Module 10
Tấn Công Từ Chối Dịch Vụ (DoS)

Những Nội Dung Chính Trong Chương Này

Tấn Công DoS Là Gì ?

Cơ Chế Hoạt Động Của DDoS

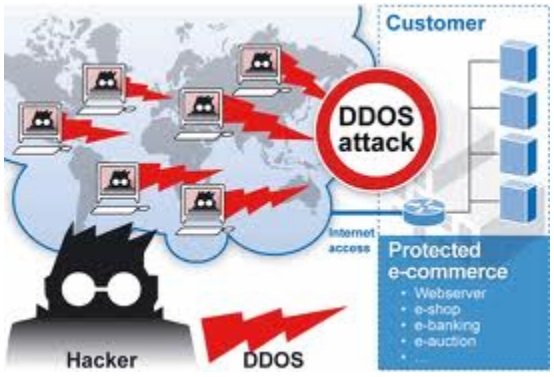
SMURF Attack

"SYN" Flooding

Phòng Chống Tấn Công Từ Chối Dịch Vụ

Tấn Công DoS Là Gì ?

Một khi không thể tìm được cách thức xâm nhập vào hệ thống mục tiêu bằng cách dò tìm và khai thác lỗi thì các hacker sẽ áp dụng phương pháp tấn công từ chối dịch vụ hay còn gọi là Denial of Service (DoS).



DoS là dạng tấn công làm cho các hệ thống máy chủ, trang web bị tê liệt không thể đáp ứng lại các yêu cầu của người dùng. Đây là một trong các hình thức tấn công đem lại hiệu quả cao cho các hacker cũng như là giải pháp sau cùng nêu như không tìm được cách nào đột nhập vào mục tiêu. DOS đánh vào bản chất tự nhiên của một quá trình truyền thông của client và server, nếu có quá nhiều clicent truy cập thì server sẽ bị quá tải, buộc lòng phải từ chối các yêu cầu truy cập khác. Trong vai trò của một CEH các bạn cần hiểu rõ về DoS và DDoS, đây là những thuật ngữ rất hay được nhắc đến trong các kì thi lấy chứng chỉ hacker mũ trắng này.

Có khá nhiều tình huống tấn công DoS được nhắc đến trên các phương tiện truyền thông gần đây, ví dụ như BKAV bị tấn công từ chối dịch vụ làm cho website không thể truy cập vào ngày 6/2/2012 hay trang web của Cục Tình báo Trung ương Mỹ đã bị hạ gục suốt đêm 10/2/2012 (giờ VN), hậu quả của một vụ tấn công từ chối dịch vụ có chủ đích (DDoS). Một tài khoản Twitter tuyên bố chính nhóm hacker khét tiếng Anonymous đã gây ra vụ việc (theo tin từ VietnamNet).

Sau đây là một số dạng tấn công từ chối dịch vụ mà các hacker thường sử dụng :

- Làm tràn ngập hệ thống mạng bằng số lượng rất lớn của các dữ liệu truyền, khiến cho các giao dịch thông thường khác không thể thực hiện được. Ví dụ vào khoảng cuối năm 2012 và đầu năm 2011 các hệ thống mạng trong nhiều công ty và tổ chức bị tê liệt khiến cho người dùng không thể kết nối đến máy chủ hay truy cập internet do nhiều máy tính bị lây nhiễm virus conflicker. Vào thời gian này tôi có nhận được khá nhiều yêu cầu hỗ trợ xử lý cũng như phát hiện nguyên nhân trên, và với giải pháp cài đặt những ứng dụng như Wiresharke để phân tích đường truyền thì nhận thấy ràng các luồng dữ liệu đề xuất phát từ những máy bị nhiễm một loạt virus có nhiều tên gọi khác nhau là conflicker hay kido ..Virus trên lây nhiễm vào các hệ thống Windows do thiếu cài đặt một bản vá lỗi có tên là Microsoft Security Bulletin MS08-067.
- Ngắt kết nối giữa hai máy tính, ngăn không cho máy khách truy cập các dịch vụ trên máy chủ.
- Chặn một host nào đó không cho truy cập dịch vụ.
- Ngắt các đáp ứng đối với một hệ thống hay người dùng.

