Mục Lục

I – Lời nói đầu:

- Xin chào toàn thể anh em trong Hacking nói chung và Hands Team nói riêng, tôi là JCAlex Min – Leader of Hands Team và hoạt động trong Hacking được hơn 3 năm, trong hơn 3 năm tôi nghiên cứu về DDos và Botnet và cũng có một số kiến thức về mảng này nên hôm nay tôi viết lại Ebook này nhằm mang lại và cũng như chia sẻ những kiến thức cơ bản mà tôi có được cho các bạn mới vào và cũng như các bạn tìm lại kiến thức cơ bản cho mình. Tôi không nhận là mình pro hay giỏi về mảng này nhưng tôi biết gì thì truyền đạt lại với các bạn mong các bạn ủng hộ và góp ý cùng tôi để tôi hoàn thiện kiến thức cho mình và sẽ viết thêm một vài Ebook nâng cao hơn chuyên sâu hơn cho các bạn khác mới vào tìm hiểu về DDos và Botnet.

- Ebook này là báo cáo của tôi (như một bài test kiến thức) về An Toàn Thông Tin Mạng với đề tài: Các kĩ thuật tấn công Website: DoS, DDoS, DRDoS & Botnet để bắt đầu làm việc bên lĩnh vực An Ninh Mạng.

- Bây giờ mời các bạn cùng tôi tìm hiểu về các kĩ thuật tấn công Website: DoS, DDoS, DRDoS & Botnet xem nó nguy hiểm và cách phòng chống như thế nào.

I - Tấn công từ chối dịch vụ (DoS):

I.1 - Giới thiệu về 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

I.2 - Lịch sử các cuộc tấn công và phát triển của DoS

- Các tấn công DoS bắt đầu vào khoảng đầu 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 đó, 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 hoá một cách thủ công bởi nhiều kẻ tấn công để tạo ra một sự phá huỷ có hiệu quả. Sự dịch chuyển đến việc tự động hoá sự đồng bộ, kết hợp này và tạo ra một tấn công song song lớn 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, amazon.com, buy.com, cnn.com và eBay.com đã đặt dưới sự tấn công (ví dụ như Yahoo bị ping với tốc độ 1 GB/s).

Từ đó các cuộc tấn công Dos thường xuyên sảy ra

Ví dụ : - 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.

- Gần đây nhất là 2 vụ DDos lớn vào các trang mạng đông người truy cập ở Việt Nam đó là: DDos vào VCCrop 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)

I.3 - Mục đích của tấn công DoS và hiểm họa

- 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

- 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…

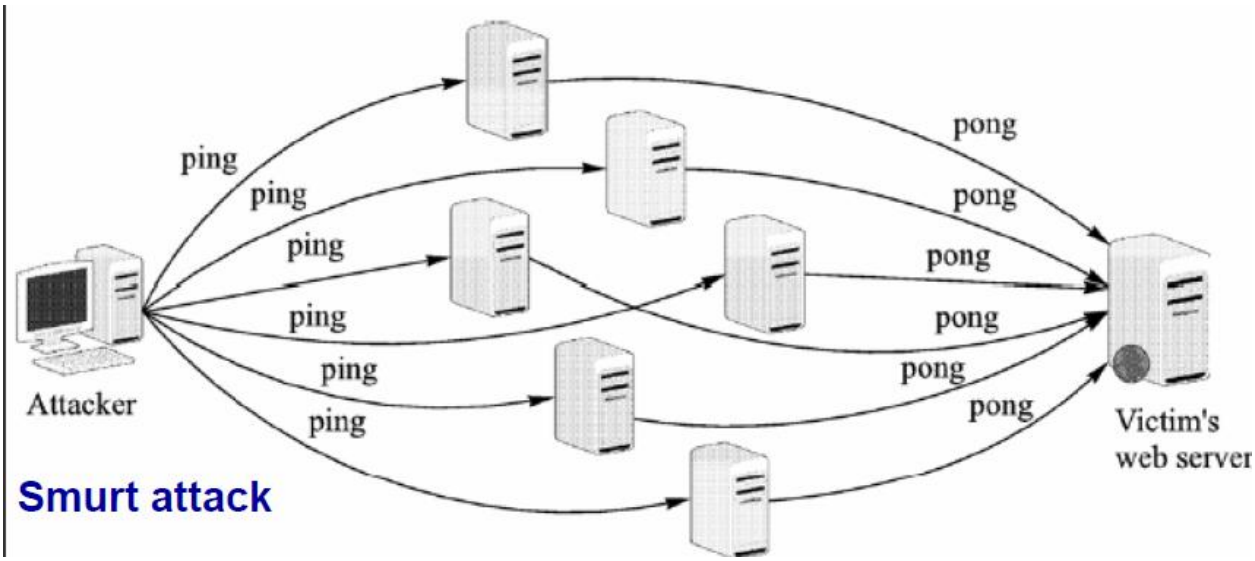
I.4 - Các hình thức tấn công DoS cơ bản :

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

4.a - Smurf :

- Smurf : là một loại tấn công DoS điển hình. Máy của attacker sẽ gởi 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 đích 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.

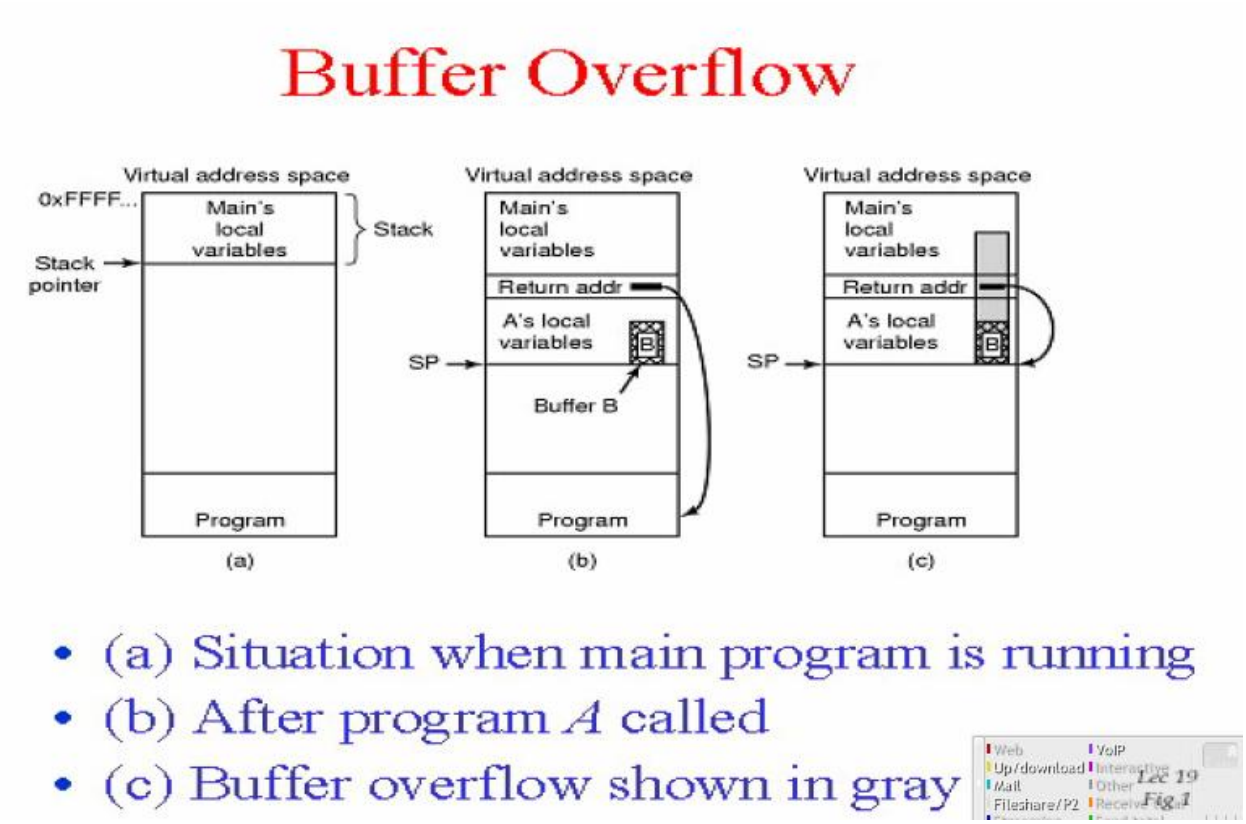


4.b - Buffer Overflow Attack :

- 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 dài quá 256 ký tự có thể sẽ xảy ra quá trình tràn bộ nhớ đệm.



