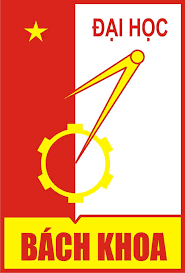
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI



**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

Tt (13)



**BÁO CÁO BÀI TẬP LỚN NHẬP MÔN AN TOÀN THÔNG TIN**

**Đề tài: Tìm hiểu các dạng tấn công từ chối dịch vụ**

Giáo viên hướng dẫn: **PGS.TS. Nguyễn Linh Giang**

Sinh viên thực hiện:

**Nguyễn Văn Khoa – 20173196**

**Trần Văn Định – 20173017**

**Chử Việt Hoàng – 20173135**

**Tống Mạnh Đạt – 20173008**

***Hà Nội, ngày 08 tháng 06 năm 2020.***

*Tt (19)*

Mục lục

[**I - Tấn công từ chối dịch vụ (DoS)** 3](#_Toc42276483)

[**A.** **Giới thiệu về DoS** 3](#_Toc42276484)

[**B.** **Lịch sử các cuộc tấn công và phát triển của DoS** 3](#_Toc42276485)

[**C.** **Mục đích của tấn công DoS và hiểm họa** 4](#_Toc42276486)

[**D.** **Các hình thức tấn công DoS cơ bản** 5](#_Toc42276487)

[**II - Tấn công từ chối dịch vụ phân tán (DDoS)** 11](#_Toc42276488)

[**A.** **Giới thiệu chung DDoS** 11](#_Toc42276489)

[**E.** **Phân loại tấn công DDoS** 14](#_Toc42276490)

[**III - DRDoS (Distributed Reflection Denial of Service)** 17](#_Toc42276491)

[**A.** **Giới thiệu về DRDOS** 17](#_Toc42276492)

**CÁC DẠNG TẤN CÔNG TỪ CHỐI DỊCH VỤ**

## **I - Tấn công từ chối dịch vụ (DoS)**

### **Giới thiệu về DoS**

* Tấn công DoS là một kiểu tấn công mà một người 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

### **Lịch sử các cuộc tấn công và phát triển của DoS**

* Các tấn công DoS bắt vào khoảng những năm 90. Đầu tiên chúng hoàn toàn “nguyên thủy”, bao gồm chỉ một kẻ tấn công khai thác băng thông tối đa từ nạn nhân, ngăn những người khác được phục vụ. Điều này được thực hiện chủ yếu bằng cách dùng các phương pháp đơn giản như ping floods, SYN floods và UDP floods. Sau các cuộc tấn công trở nên phức tạp hơn, bằng cách giả làm nạn nhân gửi vài thông điệp và để các máy khác làm ngập máy nạn nhân với các thông điệp trả lời (Smurf attack, IP spoofing…).
* Các tấn công này phải được đồng bộ hóa một cách thủ công bởi nhiều kẻ tấn công để tạo ra một sự phá hủy có hiệu quả. Sự dịch chuyển đến việc tự động hóa sự đồng bộ, kết hợp này và tạo ra một tấn công song song lớn nhất trở nên phổ biến từ 1997, với sự ra đời của công cụ tấn công DDoS đầu tiên được công bố rộng rãi, đó là Trinoo. Nó dựa trên tấn công UDP flood và các giao tiếp master-slave (khiến các máy trung gian tham gia vào trong cuộc tấn công bằng cách đặt lên chúng các chương trình được điều khiển từ xa). Trong những năm tiếp theo, vài công cụ nữa được phổ biến - TFN (tribe flood network), TFN2K, vaf Stacheldraht.
* Tuy nhiên, chỉ từ cuối năm 1999 mới có những báo cáo về những tấn công như vậy, và đề tài này được công chúng biết đến chỉ sau khi một cuộc tấn công lớn vào các site công cộng tháng 2/2000. Trong thời gian 3 ngày, các site Yahoo.com, amazone.com, buy.com, cnn.com và eBay.com đã đặt dưới sự tấn công (ví dự như Yahoo bị ping với tốc độ 1GB/s).
* Từ đó các cuộc tấn công Dos thường xuyên xảy ra

**Ví dụ:**

* Vào ngày 15 tháng 8 năm 2003, Microsoft đã chịu đợt tấn công DoS cực mạnh 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 AI-Jazeera bị tấn công làm gián đoạn trong nhiều giờ
* Gần đây nhất là 2 vụ DDos lớn vào các trang mạng đông người truy cập ở Việt Nam là: DDos vào VCCorp gây chấn động an ninh mạng ở Việt Nam trong thời gian gần đây, hacker phá hoại server gây lỗi data center hàng loạt website báo mạng như: Dân trí, Kênh 14, Soha v.v.v (chưa tìm ra thủ phạm), và vụ thứ 2 là DDos vào diễn đàn công nghệ thông tin VN-Zoom vào lúc 19 giờ ngày 26/10/2014 (do JCAlex Min thực hiện)

