MỤC LỤC

Phần I : DOS

I. Lịch sử của tấn công DoS

1. Mục tiêu

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

2. Các cuộc tấn công.

- 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

II. Định nghĩa về tấn công DoS

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

- Tấn công DoS là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.
- Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).
Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp.
Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đích của tấn công DoS:

1. Các mục đích của tấn công DoS

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.

- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.

- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó

- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.

- Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó như bị:

+ Disable Network - Tắt mạng

+ Disable Organization - Tổ chức không hoạt động

+ Financial Loss – Tài chính bị mất

2. Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS

Như chúng ta biết ở bên trên tấn công DoS xảy ra khi kẻ tấn công sử dụng hết tài nguyên của hệ thống và hệ thống không thể đáp ứng cho người dùng bình thường được vậy các tài nguyên chúng thường sử dụng để tấn công là gì:

- Tạo ra sự khan hiếm, những giới hạn và không đổi mới tài nguyên

- Băng thông của hệ thống mạng (Network Bandwidth), bộ nhớ, ổ đĩa, và CPU Time hay cấu trúc dữ liệu đều là mục tiêu của tấn công DoS.

- Tấn công vào hệ thống khác phục vụ cho mạng máy tính như: hệ thống điều hoà, hệ thống điện, hệt hống làm mát và nhiều tài nguyên khác của doanh nghiệp. Bạn thử tưởng tượng khi nguồn điện vào máy chủ web bị ngắt thì người dùng có thể truy cập vào máy chủ đó không.

- Phá hoại hoặc thay đổi các thông tin cấu hình.

- Phá hoại tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hoà…

III. Các dạng tấn công

Tấn công Denial of Service chia ra làm hai loại tấn công

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

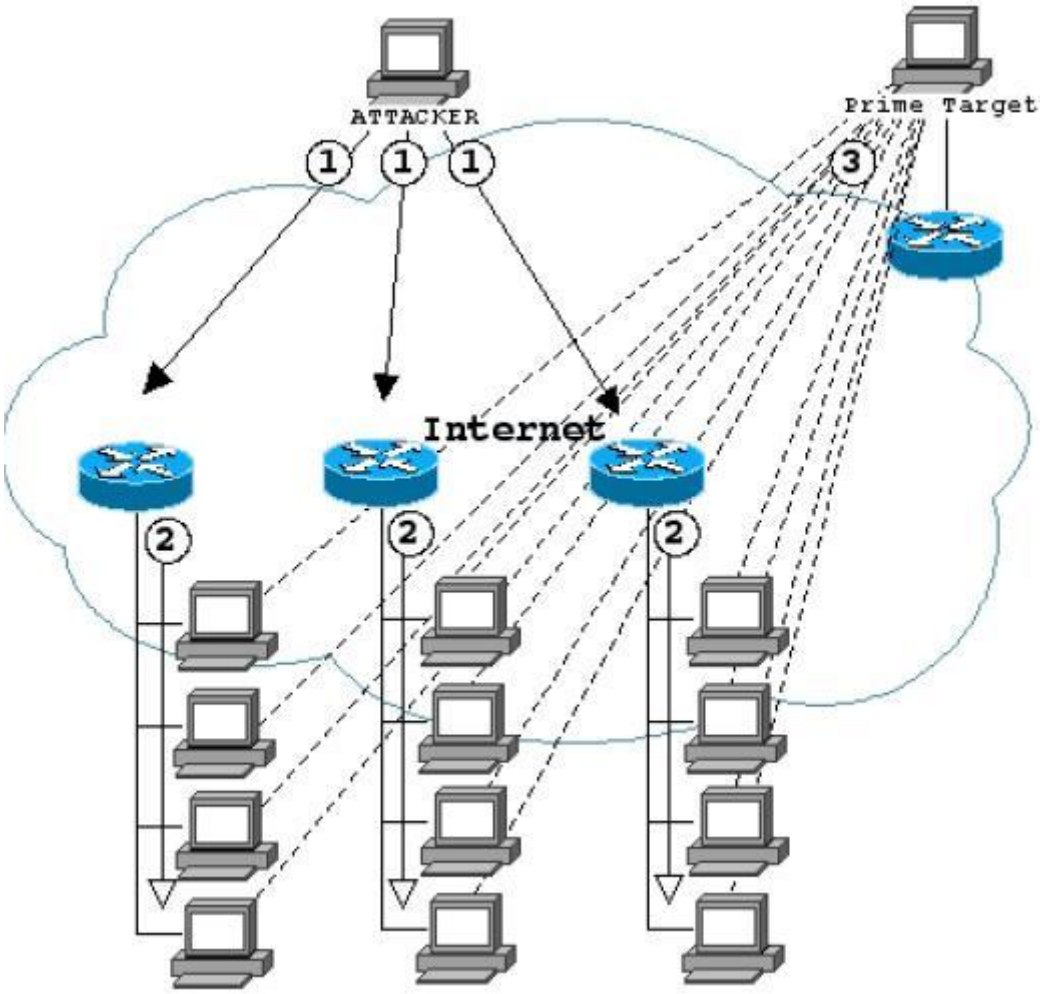
1. Các dạng tấn công DoS

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

a. Tấn công Smurf

- Là thủ phạm sinh ra cực nhiều giao tiếp ICMP (ping) tới địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công.

* Chúng ta cần lưu ý là: Khi ping tới một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại . Nhưng giờ thay đổi địa chỉ nguồn, thay địa chỉ nguồn là máy C và ping tới địa chỉ Broadcast của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ reply lại vào máy C chứ không phải pc gửi và đó là tấn công Smurf.



- Kết quả đích tấn công sẽ phải chịu nhận một đợt Reply gói ICMP cực lớn và làm cho mạng bị dớt hoặc bị chậm lại không có khả năng đáp ứng các dịch vụ khác.
- Quá trình này được khuyếch đại khi có luồng ping reply từ một mạng được kết nối với nhau (mạng BOT).
- tấn công Fraggle, chúng sử dụng UDP echo và tương tự như tấn công Smurf.

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

b. Tấn công Buffer overflow.

- Buffer Overflow xảy ra tại bất kỳ thời điểm nào có chương trình ghi lượng thông tin lớn hơn dung lượng của bộ nhớ đệm trong bộ nhớ.
- Kẻ tấn công có thể ghi đè lên dữ liệu và điều khiển chạy các chương trình và đánh cắp quyền điều khiển của một số chương trình nhằm thực thi các đoạn mã nguy hiểm. .
- 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.