4. c - 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.

VD : Ping -l 65500 address

- -l : buffer size

Khoảng năm 1997-1998, lỗi nãy đã được fix, vì vậy bây giờ nó chỉ mang tính lịch sử.

4.d - 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.

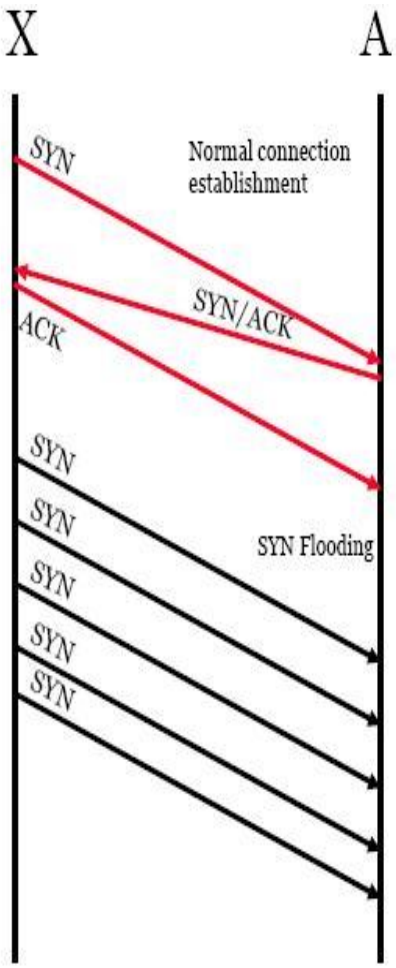
- Lợi dụng điều này, hacker có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công

- Kết quả là 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.

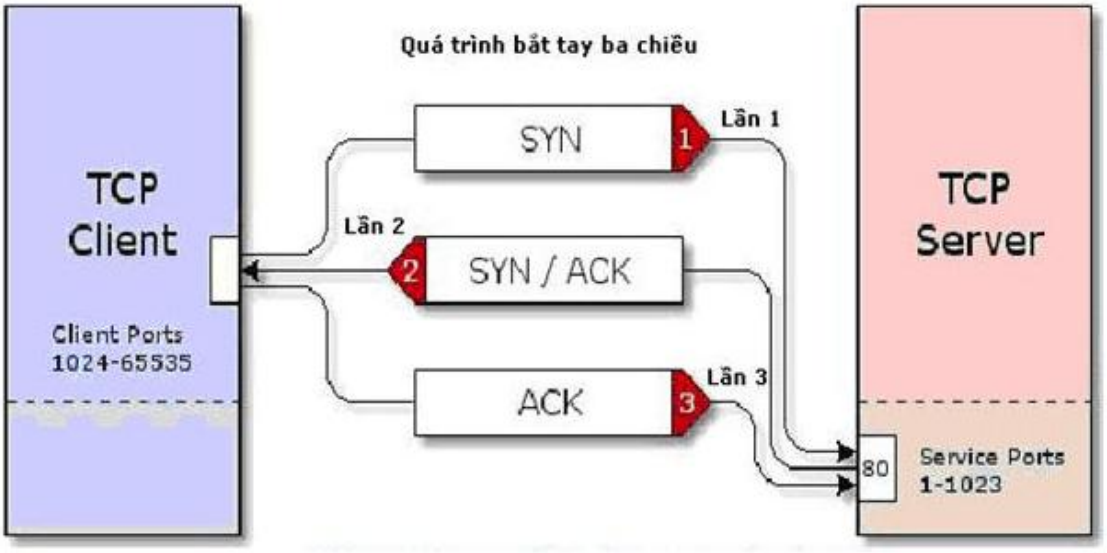
4.e - SYN Attack:

- 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 được thực hiện.



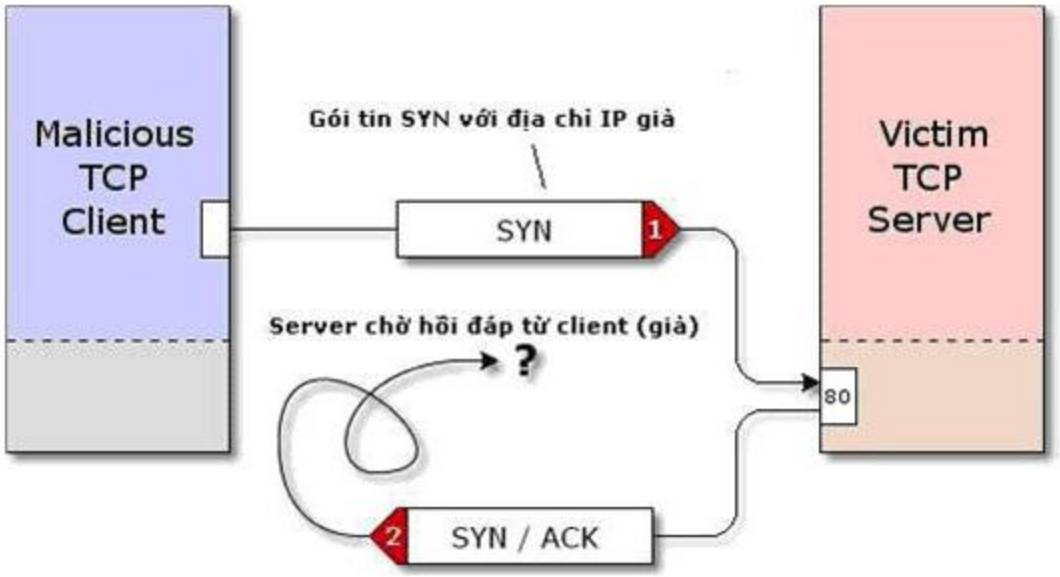
Mô hình tấn công bằng các gói SYN



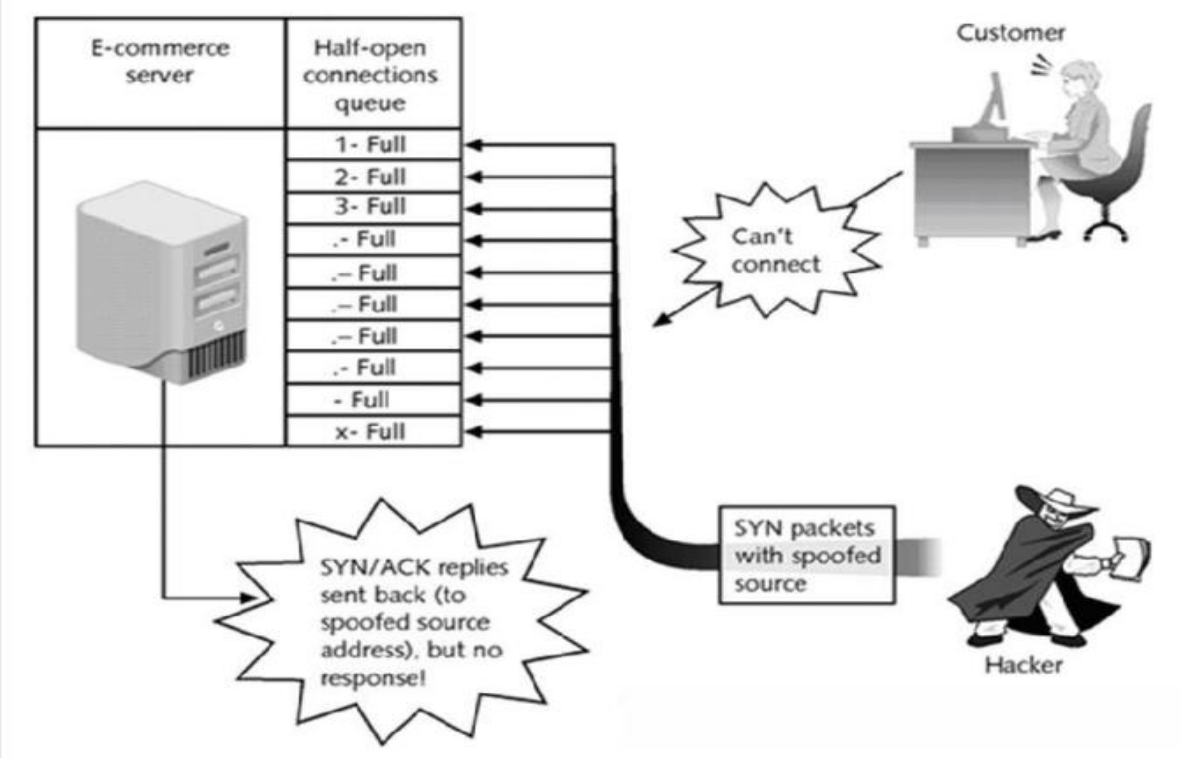
Bước 1: Client (máy khách) sẽ gửi các gói tin (packet chứa SYN=1) đến máy chủ để yêu cầu kết nối.