Có nhiều loại công cụ tấn công DoS khác nhau và mỗi loại sử dụng những cơ chế riêng để làm tràn ngập hệ thống nhưng kết quả cuối cùng vẫn là như nhau – làm cho hệ thống mục tiêu trở nên quá bận rộn hay bị quá tải mà không thể đáp ứng được các yêu cầu của người dùng, và một khi không thể đáp ứng được những yêu cầu này sẽ làm thiệt hại về mặt kinh tế, uy tín cho đơn vị chủ quản của trang web bị tấn công (thường thì DoS hay nhắm vào các trang web có chức năng kinh doanh trực tuyến, ứng dụng thương mại điện tử). Ví dụ như vào các kì đại hội thể thao diễn ra như Euro, WorldCup thì các nhà cái như Bet365.Com, SportingBet … có rất nhiều khách hàng đăng kí tham gia dự đoán kết quả của những trận cầu nóng bỏng đen đến các nguồn lợi khổng lồ. Và các hacker biết rất rõ những điều này, chính vì vậy họ thường hăm dọa những nhà cái trên sẽ tấn công DoS / DDoS làm tê liệt trang web ngăn không cho khách hàng truy cập, còn nếu không muốn bị tấn công thì phải đồng ý trả cho các hacker một khoản tiền lớn. Hình thức tống tiền này được các băng nhóm tội phạm mạng ưa chuộng vì đem đến hiệu quả cao.

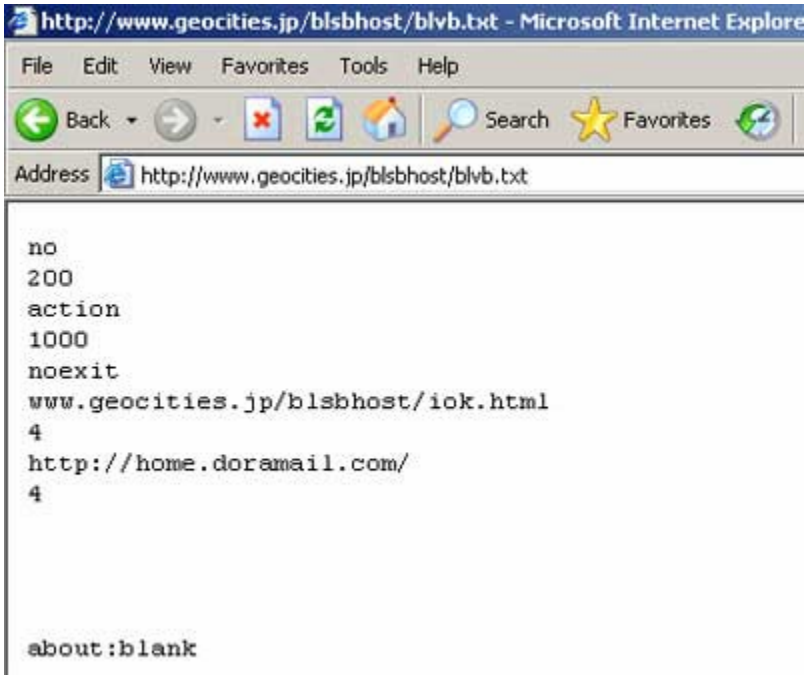
> **Lưu ý** : *DoS* là dạng tấn công khi hacker sử dụng một máy tính để tiến hành, còn *DDoS* hay *Distribute Denial of Services* (tấn công từ chối dịch vụ phân tán) là khi hacker tiến hành tấn công DoS từ nhiều máy tính khác nhau, thông thường là một hệ thống mạng *botnet*.

