ĐỒ ÁN TỐT NGHIỆP - TÌM HIỂU VỀ TẤN CÔNG TRÊN MẠNG DÙNG KỸ THUẬT DOS DDOS

DISTRIBUTED DENIAL OF SERVICE (DDOS)

GIỚI THIỆU

Distributed Denial Of Service (DDoS) là kỹ thuật tấn công làm các ISP lo âu, giới hacker chính thống thì không công nhận DdoS là kỹ thuật tấn công chính thống. Thế nhưng Black hat đang có rất nhiều ưu thế khi triển khai tấn công bằng kỹ thuật DdoS.

Việc phòng ngừa và ngăn chặn DdoS vẫn còn đang thực hiện ở mức độ khắc phục hậu quả và truy tìm thủ phạm. Vậy DdoS là gì mà có nhiều yếu tố đặc biệt như vậy? Bài viết này cố gắng trả lời câu hỏi này dưới lăng kính security. Bố cục bài viết gồm:

→ Giới thiệu về DDoS
→ Phân tích các loại tấn công kiểu DDoS
→ Phân tích các kỹ thuật Anti-DDoS
→ Nhân tố con người trong Anti- DDoS
→ Một số trường hợp tấn công DDoS

PHẦN I: GIỚI THIỆU VỀ DDOS

1/ Ngày 7/3/2000, yahoo.com đã phải ngưng phục vụ hàng trăm triệu user trên toàn thế giới nhiều giờ liền. Vài giờ sau, Yahoo đã tìm ra nguyên nhân gây nên tình trạng này, họ đang phải gánh chịu một đợt tấn công DDoS với quy mô vài ngàn máy tính liên tục gửi hàng triệu request đến các server dịch vụ làm các server này không thể phục vụ các user thông thường khác

Vài ngày sau, một sự kiện tương tự diễn ra nhưng có phần "ồn ào" hơn do một trong các nạn nhân mới là hãng tin CNN, amazon.com, buy.com, Zdnet.com, E-trade.com, Ebay.com. Tất cả các nạn nhân là những gã khổng lồ trên internet thuộc nhiều lĩnh vực khác nhau. Theo Yankke Group, tổng thiệt hại do cuộc tấn công lên đến 1.2 triệu USD, nhưng không đáng kể bằng sự mất mát về lòng tin của khách hàng, uy tín của các công ty là không thể tính được.

Làm đảo lộn mọi dự tính, thủ phạm là một cậu bé 15 tuổi người Canada, với nickname "mafiaboy". Lại là một thiên tài bẩm sinh như Kevin Mitnick xuất hiện? Không. Mafiaboy chỉ tìm tòi và download về một số chương trình công cụ của các hacker. Cậu đã dùng một công cụ DDos có tên là TrinOO để gây nên các cuộc tấn công kiểu DDoS khủng khiếp trên. Một điểm đáng lưu ý khác là Mafiaboy bị bắt do tự khoe khoang trên các chatroom công cộng, không ai tự truy tìm được dấu vết của cậu bé này.

Còn rất nhiều gã khổng lồ khác đã gục ngã dưới các cuộc tấn công kiểu DDoS sau đó, trong đó có cả Microsodt. Tuy nhiên cuộc tấn công trên là điển hình nhất về DDoS, nó nói lên một đặc điểm chết người của DDoS: "Rất dễ thực hiện, hầu như không thể tránh, hậu quả rất nặng nề".

2/ Các giai đoạn của một cuộc tấn công kiểu DdoS:

Bao gồm 3 giai đoạn:

2.1. Giai đoạn chuẩn bị:

- Chuẩn bị công cụ quan trọng của cuộc tấn công, công cụ này thông thường hoạt động theo mô hình client-server. Hacker có thể viết phần mềm này hay down load một cách dễ dàng, theo thống kê tạm thời có khoảng hơn 10 công cụ DDoS được cung cấp miễn phí trên mạng (các công cụ này sẽ phân tích chi tiết vào phần sau)

- Kế tiếp, dùng các kỹ thuật hack khác để nắm trọn quyền một số host trên mạng. tiến hành cài đặt các software cần thiết trên các host này, việc cấu hình và thử nghiệm toàn bộ attack-network (bao gồm mạng lưới các máy đã bị lợi dụng cùng với các software đã được thiết lập trên đó, máy của hacker hoặc một số máy khác đã được thiết lập như điểm phát động tấn công) cũng sẽ được thực hiện trong giai đoạn này.

2.2 Giai đoạn xác định mục tiêu và thời điểm:

- Sau khi xác định mục tiêu lần cuối, hacker sẽ có hoạt động điều chỉnh attack-network chuyển hướng tấn công về phía mục tiêu.

- Yếu tố thời điểm sẽ quyết định mức độ thiệt hại và tốc độ đáp ứng của mục tiêu đối với cuộc tấn công.