Bước 2: Khi nhận được gói tin này, server sẽ gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ giành 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.



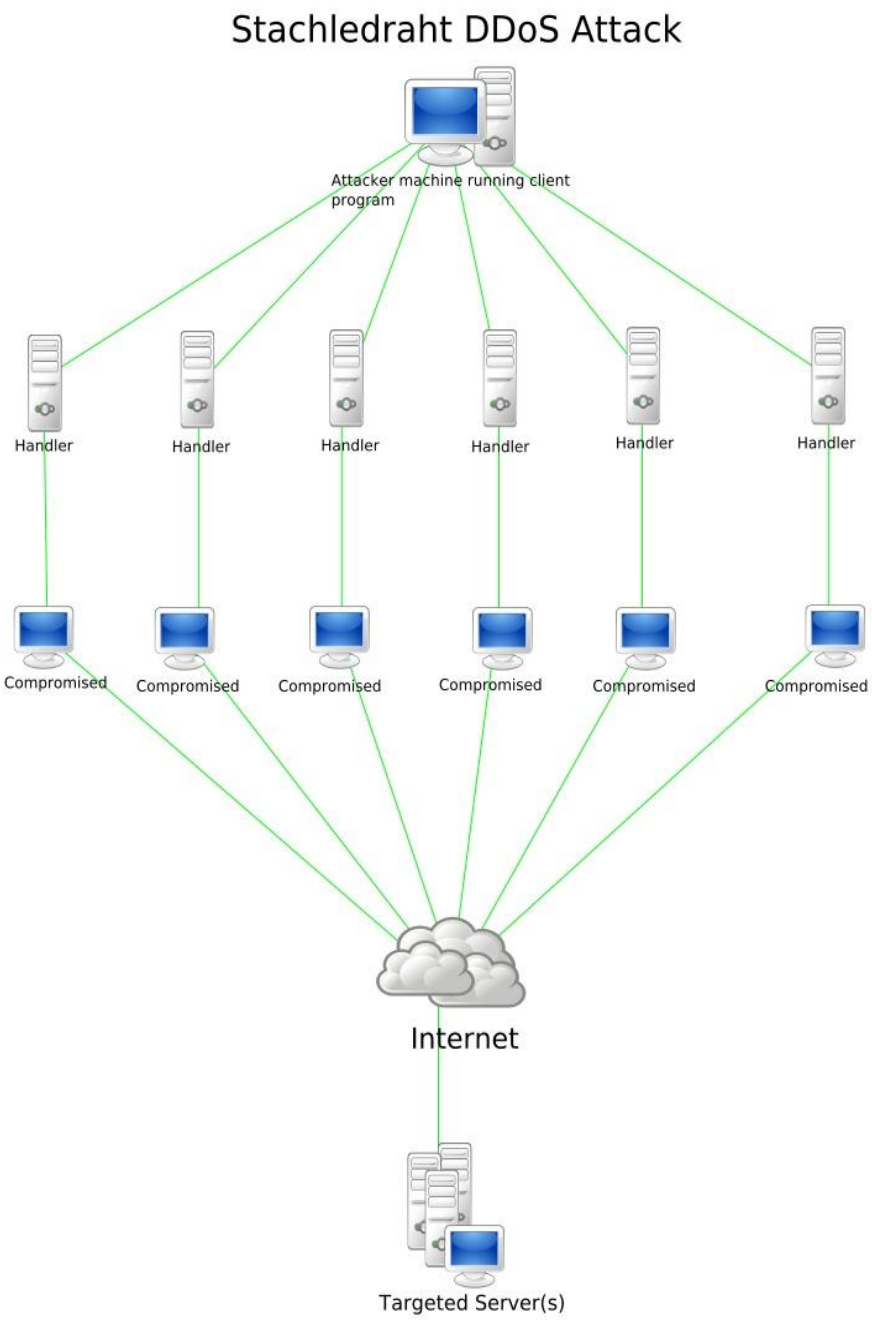
- Do TCP là thủ tục tin cậy trong việc giao nhận (end-to-end) nên trong lần bắt tay thứ hai, server gửi các gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho 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 hư khi máy tính cá nhân (PC) hay bị "treo" khi mở cùng lúc quá nhiều chương trình cùng lúc vậy .

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

II.1 - Giới thiệu 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, 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.

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 có 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 thực tế 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.

II.2 - 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 đó được gọi là tấn công DDoS.

II.3 - 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.

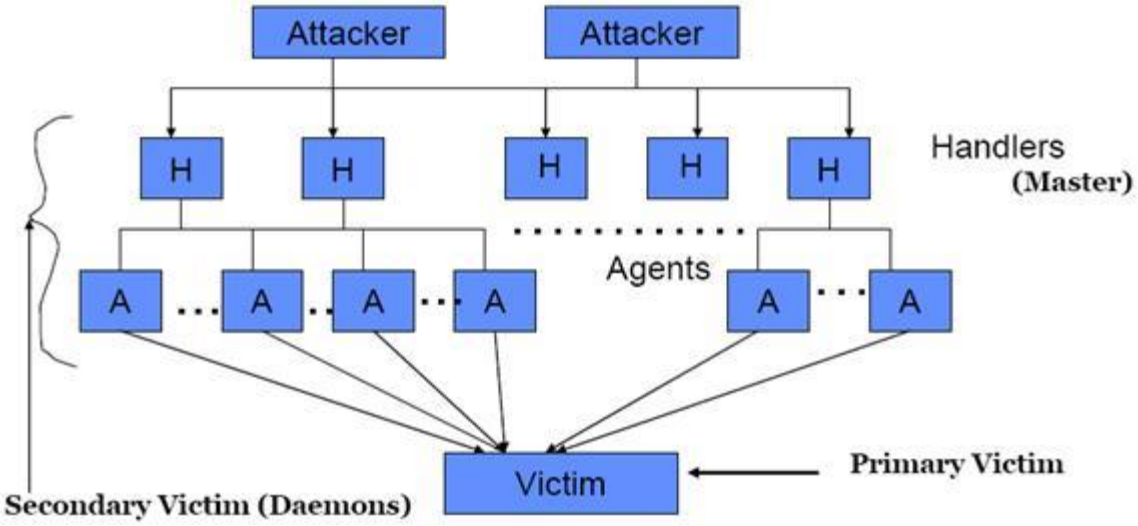
- Tuy nhiên một mạng Botnet bao gồm từ hàng nghìn tới vài trăm nghìn địa chỉ IP trên Internet và điều đó là vô cùng khó khăn để ngăn chặn tấn công.

II.4 - 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

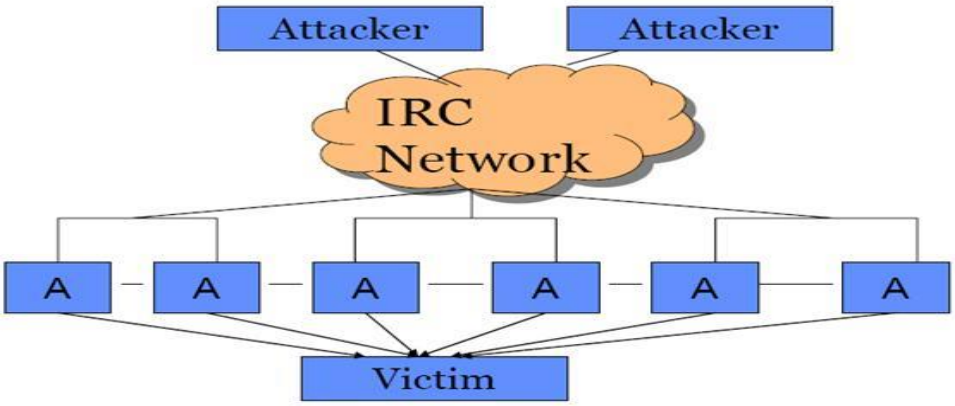
4.a - Agent Handler Model:

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



4.b - Tấn công DDoS dựa trên nền tảng IRC:

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.



II.5 - Phân loại tấn công DDoS:

- Tấn công gây hết băng thông truy cập tới máy chủ.