### **Mục đích của tấn công DoS và hiểm họa**

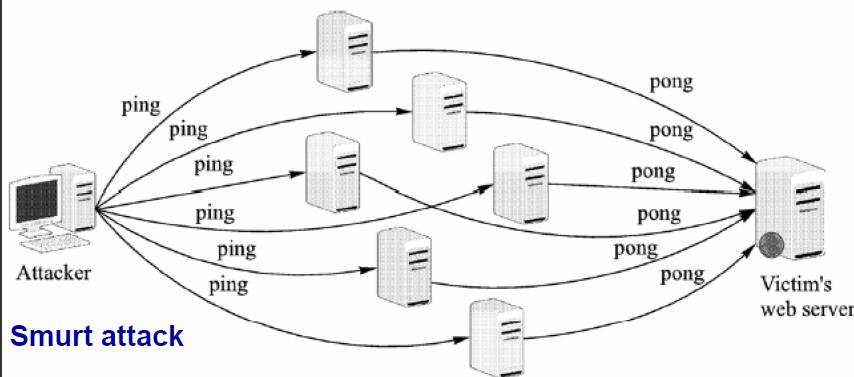
* Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (Flood), khi hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường
* Cố gắng làm ngắt kết nối giữa hai máy, mà ngăn chặn quá trình truy cập vào dịch vụ
* Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó
* Cố gắng ngăn chặn các 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
* 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 đề là mục tiêu của tấn công DoS.
* Tấn công vào hệ thống khác phục vụ cho mạng máy tính như: hệ thống điều hòa, hệ thống điện, hệ thống 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 hòa...

### **Các hình thức tấn công DoS cơ bản**

* *Smurf*
* *Buffer Overflow Attack*
* *Ping of death*
* *Teardrop*
* *SYN Attack*

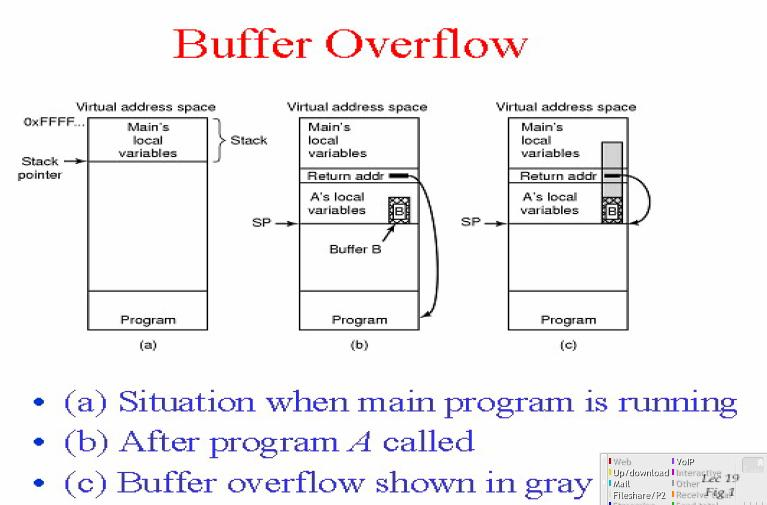
#### **Smurf**

* Smurf: là một loại tấn công DoS điển hình. Máy chủ attacker sẽ gửi rất nhiều lệnh ping đến một số lượng lớn máy tính trong một thời gian ngắn, trong đó địa chỉ IP nguồn của gói ICMP echo sẽ được thay thế bởi địa chỉ IP của nạn nhân. Các máy tính này sẽ trả lại các gói ICMP reply đến máy nạn nhân
* Kết quả: mục tiêu bị tấn công sẽ phải chịu nhận một đợt reply gói ICMP cực lớn và làm cho mạng bị rớt hoặc bị chậm lại, không có khả năng đáp ứng các dịch vụ khác



#### **Buffer Overflow Attack**

* 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
* Quá trình gửi một bức thư điện tử mà file đính kèm quá 256 ký tự có thể sẽ xảy ra quá trình tràn bộ nhớ đệm



#### **Ping of death**

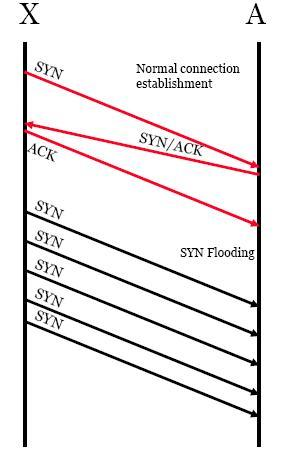
* Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của tin IP là 65.536 bytes
* Quá trình chia nhỏ gói tin IP thành những phần nhỏ được thực hiện ở layer II
* Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.536 bytes. Nhưng hệ điều hành không thể nhận biết được độ lớn của gói 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
* VD: ping -l 65500 address
  + - -l: buffer size
* Khoảng năm 1997 - 1998, lỗi này đã được fix, vì vậy bây giờ nó chỉ mang tính lịch sử