Vậy thì các hacker thường sử dụng các công cụ nào đề tấn công DoS, dưới đây là một số ứng dụng điển hình :

- **Ping of Death** : Các công cụ tấn công *Ping of Death* gởi nhiều gói tin IP với kích thước lớn đến mục tiêu làm cho các máy này phải mất nhiều thời gian và tài nguyên hệ thống để xử lý, kết quả là không thể đáp ứng được các yêu cầu kết nối thông thường của những máy tính khác dẫn đến bị từ chối dịch vụ.
- **LAND Attack** : Những công cụ có chức năng tấn công *LAND Attack* sẽ gởi các gói tin có địa chỉ IP trùng lắp với các địa chỉ IP đích khiến cho việc xử lý các yêu cầu này có thể dẫn đến tình trạng bị lặp lại (*loop*) và không thể tiếp nhận thêm các yêu cầu truy cập khác.
- **WinNuke** : Chương trình này tìm kiếm các máy tính đang mở *port* 139 để gởi các gói tin IP rác đến mục tiêu. Dạng tấn công này còn được gọi là *Out of Bound* (OOB) và làm tràn ngập bộ nhớ đệm của giao thức IP.
- *CPU Hog* : Công cụ này làm quá tải nguồn tài nguyên CPU của các máy bị tấn công .
- **Bubonic** : Là công cụ DoS hoạt động bằng cách gởi các gói tin TCP với những thiết lập ngẫu nhiên làm cho mục tiêu bị tấn công bị quá tãi hay thậm chí bị gãy đổ.
- **RPC Locator** : Đây là một dịch vụ nhạy cảm nếu như không được vá lỗi có khả năng bị tấn công gây tràn bộ đệm. Dịch vụ này hoạt động trên các hệ thống Windows để phân phối các bản cài đặt hay ứng dụng trẹn toàn hệ thống, đây cũng là một dịch vụ dễ bị tấn công gây ra tình trạng từ chối dịch vụ trên các máy chủ.
- Ngoài ra còn có các công cụ như **SSPing** hay **Targa** có thể gởi các gói tin với kích thược lớn đến mục tiêu làm tê liệt khả năng đáp ứng cũng như xử lý các dữ liệu này, điều đó cũng có nghĩa nạn nhân sẽ không thể tiếp nhận các yêu cầu khác dẫn đến tình trạng "từ chối dịch vụ".

Cơ Chế Hoạt Động Của DDoS

Tuy nhiên, các cuộc tấn công mà các bạn thường nghe trên những phương triện truyền thông thường sử dụng những công cụ khác. Các cuộc tấn công này là *DDoS*, hình thức này sử dụng các hệ thống mạng máy tính "ma" gọi là *botnet*, và mỗi máy trạm trong hệ thống này gọi là một *bot* hay *zombie* đã được các hacker cài đặt *trojan* có thể điều khiển từ xa thông qua kênh IRC hay những dữ liệu tập trung (có thể là một tập tin điều khiển đặt trên một trang web nào đó như Hình 10.1). Một trong những ví dụ tấn công của hình thức này là hacker *DanTruongX* đã tấn công vào trang web của công ty *VietCo* được phát hiện bởi các chuyên gia BKAV trước đây.