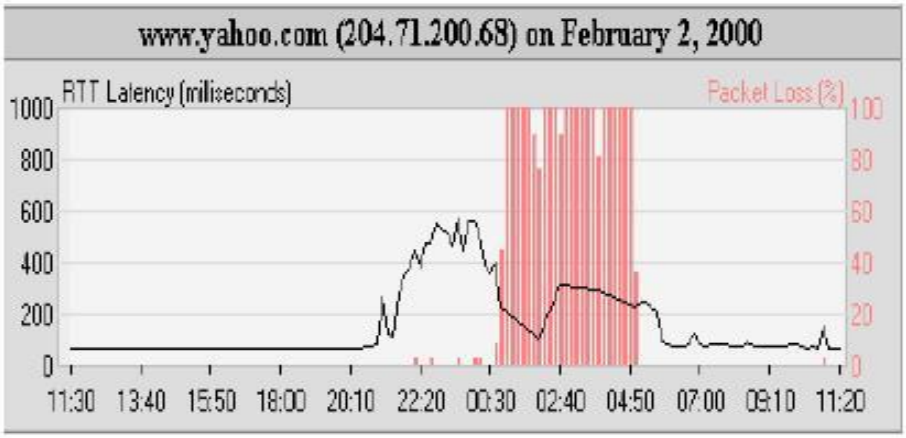
  + Flood attack

  + UDP và ICMP Flood (flood – gây ngập lụt)

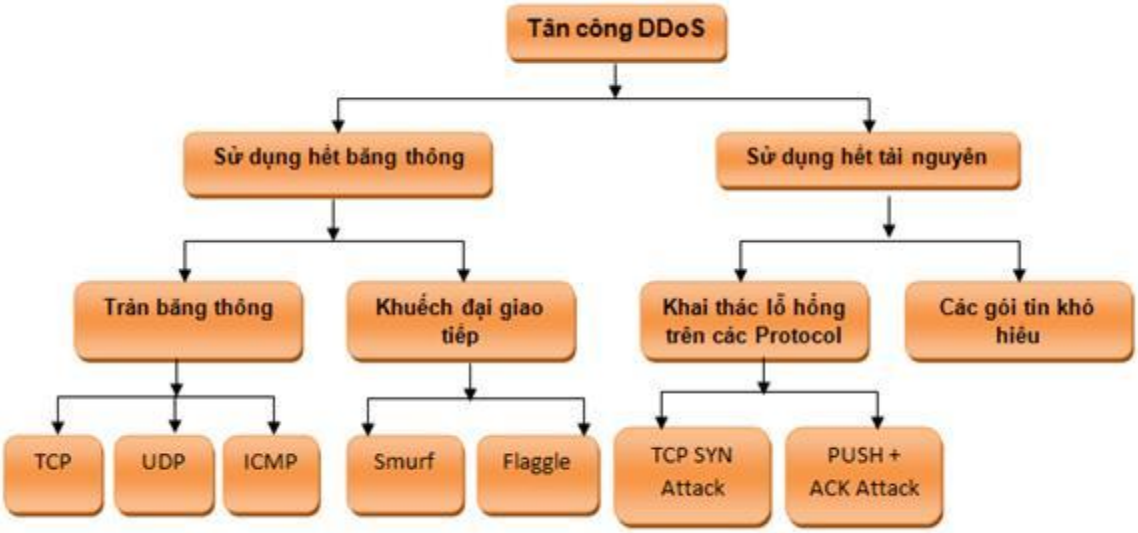
- Tấn công khuếch đại các giao tiếp

  + Smurf and Fraggle attack

Tấn công DDoS vào Yahoo.com năm 2000

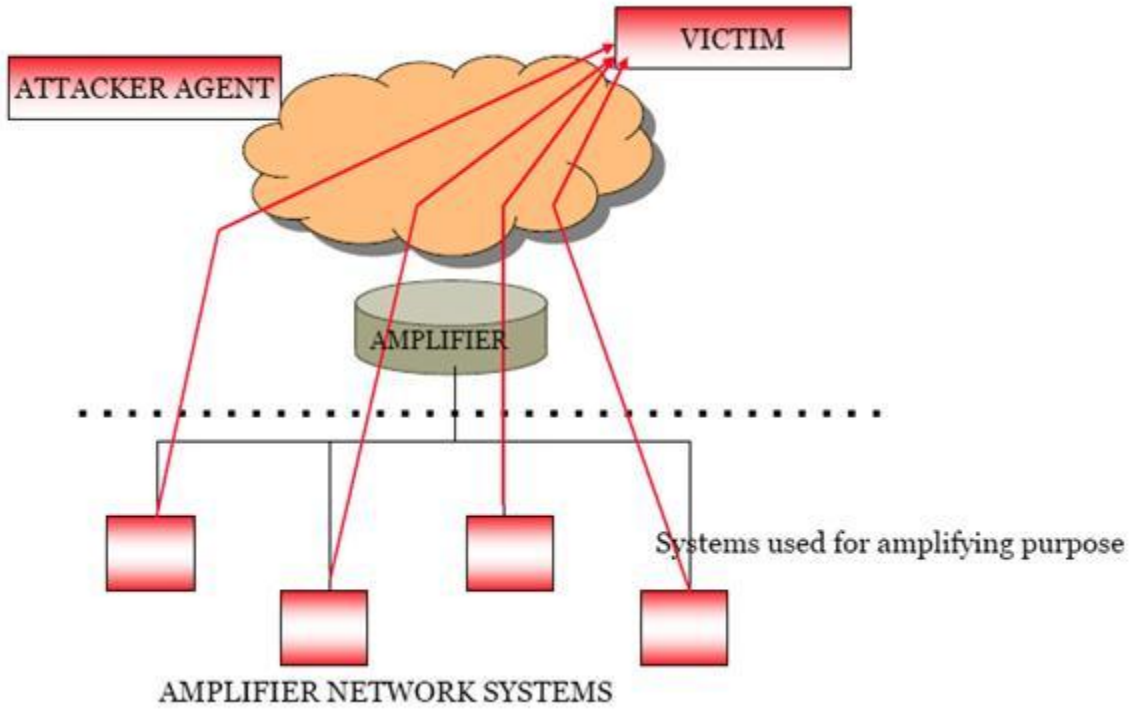


Sơ đồ phân loại tấn công DDoS:



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.



II.6 - Tấn công Reflective DNS (reflective - phản chiếu):

6.a - Các vấn đề liên quan tới tấn công Reflective DNS:

- Một Hacker có thể sử dụng mạng 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 mail 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.

6.b - 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 hay bất kỳ một trang web nào mà kẻ tấn công muôn.

- 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 cá nhân và thiết lập số lượng các giao tiếp.

II.7 - Các tools sử dụng để tấn công DDoS:

Dưới đây là các Tools tấn công DDoS.

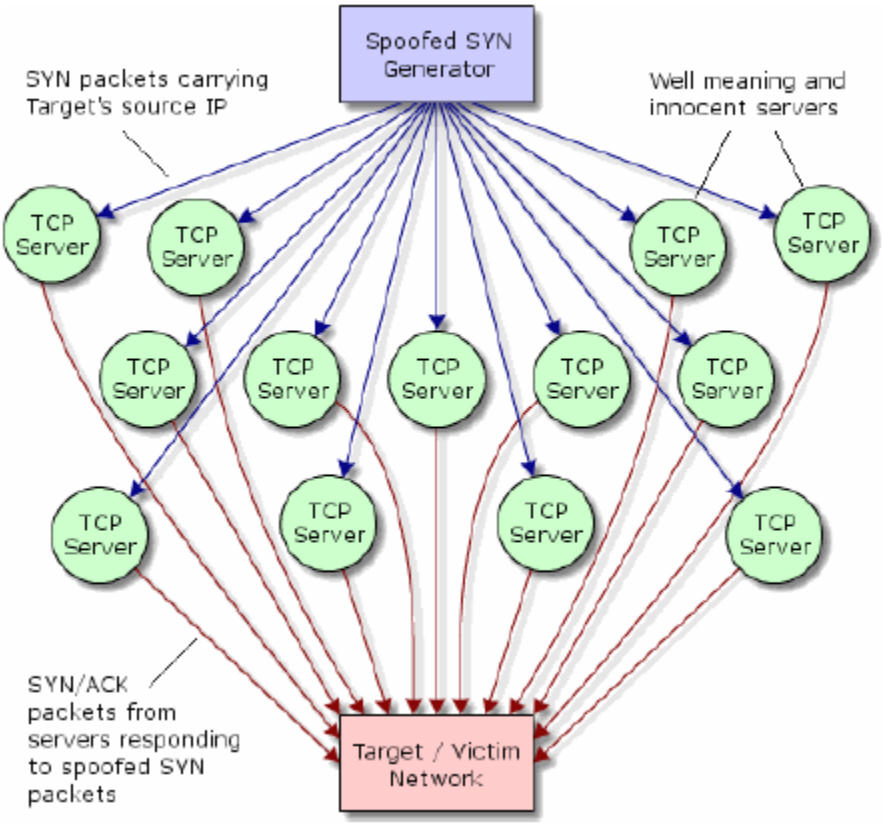
- Trinoo
- Tribe flood Network (TFN)
- TFN2K
- Stacheldraht
- Shaft
- Trinity
- Knight
- Mstream
- Kaiten

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

III - DRDoS (Distributed Reflection Denial of Service)

III.1 – Giới thiệu DRDOS.