#### **Teardrop**

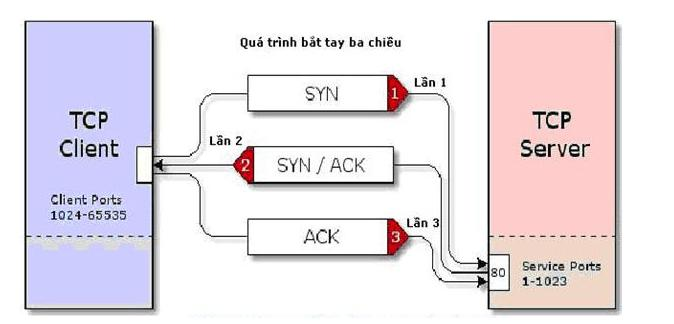
* Trong mạng chuyển mạch gói, dữ liệu được chia thành nhiều gói tin nhỏ, mỗi gói tin có một giá trị offset riêng và có thể truyền đi theo nhiều con đường khác nhau để tới đích. Tại đích, nhờ vào giá trị offset của từng gói tin mà dữ liệu lại được kết hợp lại như ban đầu.
* Lợi dụng điều này, hacker có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công
* Kết quả: máy tính đích không thể sắp xếp được những gói tin này và dẫn tới bị treo máy vì bị “vắt kiệt” khả năng xử lý

#### **SYN Attack**

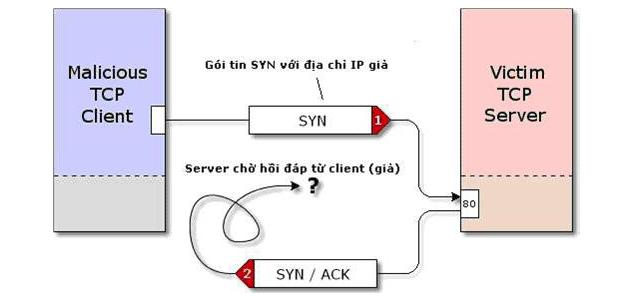
* Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối
* Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện request TCP SYN và lúc này máy chủ không còn khả năng đáp lại - kết nối không thực hiện được



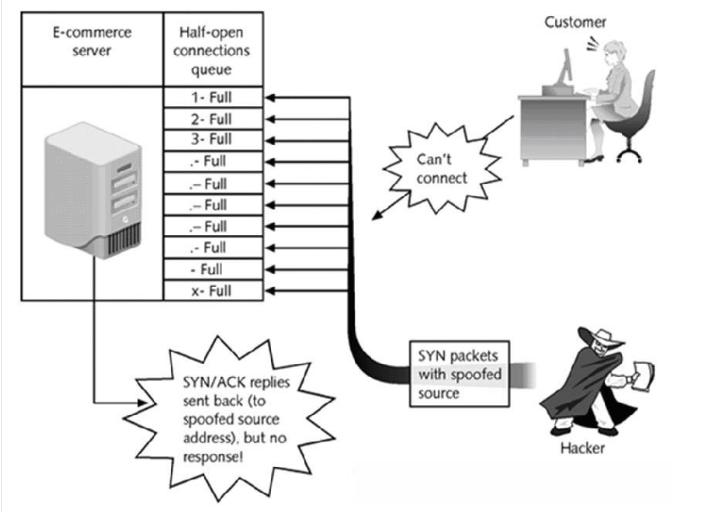
*Mô hình tấn công bằng các gói SYN*



* Bước 1: Client (máy khách) sẽ gửi các gói tin (packet chứa SYN = 1) đến máy chủ để yêu cầu kết nối
* Bước 2: Khi nhận được gói tin này server sẽ gửi lại gói tin SYN/ACK để thông báo cho client biết là đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ dành một phần tài nguyên hệ thống như bộ nhớ đệm (cache) để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của client như địa chỉ IP và cổng (port) cũng được ghi nhận
* Bước 3: Cuối cùng, client hoàn tất việc bắt tay ba lần bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối



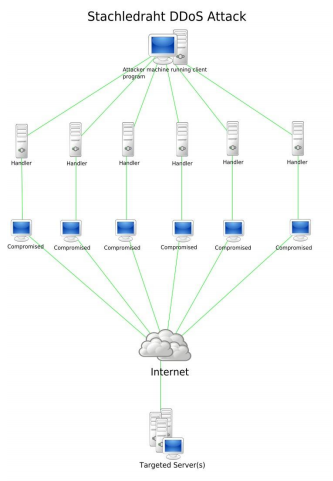
* Do TCP là thủ tục tin cậy trong việc giao nhận (end-to-end) nên trong lần bắt tay thứ hai, server gửi các gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho client đến khi nào nhận được hồi đáp của máy client



