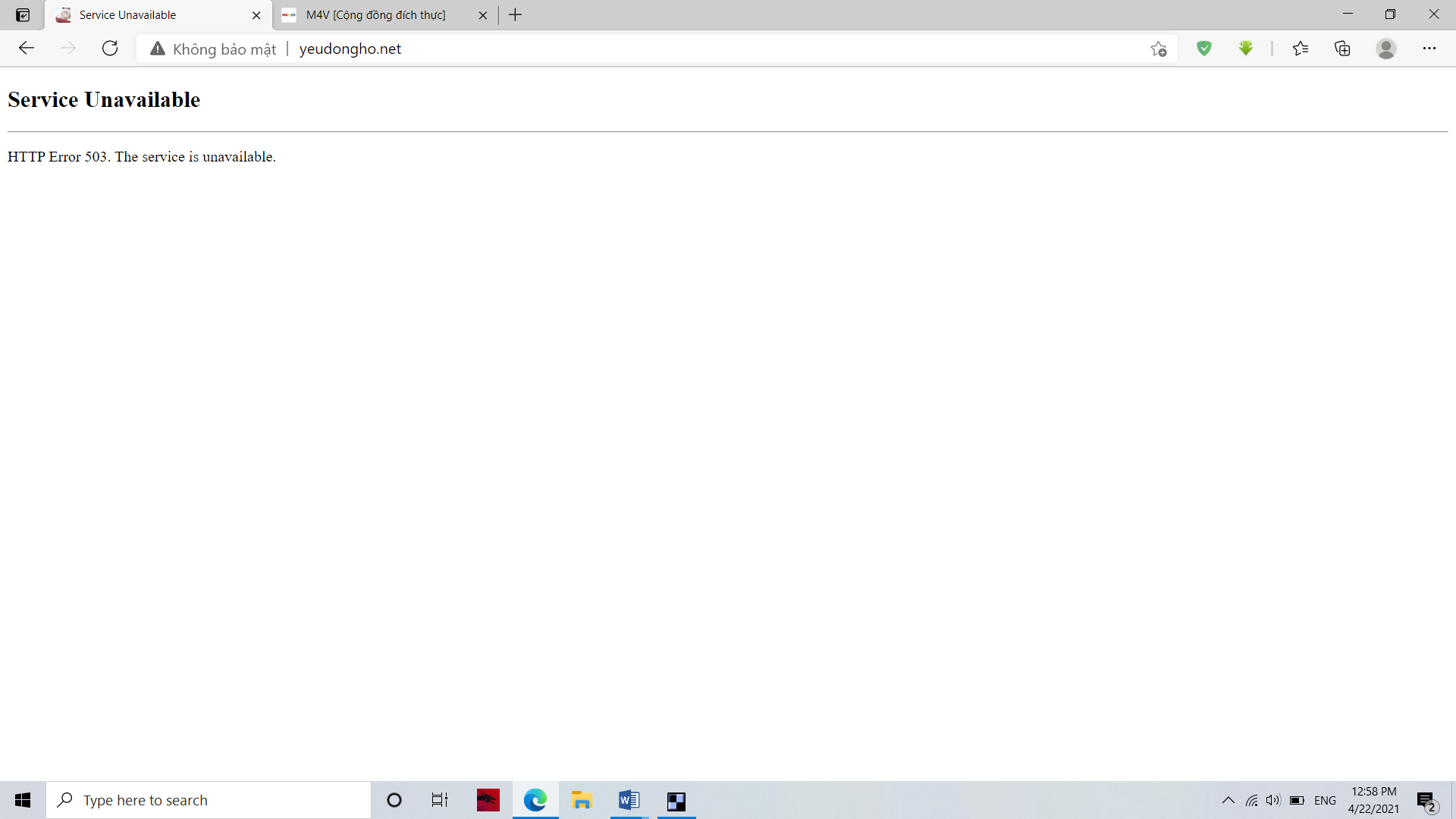
**Bước 3:** Xác định mục tiêu và bắt đầu tấn cônglà **: yeudongho.net**