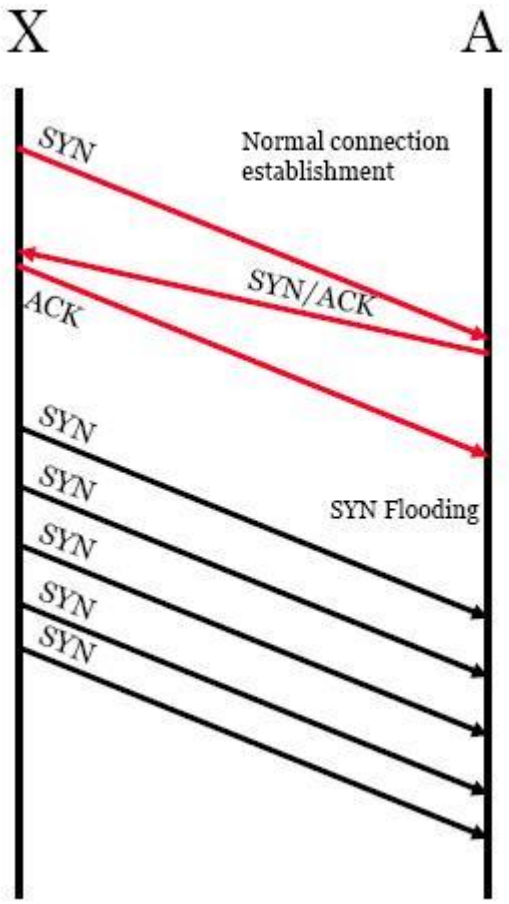
c. Tấn công Ping of Death

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

d. Tấn công Teardrop

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

e. Tấn công SYN



- Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối.
- Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện Request TCP SYN và lúc này máy chủ không còn khả năng đáp lại - kết nối không được thực hiện.
- Đây là kiểu tấn công mà kẻ tấn công lợi dụng quá trình giao tiếp của TCP theo – Three-way.

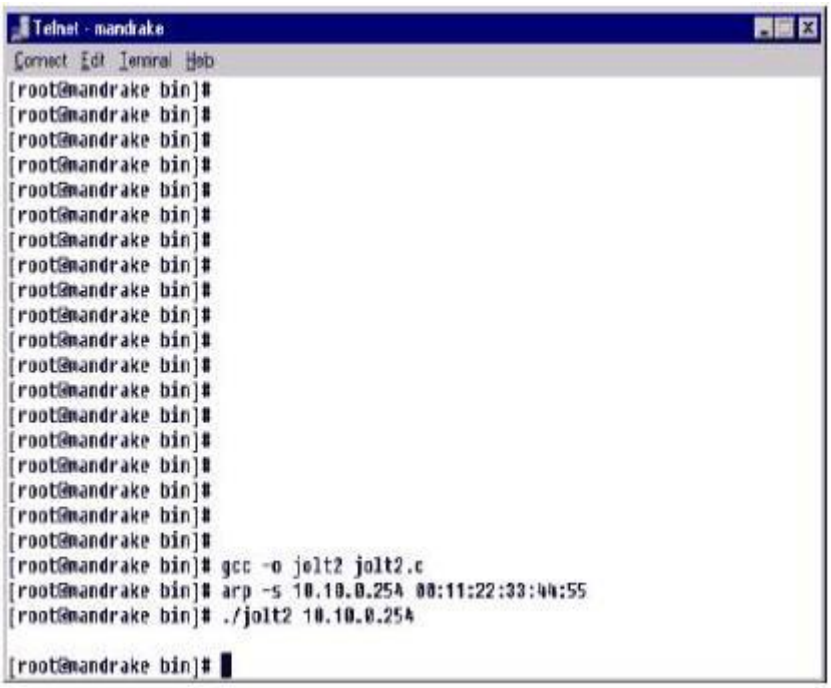
- Các đoạn mã nguy hiểm có khả năng sinh ra một số lượng cực lớn các gói TCP SYN tới máy chủ bị tấn công, địa chỉ IP nguồn của gói tin đã bị thay đổi và đó chính là tấn công DoS.
- Hình bên trên thể hiện các giao tiếp bình thường với máy chủ và bên dưới thế hiện khi máy chủ bị tấn công gói SYN đến sẽ rất nhiều trong khi đó khả năng trả lời của máy chủ lại có hạn và khi đó máy chủ sẽ từ chối các truy cập hợp pháp.
- Quá trình TCP Three-way handshake được thực hiện: Khi máy A muốn giao tiếp với máy B. (1) máy A bắn ra một gói TCP SYN tới máy B – (2) máy B khi nhận được gói SYN từ A sẽ gửi lại máy A gói ACK đồng ý kết nối – (3) máy A gửi lại máy B gói ACK và bắt đầu các giao tiếp dữ liệu.
- Máy A và máy B sẽ dữ kết nối ít nhất là 75 giây, sau đó lại thực hiện một quá trình TCP Three-way handshake lần nữa để thực hiện phiên kết nối tiếp theo để trao đổi dữ liệu.
- Thật không may kẻ tấn công đã lợi dụng kẽ hở này để thực hiện hành vi tấn công nhằm sử dụng hết tài nguyên của hệ thống bằng cách giảm thời gian yêu cầu Three-way handshake xuống rất nhỏ và không gửi lại gói ACK, cứ bắn gói SYN ra liên tục trong một thời gian nhất định và không bao giờ trả lời lại gói SYN&ACK từ máy bị tấn công.
- Với nguyên tắc chỉ chấp nhận gói SYN từ một máy tới hệ thống sau mỗi 75 giây nếu địa chỉ IP nào vi phạm sẽ chuyển vào Rule deny access sẽ ngăn cản tấn công này.