* Nếu quá trình đó kéo dài, server sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng crash (treo) nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng được. Có thể hình dung quá trình này cũng giống như khi máy tính cá nhân (PC) hay bị “treo” khi mở cùng lúc quá nhiều chương trình

## **II - Tấn công từ chối dịch vụ phân tán (DDoS)**

### **Giới thiệu chung DDoS**



* Trên Internet tấn công **Distributed Denial of Service (DDoS)** hay còn gọi là **Tấn công từ chối dịch vụ phân tán** là một dạng tấn công từ nhiều máy tính tới một đích 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 có thể gây tình trạng tương tự như hệ thống bị shutdown.
* 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 thể này thành hai loại dựa trên mục đích tấn công
* Làm cạn kiệt băng thông.
* Làm cạn kiệt tài nguyên hệ thống.
* Một cuộc tấn công từ chối dịch vụ cụ thể bao gồm cả việc thực thi malware nhằm:
* Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.
* Những lỗi gọi tức thì trong microcode của máy tính
* Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị đơ.
* Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên hoặc bị thrashing. VD: như sử dụng tất cả các năng lực có sẵn dẫn đến không một công việc nào có thể hoàn thành được.
* Gây crash hệ thống
* Tấn công từ chối dịch vụ iFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn

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 mạng Bot được sử dụng để tấn công thường được gọi là "secondary victims".
* 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 mạng Bot trên internet thực hiện tấn công DoS và được gọi là tấn công DDoS.

1. **Tấn công DDoS không thể ngăn chặn hoàn toàn**

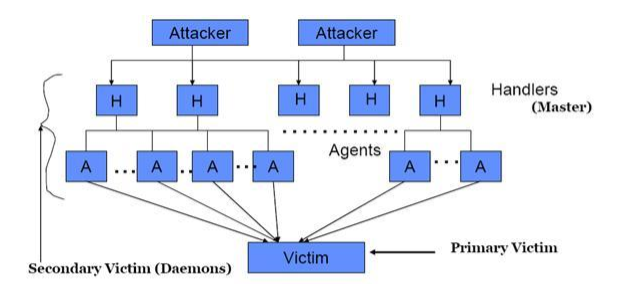
* Các dạng tấn công DDoS thực hiện tìm kiếm các lỗ hổng bảo mật trên các máy tính kết nối tới Internet và khai thác các lỗ hổng bảo mật để xây dựng mạng Botnet gồm nhiều máy tính kết nối tới Internet.
* Một tấn công DDoS được thực hiện sẽ rất khó để ngăn chặn hoàn toàn.
* Những gói tin đến Firewall có 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.

1. **Kẻ tấn công khôn ngoan**

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.

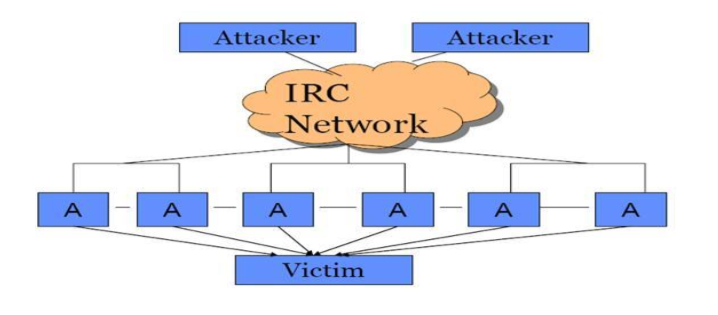
#### **Agent Handler Model:**

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



#### **Tấn công DDoS dựa trên nền tảng IRC:**

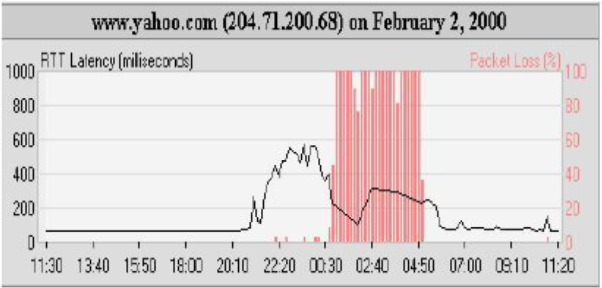
* Kẻ tấn công sử dụng các mạng IRC để điều khiển, khuếch đại và quản lý kết nối với các máy tính trong mạng Botnet.