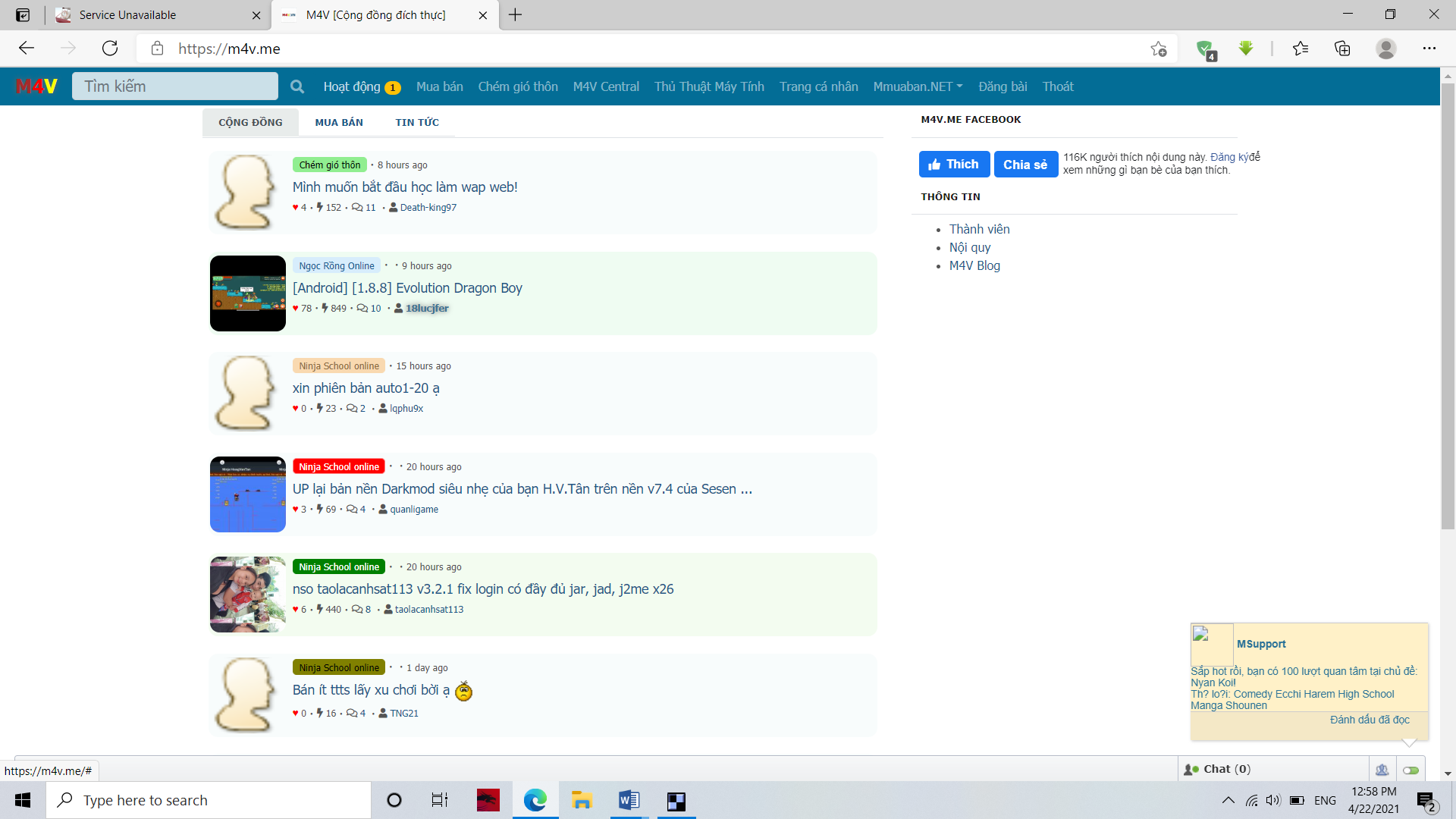
****

Nhấn vào đây để thực hiện DDoS

Nhập địa chỉ web vào đây

**Bước 4:** Kiểm tra Website bằng cách vào lại Website 1 lần nữa và đồng thời mở một trang web bất kì ở cửa sổ khác (ở đây là trang www.m4v.me), ta thấy rằng **yeudongho.net** không thể truy cập vào được trong khi đó trang m4v.vn vẫn có thể truy cập được.





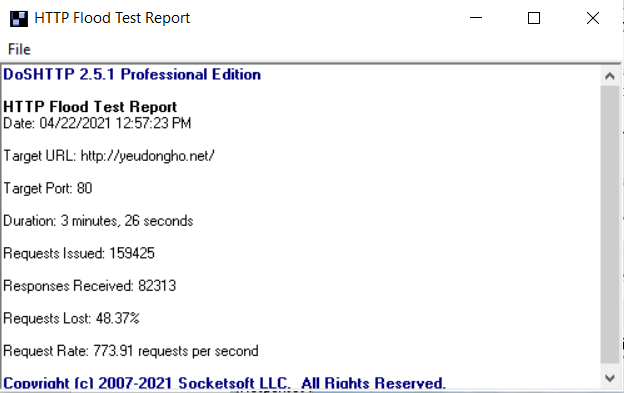
**Bước 5:** Tắt phần mềm

****

Số request được gửi đi

Nhấn vào đây để kết thúc DDoS

**Bước 6:** File báo cáo sau khi sử dụng phần mềm DoSHTTP 2.5.1



**NHẬN XÉT:** Tuy việc demo chỉ diễn ra nhanh (khoảng 1 phút 14 giây) với một tool DoSHTTP đơn giản nhưng trang web yeudongho.net đã không thể chịu nổi sức phá hoại của việc DoS khiến cho việc truy cập vào trang web không thể thực hiện được. Qua đó có thể hình dung ra được sức phá hoại kinh khủng của các tool DoS và DDoS khác nếu như được sử dụng để phá hoại một website có chủ đích và kế hoạch là như thế nào, việc đó có thể giết chết website đó nếu không có sự phòng chống từ trước. Vì vậy nên chúng ta cần áp dụng một số phương pháp để phòng chống DoS và DDoS.