IV. Các công cụ tấn công DoS

- Jolt2
- Bubonic.c
- Land and LaTierra
- Targa
- Blast20

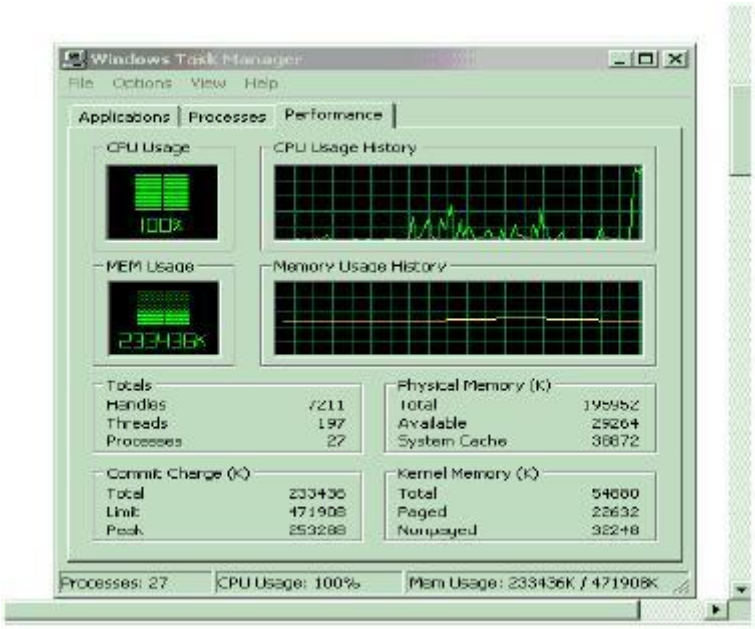
- Nemesy
- Panther2
- Crazy Pinger
- Some Trouble
- UDP Flood
- FSMax

1. Tools DoS – Jolt2



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

2. Tools DoS: Bubonic.c



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

3. Tools DoS: Land and LaTierra

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

- Kết quả này do địa chỉ IP nguồn và địa chỉ IP đích của gói tin giống nhau và gói tin không thể đi đến đích cần đến.

4. Tools DoS: Targa

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

5. Tools DoS Blast 2.0

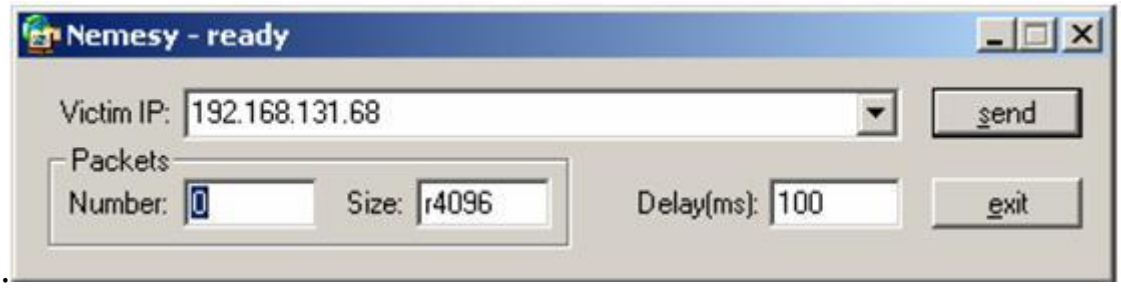
- Blast rất nhỏ, là một công cụ dùng để kiểm tra khả năng của dịch vụ TCP nó có khả năng tạo ra một lưu lượng rất lớn gói TCP và có thể sẽ gay nguy hiểm cho một hệ thống mạng với các server yếu.
- Dưới đây là cách sử dụng để tấn công HTTP Server sử dụng Blast2.0

+ Blast 192.168.1.219 80 40 50 /b "GET /some" /e "url/ HTTP/1.0" /nr /dr /v

- Tấn công máy chủ POP

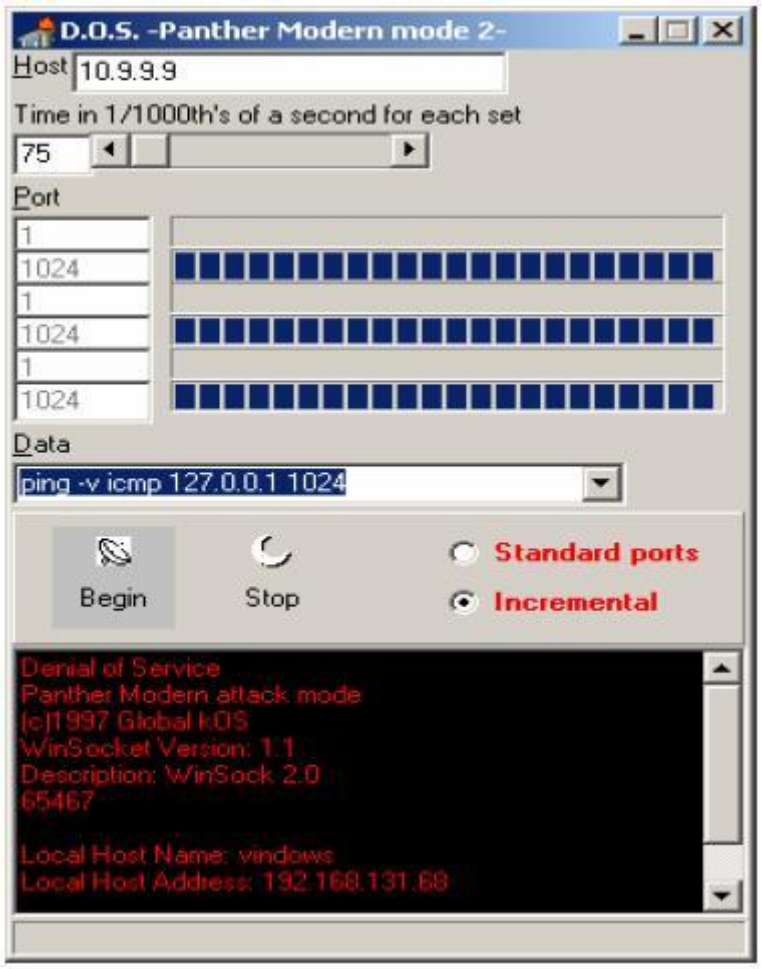
+ Blast 192.168.1.219 110 15 20 /b "user te" /e "d" /v