- Xuất hiện vào đầu năm 2002, là kiểu tấn công mới nhất, mạnh nhất trong họ DoS.
- Nếu được thực hiện bởi kẻ tấn công có tay nghề thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới trong phút chốc.
- DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS.
- 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.
- 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. Server A sẽ mở 1 connection và gủi 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 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, mộthacker 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.

III.2 - 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 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:

2.a - 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.

2.b - 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.

2.c - 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.

2.d - 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.

2.e - 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.

2.f - 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.

2.g - Phòng chống tổng quát :

1. 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.

2. 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.

3. Sử dụng các tính năng cho phép đặt rate limit trên router/firewall để hạn chế số lượng packet vào hệ thống.

4. Nếu bị tấn công do lỗi của phần mềm hay thiết bị thì nhanh chóng cập nhật các bản sửa lỗi cho hệ thống đó hoặc thay thế.

5. Dùng một số cơ chế, công cụ, phần mềm để chống lại TCP SYN Flooding.
6. 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 cùng tính năng khác để phân chia tải.

7. Tạm thời chuyển máy chủ sang một địa chỉ khác.

IV – Botnet.

Sơ lược lịch sử :

- Cuối thế kỷ 19 cũng như đầu thiên niên kỷ mới đánh dấu bước phát triển nhanh, mạnh của một số chiến lược tấn công khác biệt nhắm vào hệ thống mạng. DDoS, tức Distributed Denial of Services, hình thức tấn công từ chối dịch vụ phân tán khét tiếng ra đời. Tương tự với người anh em DoS (tấn công từ chối dịch vụ), DDoS được phát tán rất rộng, chủ yếu nhờ tính đơn giản nhưng rất khó bị dò tìm của chúng. Đã có nhiều kinh nghiệm đối phó được chia sẻ, với khối lượng kiến thức không nhỏ về nó, nhưng ngày nay DDoS vẫn đang là một mối đe doạ nghiêm trọng, một công cụ nguy hiểm của hacker. Chúng ta hãy cùng tìm hiểu về DDoS và sản phẩm kế thừa từ nó: các cuộc tấn công botnet.

IV.1 - Giới thiệu về Bot và Botnet

1.a - Bot là gì ? : là những chương trình tương tự Trojan backdoor cho phép kẻ tấn công sử dụng máy của họ như là những Zoombie (máy tính thây ma – máy tính bị chiếm quyền điều khiển hoàn toàn) và chúng chủ động kết nối với một Server để dễ dàng điều khiển , các bạn lưu ý chữ "chủ động" đó là một đặc điểm khác của bot so với trojan backdoor . Chính vì sự chủ động này mà máy tính bị cài đặt chúng kết nối trở nên chậm chạp , một đặc điểm giúp ta dễ dàng nhận diện bot .

1.b - Tại sao gọi là mạng botnet ? : mạng botnet là một mạng rất lớn gồm hàng trăm hàng ngàn máy tính Zombie kết nối với một máy chủ mIRC (Internet Replay Chat) hoặc qua các máy chủ DNS để nhận lệnh từ hacker một cách nhanh nhất . Các mạng bot gồm hàng ngàn "thành viên" là một công cụ lý tưởng cho các cuộc chiến tranh đọ máu như DDOS , spam, cài đặt các chương trình quảng cáo …..

1.c - IRC

-IRC là tên viết tắt của Internet Relay Chat. Đó là một giao thức được thiết kế cho hoạt động liên lạc theo kiểu hình thức tán gẫu thời gian thực (ví dụ RFC 1459, các bản update RFC 2810, 2811, 2812, 2813) dựa trên kiến trúc client-server. Hầu hết mọi server IRC đều cho phép truy cập miễn phí, không kể đối tượng sử dụng. IRC là một giao thức mạng mở dựa trên nền tảng TCP (Transmission Control Protocol - Giao thức điều khiển truyền vận), đôi khi được nâng cao với SSL (Secure Sockets Layer - Tầng socket bảo mật).

-Một server IRC kết nối với server IRC khác trong cùng một mạng. Người dùng IRC có thể liên lạc với cả hai theo hình thức công cộng (trên các kênh) hoặc riêng tư (một đối một). Có hai mức truy cập cơ bản vào kênh IRC: mức người dùng (user) và mức điều hành (operator). Người dùng nào tạo một kênh liên lạc riêng sẽ trở thành người điều hành. Một điều hành viên có nhiều đặc quyền hơn (tuỳ thuộc vào từng kiểu chế độ do người điều hành ban đầu thiết lập) so với người dùng thông thường.

-Các bot IRC được coi như một người dùng (hoặc điều hành viên) thông thường. Chúng là các quy trình daemon, có thể chạy tự động một số thao tác. Quá trình điều khiển các bot này thông thường dựa trên việc gửi lệnh để thiết lập kênh liên lạc do hacker thực hiện, với mục đích chính là phá hoại. Tất nhiên, việc quản trị bot cũng đòi hỏi cơ chế thẩm định và cấp phép. Vì thế, chỉ có chủ sở hữu chúng mới có thể sử dụng.

-Một thành phần quan trọng của các bot này là những sự kiện mà chúng có thể dùng để phát tán nhanh chóng tới máy tính khác. Xây dựng kế hoạch cẩn thận cho chương trình tấn công sẽ giúp thu được kết quả tốt hơn với thời gian ngắn hơn (như xâm phạm được nhiều máy tính hơn chẳng hạn). Một số n bot kết nối vào một kênh đơn để chờ lệnh từ kẻ tấn công thì được gọi là một botnet.

-Cách đây chưa lâu, các mạng zombie (một tên khác của máy tính bị tấn công theo kiểu bot) thường được điều khiển qua công cụ độc quyền, do chính những kẻ chuyên bẻ khoá cố tình phát triển. Trải qua thời gian, chúng hướng tới phương thức điều khiển từ xa. IRC được xem là công cụ phát động các cuộc tấn công tốt nhất nhờ tính linh hoạt, dễ sử dụng và đặc biệt là các server chung có thể được dùng như một phương tiện liên lạc. IRC cung cấp cách thức điều khiển đơn giản hàng trăm, thậm chí hàng nghìn bot cùng lúc một cách linh hoạt. Nó cũng cho phép kẻ tấn công che đậy nhân dạng thật của mình với một số thủ thuật đơn giản như sử dụng proxy nặc danh hay giả mạo địa chỉ IP. Song cũng chính bởi vậy mà chúng để lại dấu vết cho người quản trị server lần theo.

Điển hình ở Việt Nam chúng ta cũng có một mạng botnet IRC tương đối lớn khoảng 1000 zombi rải đều cả nước do Hacker LlyKil người Quảng Nam thực hiện kiển soát và điều khiển để tấn công truongton.net và nhiều website nổi tiếng Việt Nam vào những năm 2008. Và Llykil bị bắt khi vừa thực hiện xong cuộc tấn công và BKAV (Website chương trình diệt Virus của Việt Nam) thông qua Botnet bằng kênh chat IRC này.

-Trong hầu hết các trường hợp tấn công bởi bot, nạn nhân chủ yếu là người dùng máy tính đơn lẻ, server ở các trường đại học hoặc mạng doanh nghiệp nhỏ. Lý do là bởi máy tính ở những nơi này không được giám sát chặt chẽ và thường để hở hoàn toàn lớp bảo vệ mạng. Những đối tượng người dùng này thường không xây dựng cho mình chính sách bảo mật, hoặc nếu có thì không hoàn chỉnh, chỉ cục bộ ở một số phần. Hầu hết người dùng máy tính cá nhân kết nối đường truyền ADSL đều không nhận thức được các mối nguy hiểm xung quanh và không sử dụng phần mềm bảo vệ như các công cụ diệt virus hay tường lửa cá nhân.