2.3 Phát động tấn công và xóa dấu vết:

Đúng thời điểm đã định, hacker phát động tấn công từ máy của mình, lệnh tấn công này có thể đi qua nhiều cấp mói đến host thực sự tấn công. Toàn bộ attack-network (có thể lên đến hàng ngàn máy), sẽ vắt cạn năng lực của server mục tiêu liên tục, ngăn chặn không cho nó hoạt động như thiết kế.

- Sau một khoảng thời gian tấn công thích hợp, hacker tiến hành xóa mọi dấu vết có thể truy ngược đến mình, việc này đòi hỏi trình độ khác cao và không tuyệt đối cần thiết.

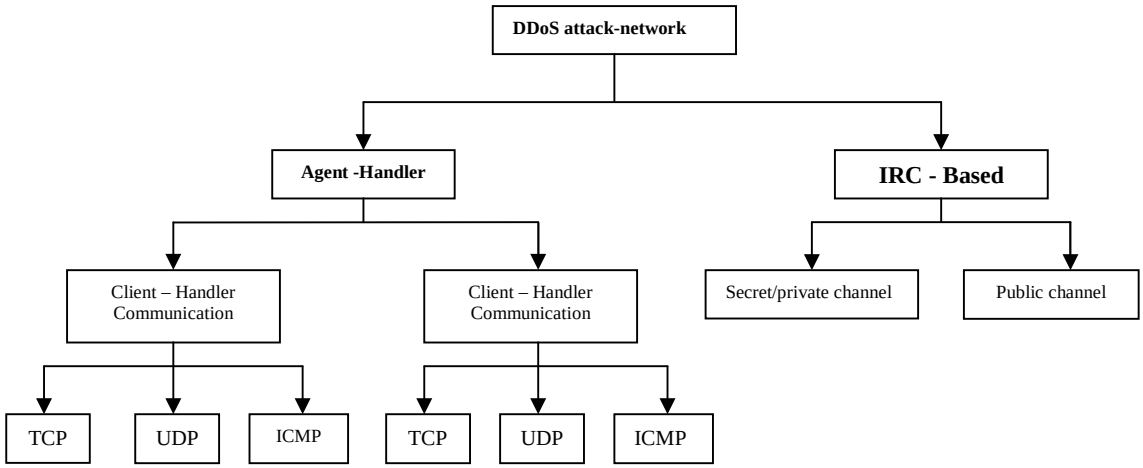
3/ Kiến trúc tổng quan của DDoS attack-network:

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



3.1 Mô hình Agent – Handler:

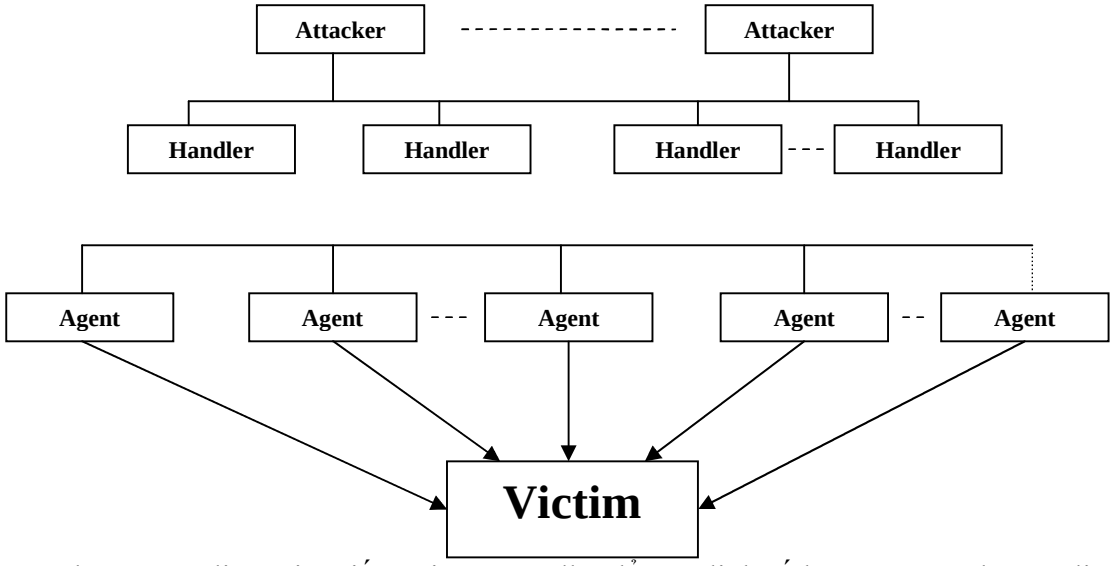
Theo mô hình này, attack-network gồm 3 thành phần: Agent, Client và Handler

→ 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.