Hình 10.1 - Tập tin điều khiển các máy tính trong mạng botnet

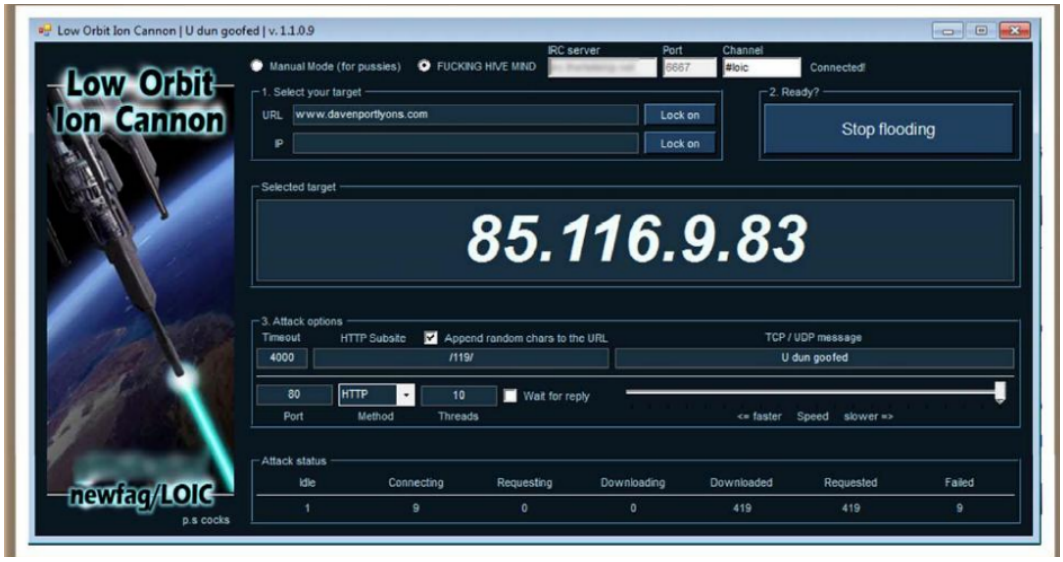
Thông thường DDoS gồm có 3 thành phần :

- *Master* hay *Handler* : Chương trình dùng để điều khiển.
- *Slave* hay *zombie*, *bot* là các máy tính bị cài đặt hay lây nhiễm các chương trình nguy hiểm và bị điều khiển bởi các *master / handler*.
- *Victim* : Những mục tiêu bị tấn công từ chối dịch vụ.

Trong các cuộc tấn công *DDoS* gần đây hacker thường sử dụng công cụ *Low Orbit Ion Cannon* (LOIC). Hiện nay, nhóm hacker hàng đầu thế giới là *Anonymous* sẽ phát triển một ứng dụng mới có tác dụng mạnh mẽ hơn có tên là *#RefRef* để thay thế cho *LOIC*.

Vậy ứng dụng DDoS đầu tiên được sử dụng là chương trình nào, có lẽ là Trojan *SubSeven*. Trong một bài tường thuật trên website của mình, chuyên gia bảo mật nổi tiếng hiện là Webmaster của www.grc.com có kể lại một lần anh ta vô tình gọi một