IV.2 - Bot và các ứng dụng của chúng

-Khả năng sử dụng bot và các ứng dụng của chúng cho máy tính bị chiếm quyền điều khiển hoàn toàn phụ thuộc vào sức sáng tạo và kỹ năng của kẻ tấn công. Chúng ta hãy xem một số ứng dụng phổ biến nhất.

2.a - DDoS

-Các botnet được sử dụng thường xuyên trong các cuộc tấn công Distributed Denial of Service (DDoS). Một kẻ tấn công có thể điều khiển số lượng lớn máy tính bị chiếm quyền điều khiển tại một trạm từ xa, khai thác băng thông của chúng và gửi yêu cầu kết nối tới máy đích. Nhiều mạng trở nên hết sức tồi tệ sau khi hứng chịu các cuộc tấn công kiểu này. Và trong một số trường hợp, thủ phạm được tìm thấy ngay khi đang tiến hành cuộc phá hoại (như ở các cuộc chiến dotcom).

Tấn công từ chối dịch vụ phân tán (DDoS)

-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, sử dụng tất cả băng thông có thể. Kẻ tấn công sau đó sẽ có toàn bộ lượng băng thông khổng lồ trên mạng để làm tràn website đích. Đó là cách phát động tấn công tốt nhất để đặt được nhiều máy tính dưới quyền kiểm soát. Mỗi máy tính sẽ đưa ra băng thông riêng (ví dụ với người dùng PC cá nhân nối ADSL). Tất cả sẽ được dùng một lần, và nhờ đó, phân tán được cuộc tấn công vào website đích. 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).

- Giới tin tặc cũng bỏ ra khá nhiều thời gian và công sức đầu tư nhằm nâng cao cách thức tấn công của chúng. Hiện nay, người dùng mạng máy tính như chúng ta đang phải đối mặt với nhiều kỹ thuật tinh vi hơn xa so kiểu tấn công DDoS truyền thống. Những kỹ thuật này cho phép kẻ tấn công điều khiển một số lượng cực kỳ lớn máy tính bị chiếm quyền điều khiển (zombie) tại một trạm từ xa mà đơn giản chỉ cần dùng giao thức IRC.

2.b - Spamming (phát tán thư rác)

- Botnet là một công cụ lý tưởng cho các spammer (kẻ phát tán thư rác). Chúng đã, đang và sẽ được dùng vừa để trao đổi địa chỉ e-mail thu thập được, vừa để điều khiển cơ chế phát tán thư rác theo cùng một cách với kiểu tấn công DDoS. Thư rác được gửi tới botnet, sau đó phân

phối qua các bot và từ đó phát tán tới máy tính đang bị chiếm quyền điều khiển. Tất cả spammer đều lấy tên nặc danh và mọi hậu quả thì máy tính bị phá hoại gánh chịu.

2.c - Sniffing và Keylogging

- Các bot cũng có thể được sử dụng một cách hiệu quả để nâng cao nghệ thuật cổ điển của hoạt động sniffing. Nếu theo dõi lưu lượng dữ liệu truyền đi, bạn có thể xác định được con số khó tin lượng thông tin được truyền tải. Đó có thể là thói quen của người dùng, trọng tải gói TCP và một số thông tin thú vị khác (như mật khẩu, tên người dùng). Cũng tương tự như vậy với keylogging, một hình thức thu thập tất cả thông tin trên bàn phím khi người dùng gõ vào máy tính (như e-mail, password, dữ liệu ngân hàng, tài khoản PayPal,…).

2.d - Ăn cắp nhận dạng

- Các phương thức được đề cập ở trên cho phép kẻ tấn công điều khiển botnet để thu thập một lượng thông tin cá nhân khổng lồ. Những dữ liệu có thể được dùng để xây dựng nhận dạng giả mạo, sau đó lợi dụng để có thể truy cập tài khoản cá nhân hoặc thực hiện nhiều hoạt động khác (có thể là chuẩn bị cho nhiều cuộc tấn công khác) mà người gánh chịu hậu quả không ai khác chính là chủ nhân của các thông tin đó.

2.e - Sở hữu phần mềm bất hợp pháp

- Đây là hình thức cuối cùng, nhưng chưa phải là kết thúc. Các máy tính bị tấn công theo kiểu bot có thể được dùng như một kho lưu trữ động tài liệu bất hợp pháp (phần mềm ăn cắp bản quyền, tranh ảnh khiêu dâm,…). Dữ liệu được lưu trữ trên ổ cứng trong khi người dùng ADSL không hề hay biết.

- Còn rất nhiều, rất nhiều kiểu ứng dụng khác nữa được phát triển dựa trên botnet (như trả tiền cho mỗi lần kích chuột để sử dụng một chương trình, phishing, hijacking kết nối HTTP/HTTPS…), nhưng liệt kê ra được hết có lẽ sẽ phải mất hàng giờ. Bản thân bot chỉ là một công cụ với khả năng lắp ghép và thích ứng dễ dàng cho mọi hoạt động đòi hỏi đặt quyền kiểm soát đơn lên một số lượng lớn máy tính.

IV.3 - Các kiểu bot khác nhau

- Nhiều kiểu bot đã được xây dựng và cho phép download được cung cấp nhan nhản khắp Internet. Mỗi kiểu có những thành phần đặc biệt riêng. Chúng ta sẽ xem xét một số bot phổ biến nhất và thảo những thành phần chính và các yếu tố phân biệt của chúng.

3.a - GT-Bot

- Tất cả các bot GT (Global Threat) đều dựa trên kiểu client IRC phổ biến dành cho Windows gọi là mIRC. Cốt lõi của các bot này là xây dựng tập hợp script (kịch bản) mIRC, được dùng để điều khiển hoạt động của hệ thống từ xa. Kiểu bot này khởi chạy một phiên client nâng cao với các script điều khiển và dùng một ứng dụng thứ hai, thông thường là HideWindows để ẩn mIRC trước người dùng máy tính đích. Một file DLL bổ sung sẽ thêm một số thành phần mới vào mIRC để các script có thể chi phối nhiều khía cạnh khác nhau trên máy tính bị chiếm quyền điều khiển.

3.b - Agobot

- Agobot là một trong những kiểu bot phổ biến nhất thường được các tay bẻ khoá (craker) chuyên nghiệp sử dụng. Chúng được viết trên nền ngôn ngữ C++ và phát hành dưới dạng bản quyền GPL. Điểm thú vị ở Agobot là mã nguồn. Được modul hoá ở mức cao, Agobot cho phép thêm chức năng mới vào dễ dàng. Nó cũng cung cấp nhiều cơ chế ẩn mình trên máy tính người dùng. Thành phần chính của Agobot gồm: NTFS Alternate Data Stream (Xếp luân phiên dòng dữ liệu NTFS), Antivirus Killer (bộ diệt chương trình chống virus) và Polymorphic Encryptor Engine (cơ chế mã hoá hình dạng). Agobot cung cấp tính năng sắp xếp và sniff lưu lượng. Các giao thức khác ngoài IRC cũng có thể được dùng để điều khiển kiểu bot này.

3.c - DSNX

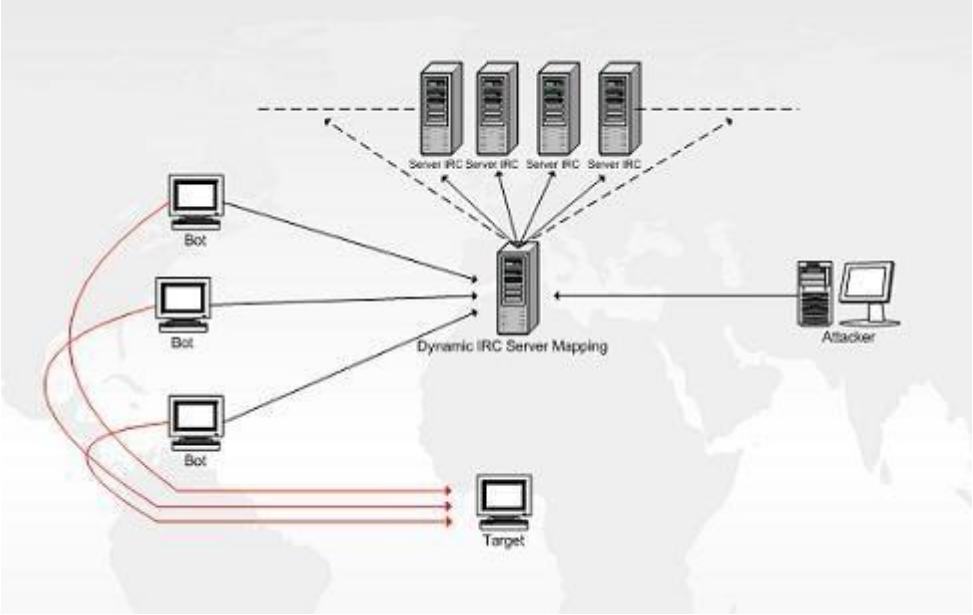
- Dataspy Network X (DSNX) cũng được viết trên nền ngôn ngữ C++ và mã nguồn dựa trên bản quyền GPL. Ở kiểu bot này có thêm một tính năng mới là kiến trúc plug-in đơn giản.