6. Tools DoS – Nemesys



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

7. Tool DoS – Panther2.

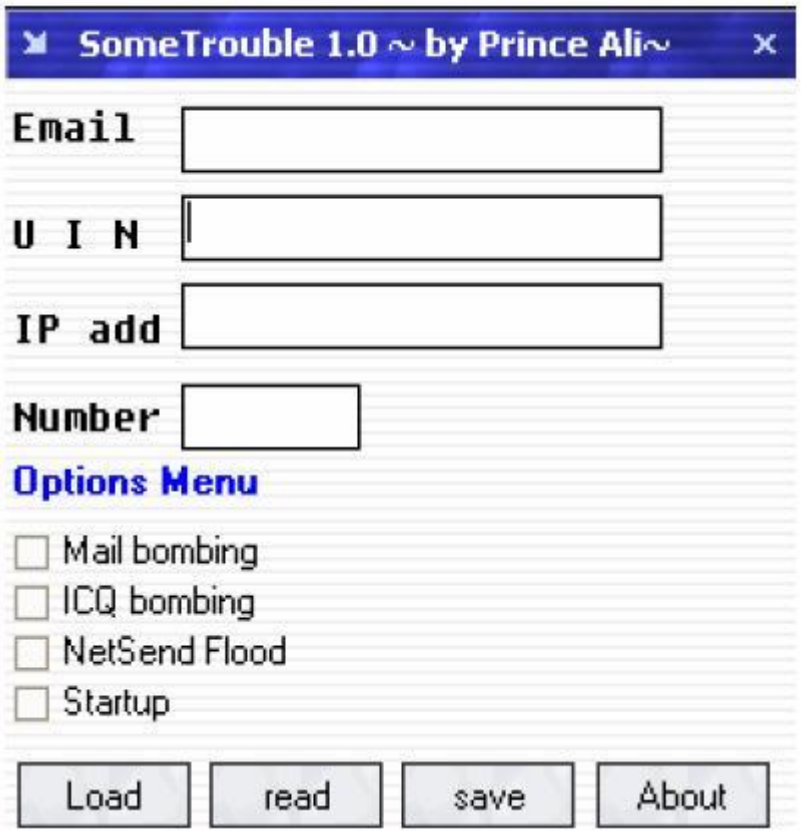


- Tấn công từ chối dịch vụ dựa trên nền tảng UDP Attack được thiết kế dành riêng cho kết nối 28.8 – 56 Kbps.
- Nó có khả năng chiếm toàn bộ băng thông của kết nối này.
- Nó có khả năng chiếm băng thông mạng bằng nhiều phương pháp ví như thực hiện quá trình Ping cực nhanh và có thể gây ra tấn công DoS

8. Tool DoS – Crazy Pinger

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

9. Tool DoS – Some Trouble



- SomeTrouble 1.0 là một chương trình gây nghẽn hệ thống mạng

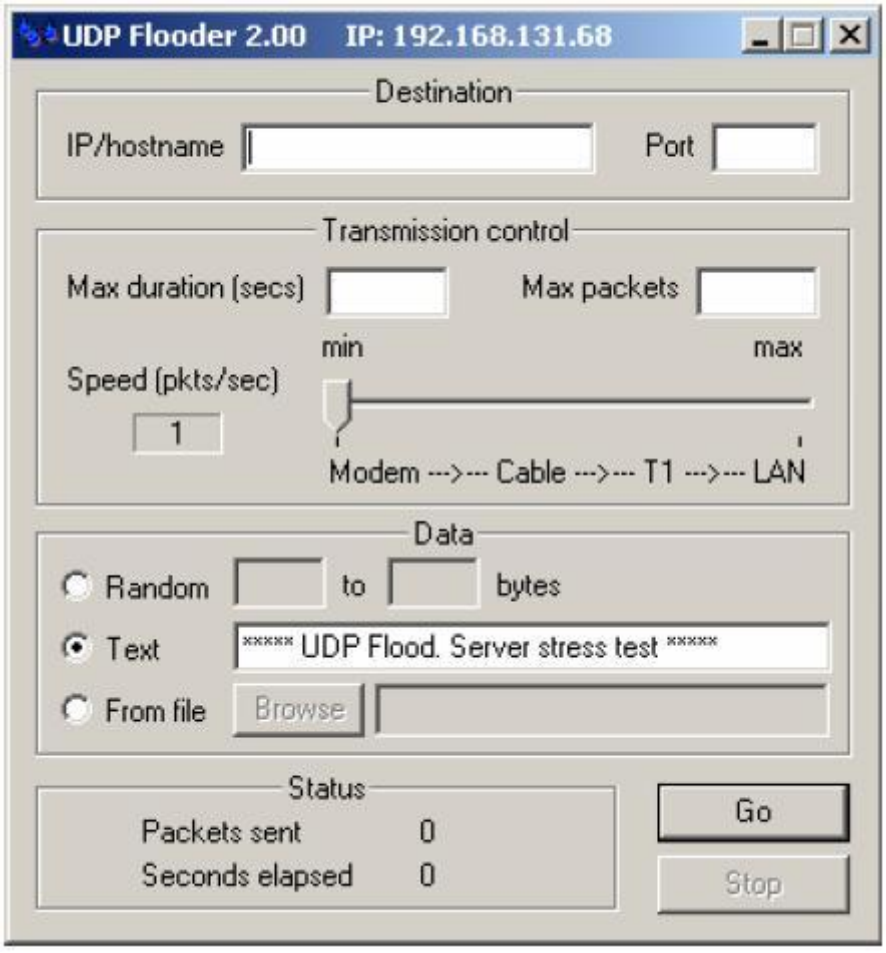
  - SomeTrouble là một chương trình rất đơn giản với ba thành phần

  + Mail Bomb (tự có khả năng Resole Name với địa chỉ mail có)