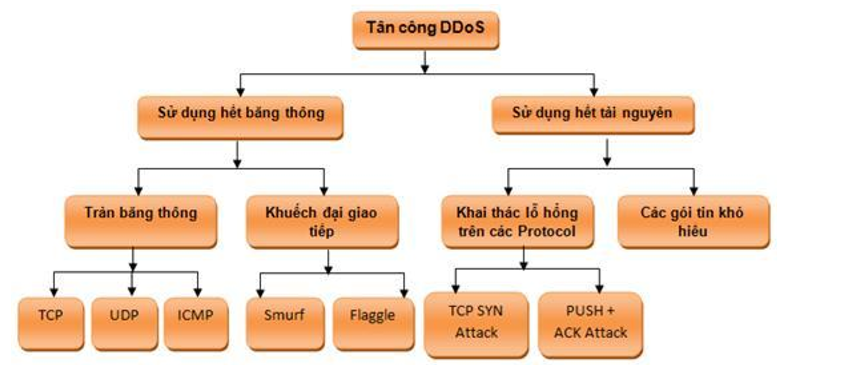
### **Phân loại tấn công DDoS**

* Tấn công gây hết băng thông truy cập tới máy chủ.
* Flood attack
* UDP và ICMP Flood (flood- gây ngập lụt)
* Tấn công khuếch đại các giao tiếp
* Smurf and Fraggle attack

*Tấn công DDos vào Yahoo.com năm 2000*

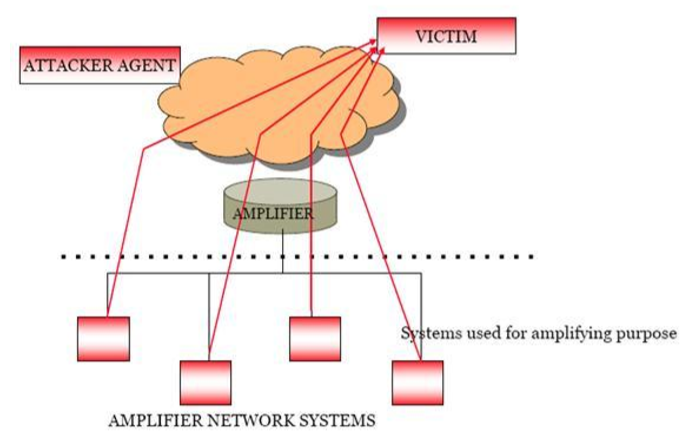


***Sơ đồ phân loại tấn công***



**Sơ đồ tấn công DDoS ở dạng khuếch đại giao tiếp:**

* Như chúng ta đã biết, tấn công Smurf là tấn công bằng cách Ping đến địa chỉ Broadcast của một mạng nào đó mà địa chỉ nguồn chính là địa chỉ của máy cần tấn công, khi đó toàn bộ các gói Reply sẽ được chuyển tới địa chỉ IP của máy tính bị tấn công.



1. **Tấn công Reflective DNS (reflective – phản chiếu)**

#### **Các vấn đề liên quan tới tấn công Reflective DNS:**

* Một Hacker có thể sử dụng botnet để gửi rất nhiều yêu cầu tới máy chủ DNS.
* Những yêu cầu sẽ làm tràn băng thông mạng của các máy chủ DNS.
* Việc phòng chống dạng tấn công này có thể dùng Firewall ngăn cấm những giao tiếp từ các máy tính được phát hiện ra
* Nhưng việc cấm các giao tiếp từ DNS Server sẽ có nhiều vấn đề lớn. Một DNS Server có nhiệm vụ rất quan trọng trên Internet.
* Việc cấm các giao tiếp DNS đồng nghĩa với việc cấm người dùng bình thường gửi email và truy cập Website.
* Một yêu cầu về DNS thường chiếm bằng 1/73 thời gian của gói tin trả lời trên máy chủ. Dựa vào yếu tố này nếu dùng một Tools chuyên nghiệp để làm tăng các yêu cầu tới máy chủ DNS sẽ khiến máy chủ DNS bị quá tải và không thể đáp ứng cho các người dùng bình thường được nữa.