3.d - SDBot

- SDBot được viết trên nền ngôn ngữ C và cũng sử dụng bản quyền GPL. Không giống như Agobot, mã nguồn của kiểu bot này rất rõ ràng và bản thân phần mềm có một lượng giới hạn chức năng. Nhưng SDBot rất phổ biến và đã được phát triển ra nhiều dạng biến thể khác nhau.

IV.4 - Các yếu tố của một cuộc tấn công.

Hình 1 thể hiện cấu trúc của một botnet điển hình:



Hình 1: Cấu trúc của một botnet điển hình

• Đầu tiên kẻ tấn công sẽ phát tán trojan horse vào nhiều máy tính khác nhau. Các máy tính này trở thành zombie (máy tính bị chiếm quyền điều khiển) và kết nối tới IRC server để nghe thêm nhiều lệnh sắp tới.

• Server IRC có thể là một máy công cộng ở một trong các mạng IRC, nhưng cũng có thể là máy chuyên dụng do kẻ tấn công cài đặt lên một trong các máy bị chiếm quyền điều khiển.

• Các bot chạy trên máy tính bị chiếm quyền điều khiển, hình thành một botnet.

Một ví dụ cụ thể

Hoạt động của kẻ tấn công có thể chia thành bốn giai đoạn khác nhau:

+ Tạo

+ Cấu hình

+ Tấn công

+ Điều khiển

- Giai đoạn Tạo phụ thuộc lớn vào kỹ năng và đòi hỏi của kẻ tấn công. Nếu là người bẻ khoá chuyên nghiệp, họ có thể cân nhắc giữa việc viết mã bot riêng hoặc đơn giản chỉ là mở rộng, tuỳ biến cái đã có. Lượng bot có sẵn là rất lớn và khả năng cấu hình cao. Một số còn cho phép thao tác dễ dàng hơn qua một giao diện đồ hoạ. Giai đoạn này không có gì khó khăn, thường dành cho những kẻ mới vào nghề.

- Giai đoạn Cấu hình là cung cấp server IRC và kênh thông tin. Sau khi cài đặt lên một máy tính đã được kiểm soát, bot sẽ kết nối tới host được chọn. Đầu tiên kẻ tấn công nhập dữ liệu cần thiết vào để giới hạn quyền truy cập bot, bảo vệ an toàn cho kênh và cuối cùng cung cấp một danh sách người dùng được cấp phép (những người có thể điều khiển bot). Ở giai đoạn này, bot có thể được điều chỉnh sâu hơn, như định nghĩa phương thức tấn công và đích đến.

- Giai đoạn Tấn công là sử dụng nhiều kỹ thuật khác nhau để phát tán bot, cả trực tiếp và gián tiếp. Hình thức trực tiếp có thể là khai thác lỗ hổng của hệ điều hành hoặc dịch vụ. Còn gián tiếp thường là triển khai một số phần mềm khác phục vụ cho công việc đen tối, như sử dụng file HTML dị dạng để khai thác lỗ hổng Internet Explorer, sử dụng một số phần mềm độc hại khác phân phối qua các mạng ngang hàng hoặc qua trao đổi file DCC (Direct Client–to–Client) trên IRC. Tấn công trực tiếp thường được thực hiện tự động thông qua các sâu (worm). Tất cả công việc những sâu này phải làm là tìm kiếm mạng con trong hệ thống có lỗ hổng và chèn mã bot vào. Mỗi hệ thống bị xâm phạm sau đó sẽ tiếp tục thực hiện chương trình tấn công, cho phép kẻ tấn công ghi lại tài nguyên đã dùng trước đó và có được nhiều thời gian để tìm kiếm nạn nhân khác.

- Cơ chế được dùng để phân phối bot là một trong những lý do chính gây nên cái gọi là tạp nhiễu nền Internet. Một số cổng chính được dùng cho Windows, cụ thể là Windows 2000, XP SP1 (xem Bảng 1). Chúng dường như là đích ngắm yêu thích của hacker, vì rất dễ tìm ra một máy tính Windows chưa được cập nhật bản vá đầy đủ hoặc không cài đặt phần mềm tường lửa. Trường hợp này cũng rất phổ biến với người dùng máy tính gia đình và các doanh nghiệp nhỏ, những đối tượng thường bỏ qua vấn đề bảo mật và luôn kết nối Internet băng thông rộng.

Cổng Dịch vụ

42 WINS (Host Name Server)

80 HTTP (lỗ hổng IIS hay Apache)

135 RPC (Remote Procedure Call)

137 NetBIOS Name Service

139 NetBIOS Session Service

445 Microsoft–DS–Service

1025 Windows Messenger

1433 Microsoft–SQL–Server

2745 Bagle worm backdoor

3127 MyDoom worm backdoor

3306 MySQL UDF (User Definable Functions)

5000 UPnP (Universal Plug and Play)

Danh sách các cổng gắn với lỗ hổng dịch vụ

- Giai đoạn Điều khiển gồm một số hoạt động thực hiện sau khi bot đã được cài đặt lên máy đích trong một thư mục chọn. Để khởi động với Windows, bot update các khoá đăng ký, thông thường là

KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\.

- Việc đầu tiên bot thực hiện sau khi được cài đặt thành công là kết nối tới một server IRC và liên kết với kênh điều khiển thông qua sử dụng một mật khẩu. Nickname trên IRC được tạo ngẫu nhiên. Sau đó, bot ở trạng thái sẵn sàng chờ lệnh từ ứng dụng chủ. Kẻ tấn công cũng phải sử dụng một mật khẩu để kết nối tới botnet. Điều này là cần thiết để không ai khác có thể sử dụng mạng botnet đã được cung cấp.

- IRC không chỉ cung cấp phương tiện điều khiển hàng trăm bot mà còn cho phép kẻ tấn công sử dụng nhiều kỹ thuật khác nhau để ẩn nhân dạng thực của chúng. Điều đó khiến việc đối

phó trước các cuộc tấn công trở nên khó khăn. Nhưng may mắn là, do đặc điểm tự nhiên của chúng, các botnet luôn tạo ra lưu lượng đáng ngờ, tạo điều kiện dễ dàng để có thể dò tìm nhờ một số kiểu mẫu hay mô hình đã biết. Điều đó giúp các quản trị viên IRC phát hiện và can thiệp kịp thời, cho phép họ gỡ bỏ các mạng botnet và những sự lạm dụng không đáng có trên hệ thống của họ.

- Trước tình hình này, những kẻ tấn công buộc phải nghĩ ra cách thức khác, cải tiến kỹ thuật C&C (Control and Command - Điều khiển qua lệnh) thành botnet hardening. Ở kỹ thuật mới này, các bot thường được cấu hình để kết nối với nhiều server khác nhau, sử dụng một hostname ánh xạ động. Nhờ đó, kẻ tấn công có thể chuyển bot sang server mới dễ dàng, vẫn hoàn toàn nắm quyền kiểm soát ngay cả khi bot đã bị phát hiện. Các dịch vụ DNS động như dyndns.com hay no-IP.com thường được dùng trong kiểu tấn công này.

DNS động

- Một DNS động (như RFC 2136) là một hệ thống liên kết tên miền với địa chỉ IP động. Người dùng kết nối Internet qua modem, ADSL hoặc cáp thường không có địa chỉ IP cố định. Khi một đối tượng người dùng kết nối tới Internet, nhà cung cấp dịch vụ mạng (ISP) sẽ gán một địa chỉ IP chưa được sử dụng lấy ra từ vùng được chọn. Địa chỉ này thường được giữ nguyên cho tới khi người dùng ngừng sử dụng kết nối đó.