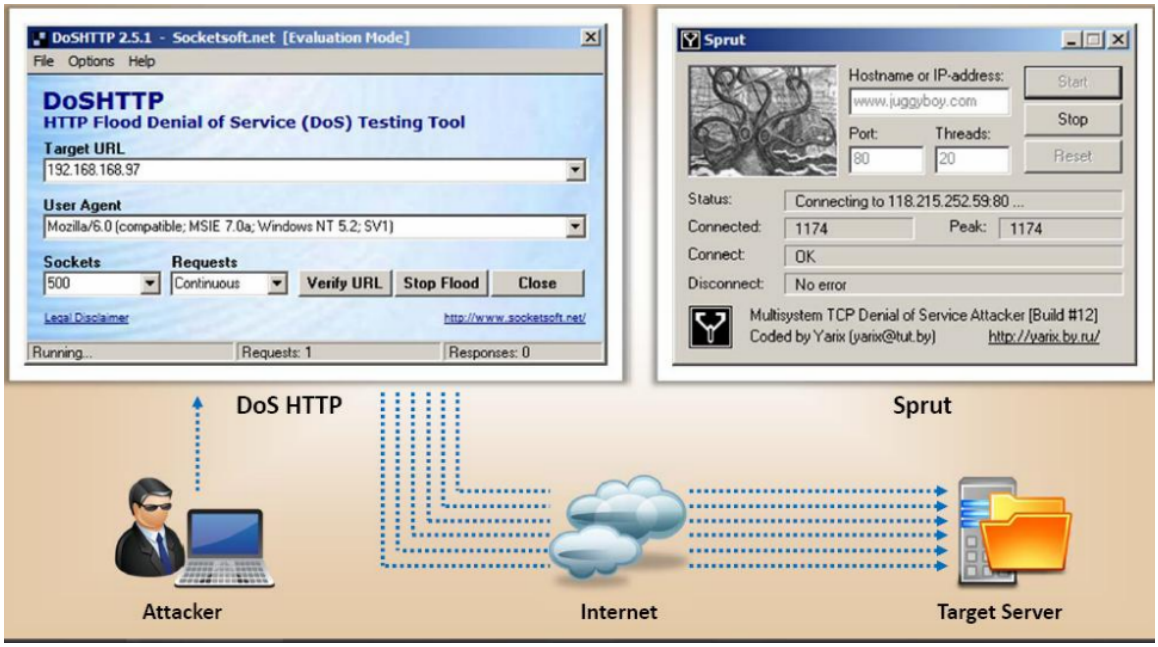
hacker trẻ tuổi là *script kiddi*, một thuật ngữ am chỉ những kẽ chỉ biết sử dụng công cụ để khai thác mà không có sự hiểu biết chuyên sâu của hacker đúng nghĩa. Điều này đã làm hacker trẻ tuổi trên bị *chạm tự ái* và anh ta đã cùng với một người bạn phát triển công cụ có tên gọi là *Sub Seven,* sau đó cài đặt cũng như lây nhiễm trên một số lượng lớn các máy tính tạo thành hệ thống *botnet* mạnh mẽ. Tiếp theo, anh ta cũng với người bạn có nickname *hellfire* của mình đã cùng điều khiển hệ thống *botnet* trên qua kênh IRC khởi động các cuộc tấn công từ chối dịch vụ làm cho trang web *grc.com* bị tê liệt trong một thời gian dài. Sau cùng, webmaster của *GRC* cũng là một hacker lão luyện đã phải tự mình dò tìm ra thủ phạm và gởi đến hacker trẻ tuổi này lời xin lỗi cho nhận xét vô tình của mình, đồng thời cũng đưa ra cảnh cáo liên quan đến hình phạt của luật pháp dành cho những kẻ tấn công) để yêu cầu ngừng tất cả những cuộc tấn công trên.



Hình 10.2 - Giao diện của Low Orbit Ion Cannon

Ngoài cách sử dụng *botnet* thì một số công cụ vẫn được các hacker ứng dụng để tiến hành tấn công DDoS như *Trinoo*, một ứng dụng có thể gởi các dữ liệu sử dụng giao thức vận chuyển *User Datagram Protocol* (UDP) với địa chỉ gốc được giả mạo hay sử dụng một danh sách các IP khác nhau, làm cho mục tiêu bị tấn công phải vất vã trong quá trình đáp ứng lại các địa chỉ giả này mà không hề biết đó chỉ là những thông tin giả ví lý do UDP là một giao thức thiếu tin cậy không có cơ chế kiểm tra đầy đủ cho tính hợp lệ của IP nguồn. *Trinoo* hoạt động trên nền Linux, trên Windows có phiên bản tương tự gọi là *WinTrinoo* hay biên thể khác của nó là *Sharf*.