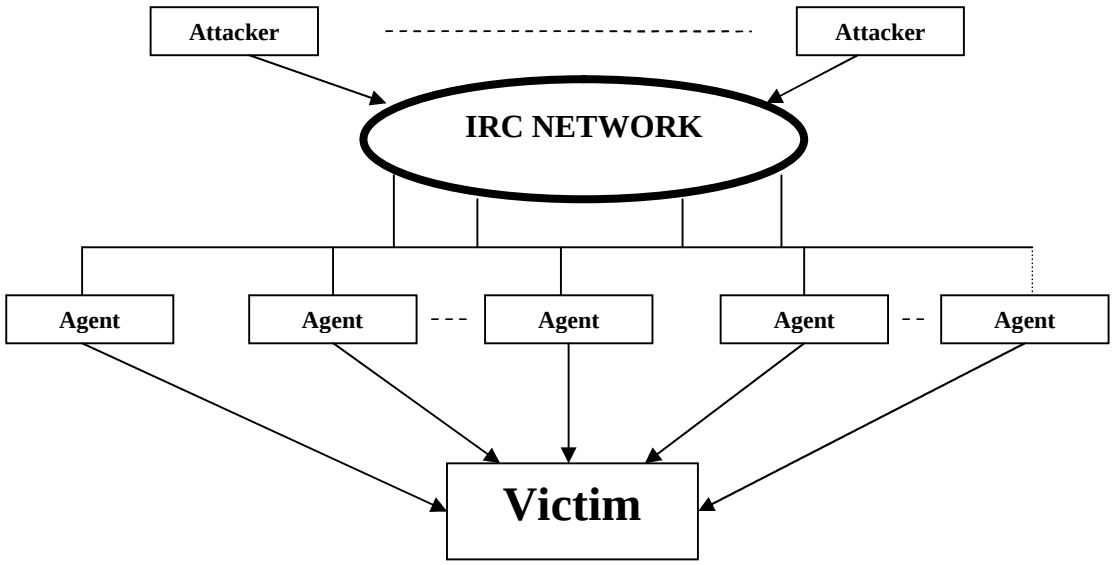
Thông thường Attacker sẽ đặt Handler software trên một Router hay một server có lượng traffic lưu thông nhiều. Việc này nhằm làm cho các giao tiếp giữa Client, handler và Agent khó bị phát hiện. Các gia tiếp này thông thường xảy ra trên các protocol TCP, UDP hay ICMP. Chủ nhân thực sự của các Agent thông 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.

3.2 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

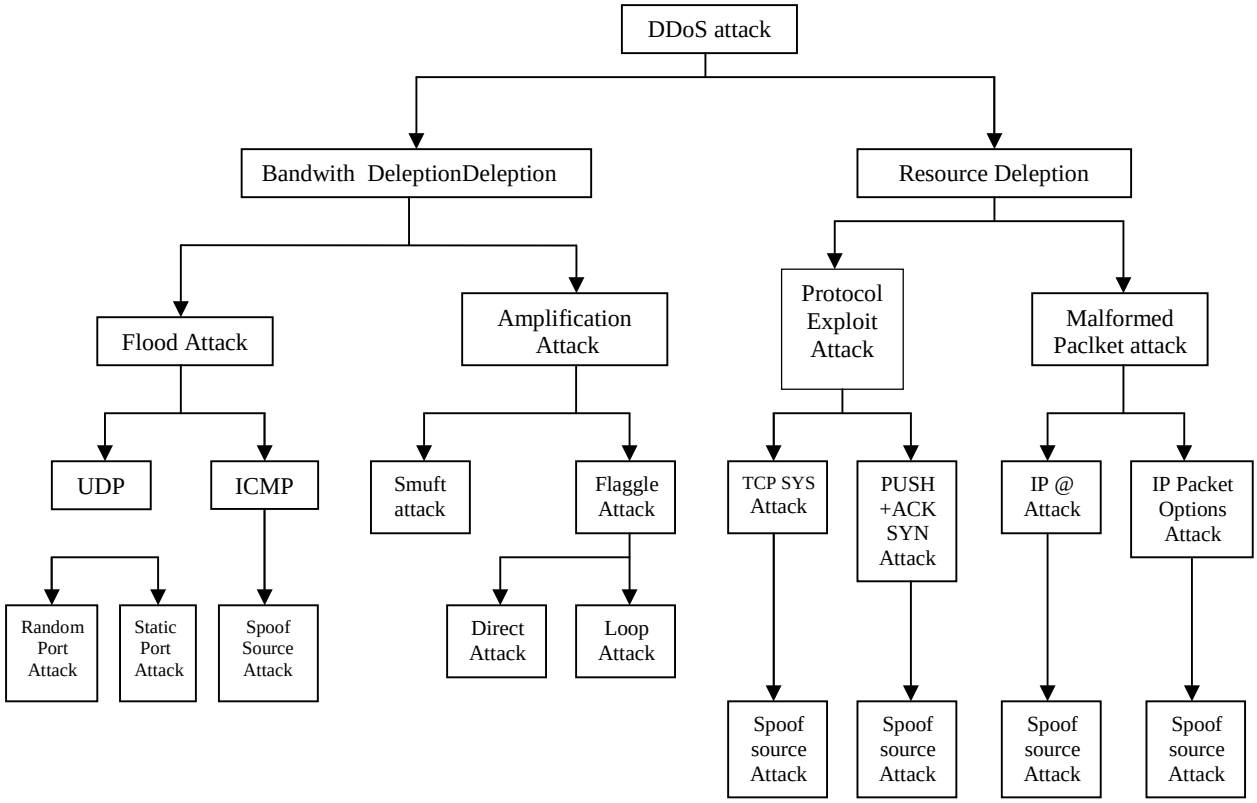
+ IRC traffic có thể di chuyển trên mạng với số lượng lớn mà không bị nghi ngờ