  + ICQ Bomb

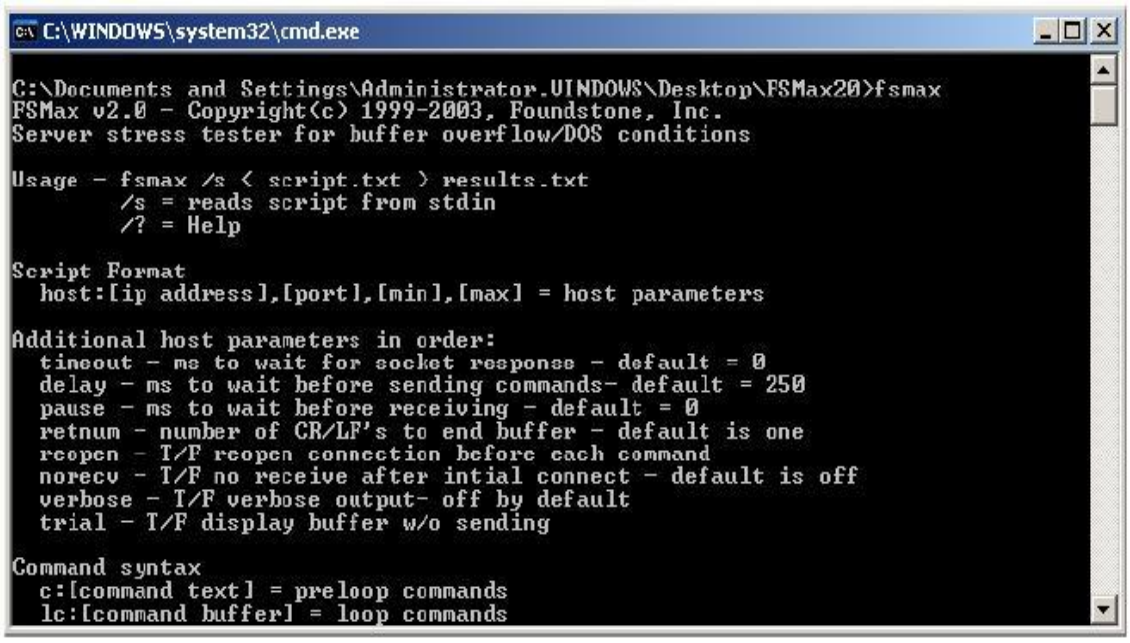
  + Net Send Flood

10. DoS Tools – UDP Flood



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

11. Tools DoS – FSMAX



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

V. Kết luận phần I.

- Khi sử dụng một Tool tấn công DoS tới một máy chủ đôi khi không gây ảnh hưởng gì cho máy chủ - Giả sử bạn sử dụng tool Ping of Death tới một máy chủ, trong đó máy chủ kết nối với mạng tốc độ 100Mbps bạn kết nối tới máy chủ tốc độ 3Mbps - Vậy tấn công của bạn không có ý nghĩa gì.
- Nhưng bạn hãy tưởng tượng có 1000 người như bạn cùng một lúc tấn công vào máy chủ kia khi đó toàn bộ băng thông của 1000 người cộng lại tối đa đạt 3Gbps và tốc độ kết nối của máy chủ là 100 Mbps vậy kết quả sẽ ra sao các bạn có khả năng tưởng tượng.

Phần II : DDOS-BOT-BOTNET

Một trong những phương thức tấn công DDoS hiệu quả và phổ biến nhất hiện nay là hoạt động dựa trên hàng trăm máy tính bị chiếm quyền điều khiển (tức các zombie). Những zombie này thường bị kiểm soát và quản lý qua các mạng IRC, sử dụng được gọi là các botnet. Botnet hoạt động như thế nào

Một số cách thức tin tặc có thể dùng để tấn công và chiếm quyền điều khiển máy tính đích, cùng một số biện pháp đối phó hiệu quả nhằm bảo vệ máy tính trước những mối đe doạ nguy hiểm luôn rình rập xung quanh. Tìm hiểu về:

• Như thế nào là bot, botnet; cách thức hoạt động của chúng.
• Những thành phần phổ biến nhất trong bot.
• Một host có thể bị tấn công và chiếm quyền điều khiển như thế nào.
• Biện pháp ngăn chặn hiệu quả và cách đối phó trước hoạt động phá hoại của chúng.

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.

I. Giới thiệu về Bot và Botnet

Bot là viết tắt của robot, tức các chương trình tự động hoá (chứ không phải là người máy như nghĩa chúng ta vẫn gọi) thường xuyên được sử dụng trong thế giới Internet. Người ta định nghĩa spider được dùng bởi các công cụ tìm kiếm trực tuyến, ánh xạ website và phần mềm đáp ứng theo yêu cầu trên IRC (như eggdrop) là robot. Các chương trình tự động phản ứng khi gặp sự kiện ngoài mạng nội bộ cũng được gọi là robot. Trong bài này, chúng ta sẽ quan tâm tới một kiểu robot cụ thể (hay bot như tên tắt vẫn thường được gọi) là IRC bot. IRC bot sử dụng các mạng IRC như một kênh liên lạc để nhận lệnh từ người dùng từ xa. Ví dụ cụ thể như, người dùng là một kẻ tấn công, còn bot là một Trojan horse. Một lập trình viên giỏi có thể dễ dàng tạo ra một số bot riêng của mình, hoặc xây dựng lại từ các bot có sẵn. Chúng có thể dễ dàng ẩn nấp trước những hệ thống bảo mật cơ bản, sau đó là phát tán đi nhanh chóng trong thời gian ngắn.

1. 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 cần 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.

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.

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.

II. 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).

1. 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. 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.

3. 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,…).

4. Ăn cắp nhân 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 nhân 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.

5.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.

III. 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.

1. 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.

2. Agobot

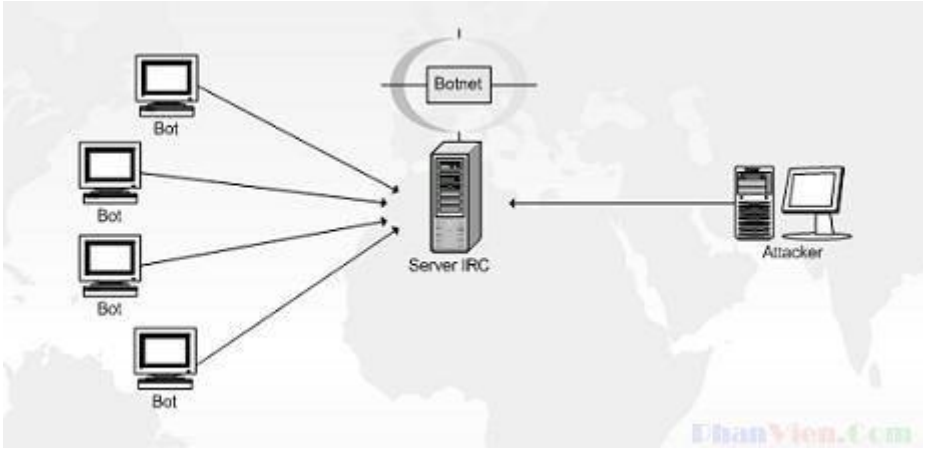
Agobot là một trong những kiểu bot phổ biến nhất thường được các tay bẻ khoá (craker) chuyên nghiệp sử dụng. Chúng được viết trên nền ngôn ngữ C++ và phát hành dưới dạng bản quyền GPL. Điểm thú vị ở Agobot là mã nguồn. Được modul hoá ở mức cao, Agobot cho phép thêm chức năng mới vào dễ dàng. Nó cũng 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. 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.