#### **Tool tấn công Reflective DNS - ihateperl.pl:**

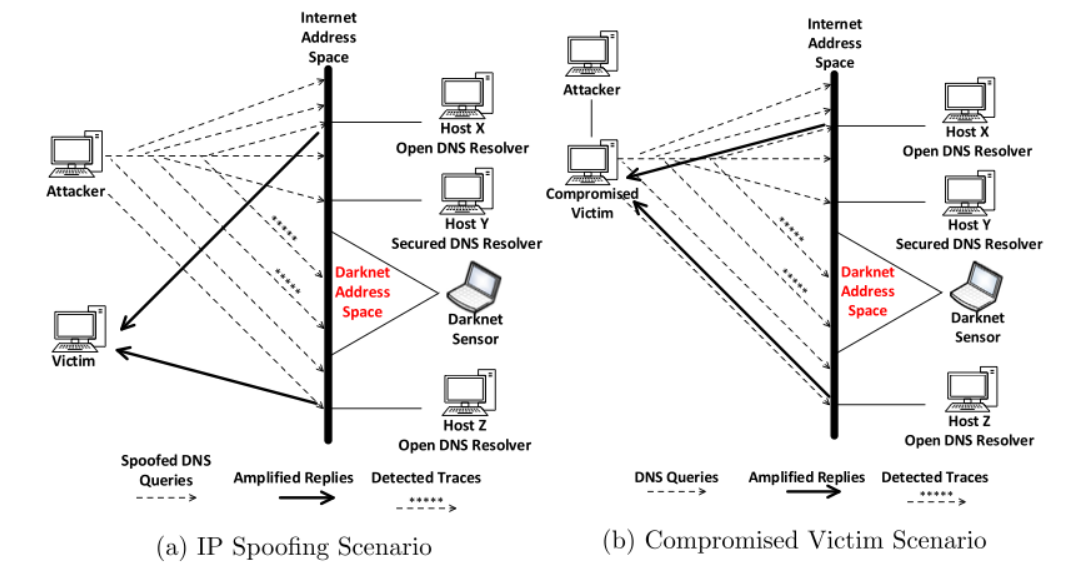
* Ihateperl.pl là chương trình rất nhỏ, rất hiệu quả, dựa trên kiểu tấn công DNS - Reflective.
* Nó sử dụng một danh sách các máy chủ DNS để làm tràn hệ thống mạng với các gói yêu cầu Name Resolution.
* Bằng một ví dụ nó có thể sử dụng google.com để resole gửi tới máy chủ và có thể đổi tên domain đó thành [www.vnexperts.net](http://www.vnexperts.net) hay bất kì một trang web nào mà kẻ tấn công muốn.
* Cách sử dụng công cụ này rất đơn giản: ta chỉ cần tạo ra một danh sách các máy chủ DNS, chuyển cho địa chỉ IP của máy tính cá nhân và thiết lập số lượng các giao tiếp

1. **Các tools sử dụng để tấn công DDoS**

* 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 được download miễn phí trên Internet và lưu ý đây chỉ là tools yếu để mang tính Demo về tấn công DDoS mà thôi (nguồn https://www.softwaretestinghelp.com/ddos-attack-tools/)

## **III - DRDoS (Distributed Reflection Denial of Service)**

### **Giới thiệu về DRDOS**

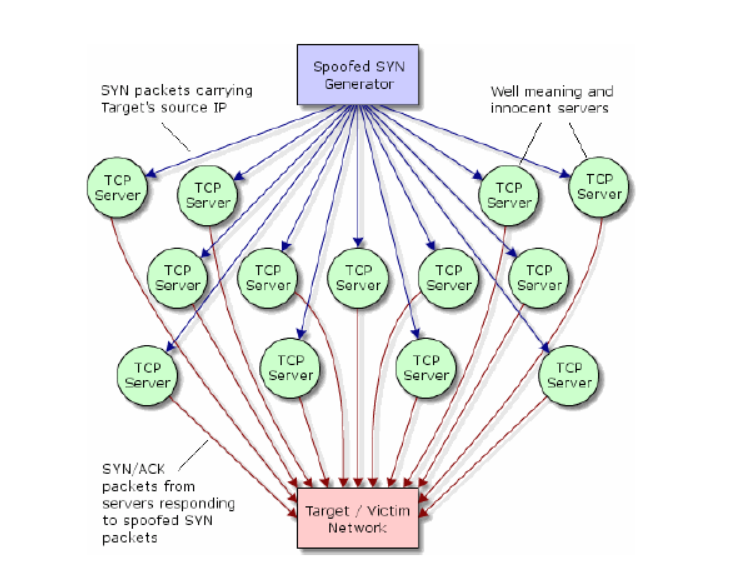
****

* Vào lúc 2 giờ sáng ngày 11 - 1 - 2002, Trang web GRC.COM đã bị đánh tung khỏi Internet bằng một kiểu tấn công từ chối dịch vụ mới. 1072519399 packet bị chặn đứng trước khi cuộc tấn công bị dừng. Đây chính là những thông tin được Steve Gibson mô tả trong bài báo về DRDoS
* Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy chủ, tức là làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ vào xương sống của Internet và tiêu hao tài nguyên máy chủ. Nếu được thực hiện bởi kẻ tấn công có tay nghề thì nó có thể hạ gục bất cứ hệ thống nào trên toàn thế giới trong phút chốc
* DRDoS là thế hệ tiếp theo của DDOS, phối hợp giữa hai kiểu DoS và DDoS
* Bây giờ, chúng ta hãy nhớ lại phương pháp SYN attack truyền thống của DoS, phương pháp này dựa trên bước thứ nhất để mở connection của TCP để tạo các “open half” connection làm Server bị ăn mòn hết tài nguyên. Các SYN packet được gửi trực tiếp đến Server sau khi đã giả mạo IP nguồn. IP giả mạo sẽ là 1 IP không có thật trên Internet để cho Server không thể nào hoàn thành được connection.