+ 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.

PHẦN II/ **PHÂN LOẠI TẤN CÔNG KIỂU 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 thể này thành hai loại dựa trên mục 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.



I/ 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 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.

1/ 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.

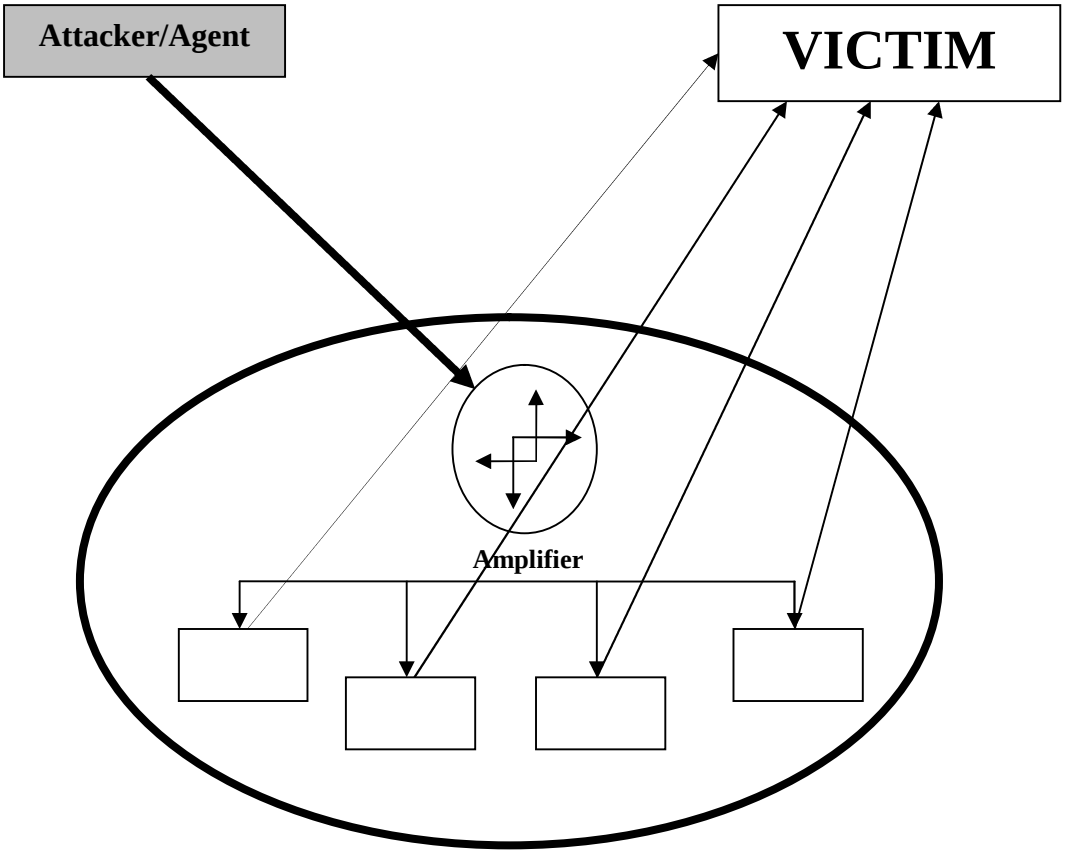
+ ICMP Flood Attack: được thiết kế nhằm mục đích quản lý mạng cũng như định vị thiết bị mạng. Khi các Agent gởi một lượng lớn ICMP_ECHO_REPLY đến hệ thống mục tiêu thì hệ

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.