4. 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.
Các yếu tố của một cuộc tấn công



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.

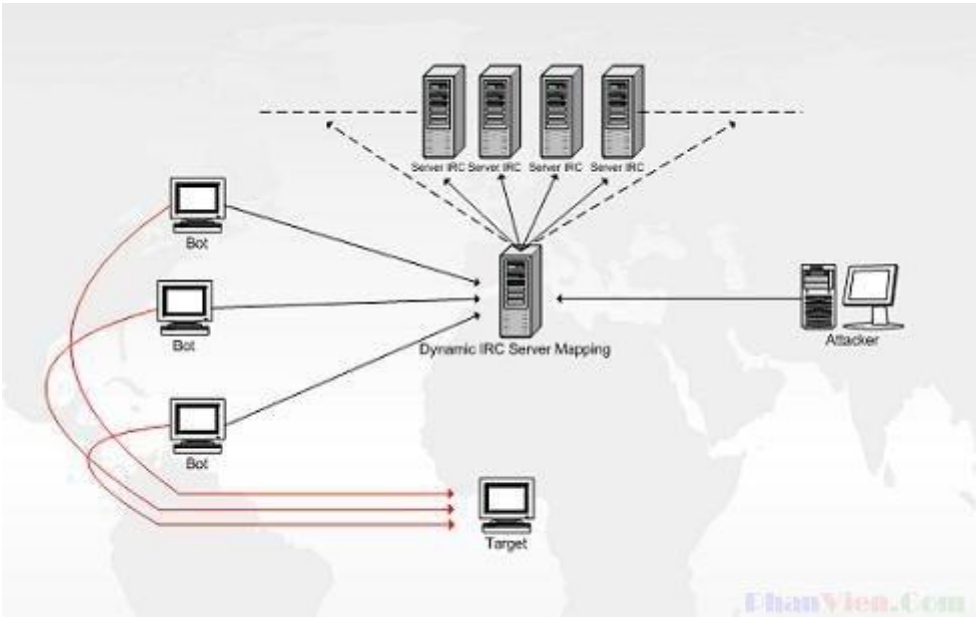
• Server IRC có thể là một máy công cộng ở một trong các mạng IRC, nhưng cũng có thể là máy chuyên dụng do kẻ tấn công cài đặt lên một trong các máy bị chiếm quyền điều khiển.
• Các bot chạy trên máy tính bị chiếm quyền điều khiển, hình thành một botnet.
Một ví dụ cụ thể
Hoạt động của kẻ tấn công có 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.
CổngDịch vụ42WINS (Host Name Server)80HTTP (lỗ hổng IIS hay Apache)135RPC (Remote Procedure Call)137NetBIOS Name Service139NetBIOS Session Service445Microsoft–DS–Service1025Windows Messenger1433Microsoft–SQL–Server2745Bagle worm backdoor3127MyDoom worm backdoor3306MySQL UDF (User Definable Functions)5000 UPnP (Universal Plug and Play)

Bảng 1: 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 HKEY_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.



Hình 2: Kỹ thuật botnet hardening

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.

5. DNS động

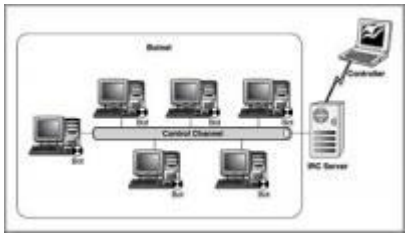
Một DNS động (như RFC 2136) là một hệ thống liên kết tên miền với địa chỉ IP động. Người dùng kết nối Internet qua modem, ADSL hoặc cáp thường không có địa chỉ IP cố định. Khi một đối tượng người dùng kết nối tới Internet, nhà cung cấp dịch vụ mạng (ISP) sẽ gán một địa chỉ IP chưa được sử dụng lấy ra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

Bây giờ là một vụ tấn công mẫu, cho phép chúng ta quan sát và hiểu một chương trình Command and Control (điều khiển qua lệnh) được thực hiện như thế nào. Hai máy tính sẽ được sử dụng. Máy đầu tiên chạy một server IRC dựa trên UnrealIRCd 3.2.3 và hai hệ điều hành Windows XP SP1 ảo dựa trên VMware Workstation (hai máy đích có khả năng bị tấn công). Máy thứ hai dành cho người chủ trì, điều khiển botnet qua Irssi, một text IRC client.

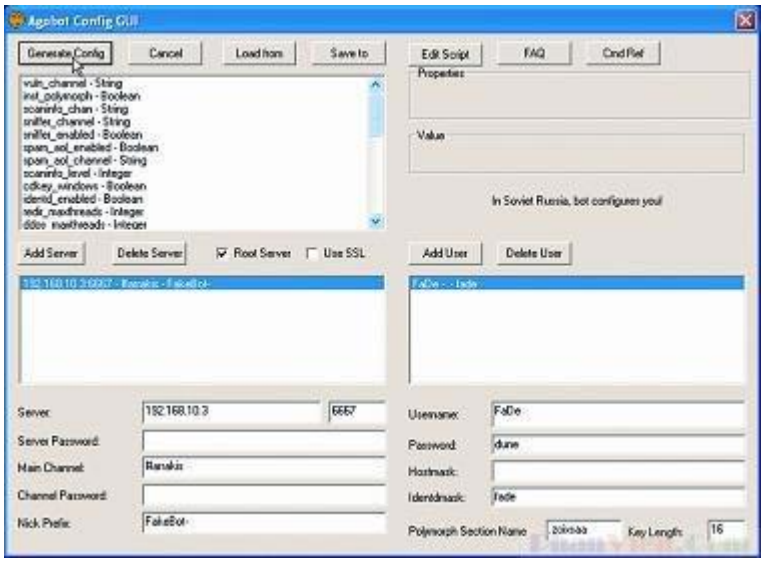


Để tạo chương trình thiết kế đối chiếu (reverse engineering) thật khó, Agobot thực hiện một số thường trình tự bảo vệ trước các bộ gỡ lỗi như SoftICE hay OllyDbg và trước các máy ảo như VMware, Virtual PC. Điều đó là cần thiết để hack được mã nguồn nhằm vượt qua chương trình bảo vệ của VMware, trước khi có thể cài đặt bot lên các máy ảo mẫu của chúng ta.