* Ta có Server A và Victim, giả sử ta gửi 1 SYN packet đến Server A trong đó IP nguồn đã bị giả mạo thành IP của Victim, khi đó Server A sẽ mở 1 connection và gửi SYN/ACK packet cho Victim vì nghĩ rằng Victim muốn mở connection với mình. Và đây chính là khái niệm của Reflection (Phản xạ). Hacker sẽ điều khiển Spoof SYN generator, gửi SYN packet đến tất cả các TCP Server lớn, lúc này các TCP Server này vô tình thành Zombie cho Hacker để cùng tấn công Victim và làm nghẽn đường truyền của Victim.

→ Với nhiều server lớn tham gia nên server mục tiêu sẽ nhanh chóng bị quá tải, bandwidth bị chiếm dụng bởi server lớn.



* Tính “nghệ thuật” là ở chỗ chỉ cần với một máy tính với modem 56kbps, một hacker lành nghề có thể đánh bại bất cứ máy chủ nào trong giây lát mà không cần chiếm đoạt bất cứ máy nào để làm phương tiện thực hiện tấn công.

1. **Cách phòng chống**

* Có rất nhiều giải pháp và ý tưởng được đưa ra nhằm đối phó với các cuộc tấn công kiểu DDoS. Tuy nhiên không có giải pháp và ý tưởng nào là giải quyết trọn vẹn bài toán Anti-DDoS. Các hình thái khác nhau của DDoS liên tục xuất hiện theo thời gian song song với các biện pháp đối phó, tuy nhiên cuộc đua vẫn tuân thủ theo quy luật tất yếu của bảo mật máy tính:” Hacker luôn đi trước giới bảo mật một bước”.
* **Có 3 giai đoạn chính trong quá trình Anti-DDoS:**
* Giai đoạn ngăn người: tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler
* Giai đoạn đối đầu với cuộc tấn công: phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.
* Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm

Các giai đoạn chi tiết trong phòng chống DRDoS:

1. **Tối thiểu hóa lượng Agent:**

* Từ phía User: một phương pháp rất tốt để ngăn ngừa tấn công DDoS là từng internet của user sẽ tự đề phòng không để bị lợi dụng tấn công hệ thống khác. Muốn đạt được điều này thì ý thức và kỹ thuật phòng chống phải được phổ biến rộng rãi cho các internet user. Attack-Network sẽ không bao giờ hình thành nếu không có user nào bị lợi dụng thành Agent. Các user phải liên tục thực hiện các quá trình bảo mật trên máy vi tính của mình. Họ phải tự kiểm tra sự hiện diện của các Agent trên máy của mình, điều này là rất khó khăn đối với user thông thường.
* Một số giải pháp tích hợp sẵn khả năng ngăn ngừa việc cài đặt code nguy hiểm vào hardware và software của từng hệ thống. Về phía user họ nên cài đặt và update liên tục software như antivirus, anti trojan và server patch của hệ điều hành.
* Từ phía Network Service Provider: thay đổi cách tính tiền dịch vụ truy cập theo dung lượng sẽ làm cho các user lưu ý đến những gì họ gửi, như vậy về mặt ý thức tăng cường phát hiện DDoS Agent sẽ tự nâng cao ở mỗi User.

1. **Tìm và vô hiệu hóa các Handler:**

* Nhân tố vô cùng quan trọng trong attack-network là Handler, nếu có thể phát hiện và vô hiệu hóa Handler thì khả năng Anti-DDoS thành công là rất cao. Bằng cách theo dõi các giao tiếp giữa Handler và Client hay Handler và Agent ta có thể phát hiện ra vị trí của Handler. Do một Handler quản lý nhiều, nên triệt tiêu được một Handler cũng có nghĩa là loại bỏ một lượng đáng kể các Agent trong Attack- Network.

1. **Phát hiện dấu hiệu của một cuộc tấn công:**

Có nhiều kỹ thuật được áp dụng:

* *Agress Filtering:* Kỹ thuật này kiểm tra xem một packet có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của một subnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các packet từ bên trong subnet gửi ra ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của internet thì khái niệm giả mạo địa chỉ IP sẽ không còn tồn tại.
* *MIB statistics:* trong Management Information Base( SNMP) của route luôn có thông tin thống kê về sự biến thiên trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của protocol mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo “quỹ thời gian vàng” cho việc xử lý tình huống.