Bên cạnh *Trinoo* còn có *Tribal Flood Netowrk (TFN)* có khả năng làm suy yếu tài nguyên cũng như băng thông của các hệ thống mục tiêu thông qua việc gởi số lượng lớn các gói tin *UDP* và cả *ICMP*. Nhưng việc gởi nhiều dữ liệu theo cách này hiện nay rất dễ bị nhận dạng cho nên *TFN* đã nâng cấp lên phiên bản *TFN2* để cho khó bị phát hiện hơn



Hình 10.3 – Các công cụ DoS khác như DoSHTTP, Sput, PHP DOS …

SMURF Attack

Đây là hình thức tấn công khá lạc hậu và vô hiệu đối với các hệ thống hiện nay. Dạng tấn công *Smurf* sẽ gởi một số lượng lớn các yêu cầu *ICMP ECHO Request (Ping)* đến nhiều mục tiêu theo dạng *broadcast* với địa chỉ nguồn giả mạo, điều này sẽ làm phát sinh số lượng lớn các đáp ứng của các máy tính nhận được yêu cầu của máy tấn công dẫn đến băng thông bị chiếm dụng và hệ thống mạng máy tính có khả năng tê liệt.

"SYN" Flooding

Không như UDP là một giao thức vận chuyển thiếu tin cậy, TCP là giao thức tin cậy hơn trong truyền thông với quy trình bắt tay ba bước *Three-way handshake* chặt chẽ. Khi một máy tính cần kết nối sẽ gởi những tín hiệu yêu cầu đồng bộ hóa là các cờ *SYN*. Nhưng khi có quá nhiều yêu cầu được đồng bộ được tạo ra bởi các hacker thông qua những công cụ tấn công thì máy nhận sẽ bị quá tải với việc đáp ứng và không thể tiếp nhận thêm các yêu cầu kết nối hợp lệ khác. Đây chính là dạng tấn công *SYN Flooding*.

Phòng Chống Tấn Công Từ Chối Dịch Vụ Như Thế Nào ?

Có nhiều cách thức để nhận biết và phòng chống bị tấn công từ chối dịch vụ khác nhau. Trước tiên chúng ta cần vá những lỗ hỗng bảo mật của các dịch vụ hay ứng dụng đang chạy trên máy chủ để tránh bị hacker lợi dụng tấn công từ chối dịch vụ như *RPC Locator service*. Sau đây là một số giải pháp cần được quan tâm :

- **Network-ingress filtering** : Tất cả các hệ thống hay thiết bị cung cấp những kết nối và truy cập mạng cần thực hiện cơ chế lọc *Network-infgress filtering* nhằm loại bỏ các luồn dữ liệu xuất phát từ các địa chỉ giả mạo, có nguồn gốc không rõ ràng. Điều này không ngăn ngừa được các cuộc tấn công nhưng có thể giúp chúng ta chặn đứng chúng cũng như có thể truy tìm khi có những hành động trái phép diễn ra. Các thiết bị dạng này như *Cisco IPS Source IP Reputation Filtering, Black Hole Filtering …*

- **Rate-limiting network system** : Nhiều bộ định tuyến hiện nay có khả năng hạn chế và kiểm soát băng thông trên những giao thức khác nhau, kỹ thuật này còn được gọi là *trafic shapping*.

- **Instruction Detect System** : Triển khai các hệ thống dò tìm xâm phạm trái phép để phát hiện kịp thời các luồng truyền thông nguy hiểm, những cuộc tấn công hay các virus / worm lan truyền trên mạng. Một trong các ứng dụng IDS nguồn mở được sử dụng phổ biến như Snort (www.snort.org).

- **Sử dụng công cụ Host-auditing** : Một số chương trình có khả năng quét các tập tin trên hệ thống để tìm ra các công cụ tấn công *DDoS* hay các chương trình *botnet* nguy hiểm.

- **Sử dụng công cụ Network-auditing** : Chạy các chương trình quét mạng để phát hiện các *agent* (các thành viên của mạng *botnet*) và loại bỏ chúng.