2/ 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,

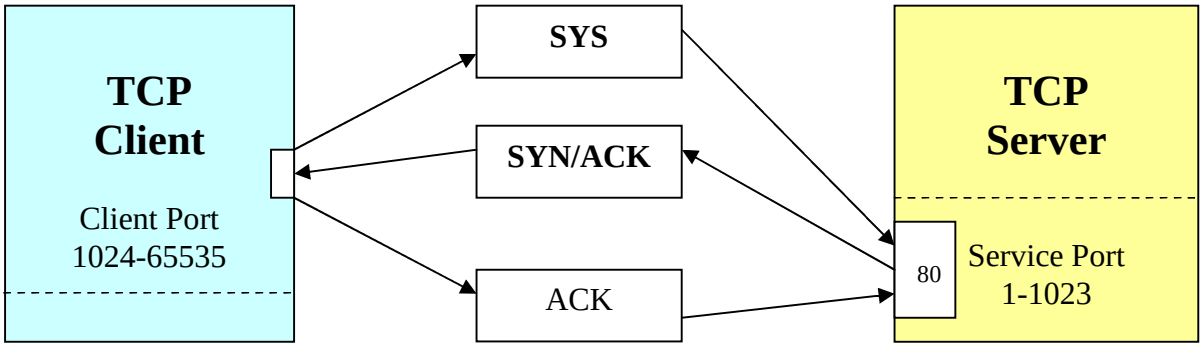
sau đó từ nạn nhân một ECHO REPLY lại gửi trở về địa chỉ broadcast, quá trình cứ thế tiếp diễn. Đây chính là nguyên nhân Flaggle Attack nguy hiểm hơn Smuft Attack rất nhiều.

II/ Những kiểu tấn công làm cạn kiệt tài nguyên: (Resource Deleption Attack)

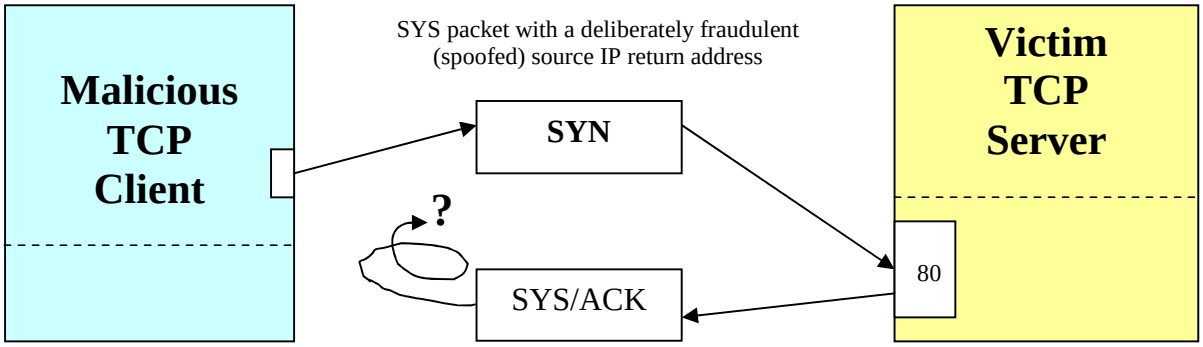
Theo định nghĩa: Resource Deleption Attack là kiểu tấn công trong đó Attacker gởi những packet dùng các protocol sai chức năng thiết kế, hay gửi những packet với dụng ý làm tắt nghẽn tài nguyên mạng làm cho các tài nguyên này không phục vụ user thông thường khác được.

1/ Protocol Exploit Attack:

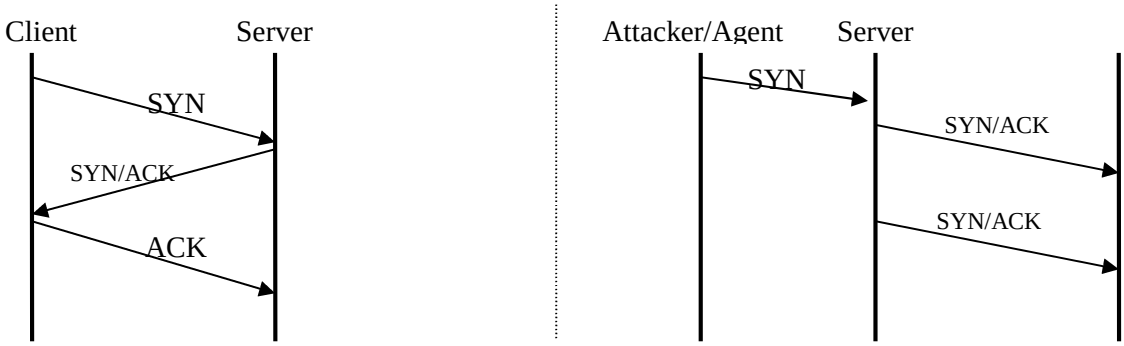
+ TCP SYS Attack: Transfer Control Protocol hỗ trợ truyền nhận với độ tin cậy cao nên sử dụng phương thức bắt tay giữa bên gởi và bên nhận trước khi truyền dữ liệu. Bước đầu tiên, bên gửi gởi một SYN REQUEST packet (Synchronize). Bên nhận nếu nhận được SYN REQUEST sẽ trả lời bằng SYN/ACK REPLY packet.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

2/ Malformed Packet Attack:

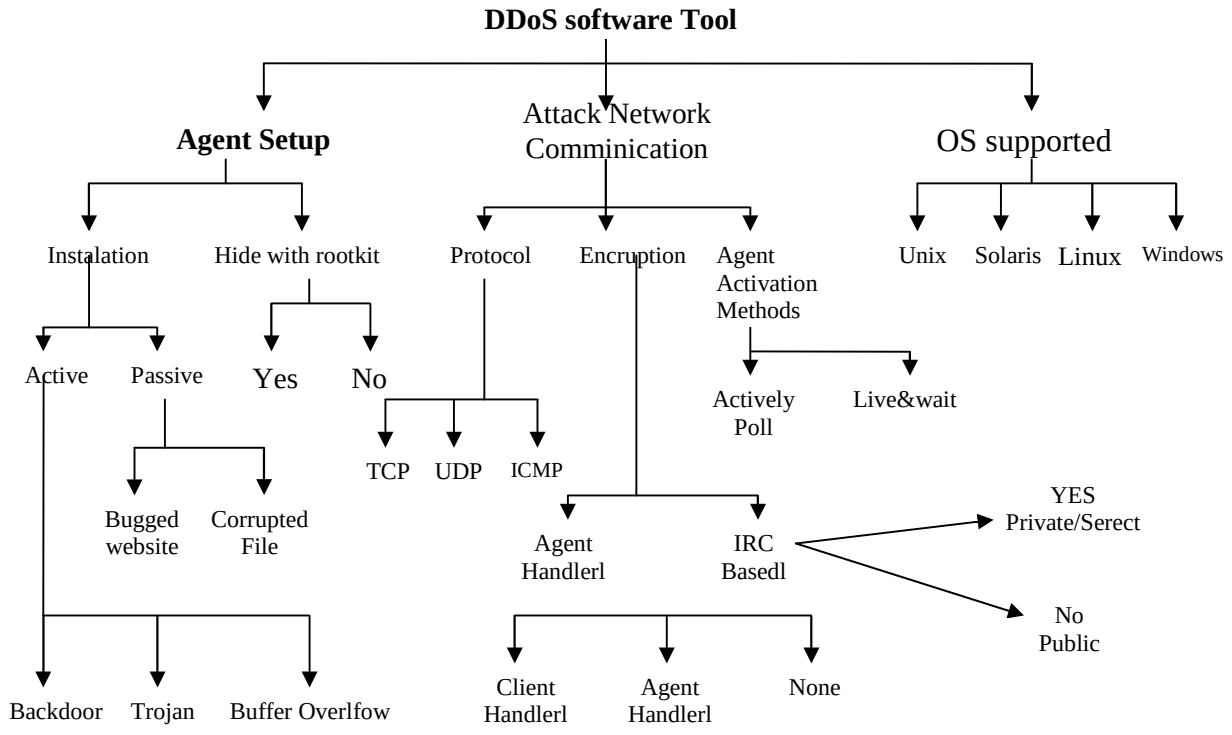
Malformed Packet Attack là cách tấn công dùng các Agent để gởi các packet có cấu trúc không đúng chuẩn nhằm làm cho hệ thống của nạn nhân bị treo.

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.

3/ 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.

3.1/ 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.

3.2/ 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.

3.3/ 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.

3.4/ 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

4/ Một số công cụ 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.

4.1. 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.

4.2. 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.

PHẦN III: NHỮNG KỸ THUẬT ANTI – DDOS:

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 giải pháp đối phó, tuy nhiên cuộc đua vẫn tuân theo quy luật tất yếu của bảo mật máy tính: “Hacker luôn đi trước giới bảo mật một bước”.