1. **làm suy giảm hay dừng cuộc tấn công:**

Dùng các kỹ thuật sau:

* *Load balancing:* Thiết lập kiến trúc cân bằng tải cho các server trọng điểm sẽ làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDoS. Tuy nhiên, điều này không có nghĩa lắm về mặt thực tiễn vì quy mô của cuộc tấn công là không có giới hạn.
* *Throttling:* thiết lập cơ chế điều tiết trên router, quy định khoảng tải hợp lý mà server bên trong có thể xử lý được. Phương pháp này cũng có thể được dùng để ngăn chặn khả năng DDoS traffic không cho user truy cập dịch vụ. Hạn chế của kỹ thuật này là không phân biệt được giữa các loại traffic, đôi khi làm dịch vụ bị gián đoạn với user, DDoS traffic vẫn có thể xâm nhập vào mạng dịch vụ nhưng số lượng hữu hạn.
* *Drop request:* Thiết lập cơ chế drop request nếu nó vi phạm một số quy định như: thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gân deadlock. Kỹ thuật này triệt tiêu khả năng làm cạn kiệt năng lực hệ thống, tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống, cần cân nhắc khi sử dụng.

1. **Chuyển hướng của cuộc tấn công:**

* Honeyspots: kỹ thuật đang được nghiên cứu. Là một hệ thống được thiết kế nhằm đánh lừa attacker tấn công vào khi xâm nhập hệ thống mà không chú ý đến hệ thống quan trọng thực sự.
* Honeyspots không chỉ đóng vai trò “Lê Lai cứu chúa” mà còn rất hiệu quả trong việc phát hiện và xử lý xâm nhập, vì trên Honeyspots đã thiết lập sẵn các cơ chế giám sát và báo động.
* Ngoài ra Honeyspots còn có giá trị trong việc học hỏi và rút kinh nghiệm từ Attacker, do Honeyspots ghi nhận khá chi tiết mọi động thái của attacker trên hệ thống. Nếu attacker bị đánh lừa và cài đặt Agent hay Handler lên Honeyspots thì khả năng bị triệt tiêu toàn bộ attack-network là rất cao.

1. **Giai đoạn sau tấn công:**

Trong giai đoạn này thông thường thực hiện các công việc sau:

* Traffic Pattern Analysis: Nếu dữ liệu về hệ thống kê biến thiên lượng traffic theo thời gian đã được lưu lại thì sẽ được đưa ra phân tích. Quá trình phân tích này rất có lợi cho việc tinh chỉnh lại hệ thống Load Balancing và Throttling. Ngoài ra các dữ liệu này còn giúp quản trị mạng điều chỉnh lại các quy tắc kiểm soát traffic ra vào mạng của mình.
* Packet Traceback: bằng cách dùng kỹ thuật Traceback ta có thể truy ngược lại vị trí của Attacker ( ít nhất là subnet của attacker). Từ kỹ thuật Traceback ta phát triển thêm khả năng Block Traceback từ attack khá hữu hiệu. Gần đây đã có một kỹ thuật Traceback khá hiệu quả có thể truy tìm nguồn gốc của cuộc tấn công dưới 15 phút, đó là kỹ thuật XXX.
* Bevent logs: Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể ra nhiều manh mối và chứng cứ quan trọng.

1. **Phòng chống tổng quát:**

* Khi bạn phát hiện máy chủ mình bị tấn công hãy nhanh chóng truy tìm địa chỉ IP đó và cấm không cho gửi dữ liệu đến máy chủ.
* Dùng tính năng lọc dữ liệu của router/firewall để loại bỏ các packet không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.
* Sử dụng các tính năng cho phép đặt limit trên router/firewall để hạn chế số lượng packet vào hệ thống.
* Nếu bị tấn công do lỗi phần mềm hay thiết bị thì nhanh chóng cập nhật các bản sửa lỗi cho hệ thống đó hoặc thay thế.
* Dùng một số cơ chế, công cụ, phần mềm để chống lại TCP SYN Flooding.
* Tắt các dịch vụ khác nếu có trên máy chủ để giảm tải và có thể đáp ứng tốt hơn. Nếu được có thể nâng cấp các thiết bị phần cứng để nâng cao khả năng đáp ứng của hệ thống hay sử dụng thêm các máy chủ cung tính năng khác để phân chia tải.
* Tạm thời chuyển máy chủ sang một địa chỉ khác.

**VI - Tài liệu tham khảo**

1. **Sách**

[1] – Tactical Perimeter Defense

[2] – Slide “An Toàn Mạng” – ThS T. Ng. Nhật Quang  
**2. Website**

[1] - <http://www.hvaonline.net>

[2] - <http://ceh.vn>

[3] - http://huynhdegroup.ne

[4] - http://handsteamsys.com