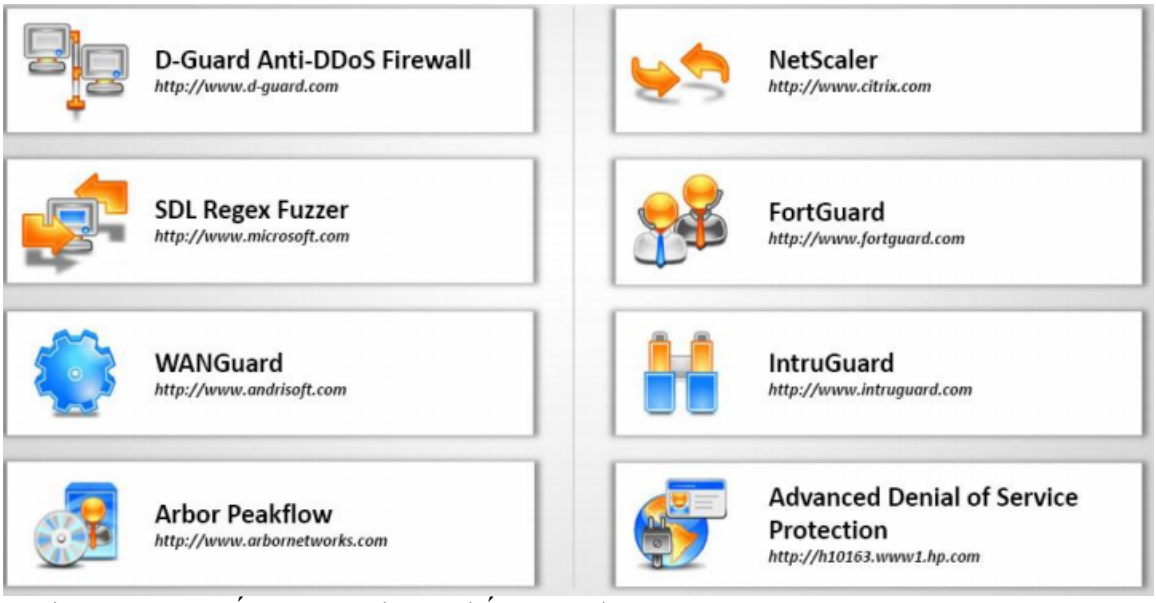
- **Sử dụng các chương trình dò tìm công cụ DoS** : Thường xuyên quét tìm các công cụ *DoS* trên hệ thống với những chương trình thích hợp như *Find_ddos, SARA, Zombi Zapper* để phát hiện và xử lý kịp thời các mầm mống gây nên sự cố từ chối dịch vụ.

- **Tắt các dịch vụ không cần thiết** : Đóng các cổng hay tắt những dịch vụ không cần thiết hay hạn chế sự dụng những chức năng như *get, strcpy …*

- **Cấu hình firewall để chặn tất cả các tín hiệu ICMP từ bên ngoài.**

- **Thường xuyên cập nhật hệ thống** : Cập nhật các bản vá lỗi mới nhất cho hệ thống và ứng dụng liên quan.

- **Sử dụng các hệ thống bảo vệ DDoS** chuyên dụng như IntelliGuard DDoS Protection System (DPS) hay các chương trình phòng chống *DDoS* như Hình 10.4



Hình 10.4 - Một số công cụ phòng chống DoS/DDoS

Tổng Kết

Chương này đã trình bày về các dạng tấn công nguy hiểm hàng đầu hiện nay là DoS và DDoS cùng những công cụ điển hình mà các bạn cần ghi nhớ. Cần phân biệt sự khác nhau của tấn công từ chối dịch vụ thông thường và tấn công từ chối dịch vụ theo mô hình phân tán, lưu ý các công cụ và biên pháp dò tìm, phòng chống bị tấn công DoS / DDoS. Thường xuyên kiểm tra các lổ hỗng bảo mật và cập nhật các bản vá lỗi kịp thời. Trong chương tiếp theo chúng ta sẽ tìm hiểu về Session Hijacking.