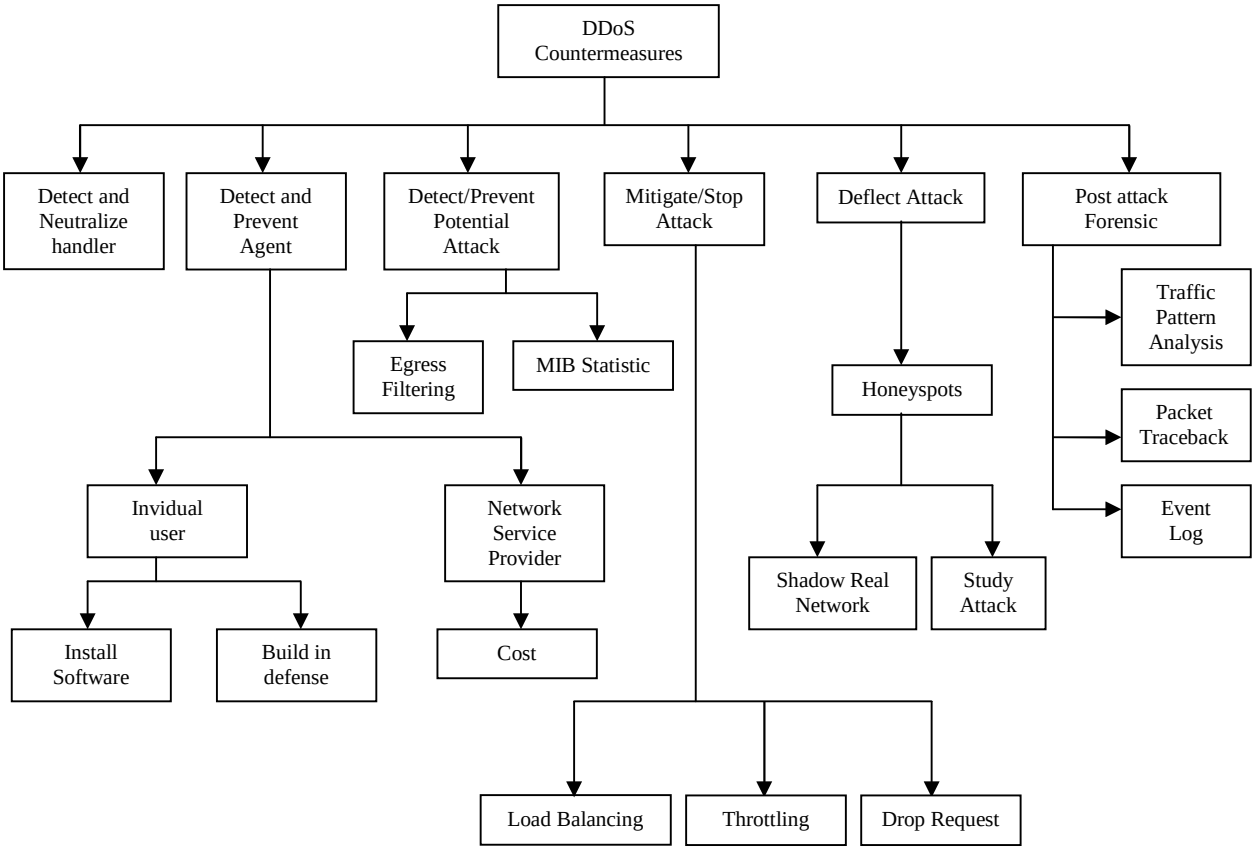
Có ba giai đoạn chính trong quá trình Anti-DDoS:

- Giai đoạn ngăn ngừa: 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 DDoS:



1/ Tối thiểu hóa số lượng Agent:

- Từ phía User: một phương pháp rất tốt để năng ngừa tấn công DDoS là từng internet 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 trở 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 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 thông ào hardware và software của từng hệ thống. Về phía user họ nên cài đặt và updat liên tục các 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 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. :D

2/ Tìm và vô hiệu hóa các Handler:

Một 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 va 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.

3/ 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 nhiệm giả mạo địa chỉ IP sẽ không còn tồn tại.

- **MIB statistics**: trong Management Information Base (SNMP) của route luôn có thông tin thống kể 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.

4/ 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 ý 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 một 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 với 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, gây 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.

5/ Chuyển hướng của cuộc tấn công:

Honeyspots: Một kỹ thuật đang được nghiên cứu là Honeyspots. Honeyspots 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.

6/ Giai đoạn sau tấn công:

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

-**Traffic Pattern Analysis:** Nếu dữ liệu về 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 ích cho việc tinh chỉnh lại các 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 attacker 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 tìm ra nhiều manh mối và chứng cứ quan trọng.

PHẦN IV: Những vấn đề có liên quan đến DDoS

DDoS là một kiểu tấn công rất đặc biệt, điểm cực kỳ hiểm ác của DDoS làm cho nó khắc phục là "DDos đánh vào nhân tố yếu nhất của hệ thống thông tin – con ngườ - mà lại là dùng người chống người". Từ đặc điểm này của DDoS làm phát sinh rất nhiều các vấn đề mà mọi người trong cộng đồng Internet phải cùng chung sứ mới có thể giải quyết.

Các yếu điểm:

1/ Thiếu trách nhiệm với cộng đồng:

Con người thông thường chỉ quan tâm đầu tư tiền bạc và công sức cho hệ thống thông tin của "chính mình". DDoS khai thác điểm này rất mạnh ở phương thức giả mạo địa chỉ và Broadcast amplification.

- **IP spoofing**: một cách thức đơn giản nhưng rất hiệu quả được tận dụng tối đa trong các cuộc tấn công DDoS. Thực ra chống giả mạo địa chỉ không có gì phức tạp, như đã đề cập ở phần trên, nếu tất cả các subnet trên internet đều giám sát các packet ra khỏi mạng của mình về phương diện địa chỉ nguồn hợp lệ thì không có một packet giả mạo địa chỉ nào có thể truyền trên internet được.

Đề nghị: "Tự giác thực hiện Egress Filtering ở mạng do mình quản lý". Hi vọng một ngày nào đó sẽ có quy định cụ thể về vấn đề này cho tất cả các ISP trên toàn cầu.