Cấu hình

Bước đầu tiên là cấu hình bot thông qua giao diện đồ hoạ đơn giản của nó (Xem hình 3). Thông tin được nhập vào bao gồm tên, số cổng IRC server, tên kênh, danh sách người sử dụng với mật khẩu master (chủ điều khiển), cuối cùng là tên file và thư mục cài đặt bot. Một số thành phần bổ sung cũng được

kích hoạt như hỗ trợ sniffing và cơ chế trạng thái. Kết quả của giai đoạn này là file config.h, file nền tảng trong quá trình biên dịch bot được tạo.



Điều khiển theo lệnh (Command and Control)

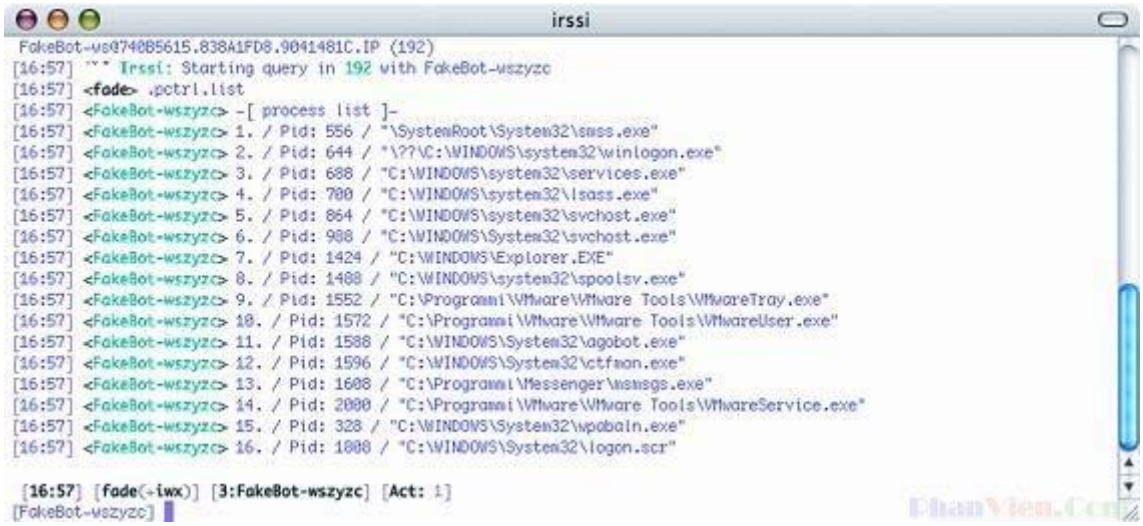
Sau khi bot được biên dịch, hai hệ thống còn lại sẽ tấn công theo kiểu "thủ công". Máy chủ (master) kết nối tới IRC server và liên kết với kênh dẫn để có thể ra lệnh điều khiển cho bot

Muốn thu được quyền điều khiển qua các bot, một cơ chế thẩm định là cần thiết. Cơ chế này được tạo đơn giản bằng cách gửi một lệnh tới kênh

.login FaDe dune

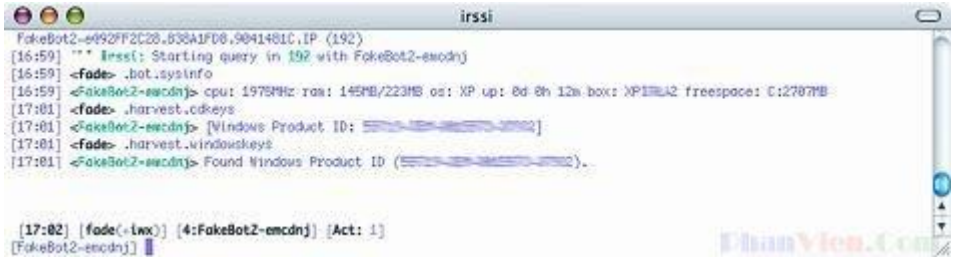
Sau đó, bot đầu tiên được yêu cầu đưa ra danh sách tất cả chương trình đang chạy trên máy tính bị chiếm quyền kiểm soát (xem hình 6):

/msg FakeBot–wszyzc .pctrl.list



Sau đó, bot thứ hai được yêu cầu đưa ra thông tin và khoá cdkey của các chương trình ứng dụng cài đặt trên máy (hình 7):

/msg FakeBot2–emcdnj .bot.sysinfo
/msg FakeBot2–emcdnj .harvest.cdkeys



Ở ví dụ này chúng ta sử dụng những tính năng hết sức đơn giản. Còn thực tế, Agobot cung cấp một tập hợp rất phongphus các lệnh và chức năng. Một trong số chúng bạn có thể xem ở Bảng 2:

LệnhMô tảcommand.listDanh sách tất cả các lệnh có thể sử dụngbot.dnsXử lý một địa chỉ IP hoặc hostnamebot.executeChạy một file .exe trên máy từ xabot.openMở một file trên máy từ xabot.command Chạy một lệnh với system()irc.serverKết nối tới một IRC serverirc.joinNhập thông tin của một

kênh dẫn cụ thểirc.privmsgGửi thư riêng cho một người dùnghttp.executeDownload và thực thi file qua HTTPftp.executeDownload và thực thi file qua FTPddos.udpfloodKhởi động một chương trình UDP tránddos.synflood Khởi động một Syn tránddos.phaticmpKhởi động một PHATicmp tránredirect.httpKhởi động một HTTP proxyredirect.socks Khởi động một SOCKS4 proxypctrl.listĐưa ra danh sách chương trìnhpctrl.kill Loại bỏ các chương trình

Bảng 2: Một số lệnh Agobot

Bảo vệ máy tính của bạn như thế nào

Bây giờ chúng ta sẽ xem xét một số phương thức bảo vệ trước khả năng xâm phạm và phá hoại của kiểu tấn công bot, dưới góc nhìn của cả người dùng và nhà quản trị.