- Cơ chế này giúp các hãng cung cấp dịch vụ mạng (ISP) tận dụng được tối đa khả năng khai thác địa chỉ IP, nhưng cản trở đối tượng người dùng cần thực hiện một số dịch vụ nào đó qua mạng Internet trong thời gian dài, song không phải sử dụng địa chỉ IP tĩnh. Để giải quyết vấn đề này, DNS động được cho ra đời. Hãng cung cấp sẽ tạo cho dịch vụ một chương trình chuyên dụng, gửi tín hiệu tới cơ sở dữ liệu DNS mỗi khi địa chỉ IP của người dùng thay đổi.

- Để ẩn hoạt động, kênh IRC được cấu hình giới hạn quyền truy cập và ẩn thao tác. Các mô hình IRC điển hình cho kênh botnet là: +k (đòi hỏi phải nhập mật khẩu khi dùng kênh); +s (không được hiển thị trên danh sách các kênh công cộng); +u (chỉ có người điều hành (operator) là được hiển thị trên danh sách người dùng); +m (chỉ có người dùng ở trạng thái sử dụng âm thanh +v mới có thể gửi tin đến kênh). Hầu hết mọi chuyên gia tấn công đều dùng server IRC cá nhân, mã hoá tất cả liên lạc trên kênh dẫn. Chúng cũng có khuynh hướng sử dụng nhiều biến thể cá nhân hoá của phần mềm IRC server, được cấu hình để nghe trên các cổng ngoài tiêu chuẩn và

sử dụng phiên bản đã được chỉnh sửa của giao thức, để một IRC client thông thường không thể kết nối vào mạng.

IV.5 - Cách phòng chống Botnet:

- Botnet là một mối đe dọa đang ngày một lan rộng, tuy nhiên chúng ta có nhiều cách đối phó để giảm được các tác hại gây ra từ nó, chúng tôi sẽ giới thiệu 6 cách khá chuyên nghiệp có thể chống trả lại được botnet.

5.a - Thuê một dịch vụ lọc Web

- Dịch vụ lọc Web là một trong những cách tốt nhất để đấu tranh với bot. Các dịch vụ này quét website khi thấy xuất hiện hành vi không bình thường hoặc có các hành động mã nguy hiểm và khóa site đó từ người dùng.

- Websense, Cyveillance và FaceTime Communications là các ví dụ điển hình. Tất cả sẽ kiểm tra Internet theo thời gian thực tìm các website bị nghi ngờ có hành động nguy hiểm như tải JavaScript và các trò lừa đảo khác ngoài ranh giới của việc duyệt web thông thường. Cyveillance và Support Intelligence cũng cung cấp dịch vụ cho biết về các tổ chức website và ISP đã phát hiện là có malware, vì vậy các máy chủ bị tấn công có thể được sửa chữa kịp thời.

5.b - Chuyển đổi trình duyệt

- Một cách khác để ngăn chặn sự xâm nhập của bot là không nên sử dụng một trình duyệt. Internet Explorer hay Mozilla Firefox là hai trình duyệt phổ biến nhất và vì vậy chúng cũng là các trình duyệt mà malware tập trung tấn công tới. Chúng ta có thể dùng Apple Safari, Google Chrome, Opera, Netscape, ... Tương tự như vậy đối với các hệ điều hành. Theo thống kê thì Macs là hệ điều hành an toàn với botnet bởi vì hầu hết chúng đều nhằm vào Windows. Ngoài có thể sử dụng hệ điều hành họ *nix để ngăn chặn các phần mềm mã độc như virus, trojan, spyware , sworm .... vì các phần mềm mã độc này chỉ chạy trên hệ điều hành phổ biến nhất là Windows.

5.c - Vô hiệu hóa các kịch bản

- Một cách nữa là vô hiệu hóa trình duyệt khỏi các kịch bản nói chung (script), điều này có thể gây khó khăn cho một số nhân viên sử dụng ứng dụng tùy chỉnh và dựa trên nền web trong công việc của họ.

5.d - Triển khai các hệ thông phát hiện xâm phạm và ngăn chặn xâm phạm

- Một phương pháp khác đó là điều chỉnh các IDS và ISP để chúng có thể tìm kiếm được các hoạt động tương tự như botnet.

- Ví dụ, một máy tính nào đó bất ngờ gặp vấn đề sự cố trên Internet Relay Chat là hoàn toàn đáng nghi ngờ. Cũng giống như việc kết nối vào các địa chỉ IP ở xa hoặc địa chỉ DNS không hợp lý. Tuy vấn đề này là khó phát hiện nhưng chúng ta có cách phát giác khác khi phát hiện thấy sự thu hút bất ngờ trong lưu lượng SSL trên một máy tính, đặc biệt trong các cổng không bình thường. Điều đó có thể là kênh mà botnet chiếm quyền điều khiển đã bị kích hoạt.

- Chính vì vậy chúng ta cần một ISP để kiểm tra về những hành vi không bình thường để chỉ thị cảnh báo các tấn công dựa trên HTTP và thủ tục gọi từ xa, Telnet- và giả mạo giao thức giải pháp địa chỉ, các tấn công khác. Mặc dù vậy chúng ta phải nên chú ý rằng nhiều bộ cảm biến ISP sử dụng phát hiện dựa trên chữ ký, điều đó nghĩa là các tấn công chỉ được bổ sung vào cơ sở dữ liệu khi nào chúng được phát hiện. Chính vì vậy các ISP phải cập nhật kịp thời để nhận ra được các tấn công này, bằng không bộ phát hiện sẽ không còn giá trị.

5.e - Bảo vệ nội dung được tạo bởi người dùng

- Các hoạt động website của riêng bạn cũng phải được bảo vệ để tránh trở thành kẻ tòng phạm không chủ tâm đối với những kẻ viết malware. Các blog công cộng và forum của công ty nên được hạn chế chỉ ở dạng văn bản.

- Nếu site của bạn cần cho các thành viên trao đổi file thì nó phải được thiết lập để cho phép các kiểu file được giới hạn và đảm bảo an toàn, ví dụ với các file có đuôi mở rộng .jpeg hoặc .mp3. (Tuy vậy những kẻ viết malware cũng đã bắt đầu nhắm vào đối tượng người chơi MP3)

5.f - Sử dụng công cụ phần mềm

- Nếu bạn phát hiện thấy máy tính bị tiêm nhiễm mà hệ thống không có cách nào tốt nhất để giải quyết với tình huống này. Bạn không phải lo sợ điều đó vì các công ty như Symantec xác nhận rằng họ có thể phát hiện và xóa sạch sự tiêm nhiễm rootkit nguy hiểm nhất. Công ty này đã đưa ra một công nghệ mới trong Veritas, VxMS (Dịch vụ bản đồ hóa Veritas – Veritas Mapping

Service), đưa ra bộ quét chống virus bỏ qua Windows File System API, thành phần được điều khiển bởi hệ điều hành có thể gây ra lỗ hổng bởi một rootkit. VxMS truy cập trực tiếp vào các file thô của hệ thống Windows NT File System. Bên cạnh đó các hãng phần mềm chống virus khác cũng đang cố gắng trong việc chống lại rootkit này gồm có McAfee và FSecure.

V – 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.
- Các kỹ thuật trên đang và vẫn là vấn nạn nguy hại lớn cho nền Internet toàn cầu. Có rất nhiều việc phải làm và chuẩn bị để kiểm soát được chúng. Chúng ta phải có những bước đi cụ thể và mạnh mẽ hơn để cùng khống chế loại hình tấn công này.

VI – Tài Liệu Tham Khảo

1 - Sách:

[1] - Tactical Perimeter Defense

[2] - Slide "An Toàn Mạng" – Th.s T. Ng. Nhật Quang.

2 – Website:

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

[2] - http://ceh.vn

[3] - http://huynhdegroup.net

[4] - http://handsteamsys.com

Ebook này tôi có tham khảo một số bài viết cũng như tài liệu của một số đàn anh đi trước.

Xin chân thành cảm ơn Hacker Llykil (người thực hiện DDos Trường Tồn và Bkvn cùng hàng loạt Website khác năm 2008) cũng như anh Hồ Đức Dũng (Mr.Soleil) một số người bạn đã giúp đỡ mình hoàn thành Ebook này.

Các bạn có thể liên hệ và góp ý chân thành cho mình để mình có thể học hỏi thêm và hoàn thiện hơn... Xin cảm ơn các bạn rất rất nhiều

Email:

jcalexminmagic@yahoo.com.vn

jcalexmin@gmail.com

jchakingteam@gmail.com

Facebook:

http://www.facebook.com/jcalexmin

Website:

http://jc.bl.ee

..:: JCAlex Min ::..