- **Broadcast Amplification:** tương tự IP spoofing, nó lợi dụng toàn bộ một subnet để flood nạn nhân. Vì vậy, việc giám sát và quản lý chặt chẽ khả năng broadcast của một subnet là rất cần thiết. Quản trị mạng phải cấu hình toàn bộ hệ thống không nhận và forward broadcast packet.

2/ Sự im lặng:

Hầu hết các tổ chức đều không có phản ứng hay im lặng khi hệ thống của mình bị lợi dụng tấn công hay bị tấn công. Điều này làm cho việc ngăn chặn và loại trừ các cuộc tấn công trở nên khó khăn. Mọi việc trở nên khó khăn khi mọi người không chia sẻ kinh nghiệm từ các cuộc tấn công, trong khi giới hacker thì chia sẻ mã nguồn mở của các công cụ, một cuộc chơi không cân sức ??

Đề nghị:

+ Mỗi tổ chức có liên quan nên thiết lập quy trình xử lý xâm nhập vào tổ chức, nhóm chuyên trách với trách nhiệm và quy trình thật cụ thể. Các ISP nên thiết lập khả năng phản ứng nhanh và chuyên nghiệp để hỗ trợ các tổ chức trong việc thực hiện quy trình xử lý xâm nhập của mình.

+ Khuyến khích các quản trị mạng gia nhập mạng lưới thông tin toàn cầu của các tổ chức lớn về bảo mật nhằm thông tin kịp thời và chia sẻ kinh nghiệm với mọi người

+ Tất cả các cuộc tấn công hay khuyết điểm của hệ thống đều phải được báo cáo đến bộ phận tương ứng để xử lý.

3/ Tầm nhìn hạn hẹp:

Nếu chỉ thực hiện các giải pháp trên thôi thì đưa chúng ta ra khỏi tình trạng cực kỳ yếu kém về bảo mật. Các giải pháp này không thực sự làm giảm các rủi ro của hệ thống thông tin mà chỉ là các giải pháp tình thế. Có những vấn đề đòi hỏi một cái nhìn và thái độ đúng đắn của cộng đồng Internet. Cần phải có những nghiên cứu thêm về mặt quy định bắt buộc và pháp lý nhằm hỗ trợ chúng tac giải quyết các vấn đề mà kỹ thuật không thực hiện nỗi. Một số vấn đề cần thực hiện thêm trong tương lai:

- Giám sát chi tiết về luồng dữ liệu ở cấp ISP để cảnh cáo về cuộc tấn công.
- Xúc tiến đưa IPSec và Secure DNS vào sử dụng
- Khẳng định tầm quan trọng của bảo mật trong quá trình nghiên cứu và phát triển của Internet II.
- Nghiên cứu phát triển công cụ tự động sinh ra ACL từ security policy và router và firewall.
- Ủng hộ việc phát triển các sản phẩm hướng bảo mật có các tính năng: bảo mật nặc định, tự động updat.
- Tài trợ việc nghiên cứu các protocol và các hạ tầng mới hỗ trợ khả năng giám sát, phân tích và điều khiển dòng dữ liệu thời gian thực.
- Phát triển các router và switch có khả năng xử lý phức tạp hơn.
- Nghiên cứu phát triển các hệ thống tương tự như Intrusion Dectection, hoạt động so sánh trạng thái hiện tại với định nghĩa bình thường củ hệ thống từ đó đưa ra các cảnh báo.
- Góp ý kiến để xây dựng nội quy chung cho tất cả các thành phần có liên quan đến internet.
- Thiết lập mạng lưới thông tin thời gian thực giữa những người chịu trách nhiệm về hoạt động của hệ thống thông tin nhằm cộng tác-hỗ trợ-rút kinh nghiệm khi có một cuộc tấn công quy mô xảy ra.
- Phát triển hệ điều hành bảo mật hơn.

- Nghiên cứu các hệ thống tự động hồi phục có khả năng chống chọi, ghi nhận và hồi phục sau tấn công cho các hệ thống xung yếu.
- Nghiên cứu các biện pháp truy tìm, công cụ pháp lý phù hợp nhằm trừng trị thích đáng các attacker mà vẫn không xâm phạm quyền tự do riêng tư cá nhân.
- Đào tạo lực lượng tinh nhuệ về bảo mật làm nòng cốt cho tính an toàn của Internet.
- Nhấn mạnh yếu tố bảo mật và an toàn hơn là chỉ tính đến chi phí khi bỏ ra xây dựng một hệ thống thông tin.

Khi nào có thời gian. tôi sẽ viết và phân tích một số trường hợp tấn công cụ thể đã xảy ra và cách phòng chống của các chuyên gia security của thế giới. Để mọi người có thể hiểu rõ hơn bài viết này.

Mong “Neo”, “lethanhlong2k”, “tsbeginnervn”; “Chú bé ham học”… và mọi người cho ý kiến và phân tích chi tiết bài viết này để hoàn thiện hơn.

Cảm ơn.