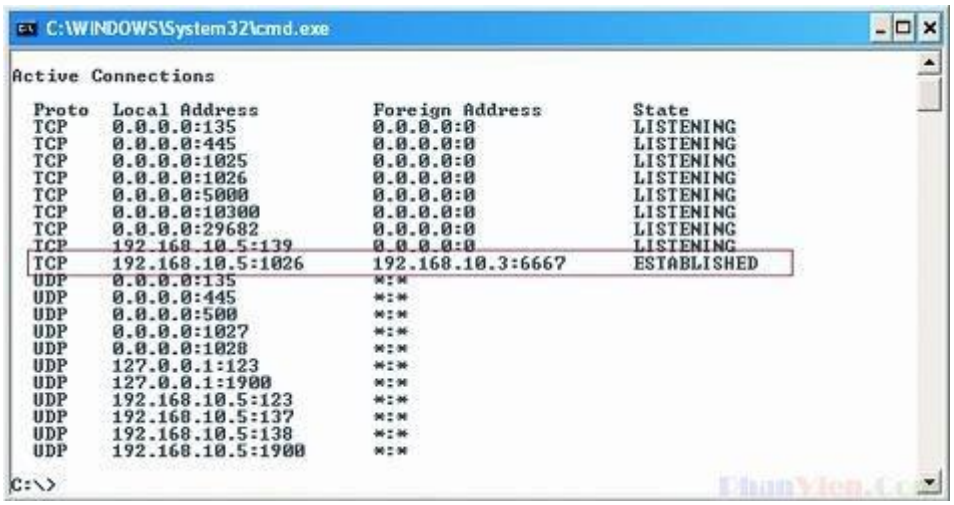
Các chiến lược bảo vệ cho người dùng PC

Như đã đề cập tới ở trên, tấn công bot chủ yếu được thực hiện qua các loại sâu, lướt trên mạng để tìm kiếm lỗ hổng thâm nhập được. Do đó, bước đầu tiên là phải cập nhật thường xuyên, download cá bản vá và bản update hệ thống cho cả hệ điều hành cũng như các ứng dụng truy cập Internet. Sử dụng chương trình update tự động là một ý kiến hay. Bạn cũng nên cẩn thận khi mở các file đính kèm đáng ngờ trong e-mail. Cũng sẽ là khôn ngoan khi loại bỏ hỗ trợ hình thức ngôn ngữ kịch bản như ActiveX và JavaScript (hoặc ít nhất là kiểm soát việc sử dụng của chúng). Cuối cùng, yếu tố cơ sở là bạn phải dùng ít nhất một chương trình diệt virus, trojan và luôn luôn update phiên bản mới nhất của chúng. Dẫu vậy, nhiều bot được cấu hình lần tránh khỏi sự kiểm soát của các chương trình diệt virus. Vì thế, bạn nên dùng thêm phần mềm

tường lửa cá nhân, nhất là khi sử dụng máy tính nối mạng liên tục 24 giờ/ngày.

Dấu hiệ chính khi có hiện diện của bot là tốc độ máy và tốc độ kết nối mạng trở nên cực kỳ chậm. Một cách kiểm tra các kết nối đáng ngờ đơn giản và hiệu quả là sử dụng công cụ netstat (xem hình 8):

C:/>netstat –an



Netstat

Netstat là một công cụ linh hoạt, tương thích được cả trên hệ điều hành Windows và các hệ thống *NIX. Chức năng của nó là kiểm soát các cổng đã được kích hoạt. Netstat kiểm tra quá trình nghe trên cổng TCP và UDP, sau đó cung cấp thông tin chi tiết và hoạt động mạng. Trên hệ thống *NIX, netstat hiển thị tất cả các dòng mở. Nó cũng sử dụng các bộ lọc chọn ngoài.

Trạng thái kết nối có thể trên Netstat gồm:
* ESTABLISHED – tất cả các host đều được kết nối
* CLOSING – host từ xa đang đóng kết nối

* LISTENING – host đang nghe kết nối đến
* SYN_RCVD – một host từ xa đuwocj yêu cầu khởi động kết nối
* SYN_SENT – host đang khởi động kết nối mới
* LAST_ACK – host phải gửi báo cáo trước khi đóng kết nối
* TIMED_WAIT, CLOSE_WAIT – một host từ xa đang kết thúc kết nối
* FIN_WAIT 1 – client đang kết thúc kết nối
* FIN_WAIT 2 – cả hai host đều đang kết thúc kết nối

Quan sát các kết nối ESTABLISHED tới cổng TCP trong phạm vi 6000 đến 7000 (thông thường là 6667). Nếu bạn thấy mình tính của mình bị xâm hại, hãy ngắt nó ra khỏi mạng Internet, làm sạch hệ thống, khởi động lại và kiểm tra.

Chiến lược bảo vệ cho người quản trị

Các quản trị viên thường phải cập nhật liên tục thông tin về những lỗ hổng mới nhất, cũng như đọc thường xuyên về tài nguyên bảo mật trên Internet mỗi ngày. Một số công cụ hỗ trợ Bugtraq, đưa ra bản mô tả tóm tắt danh sách thư là một ý kiến hay. Các quản trị viên cũng nên cố gắng tuyền truyền, nâng cao nhận thức cho người dùng của mình về vấn đề bảo mật và các chính sách bảo mật.

Nghiên cứu nhật ký thường trình (bản ghi log) do IDS và nhiều hệ thống tường lửa, mail server, DHCP, proxy server tạo ra cũng rất cần thiết. Điều này có thể giúp phát hiện ra lưu lượng bất thường, một dấu hiệu của sự hiện diện bot và nhờ đó có biện pháp ngăn chặn kịp thời. Sau khi lưu lượng bất thường được chú ý, một siffer sẽ đến để nhận dạng mạng con và máy tính tạo ra nó. Tất cả các biện pháp dường như đều quen thuộc và không mấy khó khăn, nhưng mọi người thường quên, hoặc bỏ qua chúng.

Bạn cũng có thể sử dụng một số kỹ thuật phức tạp hơn như honeybot. Honeybot là các máy được xây dựng với mục đích hấp dẫn kẻ tấn công. Vai trò của chúng là trở thành máy tính nạn nhân, giúp người quản trị định vị chính nguồn của vấn đề và nghiên cứu phương thức tấn công.

Nhưng kết luận cuối cùng thì, cho dù công cụ hỗ trợ là gì đi chăng nữa, biện pháp phòng chống và bảo vệ tốt nhất trước các cuộc tấn công botnet là bản thân người dùng và nhận thức của họ.